TIETOTURVAA HUOLTOVARMUUS-KRIITTISILLE YRITYKSILLE

Kooste automaatiota hyödyntävälle teollisuudelle suunnattujen tietoturva-projektien tuloksista

VTT

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

TIETOTURVAA HUOLTOVARMUUS-KRIITTISILLE YRITYKSILLE

Kooste automaatiota hyödyntävälle teollisuudelle suunnattujen tietoturvaprojektien tuloksista

Huoltovarmuuskeskus
Projektin ohjausryhmän puheenjohtaja,
varautumispäällikkö Tero Kauppinen

Projektipäällikkö, erikoistutkija Pasi Ahonen, VTT

www.huoltovarmuus.fi
Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja 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
VTT on kansainvälisesti verkottunut, monitieteknologinen tutkimuskeskus, joka tuottaa asiakkailleen korkeatasoisia teknologisia ratkaisuja ja innovaatiopalveluja. VTT lisää asiakkaidensa kansainvälistä kilpailukykyä ja edistää näin yhteiskunnan kestävää kehitystä, työllisyyttä ja hyvinvointia.

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

VTT

Julkaisija: Huoltovarmuuskeskus
Teksti, kuvitus, taiton viimeistely: VTT
Painopaikka: Erweko, Oulu
Julkaisuvuosi: 2013
ISBN: 978-952-5608-18-2 (nid.)
ISBN: 978-952-5608-19-9 (pdf)

SISÄLTÖ

OSA 1

ESIPUHE JA YHTEENVETO

1 ESIPUHE JA YHTEENVETO

Esipuhe

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY

Tämä julkaisu on kooste automaatiota hyödyntävälle teollisuudelle suunnattujen tietoturvaprojektien tuloksista. Automaatiojärjestelmien tietoturvallisuuden ja sen erityispiirteiden hyvä hallinta on tärkeä osa kriittisen infrastruktuurin ja tehtaiden ja laitosten toiminnan jatkuvuudenhallintaa. Tätä osaamista syvennetään alan kaikkien toimijoiden hyödyksi ja huoltovarmuuden edistämiseksi teollisuuden, VTT:n, Huoltovarmuuskeskuksen ja Viestintäviraston (CERT-FI) yhteisprojekteissa.

Yhteiskunnan riippuvuus automaatiosta kasvaa nopeasti teollisuudessa ja myös muilla toimialoilla. Emme enää tule toimeen ilman automatisoituja ja kaukokäyttöisiä ratkaisuja, jotka voivat ulottua maamme rajojen ulkopuolelle. Viennissä teollisuusyritystemme asiakkailleen tarjoamissa ratkaisuissa automaation merkitys on keskeinen. Kehitys näyttää nopeutuvan. Palvelurakenteet monimutkaistuvat. Uudenlaisiin riskeihin on varauduttava automaatioratkaisujen elinkaaren kaikissa vaiheissa, jotta palveluiden ja toimintojen keskeytykset eivät haittaisi yhteiskunnan kriittisiä toimintoja.

Yhteiskunnan huoltovarmuutta kehitetään laajassa kumppanuus- ja yhteistyöverkostossa, johon kuuluu elinkeinoelämän toimijoita kaikilta aloilta, valtionhallinnon ja kuntahallinnon toimijoita sekä toimialajärjestöjä.

Suomen kyberturvallisuusstrategiassa (valtioneuvoston periaatepäätös 24.1.2013) todetaan, että yhteiskunnan lisääntynyt tietointensiivisyys, ulkomaisen omistuksen kasvu ja toimintojen ulkoistaminen, tieto- ja viestintäjärjestelmien keskinäinen integraatio, kaikille avointen tietoverkkojen käyttö sekä lisääntynyt riippuvuus sähköstä ovat asettaneet uudenlaisia vaatimuksia yhteiskunnan elintärkeiden toimintojen turvaamiseksi normaalioloissa, normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa.

Turvallinen kybertoimintaympäristö helpottaa yksilöiden ja yritysten oman toiminnan suunnittelua, mikä lisää taloudellista aktiviteettia. Hyvä toimintaympäristö parantaa myös Suomen kansainvälistä houkuttelevuutta investointikohteena.

Tämän julkaisun avulla pyritään osaltaan tukemaan turvallisen teollisen kybertoimintaympäristön kehittämistä sekä automaatiota hyödyntävien että ratkaisuja tarjoavien yritysten näkökulmasta.

Aiheeseen liittyvää esitysmateriaaliaineistoa saa digitaalisessa muodossa Huoltovarmuuskeskuksen www-sivujen kautta kohdasta www.huoltovarmuus.fi –Julkaisut.

26.11.2013

Tero Kauppinen

Varautumispäällikkö, automaatioprojektin puheenjohtaja

Huoltovarmuuskeskus

Pohjoinen Makasiinikatu 7 A, 00130 Helsinki

tero.kauppinen@nesa.fi

www.huoltovarmuus.fi

Yhteenveto

Tässä kirjasessa esitellyissä hankkeissa työstettiin teollisuuden tietoturvaan liittyviä tärkeimpiä teemoja yhteistyössä erityisesti teollisuuden automaatioinsinöörien, automaatiojärjestelmätoimittajien ja palveluntarjoajien, Huoltovarmuuskeskuksen, VTT:n, Tampereen Teknillisen Yliopiston ja CERT-FI:n muodostamassa verkostossa.

Pääosa tuloksista saavutettiin erilaisten työpajojen ja katselmointitilaisuuksien yhteydessä, joissa soveltuvia malliratkaisuja ja yrityskäytäntöjä kehitettiin edelleen soveltuvaksi lähinnä suomalaisen automaatiota hyödyntävän teollisuuden tarpeisiin. Hankkeissa syntyneitä julkisia tuloksia on jo esitelty monissa tulostenesittelytilaisuuksissa, joiden osallistujiksi on pyydetty tärkeimpiä automatisoidun tuotannon tietoturvaan vaikuttavia tahoja ja asiantuntijoita.

Julkiset tulokset sisältävät mm. seuraavanlaisia teemoja:

- Automaation tietoturvan kartoitus
- Teollisuuden tietoverkkojen ja etäyhteyksien hallinta ja seuranta
- Tehtaan tietoturvaohjeet, koulutus ja muutosten hallinta
- Hankintakäytännöt ja vaatimukset toimittajille
- Soveltuvien tietoturvamenetelmien evaluoinnit (sovellusten sallimislistaus, tietoturvatestaus)
- Tuotannon riskien hallinta ja jatkuvuuden varmistaminen.

Teollisuuden käyttöön soveltuvia tietoturvastandardeja ja 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 olla vaikeaa tai työlästä. Niinpä eri ratkaisuja tulisikin etukäteen arvioida ja testata eri menetelmien soveltuvuutta tuotantoon ennen tietoturvaratkaisun valintaa ja käyttöönottoa. Tähän arviointiin tai testaamiseen tarvitaan usein lisätukea yrityksen ulkopuolelta, sillä yksin automaatiohenkilöstön ydinosaaminen ei tähän välttämättä riitä.

Yhteistyön merkitys korostuu tänä päivänä tietoturvallisuuden ylläpidossa useimmilla sektoreilla, ei ainoastaan teollisuudessa. Toimivaa yhteistyötä ja yhteisiä pelisääntöjä tarvitaan automaatiojärjestelmien hankinnan ja käyttöönoton aikaisessa tietoturvan hallinnassa, mutta myös laajemmin koko tuotannon elinkaaren aikana, mm. halutun tietoturvatason ylläpitämisessä ja seuraamisessa. Erityisesti tietoverkkojen seurannan tarve on tänä päivänä korostunut, dataverkkojen kautta tapahtuvan häirinnän, teollisuusvakoilun ja tiedustelupalvelujen pitkälle kehittyneen soluttautumisen takia.

Teollisuudelle tarjottavien tietoturvapalvelujen räätälöinti ja osumistarkkuus tuleekin saada entistä paremmaksi. Tuotantotoiminnassa tulee varautua myös tulevaisuuden toimintaympäristöihin, jotka usein sisältävät yhä lisääntyvää järjestelmäintegraatiota, sekä julkisissa verkoissa tarjottujen tietojen ja tietopalvelujen käyttöä.

OSA 2

LYHYT JOHDANTO HANKKEISIIN

2 LYHYT JOHDANTO HANKKEISIIN

Jatkuvasti kasvavien tietoturvariskien hallitsemiseksi teollisuusyritysten tulee ottaa käyttöön hyväksi havaitut ja omaan tuotantotoimintaansa sovitetut ja tietoturvalliset toimintakäytännöt, -ohjeet, vaatimukset ja esimerkkimallit. Tuottaessaan palveluita ja hyödykkeitä elinkeinoelämän toimijoiden on varmistettava mm. toimintaverkostonsa prosessien ja osaamisen toimintakyky.

Hyvin usein tuotantolaitoksen toiminta on voimakkaasti riippuvainen ulkoisista palvelu- ja hyödyketoimittajista, tuotantoa ei voida jatkaa ilman sähköä, vettä, lämpöä, tietoliikenneyhteyksiä jne. Automatisoidun tuotannon kattava suojaaminen vaatii monen alan osaamista. Yrityksen tulee mm. määritellä tuotantojärjestelmien hankintaan, hallintaan ja ylläpitoon liittyvät tietoturvavaatimukset. Erityisesti automaatiojärjestelmien tietoturvallisuuden hallintaan liittyvät toimet ovat tärkeä osa kriittisen infrastruktuurin sekä tehtaiden ja laitosten toiminnan jatkuvuudenhallintaa. Tällaista osaamista on viime vuosien aikana syvennetty alan kaikkien toimijoiden hyödyksi ja huoltovarmuuden edistämiseksi Huoltovarmuuskeskuksen, Viestintäviraston (CERT-FI), teollisuuden ja VTT:n yhteisprojekteissa.

Tähän kirjaseen mukaan luetut, VTT:n toteuttamat teollisuuden tietoturvahankkeet esitellään lyhyesti seuraavissa alaluvuissa.

2.1 TITAN – Tietoturvaa teollisuusautomaatioon

Tekesin Turvallisuusohjelmaan kuuluneen ”Tietoturvaa teollisuusautomaatioon” (TITAN) hankkeen (2008—2010) VTT:n päätulokset koottiin TITAN-käsikirjaan [TITAN], joka on edelleen saatavilla julkisena VTT:n verkkojulkaisuna.

TITAN-hanke oli ns. sateenkaariprojekti, jonka alkuvaiheen tavoitteena oli kartoittaa laajasti kipeimmin parantamista vaativia teollisuuden tietoturvan kipupisteitä. Hankkeen kuluessa päätavoitteena oli selvittää teollisuusautomaatioympäristöön soveltuvat tärkeimmät tietoturvamenettelytavat ja -ratkaisut sekä aloittaa näiden jatkokehittäminen erityisesti suomalaisten teollisuusyritysten tarpeet huomioiden.

Hankkeessa siis mietittiin automaation tietoturva-asioita laajasti yhdessä alan suomalaisten toimijoiden kesken. Pohdintojen ensimmäisinä tuloksina syntyi jäsennelty kuva suomalaisen teollisuusautomaation kipupisteistä: siitä, millaiset tekijät vaikuttavat erityisen negatiivisesti tietoturvatilanteen hallinnassa pitämiseen.

Tärkeimpiä tietoturvaan negatiivisesti vaikuttavia tekijöitä suomalaisessa teollisuusautomaatiossa olivat:

- Yhteisen tietoturvastandardin puuttuminen
- Ulkopuoliset tekijät ja ulkoinen paine
- Pitkän elinkaaren hallitsemisen vaikeus
- Koulutuksen ja osaamisen haasteet.

Koska yhteinen tietoturvastandardi puuttui, projektissa päätettiin, että suomalaisille automaatioteollisuuden toimijoille koostetaan käytännön lähtökohdista käsin suomenkielinen, sovellettavissa oleva ohjeistus tietoturvan hallitsemiseen paremmin.

Tulokset

VTT-projektin lopputuloksena syntyneessä TITAN-käsikirjassa esiteltiin tiiviisti tärkeimpiä teollisuusautomaation tietotur-

Kuva 1. TITAN-käsikirja. [TITAN]

vaa sivuavia trendejä, standardeja, vaatimuksia, referenssimalleja, ohjeita, testausmenetelmiä ja -kokemuksia.

Tutkimuksissa päädyttiin muun muassa seuraaviin johtopäätöksiin:

- Standardien mukaisen, turvallisen automaatiojärjestelmän hankinta on vaikeaa, joten yrityksen hankintaprosessin kehittämiseen kannattaa varata aikaa ja resursseja.
- Yhtenäisiä hankintakäytäntöjä täytyy edelleen kehittää. Lisäksi tietoturvan parantaminen vaatii selkeitä, helppokäyttöisiä ja tehokkaita työkaluja ja käytäntöjä, jotka voidaan ottaa käyttöön kaikilla tarvittavilla osa-alueilla kriittisten järjestelmien toiminnan jatkuvuuden varmistamiseksi.
- Tietoturvavaatimukset tulee työstää kehittäjien ja käyttäjien ymmärtämään muotoon.
- Kansallisella tasolla tarvitaan lisää yhteistyöfoorumeita ja verkostoja tietoturvatilanteen kartoittamiseksi ja tulevaisuuden riskiskenaarioiden tunnistamiseksi.
- Kilpailu- ja toimintakyvyn varmistaminen tulevaisuudessa edellyttää avoimuuden ja monenkeskisen kommunikaation lisäämistä muun muassa operaattoreiden, laite- ja ohjelmistovalmistajien, automaatiojärjestelmätoimittajien, asiakkaiden, sääntelijöiden sekä kuluttajien välisissä ja keskinäisissä verkostoissa.

Tulosaineisto

TITAN-käsikirja on julkisesti saatavilla verkkojulkaisuna VTT:n Internet-sivuilla http://www.vtt.fi/inf/pdf/tiedotteet/2010/T2545.pdf

2.2 TEO-TT – Teollisuuden tietoturvan kansallinen kehittäminen teematyöpajoissa

Tietoturvallisia toimintatapoja huoltovarmuuskriittiselle teollisuudelle

Huoltovarmuuskeskus toteutti yhdessä VTT:n ja Viestintäviraston CERT-FI-yksikön kanssa projektin, jonka tavoitteena oli teollisuuden tietoturvan kansallinen kehittäminen teematyöpajoissa noin 3 kk välein alkaen syksystä 2011 ja päättyen vuoden 2012 lopulla. Kohderyhmänä olivat suomalaisen teollisuuden käytännön toimijat, lähinnä tuotantolaitosten automaatiosta vastaavat insinöörit, mutta myös tuotannosta, turvallisuudesta, tuotantojärjestelmien hankinnoista ja ylläpidosta vastaavat toimihenkilöt. Tulosmateriaalit ja toimintatavat kehitettiin yhteistyössä Huoltovarmuuskeskuksen, VTT:n, CERT-FI:n sekä teollisuuden johtavien yritysten kanssa.

Motivaatio

Miksi työpajoja tarvittiin?

- Työpajoja suunniteltaessa vuosi 2010 oli motivaatiohuippu:
  - Julkisuuteen tulleet teollisuuteen kohdistuneet tietoturvahyökkäykset olivat motivoineet vahvasti automaation käyttäjäorganisaatioita parantamaan tuotantonsa tietoturvaa.
- Tarvittiin ja edelleen tarvitaan kustannustehokkaita tapoja parantaa tietoturvaa:
  - Koska kaikessa toiminnassa säästetään, myös tietoturvatoimenpiteiden tulee olla tehokkaasti toimivia, ennakkoon koeteltuja, suunniteltuja sekä helposti sovellettavia.
- Paras tapa oppia käytännössä tarvittavia taitoja on kuulla kokemuksia vertaisiltaan:
  - Tarinat vertaisyritysten onnistumisista ja epäonnistumisista olivat työpajojen parasta antia.
  - Toimintatapoja ei tarvitse kokeilla kantapään kautta → vakavan onnettomuuden vaara.

Työpajat

Projektin keskeinen sisältö oli teollisuuden tietoturvaan keskittyvien teematyöpajojen järjestäminen. Teollisuus osallistuikin keskeisesti ja erittäin motivoituneita osallistujia käyttäen kaikkiin projektissa järjestettyihin työpajoihin, jotka olivat:

TEO-TT Työpajat	Osallistujia
1. Teollisuuslaitoksen automaatio-ohjauksen tietoturvan kartoitus (19.syyskuuta 2011).	37
2. Teollisuuden tietoverkkojen turvallinen hallinta (14. joulukuuta 2011).	37
3. Turvalliset automaatiojärjestelmien hankintakäytännöt ja toimittajan hallintakäytännöt (2. helmikuuta 2012).	30
4. Automaatiojärjestelmien riskien hallinta (10. toukokuuta 2012).	30
5. Automaatiojärjestelmien tietoturvatestaus (13. syyskuuta 2012).	38
6. Tuotannon jatkuvuuden arviointi ja varmistaminen (22. marraskuuta 2012).	35

Taulukko 1. TEO-TT-Työpajojen teemat, ajankohdat ja osallistujamäärät. [TEO-TT].

TEO-TT hankkeessa saavutettiin perustavanlaatuisia tuloksia:

- Kehitettiin asiantuntijaverkosto käytännön toimijoiden käyttöön
- Kehitettiin yhteistä näkemystä, tietoturvakäytäntöjä ja toimintatapoja automaatiojärjestelmien turvaamiseen
- Saatiin toimiva yhteistyömalli työpajoihin.

Yhteistyömalli työpajoissa
1. Työpajojen tavoitteena on keskustella erilaisista käytännön tavoista ratkaista kipupisteet ja ongelmakohdat → Ratkaisuja on olemassa mutta ne pitää osata ottaa käyttöön.
2. Osallistujat kertovat kehityskohteensa tai kipupisteensä aihepiirin alueella.
3. Edelläkävijäyritysten Case-alustukset aihepiirin hyviin käytäntöihin.
4. Alustukset synnyttävät välittömiä lisäkysymyksiä ja suoraa keskustelua osallistujien välillä.
5. Pienryhmätyöskentelyä alustusten pohjalta (osassa työpajoista).
6. Lopuksi ryhmätöiden tulokset vedetään yhteen ja kuvataan tarkemmin hyviä toimintatapoja.

Taulukko 2. Yhteistyömalli TEO-TT-Työpajoissa. [TEO-TT].

Keskeiset hyödyt

Projektilla todettiin olleen yleisesti hyvä vaikuttavuus teollisuuteen, mikä saavutettiin varmistamalla teollisuuden laaja osallistuminen, oikea kohderyhmien valinta, aiheiden ja käsittelyn sopiva taso sekä osaajaverkoston jatkuva kehittyminen. Lisäksi saavutettiin koordinoitu eteneminen ja teollisuuden tietoturvaosaamisen kansallinen kehittäminen tehokkaalla tavalla syksystä 2011 aina vuoden 2012 lopulle asti.

Kukin työpaja sisälsi esimerkinomaiset alustukset aihepiirin hyviin käytäntöihin pääasiassa edelläkävijäyritysten alustuksin. Nämä alustukset synnyttivät erittäin hedelmällistä keskustelua erilaisista käytännön tavoista ratkaista yritysten polttavat kipupisteet.

Tulosten keskeiset hyödyt suomalaiselle teollisuudelle olivat:

- Kansainvälisten markkinoiden asettamat vaatimukset toiminnan jatkuvuudelle ja tietoturvalle pystytään nyt toteuttamaan hallitummin.
- Aihepiirin tietoperustaa ja ajattelutapaa parannettiin yhteisellä toimintatavalla teollisuuden toimintaedellytysten turvaamiseksi. Mm. teollisuus, järjestelmätoimittajat sekä viranomaiset pohtivat yhteistyössä ratkaisuja keskeisiin ongelmiin.
- Kehitetty tietoturvaosaaminen jalkautetaan – teollisuus on nyt laajasti mukana ja yhdessä kehittämässä käytännön valmiuksia, tietoturvavaatimuksia ja -ohjeita teollisuustuotannon ja siihen liittyvän liiketoiminnan ja palvelujen jatkuvuuden varmistamiseksi.

Tulosaineisto

Työpajojen ennakkomateriaalit, alustukset, ryhmätyöt, yhteenvedot ja referenssit löytyvät [TEO-TT] hankealueelta HUOVIssa. Valitse työpaja Taulukon 1. mukaan.

2.3 COREQ-VE – Yhteinen tietoturvavaatimuskanta teollisuudelle – Toimittajan hallinnan vaatimukset

Käytännöllinen TIETOTURVAVAATIMUSKANTA automaatiotoimittajien hallintaan yhteistyössä teollisuuden kanssa

COREQ-VE-hankkeen idea syntyi automaatiota hyödyntävän teollisuuden tarpeista pystyä järjestelmällisesti tukemaan yhä enemmän moderneja ICT-järjestelmiä kohti suuntautuvan ja lisääntyvää ulkoistusta hyödyntävän automatisoidun tuotannon jatkuvuuden ja tietoturvan hallintaa. Teollisuudessa huomattiin, että tietoturvakysymyksiin tarvitaan selkeämpää ohjeistusta tuotannon elinkaaren kaikissa vaiheissa. Tukea tarvitaan hankinnan alkuvaiheessa järjestelmätoimittajien ja sovelluskehittäjien tietoturvakäytäntöjen määrittelyyn, mukaan lukien erityisesti projektitoimituksen elinkaaren tietoturva aina jatkuviin automaatiopalvelusopimuksiin ja järjestelmän elinkaaren loppuun saakka.

VTT:n vetämässä ”Common REQuirements for Vendors” (COREQ-VE) -hankkeessa tavoitteena oli kehittää suomalaisen teollisuuden – tehtaiden ja laitosten – yhteiseen käyttöön tietoturvavaatimuskanta helpottamaan automaatiojärjestelmähankintojen ja automaatiotoimittajien tietoturvallisuuden hallintaa.

Kenelle: Eri toimialojen tehtaiden tai laitosten automaatiojärjestelmien toimivuudesta ja hankinnoista vastaavat henkilöt.

Mihin tarkoitukseen? Toimittajahallinnan tietoturvavaatimuskanta:

- Luo yhteistä käsitystä automaation tietoturvallisuuden menettelyistä
- Tukee tehtaiden/laitosten tuotantotoiminnan jatkuvuutta ja tietoturvallisuutta
- Tukee tehtaiden/laitosten tuotannosta vastaavien insinöörien, automaatiojärjestelmätoimittajien, sekä verkko-operaattoreiden tietoturvatehtävien työnjakoa
- Asettaa vaatimuksia automaatiotoimittajille ja palveluntarjoajille tietoturvahyökkäyksiin varautumisen kehittämiseen
- Parantaa tietoturvatietoisuutta.

Tulosaineisto

COREQ-VE-hankkeessa kehitettiin talven 2011—2012 kuluessa malleja tietoturvan hallitsemiseksi automaatiojärjestelmien hankintojen koko elinkaaressa:

- TIETOTURVAVAATIMUSKANTA jatkuvuuden varmistamiseksi automaatiojärjestelmien elinkaaressa: n. 250 priorisoitua vaatimusta englanniksi
- TIIVISTETYT TIETOTURVAOHJEET automaation hankintoihin seuraavilta osa-alueilta: *Tietoturvalliset etäyhteydet, Langattomat järjestelmät, Kovennus, Muutostenhallinta, Käyttäjäoikeudet*.

Varsinkin kehitetyn tietoturvavaatimuskannan soveltuvuutta automaatioteollisuuden käyttöön parannettiin kohdennetuilla yrityskäynneillä sekä yleisemmillä teollisuuden edustajille järjestetyillä katselmointitilaisuuksilla. Erityisesti minimivaatimusten asettamiseen ja priorisointiin käytettiin runsaasti yhteistä työaikaa keskittyen samalla vaatimusten ymmärrettävyyden ja yksikäsitteisyyden vahvistamiseen.

Vaikka COREQ-VE-hankkeen tulokset otettiinkin jo valmistuttuaan välittömästi teollisuuden käyttöön, niitä päivitettiin myöhemmin COREQ-ACT-hankkeen yhteydessä. Näin ollen tulokset referenssseineen ovat saatavilla HUOVI-portaalin Teollisuuden tietoturvan työpajat [TEO-TT] -hankealueen yhteyteen lisätyissä COREQ-ACT-projektin tuloskansioissa.

2.4 COREQ-ACT – Tietoturvan aktiiviset teollisuus-caset

Koeteltuja konsepteja tietoturvan jalkauttamiseksi teollisuustuotantoon

TEO-TT- ja COREQ-VE-hankkeiden aikana havaittiin, että teollisuudella on vaikeuksia ottaa todelliseen tuotantokäyttöön kaikkia tarvittavia tietoturvaratkaisuja ja käytäntöjä. Tämä johtui usein aiempien käyttökokemusten puutteesta ja varsin tyypillisestä resurssien vähäisyydestä, mutta myös yrityksen teollisuustuotannolle räätälöidyn tietoturvakonseptin puutteesta. Ilman yhtenäistä ja konkreettista koko tuotannon ja siihen liittyvien järjestelmien kattavaa suojauskokonaisuuden määrittelyä ja sisäistämistä tuotannon tietoturvan käytännön toteutus jää valitettavan usein vajavaiseksi. Jatkuvasti kasvavien tietoturvariskien hallitsemiseksi teollisuusyritysten tulisikin ottaa käyttöön hyväksi havaitut ja omaan tuotantotoimintaansa sovitetut tietoturvakonseptit ja mallit, tietoturvavaatimukset, luvitukset, valvotut toimintakäytännöt sekä ohjeet.

COREQ-ACT – ”Tietoturvan aktiiviset teollisuus-caset” -hankkeessa tavoitteena oli luoda koeteltuja konsepteja suomalaiselle teollisuudelle tietoturvavaatimusten jalkauttamiseksi tuotantokäytössä jo oleviin ja tuleviin automaatiojärjestelmiin. Huoltovarmuuskriittisille yrityksille julkistetut tulokset perustuvat todellisiin yritys-caseihin.

Keskeiset hyödyt

Hankkeen päälähtökohtana oli jälleen suomalaisen teollisuuden jatkuvuuden ja toimintakyvyn varmistaminen myös tietoturvan ja jatkuvuuden uhkia vastaan:

- Työn perustana oli osallistuvien yritysten omat yritys-caset, joilla tavoiteltiin selkeitä parannuksia yrityksen kykyyn ylläpitää tuotantotoimintaa ja kehittää liiketoimintaa lisääntyvistä yleisistä turvallisuus- ja tietoturvauhkista huolimatta.
- Yrityskohtaisten tulosten tuli olla selkeästi myös muiden yritysten hyödynnettävissä. Tämän vuoksi projektissa tuotettiin julkiset tulokset yrityskohtaisista tuloksista mm. poistamalla ratkaisukuvauksista yrityssalaisuudet sekä muut liialliset yksityiskohdat.
- Hankkeen julkiset tulokset ja materiaalit jaetaan kaikkien relevanttien toimijoiden hyödyksi Huoltovarmuuskeskuksen HUOVI-portaalin kautta.

Tulosaineisto

Projektin tulokset syntyivät kiinteässä yhteistyössä osallistuvien yritysten kanssa. Kukin osallistuva yritys määritteli ydinliiketoimintansa jatkuvuuden varmistamiselle oleellisen yritystapauksen (case) tai useita pienempiä tapauksia. Näitä hyväksi käyttämällä projektissa kehitettiin:

- Teollisuuden tietoturvalliset toimintakäytännöt, -ohjeet, vaatimukset ja esimerkkimallit
- Ohjeita (ja kokemuksia) edellisten jalkauttamisesta organisaatioon.

Projektissa pyrittiin tietoisesti tulosten erityiseen:

- YMMÄRRETTÄVYYTEEN ja yksinkertaistamiseen alati muuttuvia teknisiä yksityiskohtia välttäen
- HELPPOKÄYTTÖISYYTEEN ja helppoon KÄYTTÖÖNOTETTAVUUTEEN – tiedostot räätälöitävissä omaan käyttöön.

COREQ-ACT-hankkeen tulokset ovat saatavilla HUOVI-portaalissa Teollisuuden tietoturvan työpajat [TEO-TT] -hankkeen alaisissa COREQ-ACT-tuloskansioissa.

Seuraavassa kuvassa on pääosa kutsusta viimeiseen COREQ-ACT-tulosten esittelytilaisuuteen, joka pidettiin huoltovarmuuskriittisille toimijoille syyskuussa 2013.

KUTSU TULOSTEN ESITTELYTILAISUUTEEN

Huoltovarmuuskeskuksen, Viestintäviraston & VTT:n teollisuusautomaation tietoturvaprojektin tulosten esittelytilaisuus

Ajankohta: keskiviikko 4.9.2013, klo 9.30 - 14.00

Paikka: VTT, Vuorimiehentie 3 (Digitalo, Tila AP107), Espoo, Otaniemi

Koeteltuja konsepteja tietoturvan jalkauttamiseksi tuotantoon

Hankkeen tavoite: VTT:n vetämässä "Tietoturvan aktiiviset teollisuus-caset" (COREQ-ACT) hankkeessa tavoitteena on ***luoda koeteltuja konsepteja suomalaiselle teollisuudelle tietoturvavaatimusten jalkauttamiseksi tuotantokäytössä oleviin ja tuleviin automaatiojärjestelmiin***. Tulokset perustuvat todellisiin yritys-caseihin.

Kenelle: Huoltovarmuuskriittisten yritysten edustajille. Eri toimialojen tehtaiden tai laitosten automaatiojärjestelmien tietoturvasta, toimivuudesta ja mm. hankinnoista vastaavat toimihenkilöt.

Ohjelma:

Aamukahvit

1. Tilaisuuden avaus (Huoltovarmuuskeskus)
2. COREQ-ACT projektin lyhyt esittely ja tilanne (VTT)
3. Tehtaan tietoturvaohjeet (malliesimerkki)
4. Toimittajahallinnan tietoturvavaatimuskanta (päivitetty)
5. Automaatiohankintojen lyhyet tietoturvaohjeet (päivitetty)
6. Tietoturva kunnossapidon muutostöissä (koulutusmateriaali)
7. Automaation tietoverkkojen suojaamisen jalkautus

Lounas

8. Automaation etäyhteyksien mallit
9. Etäyhteyksien monitorointi käytännössä
10. Application whitelisting -ohjelmistotuotteiden testaus

Tulosten kommentointi (myös tilaisuuden aikana)

Taustaa: Jatkuvasti kasvavien tietoturvariskien hallitsemiseksi teollisuusyritysten tulee ottaa käyttöön hyväksi havaitut ja omaan tuotantotoimintaansa sovitetut ja tietoturvalliset toimintakäytännöt, -ohjeet, vaatimukset ja esimerkkimallit.

Yhteiskunnan huoltovarmuutta kehitetään laajassa kumppanuus- ja yhteistyöverkostossa, johon kuuluu elinkeinoelämän toimijoita kaikilta aloilta, valtionhallinnon ja kuntahallinnon toimijoita sekä toimialajärjestöjä. Tuottaessaan palveluita ja hyödykkeitä, elinkeinoelämän toimijoiden on varmistettava toimintaverkostonsa toimintakyky mm. prosessien ja osaamisen osalta. Tuotantolaitoksen toiminta on voimakkaasti riippuvainen ulkoisista palvelu- ja hyödyketoimittajista. Automatisoidun tuotannon suojaaminen vaatii laajaa osaamista, sillä yrityksen tulee osata täsmentää mm. tuotantojärjestelmien hankintaan, hallintaan ja ylläpitoon liittyvät tietoturvavaatimukset. Automaatiojärjestelmien tietoturvallisuuden hyvä hallinta on tärkeä osa tehtaiden/laitosten toiminnan jatkuvuudenhallintaa ja sitä syvennetään alan kaikkien toimijoiden hyödyksi ja huoltovarmuuden edistämiseksi Huoltovarmuuskeskuksen, Viestintäviraston (CERT-FI), teollisuuden ja VTT:n yhteisprojekteissa.

Kuva 2. COREQ-ACT-tulosten esittelytilaisuuden kutsu. Ks. HUOVI-portaalin Teollisuuden tietoturvan työpajat [TEO-TT] -hankkeen kalenteri.

OSA 3

TULOKSIA

3 TULOKSIA

Edellä esitellyissä hankkeissa työstettiin teollisuuden tietoturvaan liittyviä tärkeimpiä teemoja yhteistyössä erityisesti teollisuuden automaatioinsinöörien, automaatiojärjestelmätoimittajien ja palveluntarjoajien, Huoltovarmuuskeskuksen, VTT:n, Tampereen Teknillisen Yliopiston ja CERT-FI:n muodostamassa verkostossa.

Pääosa huoltovarmuuskriittisille toimijoille julkistetuista tuloksista viimeisteltiin erilaisten työpajojen ja katselmointitilaisuuksien yhteydessä, joissa soveltuvia malliratkaisuja ja yrityskäytäntöjä kehitettiin edelleen paremmin soveltuvaksi suomalaisen automaatiota hyödyntävän teollisuuden tarpeisiin. Näitä eri hankkeissa syntyneitä tuloksia on esitelty monissa kohdistetuissa tulostenesittelytilaisuuksissa, joiden osallistujiksi on pyydetty tärkeimpiä automatisoidun tuotannon tietoturvaan vaikuttavia avainhenkilöitä.

Huoltovarmuuskriittisille toimijoille esitetyt julkiset tulokset sisältävät mm. seuraavanlaisia teemoja:

- Automaation tietoturvan kartoitus
- Teollisuuden tietoverkkojen ja etäyhteyksien hallinta ja seuranta
- Tehtaan tietoturvaohjeet, koulutus ja muutosten hallinta
- Hankintakäytännöt ja vaatimukset toimittajille
- Tekniset tietoturvamenetelmät (tietoturvatestaus, sallimislistaus)
- Tuotannon riskien hallinta ja jatkuvuuden varmistaminen.

3.1 Automaation tietoturvan kartoitus

Automatisoidun tuotannon tietoturvan nykytilanteen kartoittaminen on välttämätön edellytys yrityksen tuotannon jatkuvuuden varmistamiseksi ja ennakkovarautumisen vahvistamiseksi erilaisia kyberriskejä vastaan. Tuotantokokonaisuuteen liittyy usein yllättävän useita erilaisia järjestelmiä ja tietopääomia, dataa, pääsynvalvontaa, työlupia, toimintatapoja ja -ohjeita. Tästä syystä automaation tietoturvatilanne voidaan kartoittaa useista erilaisista lähtökohdista, riippuen yrityksen lähtötilanteesta ja jo tunnetuista kehitystarpeista. Hankkeiden automaation tietoturvan kartoitus jaettiin ainakin kahteen eri kategoriaan:

- Tietoturvan yleiskartoitus tuotannon automaatiossa
- Automaatioverkon kartoitus.

3.1.1 Tietoturvan yleiskartoitus tuotannon automaatiossa

Motivaatio: Julkisuuteen tulleet teollisuuteen kohdistuneet tietoturvahyökkäykset olivat motivoineet automaation käyttäjäorganisaatiot parantamaan tuotannon tietoturvaa. Hyvä motivaatio on perusedellytys perusteellisen tietoturvakartoituksen ja nykytilan selvittämisen aloittamiselle ja varsinkin loppuun asti saattamiselle. Myös johdon motivaatio edellyttää yleistä tietoturvatietoisuuden lisäämistä sekä varsinkin tapahtumatietoa todellisista haavoittuvuuksista ja toteutuneista riskeistä omassa tai omaa vastaavissa organisaatioissa.

Hankkeiden kuluessa olemme oppineet,

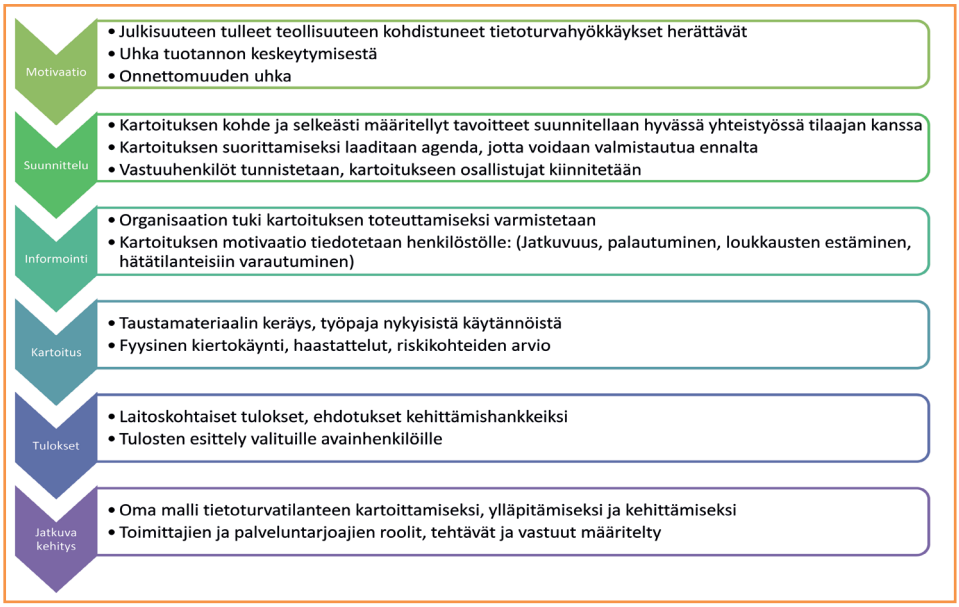
että tietoturvan yleiskartoitus voidaan toteuttaa onnistuneesti, kunhan huomioidaan seuraavat seikat.

Yleiskartoituksen suunnittelu

- Kartoituksen kohde ja selkeästi määritellyt tavoitteet suunnitellaan hyvässä yhteistyössä tilaajan kanssa.
- Kartoituksen suorittamiseksi laaditaan agenda, jotta tilaisuuksiin voidaan valmistautua ennalta.
- Vastuuhenkilöt tunnistetaan, kartoitukseen osallistujat kiinnitetään.
- Organisaation tuki kartoituksen toteuttamiseksi varmistetaan.

Lisäksi on usein hyvä, jos puolueeton osapuoli vastaa kartoituksen kokonaisuudesta.

- Välttämätön edellytys on, että kartoituskohteen henkilöstö voi luottaa kartoittajaan.
- Kartoituksen tavoitteena on kehittää toimintaa tietoturvallisemmaksi, ei syyllisten löytäminen tai rangaistusten jakaminen.
- Tulosten käyttötarkoitus on määriteltävä edeltäkäsin (tuloksia käytetään toiminnan kehittämiseen, ei kartoitusta tekevän osaston toimivallan laajentamiseen tai erinomaisuuden korostamiseen).



Kuva 3. Yleiskartoituksen vaiheet. [TEO-TT] Ks. kansio: Kooste TEO-TT tuloksista.

Yleiskartoituksen toteutus-vaiheen tyypillisiä tehtäviä on listattu seuraavassa taulukossa.

Yleiskartoituksen toteutuksen vaiheet
0. Alkuesittelyt.
1. Työpaja tuotantolaitoksen nykyisistä työkäytännöistä ja ohjeistuksesta.
2. Tuotantolaitoksen kiertokäynti.
3. Avainhenkilöiden haastattelut.
4. Tulosraportin laadinta.
5. Kartoitustulosten esittely.
6. Keskustelu kartoitustuloksista ja suositelluista kehityskohteista.

Taulukko 3. Yleiskartoituksen toteutuksen vaiheet. Ks. [TEO-TT] TEO-TT-Työpaja 1.

Yleiskartoituksen lopputulokset

Tämän yleisluontoisen kartoituksen lopputuloksena syntyvät esim. seuraavat tulokset (kartoitukselle edeltäkäsin asetettujen tavoitteiden mukaisesti):

- Automaatiokäytön tietoturvatilanteen yleiskartoituksen laitoskohtaiset tulokset:
    - Yleiskuva tietoturvan puutteellisista osa-alueista (gaps)
    - Löydökset (findings) ja niiden perustelut (reasoning)
    - Tehtävälista (task list)
    - Suosituksia tietoturvan parantamiseksi (recommendations).
- Ehdotus tietoturvan kehittämishankkeiksi (initial improvement programs)
- Työnkulun määrittely automaation tietoturvakartoituksen toistettavaan suoritukseen.

Huom: Tulokset on luokiteltava luottamuksellisiksi ja vain rajatun ryhmän käyttöön.

Mikäli yleiskartoituksesta halutaan saada vielä enemmän irti samalla kertaa, voidaan toteuttaa alustavaa selvitystä esimerkiksi seuraavista asioista:

- Tehdasverkon tietoliikenteen pika-analyysi tuotantokäytön verkkoliikennettä monitoroimalla tai tallettaen dataliikennettä esim. sopivista yhdyskäytävistä tai isäntäkoneista
- Luonnostelua tuotannon tietoturvavaatimuskannan pohjaksi lähtien tuotannon jatkuvuuden ja riskien hallinnan tavoitteista.

Näiden kahden lisäanalyysin laadukas toteuttaminen vaatii kuitenkin yleensä erityisosaamista ja aikaa enemmän kuin muutaman työpäivän. Mutta jos nykytilanteesta halutaan saada nopeasti hieman tarkempi tilannekuva, niin tämän tyyppisiin lisäanalyyseihin kannattaa varata tarvittavat resurssit ja osaava tuki organisaation sisältä.

Mikäli tukea ulkoiselle selvitystyölle ei saada organisaation sisältä, saatetaan ko. selvityksillä aikaansaada enemmän vahinkoa tai kysymyksiä kuin tilanteeseen sopivaa ja suunniteltua tietoturvan hallinnan kehitystä. Vaarana on myös arkaluontoisen tietoturvan varmistamiseen liittyvän tiedon vuoto asiattomille tahoille, mikäli NDA- ym. sopimuksia ei allekirjoiteta ja noudateta. Myös tietoturvan kehittämisen keinot, osapuolet ja menetelmät saattavat vaatia riskianalyysin ennen niiden käyttöönottoa ko. yrityksessä, sillä mitään toimintaa ei tulisi toteuttaa ilman selkeää suunnitelmaa tulevista tehtävistä ja käytettävistä työkaluista tai ilman tietoa mahdollisista seurauksista ja haittavaikutuksista.

3.1.2 Automaatioverkon kartoitus

Ennen uusien verkkosuojauksen kehityspanosten kiinnittämistä on tärkeää selvittää yksityiskohtaisesti yrityksen tuotantoyksiköissä käytettyjen tietoverkkojen nykytila. Tällöin parannus- ja kehityshankkeilla saadaan paras mahdollinen vaikuttavuus tuotantoverkon tietoturvan tasoon ja tuotannon jatkuvuuden varmistamiseen. Kartoitustulos dokumentoi samalla kehitystyön tarpeet ja antaa selkeät perusteet tarvittaville kehityshankkeille verkkojen suojauksen parantamiseksi. Tuotantoverkkojen yksityiskohtainen kartoittaminen antaa myös konkreettisen pohjan erilaisten verkko-ongelmien selvittämiselle sekä tukee yrityksen tietoturvakonseptin kehittämistä.

Esimerkiksi tuotantoautomaatioverkkojen ja niihin liittyvän tehdasverkon todellisen järjestelmäkokoonpanon, verkkoarkkitehtuurin, käytettyjen liityntöjen ja datayhteyksien täytyy olla hyvin dokumentoituja ennen kuin ko. verkon tietoturvaa voidaan arvioida ja tämän jälkeen kehittää systemaattisesti ja kustannustehokkaasti. Verkon kartoitus selvittää juuri näitä seikkoja. Verkkokartoituksessa tulee samalla selventää tehtaan/tuotannon nykyisten dataverkkojen eri tehtävät. Tällaisia (osaverkkoja) voivat olla mm.:

- tehdasverkko
- lähettämön/varaston aliverkot, jne.
- valvomoverkko
- automaatioverkko
- kenttäväylät, I/O:t, jne.
- turvaväylät
- langaton verkko, vierailijaverkko, jne.

Kartoituksen jälkeen mm. itsenäisten osaverkkojen eriytys voidaan varmistaa systemaattisesti ja hallitusti yrityksen tietoturvakonseptin mukaisesti. Automaatioverkon kartoitukseen voikin kuulua seuraavia osatehtäviä:

Automaatioverkon kartoitus
Kartoitetaan ja dokumentoidaan kaikki tuotantoon liittyvät verkot yksityiskohtaisesti puutteineen.
Dokumentoidaan mm. kaikki fyysinen johdotus (esim. verkkokytkimistä), todellinen verkkotopologia ja arkkitehtuuri.
Kartoitetaan kaikki tehdasverkon laitteet, käyttöjärjestelmät, ohjelmistot, sovellukset jne.
Kartoitetaan mm. kaikki käytössä olevat IP-osoitteet ja MAC-osoitteet.
Selvitetään kaikki tehdyt riskianalyysit ja jatkuvuuden varmistamisen toimet, verkkojen nykyinen suojaus ja eriytys.
Selvitetään nykyiset verkkosuunnitelmat ja tulevaisuuden kehitystarpeet.
Selvitetään tuotantoon liittyvien verkkojen uudet uhat ja haavoittuvuudet.

Taulukko 4. Automaatioverkon kartoituksen osatehtäviä. Ks. [TEO-TT] COREQ-ACT-projektin kansio: Automaation tietoverkkojen suojaaminen käytännössä.

Kartoittamisessa on erittäin tärkeää huolellinen selvitystyö mm. verkkojen nykyisen johdotuksen, laitteiden ja ohjelmistojen kirjaamiseksi esim. laite- ja ohjelmistorekistereihin. Samoin tärkeää on kaikkien loogisten datayhteyksien selvittäminen ja komponenttidiagrammien piirtäminen (esim. käyttöönotto-dokumenttien päivittäminen, jokaisen käytetyn rajapinnan dokumentointi ja eri datayhteyksien käyttäjien ja käyttötarpeiden selvittäminen). Kartoituksessa selvitetään siis laitteiden ja järjestelmien välisten tiedonsiirtoyhteyksien merkitys, sovellukset, niiden datayhteydet, protokollat ja portit. Ts. kaikki tiedonsiirto, myös yhteydetön (esim. UDP) dataviestintä selvitetään.

Mahdollinen erityisasiantuntijoiden käyttö esim. pistotestaukseen tai porttiskannaukseen (ei tuotannon aikana) tulee suunnitella ja valmistella huolella.

3.2 Teollisuuden tietoverkkojen ja etäyhteyksien hallinta ja seuranta

Teollisuudessa käytettävien erilaisten tieto- ja tehdasverkkojen tietoturvan hallinta on vaativa ja monitahoinen tehtävä. Tämä johtuu mm. siitä, että tuotantolaitoksen sisäiset verkot tulisi jakaa useisiin toiminnallisesti erilaisiin vyöhykkeisiin, joilla kullakin on omat erityispiirteensä, esim. määrätyt reaaliaika- ja/tai saatavuusvaatimuksensa.

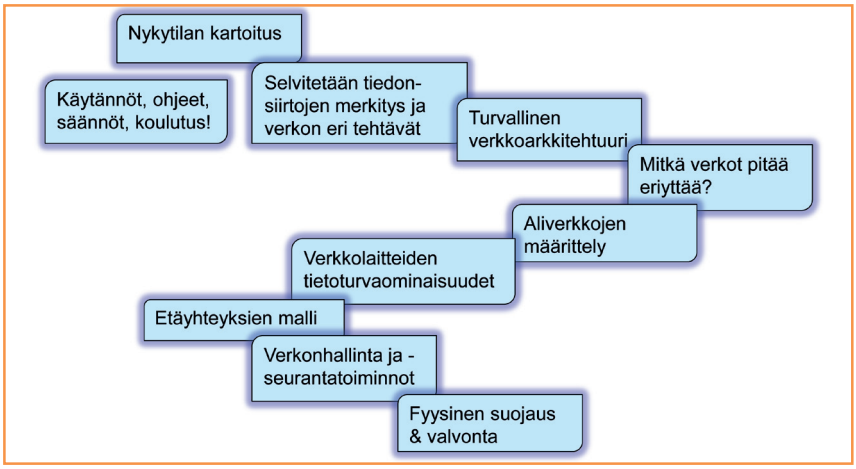
Toisaalta yrityksen tuotantoyksiköiden välisten tietoverkkojen käyttö tyypillisten ICT-tuotteiden ja julkisten verkko-operaattoreiden palvelujen avulla tähtää saatavuuden varmistaviin datayhteyksiin. Joissain tapauksissa vastaavat yhteydet toteutetaan kahdennetuilla kuituyhteyksillä, millä tähdätään saatavuuden mahdollisimman hyvin varmistaviin datayhteyksiin sekä verkon turvaamiseen ulkoisilta vaikutuksilta.

Toisaalta automaatioverkkojen tehtävänä on toimia häiriöttömästi itsenäisinä soluina, joiden toiminta ei ole riippuvaista ulkoisista yhteyksistä tai järjestelmistä. Automaatioverkkojen tietoliikennettä ja automaatioprotokollia ei tule sallia muissa verkoissa, eikä muista verkoista tule sallia suoraa pääsyä automaatioverkkoihin. Usein automaatioverkon ja muiden verkkojen väliset tietoyhteydet kuitenkin tarvitaan.

3.2.1 Tietoturvallisen automaatioverkon jalkautus

Tietoturvallisen automaatioverkon jalkautus vaatii paneutumista moniin erilaisiin asioihin. Näitä ovat:

- Tietoturvan merkityksen ja nykytilan ymmärtäminen, sekä johdon tuki ja panostus (työaika + budjetti)
- Laaja-alaisen kehitysryhmän muodostaminen ja faktoihin (esim. kartoitukseen) perustuvan kehityssuunnitelman laadinta (roolit & tehtävät)
- Automaatioverkon suojauskonseptin määritteleminen ja ymmärrettävät tuotannon tietoturvapolitiikat (vaatii oman henkilöstön panostusta)
- Tietoturvavaatimusten määrittely ja tietoturvan tuominen jo hankintavaiheeseen
- Selkeät tietoturvaohjeet, -käytännöt ja -säännöt sekä edellisten toteuman valvonta.



Kuva 4. Automaatioverkon suojaamisen osatehtäviä. Ks. [TEO-TT] COREQ-ACT-projektin kansio: Automaation tietoverkkojen suojaaminen käytännössä.

Automaatioverkkojen suojaaminen vaatiikin monentyyppisten asioiden huomioimista ja erityisesti erilaisten häiriöitä aiheuttavien tapahtumien välttämistä. Tähän tarvitaan sisäistä ohjeistusta, jolla säännellään sallittuja tehtäviä niin ihmisten kuin laitteiden ja ohjelmistojenkin osalta. Näitä tehtäviä on käsitelty tarkemmin [TEO-TT] COREQ-ACT-projektikansion tuloksessa ”Automaation tietoverkkojen suojaaminen käytännössä”.

Usein verkon suojaamisen jalkautuksessa korostuukin automaatioverkon kartoituksen ja nykytilan selvittämisen lisäksi erilaisten yksinkertaisten käytäntöjen, ohjeiden ja sääntöjen laadinta sekä niiden (ja yleisen tietoturvatietoisuuden) opetus. Käytännöt, ohjeet ja säännöt eivät saa olla monitulkintaisia, vaan ne tulee laatia yhteistyössä käyttäjien kanssa sellaisiksi, että mahdollisuus vääriin tulkintoihin minimoidaan.

Turvallisen verkkoarkkitehtuurin määritteleminen on erittäin oleellista, samoin kuin hyvä ymmärrys ja suunnitelma siitä, mitkä verkot tulee eriyttää toisistaan. Kestävässä ja tietoturvallisessa verkkoarkkitehtuurissa:

- Määritellään tietoturvavyöhykkeet joihin pääsy rajoitetaan, esim.:
    - tehdasalue
    - *DMZ*-erotteluvyöhyke
    - palvelimet, valvomo
    - automaatio / kenttäväylät / turvaväylät.
- Tietoturvavyöhykkeiden yhteensovittaminen turva-alueisiin on suositeltavaa.

Tuotannon jatkuvuus tulee olla perustana kaikessa tietoverkkoarkkitehtuurin suunnitteluun liittyvissä määrittelyissä. Tämä edellyttää usein verkkojen jakoa itsenäisiin osaverkkoihin tuotantoalueen sisällä.

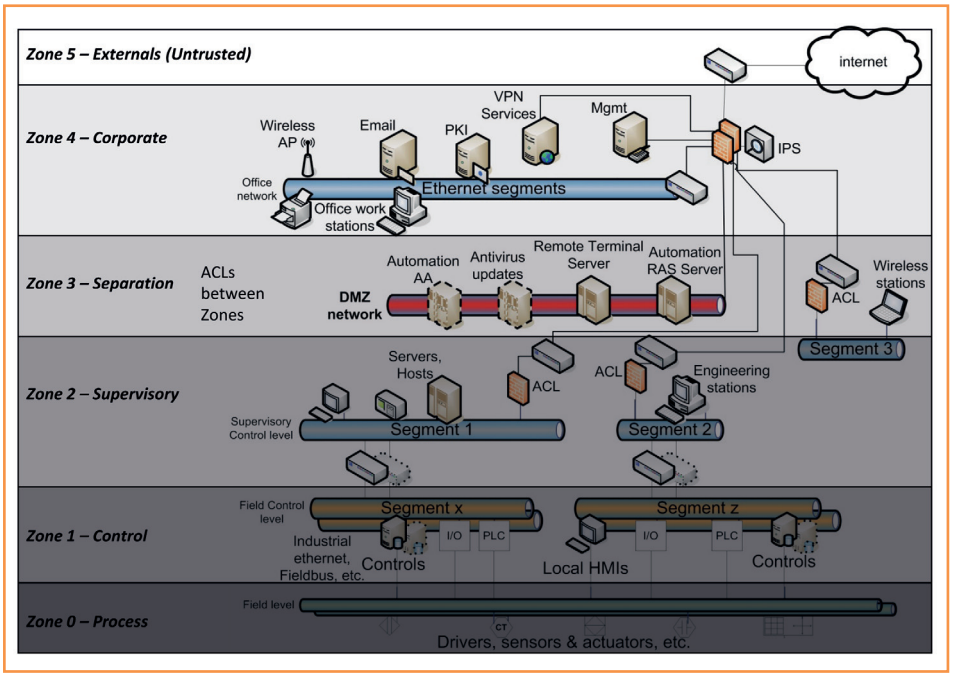
Osaverkkojen eriyttämisen suunnittelu edellyttää erilaisten ratkaisujen puntarointia ja lopulta päätösten tekoa. Päätökset riippuvat toimituksen sisällöstä. Mikäli teknisesti on mahdollista, ainakin seuraavia periaatteita kannattaa tosissaan tavoitella:

- Eristetään toiminnallisesti itsenäiset verkot, kuten tietyn toimittajan itsenäinen aliverkko
- Sallitaan aliverkossa vain rajatut protokollat kuten esim. PROFINET
- Lisätään automaatioverkon reunalle erityinen erottava palomuuri
- Mahdollinen VLAN-määrittely ja aliverkkojen välisen datan kontrollit/ suodatus
- Määritellään aliverkossa sallitut käyttöjärjestelmät, sovellukset ja niiden versiot.

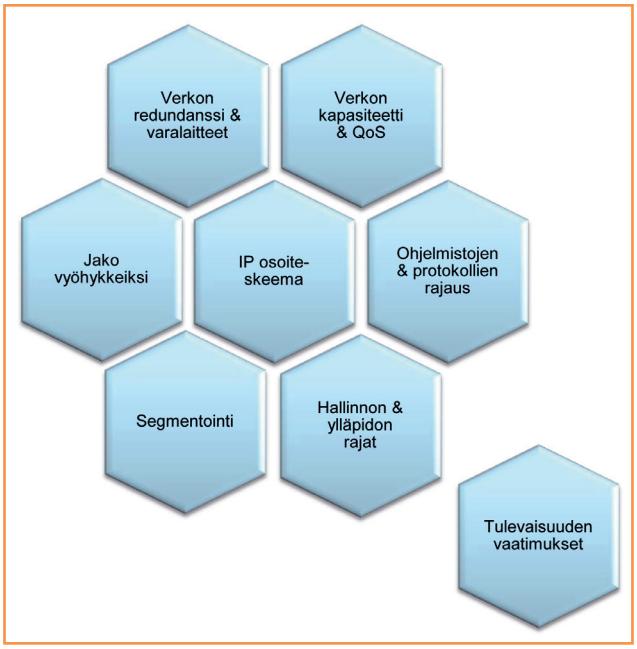
Tietoturvallisen verkkoarkkitehtuurin käytännön toteutus edellyttää, että käytettävät verkkolaitteet (verkkokytkin, reititin, palomuuri, langaton tukiasema jne.) tukevat sopivia tietoturvaominaisuuksia. Suojauskonsepti saattaa vaatia tukea esim. seuraaville ominaisuuksille: palomuuritoiminne, lokitus (esim. *syslog*), pääsynvalvontalista, *RBAC* (oikeudet lukittavissa), *VLAN*, *VPN,* ja lisäksi langaton suojausstandardi, mikäli langaton verkko on sallittu.

Tietoturvallinen verkkolaitteiden hallinta voi lisäksi edellyttää laitteilta esim. seuraavia ominaisuuksia:

- *Port security*, kiinteä IP-osoite
- Vapaan kytkinportin poisto / *disable*
- Turvallinen moodi asennukseen (*local, remote*-asennus)
- Varmuuskopiointimahdollisuus verkkoon tai ulkoiselle medialle
- Asetusmuutosten lokitus
- Verkon valvonnan eri ominaisuudet.



Kuva 5. Kestävä ja tietoturvallinen verkkoarkkitehtuuri. Ks. [TEO-TT] COREQ-ACT-projektin kansio: Automaation tietoverkkojen suojaaminen käytännössä.



Kuva 6. Tuotantoon liittyvien verkkokokonaisuuksien suojaamiseen liittyviä määrittelyjä ja tehtäviä. [TEO-TT] COREQ-ACT-projektin kansio: Automaation tietoverkkojen suojaaminen käytännössä.

Tuotannon verkkokokonaisuuksien tietoturvan hallinta ja jatkuvuuden varmistaminen helpottuvat huomattavasti, mikäli erilaisten ohjelmistojen, sovellusten ja tietoliikenneprotokollien asennus- ja käyttöluvat rajataan tiukin pelisäännöin:

- HYVÄ HALLITTAVUUS. Ainoastaan tarkkaan rajatut sovellukset, käyttöjärjestelmät ja ohjelmistot kussakin vyöhykkeessä:
    - Esim. toimittajan ylläpitämä aliverkko jossa on ainoastaan toimittajan hyväksymät ohjelmistot
    - Muut aliverkot automaatiovastaavan hyväksymillä ohjelmistoilla ja mahdollisimman yhtenevä protokollapino aliverkon eri laitteissa.
- TEKNISET SÄÄNNÖT. Yksinkertaistetaan palomuurisäännöt yllä rajatuilla sovelluksilla ja protokollavalinnoilla:
    - Sallitaan aliverkkojen välillä ainoastaan hyväksyttyjen erityissovellusten tietoliikenne
    - Kielletään oletusarvoisesti kaikki muu tiedonsiirto palomuurien läpi
    - Suositaan palomuurisääntöjä yksinkertaistavia sovelluksia (esim. OPC UA) ja tietoturvaominaisuuksia.

Päätavoitteena tuotantoyrityksellä tulisi olla, että tuotannossa on ainoastaan yksi yhteinen toimintatapa tehdas- ja automaatioverkon käyttöön, hallintaan ja ylläpitoon. Tämän tulisi sisältää yksityiskohtaiset pelisäännöt niin henkilöstölle kuin laiteasetuksillekin.

Esimerkki

Seuraavassa on listattu teknisluonteisia sääntöjä, joilla automaatioverkkojen saatavuus- ja tietoturvatavoitteet voidaan turvata ulkoisia ja sisäisiä uhkia vastaan.

- Vyöhykkeet ja verkkojen eriytys:
    - Erilliset automaatiovyöhykkeet ja segmentit, joita palomuuri ja DMZ-alue erottavat
    - Hyväksytyt automaation palomuurilaitteet ylläpitosääntöineen
    - Esim. ACL-pääsylistat palomuureissa ja VLAN-määritykset kytkimissä.
- Rajoitetut sovellukset ja tiedonsiirtoprotokollat:
    - Määrätyt *application whitelisting* ja/tai AV-tuotteet käytössä määrätyissä isäntäkoneissa
    - Automaatiosegmentissä sallitut sovellukset ja protokollat kiinnitetty.
- Sallitut tietovuot on määritelty:
    - Erityisesti verkkojen välisen dataliikenteen lähdeosoite, kohdeosoite, protokolla, portti-, sekä liikennemäärä ja käyttötarkoitus rajattu.
- Tekninen tietoturvamonitorointi on järjestetty:
    - Palomuureissa ja palvelimissa on käytössä pääsynvalvonta ja sen seuranta (*syslog* tms.)
    - Verkkoliikennettä seurataan soveltuvin osin: räätälöity IDS (yhdyskäytävät, kriittinen data).
- Etäyhteyskäytännöt ja työkalut on määritelty ja niiden käyttökohteet on rajattu:
    - VPN-yhteys on terminoitava DMZ-alueen määrättyyn etäyhteyspalvelimeen yritysverkon kautta ja automaation etäkäyttäjätodennuksen jälkeen.

Lisätietoja ja referenssejä löytyy HUOVIsta [TEO-TT] COREQ-ACT-projektikansion tuloksista ja referensseistä.

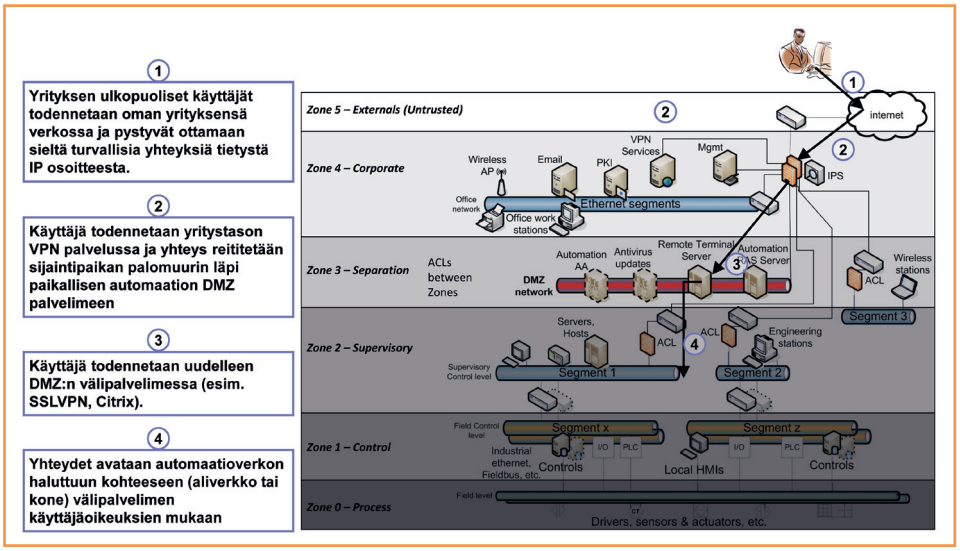
3.2.2 Automaation etäyhteyksien mallit

Kuten edellä jo mainittiinkin, automaatiojärjestelmää ei saa liittää suoraan julkisiin verkkoihin tai muita käyttötarkoituksia varten kehitettyihin järjestelmiin, sillä tällainen liityntä tarjoaisi mahdollisuuden suoraan hyökkäyspolkuun automaatiojärjestelmiä vastaan. Samasta syystä yrityksen tulee määritellä automaation etäyhteyksille tietoturvalliset ja hyväksytyt tekniikat sekä erilliseksi liityntäverkoksi eriytetty automaation DMZ-aliverkko.

Myös etäyhteyksien käyttötarkoitukset tulee määritellä ja rajoittaa etäkäyttö teknisesti vain määritellyssä työtehtävässä tarvittavaan. Etäyhteyden käyttöä tulee lisäksi valvoa sekä teknisin että hallinnollisin menettelyin.

Mikäli etäyhteyksissä halutaan varautua yritysverkon tietoliikennehäiriöön, saatetaan tarvita erillinen ja erikseen kytkettävä varayhteysteknologia. Tämäkin on määriteltävä riittävän tietoturvalliseksi, ja varayhteyden käyttöönotto on asianmukaisesti luvanvaraistettava.

Automaation etäyhteyksiä pystytäänkin käytännössä järjestämään käyttämällä lukuisia erilaisia palomuuri- ja DMZ-ratkaisuja. Vaikka tämä lisää joustavuutta, on se kuitenkin tuotannon tietoturvan hallinnan kannalta suuri ongelma. Etäyhteyden perusmalli automaatioverkkoon esitetään seuraavassa kuvassa.



Kuva 7. Perusmalli etäyhteydelle automaatioverkkoon. [TEO-TT] COREQ-ACT-projektin kansio: Automaation etäyhteyksien mallit.

Vaikka yrityksen tuotannossa käytettävien etäyhteyskäytäntöjen määrittelyssä onnistuttaisiinkin, voi näiden käytäntöjen huolimaton tekninen toimeenpano (käytettävissä olevat huonot palomuurilaitteet, konfiguraatio jne.) silti aiheuttaa automaatioon suuria riskejä.

Suurien riskien takia yrityksen on tarpeen vertailla erilaisia automaation *DMZ*-/palomuuriratkaisuja mm. tietoturvaominaisuuksien osalta ja mahdollisesti määritellä erityinen vertailukriteeristö. Seuraavassa kuvassa on esitetty eräs etäyhteysratkaisujen tietoturvaominaisuuksien vertailukriteeristö.

Vaikka ratkaisujen tietoturvaominaisuuksien vertaaminen onkin tärkeää, tulee kuitenkin muistaa, että ensisijaisesti var-

KRITEERI (lyh.)	EDUT	HAITAT
VPN YHTEYS	**TURVALLINEN ETÄYHTEYS**	**YLLÄPITOTYÖ**
Etä-PC ←→ Automaatiolaite (PLC)	Helppo suora yhteys automaatioon	Etä-PC:n riskit voivat siirtyä automaatioon
Etä-PC ←→ Automaation DMZ palvelin	Turvallinen välipalvelin suojana	Palvelimen ylläpitotyö
Etä-PC ←→ Automaation palomuuri	Suora yhteys automaation palomuuriin	Etä-PC:n riskit voivat siirtyä automaatioon
PALOMUURIT	**VERKKOJEN LOOGINEN EROTUS**	**YLLÄPITOTYÖ**
Palomuurit / ACL-kontrollit eri tasoilla	Monta järjestelmää suojaamassa	Palomuurien & ACL:ien ylläpitotyö
Palomuurien lokiseuranta käytössä	Tapahtumien seuranta	Lokien hallinta- ja seurantatyö
Protokollien suodatus käytössä	Väärän liikennetyypin esto käytössä	Harvinaisten käyttötilanteiden hankaluus
DMZ-ALUE	**TURVAVYÖHYKE**	**YLLÄPITOTYÖ**
Jako: väliverkko / aliverkot / VLANit	Häiriöiden vaikutusalue minimoitu	Monimutkaisempi ylläpitää
Suorat yhteydet ei sallittu	Ei suoria hyökkäyksiä yhteyden kautta	Enemmän komponentteja
Pakolliset välipalvelimet etäyhteyksissä	Tarkka pääsykontrolli mahdollistuu	Palvelimien ylläpitotyö
Selkeä hallintorajoihin jako käytössä	Selkeyttää vastuunjakoa ja toimenpiteitä	Vaatii useita ylläpidon rooleja/tilejä

Kuva 8. Etäyhteysratkaisuvaihtoehtojen tietoturvan vertailukriteeristö. [TEO-TT] COREQ-ACT projektin kansio: Automaation etäyhteyksien mallit.

mistetaan tuotannon jatkuvuus. Tätä varten tuotanto-osastolla tulee olla jatkuvuuden varmistamisen vaatimukset, joihin tulisi sisällyttää mm. poikkeustilanteiden käsittely (vikasietoisuus, ylläpito poikkeustilanteessa, hyökkäyskestävyys), korjaus/korvaus (laite, ohjelmisto, konfiguraatio) sekä seuranta (tiedonkeruu, jopa testaus) ja kehittäminen (harjoittelu, päivittäminen jne.).

Käyttäjät

Jotta kaikki etäkäyttäjät saadaan mukaan toteuttamaan tietoturvallista toimintatapaa, tarvitaan etäkäyttöön räätälöityjä käyttösopimuksia, koulutusta ja käytön seurantaa. Seuraavassa on esitetty muutamia näihin toimiin liittyviä esimerkkikäytäntöjä. ks. [TEO-TT] COREQ-ACT-projektikansio: Automaation etäyhteyksien mallit.

Käyttäjän tulee hyväksyä *etäyhteyssopimus* ennen etäyhteyden myöntämistä:

- Etäyhteyttä käytetään ainoastaan (tilattuihin) työtehtäviin
- Etäyhteyksissä käytettävä päätelaite pidetään puhtaina viruksista ja sitä käytetään ainoastaan työtehtäviin
- Etäyhteyksissä toimitaan salassapitosopimuksen mukaan.

Käyttäjien koulutus:

- Etäsovellusten toimintaperiaatteet
- Käytetty etäyhteystekniikka (laitteet, ohjelmistot)
- Käytössä oleva etäyhteyspolitiikka (harjoitellaan oikea käyttö).

Toteutuneesta etäyhteydestä jää jälki:

- Lokitus ja pääsynvalvonta tulisi ottaa käyttöön kohdekoneissa, mikäli mahdollista. Kuka on käynyt etäkoneessa (käyttäjätunnus), milloin (yhteysaika), ja mitä on tehty?
- Seurantakäytäntö ja -järjestelmä tulee suunnitella ja toteuttaa ja käyttäjien hyväksyä (sopimuksessa) ennen käyttöönottoa.

3.3 Tehtaan tietoturvaohjeet, koulutus ja muutosten hallinta

Tietoturvatilanteesta on vastuussa myös järjestelmän käyttäjä. Mikään tekninen suojausmenetelmä tai työkalu ei käytännössä poista käyttäjän toiminnan vaikutusta järjestelmän tietoturvatilanteeseen. On huomattava, että vaikka IT:tä hyödyntävän käyttäjän toiminta saattaa olla tietoturvan ylläpidon näkökulmasta liian passiivista, teollisuusympäristössä liiallinen tai hätiköity tietoturvaan liittyvä aktiviteetti saattaa aiheuttaa enemmän haitallisia seurauksia kuin maltillinen ohjeiden mukainen toiminta. Hyvä esimerkki väärästä toimintamallista on testaamattoman paikkauksen (*patch*) asentaminen, jolla pyritään poistamaan automaatiojärjestelmän tietoturvahaavoittuvuus. Testaamattoman paikkauksen asennus saattaa kuitenkin aiheuttaa automaatiojärjestelmän vikaantumisen.

Onkin erittäin tärkeää, että automaatiojärjestelmien eri käyttäjäryhmille laaditaan ohjeet tietoturvallisista toimintatavoista ja -malleista, joilla järjestelmien ja kriittisen tiedon riittävää suojaa ylläpidetään. Käyttäjien on myös hyvä olla mukana näiden ohjeistojen laadinnassa, jotta niistä tulisi mahdollisimman ymmärrettäviä ja yksiselitteisiä.

Turvallisen toiminnan varmistamiseksi kullekin käyttäjäryhmälle tuleekin laatia kohdennetut tietoturvaohjeet ja muutosten hallinnan säännöt sekä järjestää kohdennetut koulutustilaisuudet, joissa oikea toiminta käydään läpi. Myös väärästä toiminnasta voidaan näyttää esimerkkejä.

3.3.1 Tehtaan tietoturvaohjeet ja koulutus

Tehtaan tietoturvasääntöjä jalkautettaessa kannattaa hyödyntää seuraavia soveltamisohjeita:

Tuotantoalueella vaikuttavalle henkilöstölle ja kaikille kumppaneille laaditaan toimintaohjeet sekä järjestetään kohdistettu koulutus, motivointi ja yhteinen keskustelu käytännön toteutuksesta. Toteutumaa myös seurataan ja väärään toimintaan puututaan.

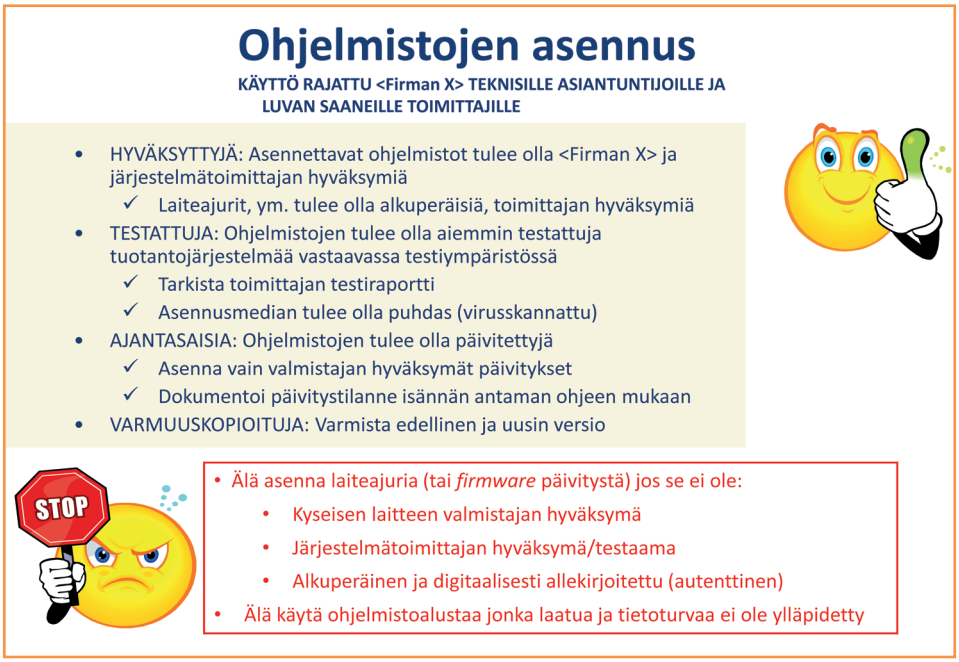
Koko tuotantoon vaikuttava toimijaketju tulee saada kokonaisuudessaan tietoturvatietoiseksi:

- Automaatio: hankinta, kehitys, käyttöönotto, käyttö, kunnossapito, huolto jne.
- ICT-järjestelmien ja verkkojen hallinta
- Kuljetukset, logistiikka, varastojärjestelyt, puhtaanapito
- Kiinteistöautomaatio, energia, kylmän ja kuuman tuotanto, turvajärjestelmät jne.

Koulutuksen ja koulutusmateriaalin laadinnan osalta tulee huomioida myös seuraavaa:

- Koulutuksessa kannattaa harjoitella oikea toiminta käytännössä (muistitikun skannaus tms.).
- Kannattaa kerätä ”väärän toiminnan kokoelma” omassa yrityksessä tapahtuneista tietoturvan vaaratilanteista tai epäonnistumisista.
- Edelliset synnyttävät keskustelua ja ymmärrystä siitä, miksi tulee toimia ohjeen mukaan.
- Räätälöidyn koulutusmateriaalin tekstin pitää olla totta ja mahdollista noudattaa käytännössä.
- IT:n ja automaation roolit ja yhteistoiminta on oltava tarkkaan sovittu.
- Myös ulkoa hankitun toiminnan on oltava yrityksen tietoturvakonseptin mukaista. Kolmannen osapuolen ohjeistus ja kompensoivat menettelyt.

Seuraavassa on esitetty yksi esimerkkisivu kohdistetusta koulutusmateriaalista.



Kuva 9. Ohjelmistojen asennukseen liittyvä ohje. Ks. [TEO-TT] COREQ-ACT-projektin kansio: Tehtaan tietoturvaohjeet — MALLIESIMERKKI OHJEESTA.

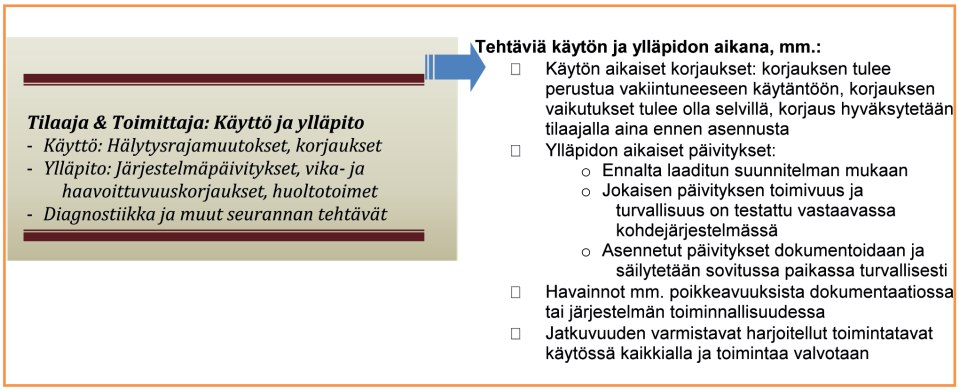
3.3.2 Muutosten hallinta

Muutosten kontrolloitu hallinta on yksi tärkeimmistä tavoista suojata automaatiojärjestelmä jatkuvuuteen ja tietoturvaan liittyviltä uhkilta. Yleensä automatisoitu tuotantojärjestelmä ja sen toiminta pyritään pitämään kaikin keinoin mahdollisimman vakaana. Tämä tarkoittaa, että esim. kaikki järjestelmämuutokset ovat ennalta testattuja, ne asennetaan tai implementoidaan kontrolloidusti tilaajan varaamassa kohteessa ja aikataulussa, ja lopuksi dokumentoidaan hyvin.

Toisaalta vikatilanteen sattuessa järjestelmä tulee pystyä palauttamaan tunnetusti toimivaan tilaan. Tämä tarkoittaa vakiintuneita varmuuskopiointi- ja palautuskäytäntöjä, joissa varmuuskopioinnin järjestelmät, kohteet, tallennus ja säilytys ovat hyvin toimivia ja testattuja. Lisäksi varmuuskopioiden luottamuksellisuudesta tulee huolehtia asiaankuuluvalla tavalla väärinkäytösten estämiseksi ja mm. järjestelmäversioiden ja -asetusten luottamuksellisuuden varmistamiseksi.

Usein muutostyö tehdään joko oman henkilökunnan tai palveluntarjoajan toimesta tai huoltosopimuksen osana. Kaikissa tapauksissa muutostyötarpeet tulee kuvata ja aikatauluttaa selkeästi ja yksikäsitteisesti ennen muutostöiden aloittamista. Muutostarpeita ilmenee lähes kaikissa automaatiojärjestelmän elinkaaren vaiheissa, usein pienempinä käytön ja ylläpidon aikana ja suurempina automaatiouusinnoissa ja uusien järjestelmien kehittämisen yhteydessä. Pitkän tähtäimen tavoitteet ja toiminnan elinkaari tulisi aina huomioida muutostöiden suunnittelussa myös tietoturvan osalta. Tietoturvasuunnitelma sopii hyvin tähän.

Seuraavassa kuvassa on esitetty esimerkki suojaustehtävistä tai -toimista tuotantojärjestelmän käytön ja ylläpidon aikana.



Kuva 10. Tehtäviä käytön ja ylläpidon aikana. Ks. [TEO-TT] COREQ-ACT-projektin kansio: Tietoturvaa kunnossapitoon – malli kohdistetun koulutusmateriaalin pohjaksi.

Kun kyseessä on laajempi tai pitempikestoinen muutostyöprojekti, huomio tulee kiinnittää kokonaisvaltaisemmin järjestelmien pitkän tähtäimen toimintakyvyn säilyttämiseen. Tällaisia tehtäviä on luonnehdittu seuraavassa kuvassa.

Kuva 11. Tehtäviä laajemman muutostyöprojektin aikana. Ks. [TEO-TT] COREQ-ACT-projektin kansio: Tietoturvaa kunnossapitoon – malli kohdistetun koulutusmateriaalin pohjaksi.

Muutostyökäytäntöjä tulee jatkuvasti parantaa, kuten muitakin sääntöjä ja ohjeita. Jatkuva muutoskäytäntöjen parantaminen edellyttää, että:

- Nykyisten muutoskäytäntöjen, -ohjeiden ja -resurssien toimivuus ja riittävyys tarkastetaan
- Muutoksissa syntyneet lopputulokset ja toteutuneet muutostentekotavat kirjataan ja talletetaan suojattuun tietoarkistoon
- Muutosten aiheuttamat riskit ja uhat kartoitetaan (ennalta käsin)
- Uusien teknologioiden käyttöönoton riskit ja vaikutukset muutoskäytäntöihin selvitetään ja kuvataan
- Toteutuneita uhkia ja vaaratilanteita analysoidaan muutostenhallinnan näkökulmasta: mitä tehtiin väärin, mitä pitäisi tehdä toisin jne.
- Muutostyökäytännöt päivitetään, muutokset toteutetaan kohteisiin suunnitelman ja ohjeiden mukaan ja muutostöitä valvotaan.

3.4 Hankintakäytännöt ja vaatimukset toimittajille

Teollinen tuotanto on pitkälle automatisoitua ja ainakin osin ulkoistettua, esim. käyttö- ja/tai ylläpitopalvelujen palvelusopimuksin. Tämä tarkoittaa sitä, että tuotantoon liittyvää ydinosaamista ja toimintatapojen hallintaa siirtyy helposti monille palvelukumppaneille, alihankintaverkoston toimijoille ja palveluntarjoajille. Tällainen kehitys aiheuttaa usein, ainakin siirtymävaiheessa, lisääntyviä riskejä tuotantojärjestelmien laadulle ja jatkuvuudelle, mutta myös tietoturvalle.

Kuitenkin myös hajautettu ja ulkoistettu tuotanto järjestelmineen tulisi kaikissa olosuhteissa hallita siten, että tuotannon turvallisuuteen ja jatkuvuuteen voidaan luottaa. Tämä edellyttää soveltuvien tietoturvavaatimusten määrittelemistä ja täytäntöönpanoa kaikkien tuotantoverkostossa vaikuttavien toimijoiden osalta.

Tuotantoyritykseen tarvitaankin mm. automaatiotoimittajien ja palveluntarjoajien toimien hallitsemiseksi tietoturvavaatimuskanta, jota voidaan helposti soveltaa, kun tuotantoon liittyviä järjestelmä-, kone-, ohjelmisto-, tai palveluhankintoja tehdään. Tuotannolle dedikoidun tietoturvavaatimuskannan määrittelemiseksi teollisuusyrityksen kannattaa hyödyntää esim. COREQ-VE- ja COREQ-ACT-hankkeissa yritysten kanssa yhdessä kehitettyä tietoturvavaatimuskantaa, ks. [TEO-TT] COREQ-ACT-projektin kansio: ”Toimittajahallinnan tietoturvavaatimuskanta (eng.)”.

Samoja vaatimuksia ei voi suoraan monistaa erilaisille tuotantoympäristöille, vaan tuotantonsa erityispiirteiden ja jatkuvuuden hallinnan vaatimusten pohjalta yritys tunnistaa omien tuotantolaitostensa minimivaatimukset tietoturvalle. Laitoskohtaiset vaatimukset ovat monesti tarpeen, sillä eri laitoksissa voi olla erilaiset automaatiojärjestelmät, ohjelmistot ja laitekanta → erilaiset palvelutoimittajat, käyttö- ja ylläpitopalvelut. Näin ollen samat tietoturvavaatimukset eivät sovi sellaisenaan kaikkiin laitoksiin, vaan niitä täytyy soveltaa tilanteen ja käyttötapausten mukaan.

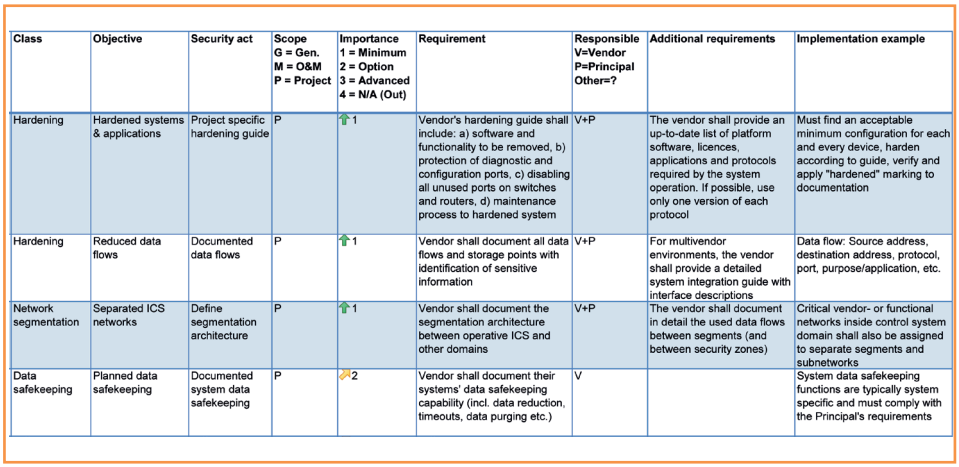
Joskus saatetaan tarvita jopa tuotantolinjakohtaisia vaatimuksia, varsinkin mikäli tuotantolinjojen kokoonpanot poikkeavat selkeästi toisistaan. Tällöin tietoturvavaatimukset tulisi käydä huolellisesti läpi automaatiotoimittajien kanssa ja liittää tietoturvavaatimukset osaksi järjestelmätoimitus-, käyttö- tai ylläpitosopimusta. Päätoimittaja velvoitetaan vastaamaan alihankkijoistaan kuin omistaan. Toteutumaa tulee seurata koko elinkaaren ajan.

Hankkeissa kehitetyn toimittajahallintaa parantavan tietoturvavaatimuskannan noin 250 yksityiskohtaista englanninkielistä vaatimusta kohdistuvat automaatiojärjestelmähankinnan elinkaaren tärkeimpiin vaiheisiin: hankevalmistelu ja järjestelmäkehitys, testaus ja käyttöönotto, sekä ylläpito ja käytön tuki. Lisäksi kuvataan organisaation vaatimukset. Kaikki vaatimukset on oletusarvoisesti priorisoitu keskimääräisen tärkeysarvion (*Importance*) mukaan seuraaviin luokkiin (eng):

- *1 = Minimum (alternative solution must be presented if requirement not fulfilled)*
- *2 = Option (may be crucial requirement depending on the case)*
- *3 = Advanced (may be crucial requirement when higher security level is required)*
- *4 = N/A (for later consideration).*

Kehitetyn vaatimuskannan laaja yrityslähtöinen katselmointi ja vaatimusten tärkeysarviointi tehtiin hyvässä yhteistyössä teollisuuden kanssa.

Seuraavassa kuvassa on esitetty ote kehitetyn vaatimuskannan sisällöstä.



Class	Objective	Security act	Scope G = Gen. M = O&M P = Project	Importance 1 = Minimum 2 = Option 3 = Advanced 4 = N/A (Out)	Requirement	Responsible V=Vendor P=Principal Other=?	Additional requirements	Implementation example
Hardening	Hardened systems & applications	Project specific hardening guide	P	1	Vendor's hardening guide shall include: a) software and functionality to be removed, b) protection of diagnostic and configuration ports, c) disabling all unused ports on switches and routers, d) maintenance process to hardened system	V+P	The vendor shall provide an up-to-date list of platform software, licences, applications and protocols required by the system operation. If possible, use only one version of each protocol	Must find an acceptable minimum configuration for each and every device, harden according to guide, verify and apply "hardened" marking to documentation
Hardening	Reduced data flows	Documented data flows	P	1	Vendor shall document all data flows and storage points with identification of sensitive information	V+P	For multivendor environments, the vendor shall provide a detailed system integration guide with interface descriptions	Data flow: Source address, destination address, protocol, port, purpose/application, etc.
Network segmentation	Separated ICS networks	Define segmentation architecture	P	1	Vendor shall document the segmentation architecture between operative ICS and other domains	V+P	The vendor shall document in detail the used data flows between segments (and between security zones)	Critical vendor- or functional networks inside control system domain shall also be assigned to separate segments and subnetworks
Data safekeeping	Planned data safekeeping	Documented system data safekeeping	P	2	Vendor shall document their systems' data safekeeping capability (incl. data reduction, timeouts, data purging etc.)	V		System data safekeeping functions are typically system specific and must comply with the Principal's requirements

Kuva 12. Ote toimittajahallinnan tietoturvavaatimuskannasta. [TEO-TT] COREQ-ACT-projektin kansio: Toimittajahallinnan tietoturvavaatimuskanta.

Kehitetyn vaatimuskannan pohjaksi otettiin alun perin prosessiteollisuuden WIB järjestön (*WIB — International Instrument Users' Association*) työstämät vaatimukset vuodelta 2010 [WIB].

Kehitettyyn vaatimuskantaan päätettiin kirjoittaa sisäinen rakenne, jolla kunkin vaatimuksen tavoitteita ja käytäntöön panoa voitaisiin selventää:

- *Number*: vaatimuksen numero
- *Class*: vaatimuksen tyyppi/luokka
- *Objective*: vaatimuksen tavoite
- *Security act*: päätoimenpide
- *Scope*: pääsoveltamiskohde
- *Importance*: tärkeysluokka
- *Requirement*: vaatimusteksti
- *Responsible*: vastuutahot
- *Additional requirements*: mahdolliset lisävaatimukset
- *Implementation example*: toteutusesimerkki.

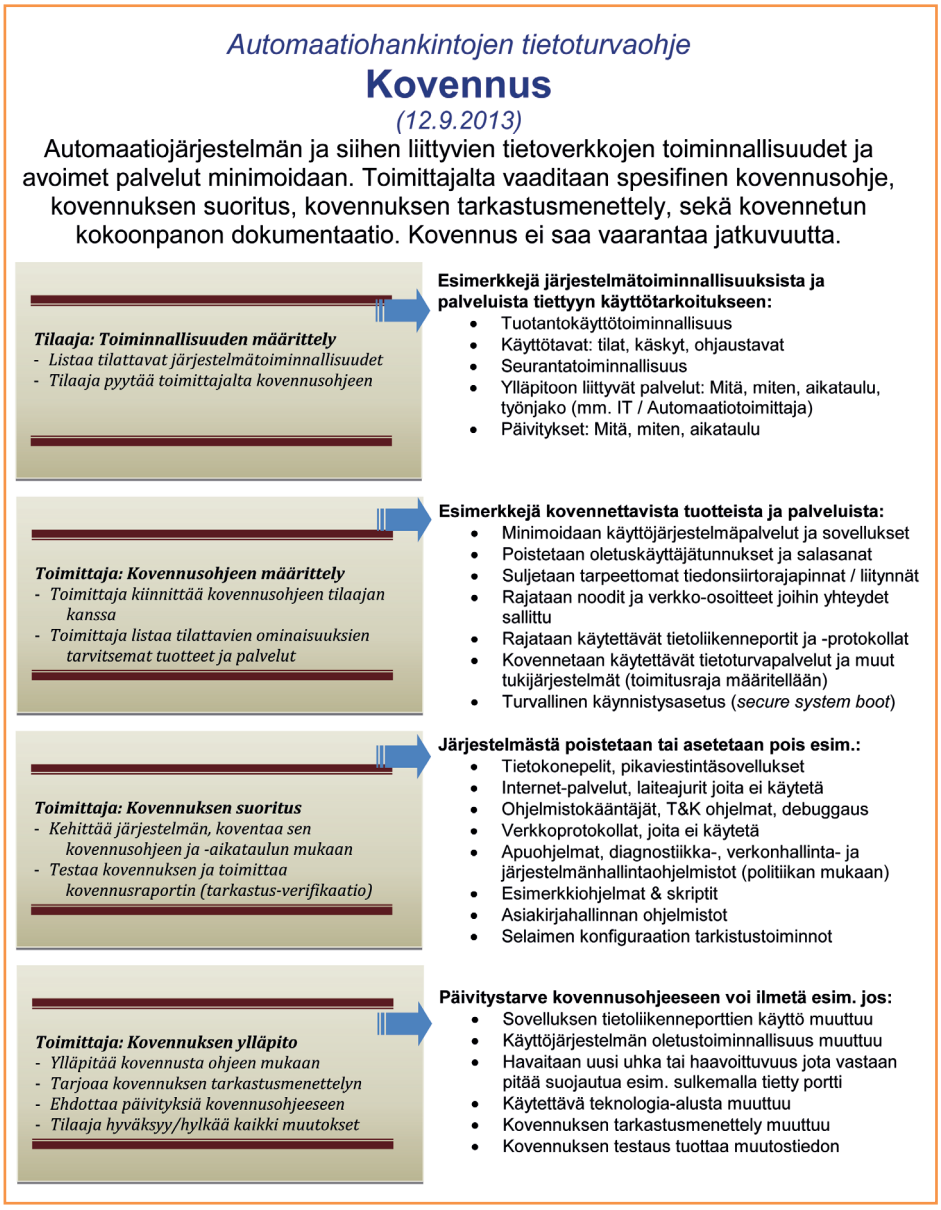
Soveltamisesimerkki: Mikäli tietyn vaatimuksen tavoite (*Objective*) on toimituksen alaisessa järjestelmässä relevantti, mutta siihen liittyvää vaatimustekstiä (*Requirement*) ei pystytä sellaisenaan implementoimaan, tällöin on sovittava sopiva kompensoiva menettely, joka turvaa vaatimuksen tavoitteet. Kompensaation tulee tietysti olla ristiriidaton muihin asetettuihin vaatimuksiin nähden. On huomattava myös, että tavoitteen toteutuminen voi vaatia yhteistyötä esim. verkon tai järjestelmän ylläpidossa omassa ja ulkoistetussa organisaatiossa, mistä tulee sopia kirjallisesti.

Automaatiohankintojen lyhyet tietoturvaohjeet

Hankkeissa kehitettiin A4-sivun mittaiset automaatiohankintojen tietoturvaohjeet seuraaviin teemoihin liittyen:

- Tietoturvalliset etäyhteydet
- Käyttäjäoikeudet
- Kovennus
- Langattomat järjestelmät
- Muutostenhallinta.

Seuraavassa kuvassa on esimerkki kovennukseen liittyvästä hankintaohjeesta.



Kuva 13. Kovennusohje automaatiohankinnoissa sovellettavaksi. [TEO-TT] COREQ-ACT-projektin kansio: Automaatiohankintojen tietoturvaohje — Kovennus.

Kovennus tarkoittaa järjestelmän minimointia ainoastaan tilaajan toimeksiannossa määriteltyihin välttämättömiin toiminnallisuuksiin. Automaatiojärjestelmän osalta tämä tarkoittaa mm. että käyttöjärjestelmien ylimääräiset palvelut ja sovellukset suljetaan ja verkkopalveluista sallitaan ainoastaan automaatiojärjestelmän käyttämät palvelut. Tilaajan vastuulla on mm. määritellä toimituksen rajaus, tilaukseen liittyvä toiminnallisuus, sekä vaatia toimittajaa laatimaan kovennusohjeen. Automaatiotoimittaja määrittelee kovennusohjeen, koventaa ja testaa järjestelmät sekä ylläpitää kovennusta ja kovennusohjetta.

3.5 Soveltuvien tietoturvamenetelmien evaluoinnit

Hankkeissa tutkittiin myös muutamia tietoturvamenetelmiä, joiden oletettiin ennakkotietojen mukaan soveltuvan hyvin teollisuusautomaatiojärjestelmien käytön aikaiseen suojaamiseen tai kehitystyön aikaisiin tietoturvatoimiin. Tällaisia menetelmiä olivat:

- Sovellusten sallimislistaus (*whitelisting*-ohjelmistotuotteiden evaluointi)
- Tietoturvatestausmenetelmät (näiden jalkautuksen pohdintaa ja työnjakoa).

Seuraavissa kappaleissa on lyhyesti esitelty COREQ-ACT- ja TEO-TT-hankkeiden tärkeimpiä automaation tietoturvamenetelmiin liittyviä tuloksia.

3.5.1 Sovellusten sallimislistaus

Sovellusten sallimislistaus sopii automaatiojärjestelmien suojaamiseen periaatteessa erinomaisesti, sillä sen avulla kohdekoneen toiminta voidaan rajoittaa ainoastaan erityisesti sallittuihin sovelluksiin. Tärkeä etu on myös se, että järjestelmään lisättävä sallimislistausohjelma ei vaadi jatkuvaa konfigurointia ja että se kuluttaa vain vähän kohdekoneen laskentaresursseja, toisin kuin monet virustorjuntatuotteet.

VTT:n Pia Olli tutki hankkeissamme ja samalla diplomityössään mm. seuraavaa:

- Suojaavatko sovellusten sallimislistaustuotteet haavoittuvuuksilta sallituiksi listatuissa ohjelmissa?
- Onko järjestelmä tällöin suojattu, vaikka siinä olevia ohjelmia ei päivitä?
- Suojaako sallimislistausohjelma järjestelmää puskuriylivuodoilta ja muilta muistihaavoittuvuuksilta?

Seuraavassa kuvassa on esitetty näyte sovellusten sallimislistaustuotteiden evaluoinnissa saavutetuista tuloksista.

Hyökkäys	McAfee	Lumension	Savant	CSP
Adobe util.printf, *puskuriylivuoto*	#	X	X	X
Microsoft Server Service, *pinon ylivuoto*	X	X	X	#
Adobe CoolType SING Table, *pinon ylivuoto*	X	X	X	+
Adobe Collab.getIcon, *pinon ylivuoto*	#	X	X	X
UltraVNC Client, *pinon ylivuoto*	#	X	X	#
Adobe JBIG2Decode, *kasan ylivuoto*	+	X	X	X
Internet Explorer Daxctle.OCX KeyFrame Method, *kasan ylivuoto*	#	X	X	X

X – hyökkäys toiminut,
– hyökkäyksellä vaikutus kohteessa, mutta ei luo yhteyttä,
+ – hyökkäys estetty

Kuva 14. Sallimislistausohjelmien testituloksia. [TEO-TT] COREQ-ACT-projektin kansio: Sovellusten sallimislistaustuotteiden testaus.

Tuloksista voidaan päätellä ainakin se, että sallimislistausta ei kannata käyttää teollisuusautomaatiojärjestelmien ainoana puolustusmekanismina. On nimittäin mahdollista, että havaitunlaiset heikkoudet erilaisille muistin ylivuotoja hyödyntäville hyökkäyksille toteutuisivat myös teollisuusympäristöissä.

Sallimislistaus antaa erityistä lisäturvaa vanhoja käyttöjärjestelmiä hyödyntäville sovelluksille, joihin ei saada alustapäivityksiä tai virustorjuntatuotteiden suojaa muista syistä. Koska sallimislistaustuote estää muutosten tekemisen ilman lupaa, voidaan tuotannon järjestelmien muutoshallintaa täten lisäksi jämäköittää.

Teoreettisella tasolla sallimislistaus olisi ideaalinen suojausmekanismi automaatioympäristöön, jossa järjestelmä pysyy muuttumattomana kauan. Käytännössä sallimislistauksen sopivuus tulee kuitenkin edelleen miettiä tapauskohtaisesti vertaillen uuden suojausjärjestelmän riskejä ja hyötyjä. Varsinaisia tuote-evaluointeja kannattaa myös jatkaa, sillä sallimislistaustuotteet kehittyvät tällä hetkellä nopeasti kypsemmiksi ja niihin lisätään uusia hyödyllisiä ominaisuuksia.

Laajemmin tätä tutkimusta ja sen aihepiiriä on kuvattu Pia Ollin diplomityössä [OLLI].

3.5.2 Tietoturvatestaus

Tietoturvatestauksen menetelmät ja työkalut ovat kehittyneet helppokäyttöisemmiksi viime vuosien aikana, ja niiden käyttö alkaakin olla pakollinen vaihe ohjelmistokehitystä ICT-järjestelmien kehityshankkeissa. Koska automatisoitu tuotantokin sisältää useimmiten yleiskäyttöisiä ja haavoittuvia ICT-komponentteja, tulee tietoturvatestaus liittää osaksi automaatiojärjestelmien ja sovellusten kehittämistä. Automaatioverkkoakaan ei voida enää pitää täysin luotettuna turvasaarekkeena, joka pysyisi täysin erillään muista verkoista ja järjestelmistä sekä niiden mahdollisista uhkista ja haittavaikutuksista.

Tietoturvatestauksessa pyritään usein tunnistamaan tietoturvaongelmia jo järjestelmien kehitys- ja käyttöönottovaiheissa. Tähän voitaneen lukea kuuluvaksi lähdekoodin analyysi, jossa ohjelmakoodista etsitään mm. ennalta haavoittuviksi tiedettyjä funktioita ja *input*-validoinnin puutteita. Toki esimerkiksi seisokkien yhteydessä voidaan testata jo käytössä olleiden järjestelmien tietoturvan tasoa esimerkiksi haavoittuvuusskannereilla tai yrittämällä hyväntahtoista automaatiojärjestelmiin tunkeutumista penetraatiotestauksella. Järjestelmäkehittäjä tai -toimittaja onkin yleensä ensisijaisesti vastuussa tietoturvatestauksesta sekä löydettyjen haavoittuvuuksien korjaamisesta.

Automaatiojärjestelmien tietoturvan kehittämisessä voidaan sopivissa vaiheissa käyttää seuraavia tietoturvatestauksen menetelmiä:

- Lähdekoodianalyysi (lähdekoodin haavoittuvuuksien tunnistamiseen)
- *Fuzz*-testaus (järjestelmän kommunikaatiorajapinnan toteutusheikkouksien etsimiseen)
- Porttiskannaus ja verkkotiedustelu (järjestelmän ja verkon toiminteiden tunnistamiseen)
- Haavoittuvuusskannaus (järjestelmän haavoittuvuuksien tunnistamiseen)
- Penetraatiotestaus (järjestelmän hyökkäyskestokyvyn selvittämiseen).

Seuraavassa kuvassa on esitetty TEO-TT-hankkeen työpajassa 5 [TEO-TT] kirjatut luonnehdinnat automaation järjestelmäkehitykseen soveltuvista tietoturvatestauksen menetelmistä. Kutakin testimenetelmää tulee käyttää turvallisesti järjestelmäkehityksen tai käyttöönoton eri vaiheissa siten, että tuotannossa olevan järjestelmän toiminta ei missään olosuhteissa vaarannu tietoturvatestauksen suorien tai epäsuorien vaikutusten vuoksi.

Testimenetelmä	Käyttötarve	Käyttökohde	Käyttöaika	Tulosten vaikutukset	Tulosten hyödyllisyys	Käyttöjärjestys
Lähdekoodi-analyysi	Riskialttiiden koodin osien tunnistaminen	Kaikki tilattu ohjelmakoodi	SW kehitys & vikakorjaukset (jatkuva)	Riskialttiin koodin korjaaminen	Hyvä, jos koodimuutokset toteutetaan	T&K:ssa, vikakorjauksissa
Fuzz-testaus	Riskialttiiden koodin osien tunnistaminen	Tietoliikenne-rajapinnat: OS, protokollat, sov.	SW kehityksen testausvaiheet (hetkellinen)	Riskialttiin koodin korjaaminen	Hyvä, jos koodimuutokset toteutetaan	T&K/FAT/SAT vaiheissa
Porttiskannaus & verkko-tiedustelu	Ylimääräisten verkko-toiminteiden tunnistaminen	Tietoliikenne-verkon konfiguraatio	Hyväksymis-/käyttöönotto-testaus (hetkellinen)	Verkko-palvelujen rajoittaminen: laitteet, portit	Hyvä, jos konfiguraatio-muutokset hallitaan	FAT/SAT vaiheissa (myös käytön aikana jos passiivinen)
Haavoittuvuus-skannaus	Tunnettujen haavoitt. tunnistaminen	Ohjelmistojen versiot	Hyväksymis-/käyttöönotto-testaus (hetk./jatkuva)	Turvattomien ohjelmistojen päivittäminen	Hyvä, jos SW päivitykset hallitaan	FAT/SAT vaiheissa (myös käytön aikana jos passiivinen)
Penetraatio-testaus	Tietoturva-aukkojen tunnistaminen	Elektroninen pääsynvalvonta (toteutus)	Hyväksymis-/käyttöönotto-testaus (hetkellinen)	Pääsynvalvonta ja suojaus-kokonaisuus paranee	Hyvä, jos testaus-resursseja on riittävästi	T&K/FAT/SAT vaiheissa

Kuva 15. Automaatioon soveltuvia tietoturvatestauksen menetelmiä. [TEO-TT] TEO-TT-Työpaja 5.

Fuzz-testaus

Fuzz-testaus on automaatiojärjestelmien tietoturvan kehittämiseen hyvin soveltuva *black-box*-testausmenetelmä, jossa testikohteen sisäistä toimintaa ei tarvitse juurikaan tuntea edeltä käsin. Etuina ovat varsinkin helppokäyttöisyys ja nopeus. *Fuzz*-testaus paljastaa hyvin mm. testikohteen kyvyn käsitellä erilaisia poikkeuksia:

- Löydetään nopeasti vakavia testikohteen kaatavia syötteitä
- Tunnistetaan järjestelmän heikot kohdat, millä voidaan löytää haavoittuvuuksia, joiden kautta järjestelmään pystytään tunkeutumaan
- Menetelmässä syötetään virheelliseksi muokattua input-dataa testikohteen rajapintaan:
    - Monenlaisia syötteitä voidaan fuzzata eli sekoittaa, mm. verkkoprotokollan syntaksin fuzzaus. Samaan aikaan monitoroidaan testikohteen selviytymistä virheellisistä syötteistä.

Haasteena *fuzz*-testauksessa on monimutkaisempien virheiden löytäminen. Kuinka pitkälle standardin mukaisia viestisekvenssejä kannattaa testauksessa edetä? Tällaiseen testaukseen tarvitaan pitkälle kehittyneet protokollaspesifiset testicaset.

Porttiskannaus ja verkkotiedustelu

Porttiskannauksessa ja verkkotiedustelussa pyritään selvittämään tuotantoon käytettävien tietoverkkojen todellinen kokoonpano ja toiminnot. Tässä tarkoituksessa analysoidaan tietoverkoista:

- Verkossa olevat laitteet (verkko-osoite, käyttöjärjestelmä, jne.)
- Laitteiden avoimet tietoliikennepalvelut, sovellukset, ym.

Aktiivisessa tiedustelussa verkkoon tai tiettyyn kohteeseen lähetetään dataa ja analysoidaan saadut vastaukset. Passiivisessa verkkotiedustelussa vain kuunnellaan verkkoliikennettä ja analysoidaan vastaanotettua dataa.

Porttiskannauksessa lähetetään esim. kyselydataa kohteen tunnettuihin portteihin ja päätellään vastauksen tai hiljaisuuden perusteella, onko portti auki vai kiinni.

Testimenetelmä	Testaustehtävä (esimerkkejä)	Vastuullinen osapuoli	Testaustulokset (mitä syntyy?)	Tulosten hyödyntäjä	Korjaavat toimenpiteet	Käytäntöönpanon seuranta
Lähdekoodianalyysi	Pakotetaan lähdekoodianalyysi ohjelmaa käännettäessä	Ohjelmistokehittäjä	Analysaattorin lokiraportti	Ohjelmistokehittäjä	Korjataan haavoittuvuudet	Ohjelmistokehittäjä / Tilaaja
***Fuzz*-testaus**	Tilataan testi - Sovitut rajapinnat ja protokollat	Järjestelmän kehittäjä	Testiraportit ja niiden analysointi	Ohjelmistokehittäjä	Korjataan haavoittuvuudet	Järjestelmän kehittäjä / Tilaaja
Porttiskannaus & verkkotiedustelu	Etsiä ylimääräiset verkkopalvelut ja konf. virheet	Järjestelmän toimittaja / Loppukäyttäjä	Verkon osoitteet ja avoimet portit	Ylläpito	Poistaa ylimääräiset palvelut	Palveluoperaattori / Tilaaja / Kolmas osapuoli
Haavoittuvuusskannaus	Etsiä toimituksen haavoittuvat ohjelmistot	Järjestelmän toimittaja	Lista: Toimitettavan ohjelmiston haavoittuvuudet	Järjestelmän toimittaja	Patchaus, päivitys, kovennukset	Järjestelmän toimittaja / Tilaaja / Kolmas osapuoli
Penetraatiotestaus	Toimitettavaan järjestelmään tunkeutuminen	Järjestelmän toimittaja / sovelluskehittäjä	Kuvaus onnistuneista hyökkäyksistä	Järjestelmän toimittaja / sov. kehittäjä / Tilaaja	Löydöksen mukaan	Järjestelmän toimittaja / Tilaaja / Kolmas osapuoli

Kuva 16. Esimerkkejä tietoturvatestausmenetelmien jalkautuksesta. [TEO-TT] TEO-TT-Työpaja 5.

Jos portti on auki, voi sen kautta selvittää tarkemmin esim. kohteen käyttöjärjestelmä- ja sovellustietoja.

Tiedustelun tuloksena pyritään siis löytämään tuotantoon liittyvistä tietoverkoista mahdollisimman paljon haavoittuvaisia verkkolaitteita, käyttöjärjestelmäversioita, sovelluksia tai palveluja. Verkkotiedustelun tuloksia voidaan käyttää järjestelmän suojaamiseen (ylläpitäjä):

- Selvittämään, onko verkkoon tunkeuduttu (esiintyykö luvatonta verkkotiedustelua?)
- Havaitsemaan poikkeamat verkossa sallituista laitteista ja palveluista
- Penetraatiotestauksen valmisteluun
- Esitiedon keräämiseen IDS-tuotteen konfiguroimiseksi jne.

Vaara: Porttiskannaus voi haitata automaatioverkon normaalitoimintaa (esim. *ping sweep*), joten tuotantokäytön aikana verkon tietoturvatestaus on aina riski!

Tietoturvatestauksen jalkautuksesta

Soveltuvien tietoturvatestauksen menetelmien käyttöönottamiseksi valitut menetelmät tulee tietysti jalkauttaa sovelluskehitysprojekteihin ja esim. huoltokatkojen työkäytäntöihin ja ohjeisiin. Jalkautuksen onnistumiseen vaikuttanee yleensä kokonainen verkosto toimijoita, joille koordinoitavia osatehtäviä on koottu yllä olevaan kuvaan, ks. TEO-TT-hankkeen työpaja 5 [TEO-TT].

Jotta automaatiojärjestelmien tietoturvataso saadaan riittävälle tasolle ja edelleen myös ylläpidettyä, tulee järjestelmäkehittäjät ja -toimittajat asettaa vastuuseen sovellustensa tietoturvatestauksesta ja järjestelmänsä haavoittuvuuskorjausten kehittämisestä ja testaamisesta tietyllä aikavälillä.

Kaikki tuotannon testaus ja vikakorjaus tulee kuitenkin aina tehdä tilaajan varaamassa aikataulussa ja hyväksynnöin. Näin varmistetaan, että kaikki ohjelmistomuutokset tehdään kontrolloidusti ja että edellinen konfiguraatio voidaan tarvittaessa palauttaa korjauksen jälkeen.

3.6 Tuotannon riskien hallinta ja jatkuvuuden varmistaminen

Tilaajan oma työpanos, suunnittelu ja varautuminen ovat avainasemassa huoltovarmuuskriittisen tuotannon riskejä tunnistettaessa ja hallittaessa, ks. [TEO-TT] Työpaja 4.

3.6.1 Tuotannon riskien hallinta

Yllättävien tapahtumien tai ilmiöiden tunnistaminen

Automaatiojärjestelmiä tai -palveluja tilaavassa yhtiössä tulee olla käytössä systemaattinen toimintamalli yllättävien, tuotantoon mahdollisesti haitallisesti vaikuttavien tapahtumien ja ilmiöiden ennakkotunnistamiseen.

Toimintamalliin tulisi kuulua, että varsinkin alansa asiantuntijat listaavat potentiaalisia tapahtumia ja ilmiöitä esim. tarkoitusta varten varattuun Intranet-sovellukseen.

- Ideoidaan ja listataan tapahtumia jotka potentiaalisesti aiheuttaisivat suurta haittaa, esim. useamman päivän tuotantokatkon.
    - Mitä muita seurauksia yllättävällä tapahtumalla olisi?
- Keihin riskejä voisi kohdistua?
- Missä paikoissa tai tilanteissa yllättäviä tapahtumia voisi sattua?
- Milloin riskit voisivat realisoitua?

Tilaajan tulisikin antaa hyvissä ajoin ja luottamuksellisesti konkreettista tietoa toiminnan riskeistä mm. järjestelmätoimittajalle. Lisäksi euromääräistäminen edesauttaa huomattavasti riskeihin puuttumista tarvittavilla tahoilla, ja dominoketjujen arviointi ja ennakoiminen lisää varautumisen motivaatiota.

Lyhyen ja pitkän tähtäimen tapahtumat ja ilmiöt kannattaa tunnistaa erikseen, kuten päivittäisen toiminnan riskit ja tulevaisuuden toiminnan tiekarttojen riskit.

Riskialttiiden järjestelmien tunnistaminen

Riskialttiiden järjestelmien tunnistamisessa voidaan käyttää taustatietojen ja oman henkilöstön asiantuntemuksen tukena ulkopuolisia palveluntarjoajia, jotka voivat tarvittaessa tehdä myös hallittua penetraatiotestausta (ei tuotannon aikana). Soveltuvat ja luotetut palveluntarjoajat tulee tietenkin evaluoida etukäteen henkilöiden taustat varmistaen. Toteutettavat testitapahtumat määritellään etukäteen, ja toteutuneet dokumentoidaan jatkoa varten luottamuksellisuutta suojaten. Testikattavuutta tulisi pyrkiä lisäämään systemaattisella työllä:

- Testit kannattaa kohdistaa erilaisiin kohteisiin ja tilanteisiin
- Testiverkkoon tai -järjestelmään investointi
- Toimittajien, ratkaisujen tai toimitusketjun kokonaisuuksien arviointi
- Järjestelmäkuvausten ja FAT-testien hyväksikäyttö testauksessa.

Tilaajan omat resurssit tulee saada tukemaan tietoturvatestausta.

Riskitietoisuuden lisääminen

Riskien tunnistaminen yksilötasolla on erittäin tärkeää riskien tunnistamisen tehostamiseksi, joten yrityksen kannattaa tukea sitä. Samalla voidaan kertoa muullekin henkilökunnalle todellisten tai kuvitteellisten esimerkkien kautta siitä, millaisia riskejä on olemassa. Kaikkien työntekijöiden on tiedostettava tuotannon riskit ja varauduttava käytännössä:

- Työstöpalavereissa tuodaan ilmi riskejä eri näkökulmista alueitten vastaavien asiantuntijoiden avulla.

- Tavoitteena on varautumisen edellytysten selvitys ja suunnittelu.

Riskitietoisuuden lisääminen sekä varautumisen suunnittelu, koulutus ja harjoittelu tulisi sisällyttää kaikkeen toimintaan. Automaatiotoimittajilta on vaadittava enemmän ja tarjottava koulutusta myös muille toimittajille. Hyvään yrityskulttuuriin tulisi kuulua mm. jatkuva tiedottaminen, tietoturvatilanteen seuraaminen (esim. CERT FI:n palvelut) sekä laitetoimittajien omien aktiviteettien seuranta. Samoin ICT-osaston tulisi aktiivisemmin tiedottaa esim. yleisistä uhkista automaatiopuolelle. Myös suunnitellut ulkoiset tai sisäiset auditoinnit paljastavat riskejä, jolloin löydökset saadaan varmemmin myös jatkokäsittelyyn ja varautumisen piiriin. Seuraavassa yhteenveto huoltovarmuuskriittisen toiminnan riskien hallinnan pääkohdista:

Riskien hallinnan yhteenveto
1. Riskin tai häiriön tunnistaminen: • Ilmiöt, tapahtumat, muutokset • Kriittiset järjestelmät, alueet ja ominaisuudet.
2. Ennaltaehkäisevät toimenpiteet ja rutiinit: • Vaatimukset ja niihin sitouttaminen, käytännöt, rutiinit • Roolit, työnjako, toteuman seuranta • Muu ennaltaehkäisevä toiminta.
3. Testaa ja harjoittele seuraavia: • Ennakkovarautumista (varajärjestelmät, -osat, -toiminnot) • Hätätilannevalmiuksien ja yleisen osaamisen kehittäminen • Hätätilanneharjoitukset, lisäresurssien pyytäminen (eskalointi).

Taulukko 2. Huoltovarmuuskriittisen toiminnan riskien hallinnan pääkohdat. Ks. [TEO-TT] TEO-TT-Työpaja 4.

Aineisto

Huoltovarmuuskeskuksen tuottamaa aineistoa riskien ja jatkuvuuden hallintaan löytyy laajemmin HUOVIsta [HUOVI] sekä tietoturvariskien hallinnan osalta ainakin hankealueelta [TEO-TT].

3.6.2 Tuotannon jatkuvuuden varmistaminen

Toiminnan jatkuvuudenhallinnan kypsyysanalyysi

Jatkuvuuden hallinnan kehittäminen lähtee liikkeelle systemaattisesta kypsyysanalyysistä. Huoltovarmuuskeskuksen kehittämällä jatkuvuudenhallinnan kypsyysanalyysityökalulla selvitetään mm. sitä, miten yrityksen ja sen tuotannon jatkuvuudenhallintaa johdetaan, arvioidaan tuotantoon vaikuttavien prosessien toimintavarmuutta sekä selvitetään koko toimijaverkoston jatkuvuudenhallinnan tila, katso [HUOVI].

Huoltovarmuuskriittisten yritysten kannattaakin ehdottomasti hyödyntää HUOVIn kypsyysanalyysityökalua sekä niihin liittyviä koulutuksia. Kypsyysanalyysityökalun käytössä tulee varmistaa, että vastaukset kysymyksiin työstetään ensin yrityksen sisällä sopivassa ryhmässä, jossa johdon mukanaolo on tärkeää.

Yleensä yrityksen jokaisen toiminnon tulee huolehtia ja vastata omalta osaltaan toimintansa jatkuvuudesta, sekä analysoida kunkin partnerinsa häiriön vaikutus omaan tuotantoonsa. Myös SOPIVA-sopimusmallin (ks. [HUOVI]) vaatimukset tulee ulottaa koko toimittajaverkostoon:

- Tee sopimus häiriön hallinnasta toimittajan kanssa, joka vastaa alihankkijoistaan kuin omistaan.
- Tilaajan kannattaa varmistaa myös vaihtoehtoinen toimittaja.

OSAT 4, 5 JA 6

JOHTOPÄÄTÖKSET, JATKOTYÖ JA REFERENSSIT

4 JOHTOPÄÄTÖKSET

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 työlästä. Niinpä eri ratkaisuja tulisikin etukäteen arvioida ja testata eri menetelmien soveltuvuutta käytännössä ennen lopullista valintaa ja käyttöönottoa. Tähän arviointiin tai testaamiseen tarvitaan usein tukea tuotantoyrityksen ulkopuolelta.

Yhteistyön merkitys korostuu tänä päivänä tietoturvallisuuden ylläpidossa kaikilla sektoreilla, ei ainoastaan teollisuudessa. Toimivaa yhteistyötä ja pelisääntöjä tarvitaan mm. hankintojen tietoturvan hallintaan, mutta myös koko tuotannon tietoturvatason ylläpitoon ja seurantaan. Erityisesti tietoverkkojen seurannan tarve on tänä päivänä korostunut teollisuusvakoilun ja tiedustelupalvelujen pitkälle kehittyneen urkinnan takia.

Tulevaisuus edellyttää koko ajan parempaa kustannustehokkuutta ja joustavuutta, mikä lisää yleiskäyttöisten ICT-ratkaisujen käyttöä myös teollisuustuotannossa ja logistiikassa. Valitettavasti tämä on jo johtanut siihen, että Internetistä tutut uhat kohdistuvat myös teollisuuden järjestelmiin. Teollisuus ei ole kuitenkaan välttämättä varautunut tällaisiin uhkiin esim. osaamisen ja investointien osalta. Nyt tarvitaankin lisää teollisuuden käyttöön soveltuvia tietoturvapalveluja ja niiden käyttöönottoa.

Teollisuudelle tarjottujen tietoturvapalvelujen 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 kriittisiä. Silti nämäkin tietovirrat täytyy saada parempaan hallintaan.

Laajamittaisempi suunnittelu tietoturvan jalkauttamiseksi teollisuuteen on tällä hetkellä (marraskuussa 2013) jo käynnissä. Näistä jatkotöistä onkin esitelty muutamia esitietoja seuraavassa luvussa.

5 JATKOTYÖ

Voimakkaasti kasvavien riskien hallitsemiseksi teollisuusyritysten tulee laajalla rintamalla arvioida ja jalkauttaa kyberturvallisuuden käytäntöjä tuotantoonsa. Laajamittainen kyberturvallisuuden jalkauttaminen kotimaiseen teollisuuteen onkin tällä hetkellä Huoltovarmuuskeskuksen ja VTT:n suunnitelmissa.

Kyseessä on aiempia hankkeita laajempi KYBER-TEO-hanke ”Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen”, jonka pääomistajana Huoltovarmuuskeskus tulisi jälleen toimimaan.

Tavoitteena on 10—15 hanketta rahoittavaa teollisuusyritystä sekä useita tuotantoa tukevia palveluyrityksiä. Näiden yritysten myötävaikutuksella kotimainen teollisuus tulee saamaan edelleen pidemmälle jalostettuja ja koestettuja malliratkaisuja ja käytäntöjä kyberturvallisuuden jalkauttamiseksi tuotantotoimintaan. KYBER-TEO-hankekokonaisuuden päätavoitteena on kehittää ja koestaa osallistuvissa yrityksissä teollisuudelle räätälöityjä palveluja kyberturvallisuuden ja jatkuvuuden varmistamiseksi ja koko muun suomalaisen huoltovarmuuskriittisen teollisuuden hyödynnettäväksi.

Alustavat KYBER-TEO-hankekokonaisuuden työpaketit (TP) ovat:

TP 1: Kybersuojauksen käytännöt ja kartoitukset

TP 2: Kyberturvallisuuden jalkauttaminen kotimaiseen tuotantoon

TP 3: Tuotantoautomaatioverkon monitorointipalvelut.

Hankekokonaisuuden julkiset väli- ja lopputulokset esitellään huoltovarmuuskriittisille yrityksille 3—4 kertaa vuodessa, päämotiivina tulosten ja kokemusten laajamittainen jakaminen kotimaisten yritysten kesken.

Hankkeessa tullaan edelleen jatkamaan erittäin hyvin toiminutta, laajaa kotimaista yhteistyötä, jossa ovat mukana mm.:

- Rahoittavat yritykset
  - Erityiset yrityskohtaiset caset
  - Projektityö (teknologian ja palvelujen kehittäminen)
  - Tulosten käyttökelpoisuuden varmistaminen, osallistuminen tulosten katselmointeihin
- Muut teollisuusyritykset (jotka hyödyntävät mm. TEO-TT-verkostoa)
  - Laajat katselmoinnit
  - Tulosten esittelytilaisuudet
- Viranomais- ja tutkimusyhteistyö
  - Tulosten sisältö, laatu, kehittäminen, levittäminen ja koulutusyhteistyö.

Neuvottelut hankkeesta kiinnostuneiden yritysten kanssa ovat parhaillaan käynnissä. Tavoitteena on aloittaa hankkeen yrityskohtainen työskentely vuoden 2014 alusta alkaen.

Yhteydenotot: pasi.ahonen@vtt.fi

6 REFERENSSIT

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

[OLLI] SOVELLUSTEN SALLIMISLISTAUS TEOLLISUUSAUTOMAATIOJÄRJESTELMISSÄ. Pia Ollin diplomityö, Oulun Yliopisto: http://herkules.oulu.fi/thesis/nbnfioulu-201308261635.pdf

[TEO-TT] TEOLLISUUDEN TIETOTURVAN TYÖPAJAT-hankealue HUOVIssa

[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

[WIB] Process Control Domain – Security Requirements for Vendors: M 2784 - X-10 Published by WIB, Second issue, October-2010

Lisätukea aihepiireittäin:

Automaation tietoturvan kartoitus

Catalog of Control Systems Security, Recommendations for Standards Developers. Homeland Security, CSSP, September 2009

ISA-62443-2-1 / IEC 62443-2-1 IACS security management system - Requirements, WG2, Published

ISA-62443-2-2 / IEC 62443-2-2 IACS security management system – Implementation guidance, WG2, Proposed

ISO/IEC 27002:2005, Information Technology -- Security techniques -- Code of practice for Information Security Management

KATAKRI, Kansallinen turvallisuusauditointikriteeristö, versio II, 2011

TEOLLISUUSAUTOMAATION TIETOTURVA. Verkottumisen riskit ja niiden hallinta. 2005 (nid.), 2010 (verkkopainos). Suomen Automaatioseura ry, Turvallisuusjaosto: http://www.cert.fi/attachments/cip/5na1SblCp/SAS29_TeollisuusautomaationTietoturva.pdf

VAHTI 2/2010: Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Organisaation tietoturvallisuuden hallinta (Excel). Tietoturvallisuuden hallinta - IT-prosessit (Excel)

VAHTI 8/2006: TIETOTURVALLISUUDEN ARVIOINTI VALTIONHALLINNOSSA

Teollisuuden tietoverkkojen ja etäyhteyksien hallinta ja seuranta

CONFIGURING & MANAGING REMOTE ACCESS FOR INDUSTRIAL CONTROL SYSTEMS. CPNI, APRIL 2011

Cyber Security Procurement Language for Control Systems. Homeland Security, CSSP, September 2009

FIREWALL DEPLOYMENT FOR SCADA AND PROCESS CONTROL NETWORKS, GOOD PRACTICE GUIDE. CPNI, FEBRUARY 2005

ISA-62443-3-2 / IEC 62443-3-2 Security assurance levels for zones and conduits, WG4, Draft for Comment

KATAKRI, Kansallinen turvallisuusauditointikriteeristö, versio II, 2011

NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security

SECURING THE MOVE TO IP-BASED SCADA/PLC NETWORKS. CPNI, November 2011

VAHTI 3/2011: Valtion ICT-hankintojen tietoturvaohje, 2011

Verkostoautomaatiojärjestelmien tietoturva. Reneco, 2013: http://energia.fi/sites/default/files/verkostoautomaatiojarjestelmien_tietoturva__2013-09-27.pdf

Tehtaan tietoturvaohjeet, koulutus ja muutosten hallinta

Cyber Security Procurement Language for Control Systems. Homeland Security, CSSP, September 2009

ISA-TR62443-2-3 / IEC/TR 62443-2-3 Patch management in the IACS environment, WG6, Draft for Comment

KATAKRI, Kansallinen turvallisuusauditointikriteeristö, versio II, 2011

Protecting Industrial Control Systems Recommendations for Europe and Member States. Deliverable – 2011-12-09, incl. Annex I-VI, ENISA

VAHTI 3/2011: Valtion ICT-hankintojen tietoturvaohje, 2011

Hankintakäytännöt ja vaatimukset toimittajille

Cyber Security Procurement Language for Control Systems. Homeland Security, CSSP, September 2009

ISA-62443-2-4 / IEC 62443-2-4 Certification of IACS supplier security policies and practices, IEC TC65/WG10, Draft for Comment

ISA-62443-3-3 / IEC 62443-3-3 System security requirements and security assurance levels, WG4, Published

ISA-62443-4-1 / IEC 62443-4-1 Product Development Requirements, WG4, Draft for Comment

KATAKRI, Kansallinen turvallisuusauditointikriteeristö, versio II, 2011

Sopimuksiin perustuva varautuminen - SOPIVA. Huoltovarmuuskeskus: www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/sopiva/

VAHTI 3/2011: Valtion ICT-hankintojen tietoturvaohje, 2011

Tekniset tietoturvamenetelmät (tietoturvatestaus, sallimislistaus)

Cyber Security Assessments of Industrial Control Systems. Homeland Security, CSSP, November 2010

ISA-TR62443-3-1 / IEC/TR 62443-3-1 Security technologies for IACS, WG1, Published

ISA-62443-4-2 / IEC 62443-4-2 Technical security requirements for IACS components, WG4 Under Development

NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment

Top 125 Network Security Tools. SecTools.Org: http://sectools.org/

Tuotannon riskien hallinta ja jatkuvuuden varmistaminen

AGA Report No. 12: Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan

Creating Cyber Forensics Plans for Control Systems. Homeland Security, CSSP, August 2008

FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems

FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems

FIPS PUB 140-3: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

IAONA Handbook: Network Security, Version 1.5

Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies. Homeland Security, CSSP, October 2009

ISO27k Toolkit: Roles and responsibilities for contingency planning, July 2008

ISO/IEC 27005:2011: Information technology - Security techniques – Information security risk management

NERC-CIP standards CIP-001 - CIP-011, e.g. CIP-009-2: Cyber Security - Recovery Plans for Critical Cyber Assets. North American Electric Reliability Corporation

NIST IR 7176, System Protection Profile - Industrial Control Systems, Version 1.0

NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems, October 2009

NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security

Sopimuksiin perustuva varautuminen - SOPIVA. Huoltovarmuuskeskus: www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/sopiva/

Teollisuuden käyttöön soveltuvia tietoturvastandardeja ja 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 olla vaikeaa tai työlästä. Niinpä eri ratkaisuja tulisikin etukäteen arvioida ja testata eri menetelmien soveltuvuutta tuotantoon ennen tietoturvaratkaisun valintaa ja käyttöönottoa. Tähän arviointiin tai testaamiseen tarvitaan usein lisätukea yrityksen ulkopuolelta.

Yhteistyön merkitys korostuu tänä päivänä tietoturvallisuuden ylläpidossa useimmilla sektoreilla, ei ainoastaan teollisuudessa. Toimivaa yhteistyötä ja yhteisiä pelisääntöjä tarvitaan automaatiojärjestelmien hankinnan ja käyttöönoton aikaisessa tietoturvan hallinnassa, mutta myös laajemmin koko tuotannon elinkaaren aikana. Erityisesti tietoverkkojen seurannan tarve on tänä päivänä korostunut, dataverkkojen kautta tapahtuvan häirinnän, teollisuusvakoilun ja tiedustelupalvelujen pitkälle kehittyneen soluttautumisen takia.

Teollisuudelle tarjottujen tietoturvapalvelujen 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 kriittisiä. Silti nämäkin tietovirrat täytyy saada parempaan hallintaan.

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY