TEOLLISUUSAUTOMAATION TIETOTURVA

Verkottumisen riskit ja niiden hallinta

Suomen Automaatioseura ry
Turvallisuusjaosto
2005
Verkkopainos 2010

1. verkkopainos

Julkaisija:
Suomen Automaatioseura ry
Turvallisuusjaosto
Asemapäällikönkatu 12 B, 00520 Helsinki
Puhelin 0201 981 220
Telefaxi 0201 981 227
office@atu.fi
www.automaatioseura.fi

Kannen kuva: Anssi Anttonen
Taitto: Taina Leino

ISBN 978-952-5183-38-2
ISSN 1455-6502
SAS julkaisusarja nro 29

Suomen Automaatioseuran turvallisuusjaosto

Tietotekniikan kehittyessä ja sen käytön nopeasti laajentuessa yhteiskunnan perusjärjestelmät, kuten teollisuus, liikenne ja jopa asuminen ovat tulleet riippuvaisiksi erilaisista automaatio- ja tietojärjestelmistä. Taloudellisten hyötyjen ohella yhä tärkeämmäksi tavoitteeksi on noussut ihmisten terveyden ja ympäristön turvaaminen varmistamalla yhteiskunnallisten ja tuotannollisten järjestelmien toiminnat ja niiden jatkuvuus.

Automaattisilla järjestelmillä voidaan lisätä turvallisuutta. Monia vaaranalaisia prosesseja ei voida hallita turvallisesti ilman nykyaikaista automaatiota. Toisaalta automaattisten turvajärjestelmien käyttö edellyttää paitsi automaatiojärjestelmän teknistä luotettavuutta myös järjestelmän kokonaisturvallisuuden hallintaa. Kun turvallisuuteen liittyvän automaation suunnittelussa ja toteutuksessa yhdistyvät koneturvallisuus, sähkötekniikka, tieto- ja tiedonsiirtotekniikat, ihminen-kone-vuorovaikutuksen näkökohdat jne., tarvitaan tämän kokonaisuuden hallintaan eri alojen ammattilaisten yhteistyötä.

Näiden eri ammattialojen yhteistoiminnan parantamiseksi perustettiin vuonna 2001 Suomen Automaatioseuran turvallisuusjaosto. Turvallisuusjaosto toimii avoimena foorumina kaikille automaation turvallisuudesta kiinnostuneille eri alojen ammattilaisille. Jaoston jäsenmäärä ylitti sadan rajan keväällä 2005. Jaoston lähtökohtana on, että automaation turvallisuuden perusperiaatteet ovat samanlaiset eri toimialoilla, kuten kemian prosesseissa, voimalaitoksissa, konejärjestelmissä jne.

Turvallisuusjaoston toiminta keskittyy lähinnä seuraaviin aihealueisiin:
- turvallisuuden hallintajärjestelmät
- automaation suunnittelu
- riskin arviointi
- vaatimusmäärittely
- turvallisuuteen liittyvät säädökset ja standardit
- ihminen–kone-vuorovaikutus
- turvajärjestelmät ja -laitteet
- turvallisuuteen liittyvät ohjelmistot
- automaation tietoturva
- kelpuutus ja sertifiointi
- koulutus.

Turvallisuusjaoston verkkosivuille toimitetaan turvallisuusjaostossa valmisteltuja aineistoja sekä linkkejä muualla julkistettuihin tärkeimpiin aineistoihin. Verkkosivuille pääsee Suomen Automaatioseuran sivuilta [1].

Teknisten järjestelmien turvallisuuden varmistamisessa on tavoitteena, että vaaranalaiset tuotantoprosessit toimivat tarkoitetulla tavalla niin tavan-

omaisessa käytössä kuin myös poikkeustilanteissa. Toiminnallisen turvallisuuden (Functional Safety) lähestymistapa on osoittautunut parhaaksi menetelmäksi, kun varmistetaan monimutkaisten teknisten järjestelmien turvallisuutta. Perustana on kattostandardi IEC 61508 sähköisten ja elektronisten ohjausjärjestelmien toiminnallisesta turvallisuudesta.

Turvallisuusjaoston toiminta keskittyy kahteen tavoitteiseen:

1. Turvallisuusjaoston tavoitteena on edistää standardin IEC 61508 ja sen sovellusstandardien käyttöä Suomessa. Tätä varten turvallisuusjaostossa toimii toiminnallisen turvallisuuden työryhmä, jonka tehtävänä on edistää edellä mainitun standardin käyttöä Suomessa ja auttaa sen soveltamisessa. Työryhmä järjestää muun muassa teemakokouksia, valmistelee soveltamisohjeita ja pitää yhteyttä muihin vastaaviin eurooppalaisiin ryhmiin.

2. Turvallisuusjaoston tavoitteena on edistää teollisuusautomaation tietoturvaa osana automaatiojärjestelmän kokonaisturvallisuutta siten, että teollisuusautomaatiojärjestelmien erityisominaisuudet otetaan huomioon. Jaoston tietoturvahankkeen tuloksena on tämä kirja, jonka tarkoituksena on antaa hyvät lähtökohdat teollisuusautomaation ympäristön tietoturvan arviointiin ja kehittämiseen esittelemällä teollisuusautomaation tietoturvan nykytilannetta, sen perusperiaatteita sekä hyviä tietoturvakäytäntöjä ja nykyaikaisia tietoturvaratkaisuja.

Palautteet tästä kirjasta ovat tervetulleita.

Matti Sundquist
Turvallisuusjaoston sihteeri
matti.sundquist@tsp.stm.fi

Alkusanat

Tietoverkkojen yleistymisen, informaation taloudellisen arvon ja laatuvaatimusten kiristymisen myötä tietoturva (Information Security) on noussut keskeiseksi tekijäksi teknisten järjestelmien turvallisuuden rinnalle.

Teollisuusautomaatiojärjestelmät toimivat verkottuneina muihin tietojärjestelmiin. Verkottumisella saavutettavien hyötyjen ohella verkottumiseen liittyy myös kasvavia tietoturvaongelmia. Kun uhkat ja haavoittuvuudet ovat lisääntyneet on myös tarve suojata tietojärjestelmiä ja niihin kuuluvia automaatiojärjestelmiä ja -verkkoja kasvanut.

Tavallisesti tietoturvaa on käsitelty lähinnä toimistoverkkojen ja Internetverkon käytön yhteydessä. Tietoturva-asiantuntijat eivät useinkaan tunne teknisiä eroja liiketaloudellisten tietoturvakysymysten ja tuotantolaitosten automaatiojärjestelmien toiminnan välillä. Vastaavasti automaatioalalla tunnetaan hyvin ohjausjärjestelmien ongelmat, mutta tietoturvan asiantuntemus on toistaiseksi vähäistä. Siten tuotannon automaatiojärjestelmät ovat tavallisesti automaatiota hyödyntävän yrityksen tietoturvan hallinnan ulkopuolella ja tietoturva on jäänyt yksinomaan automaation asiantuntijoiden hoidettavaksi. Vastuunjako on usein epäselvä.

Kun tuotanto- ja toimistojärjestelmät toimivat nykyisin verkottuneempana kokonaisuutena, vanha työnjako ei enää riitä tietoturvan varmistamiseen automaatiojärjestelmien osalta. Yritystasolla tarvitaan tietoturvastrategiaa ja sen toteuttamiseksi tietoturvaohjelmaa, joka sisältää yrityksen kaikkien toimintojen tietoturvan hallinnoimisen ja tietoturvan käytännön toimenpiteet. Tämä edellyttää kuitenkin, että tietoturvaratkaisuissa otetaan huomioon teollisuusautomaation erityispiirteet.

Tämä kirja tähtää tietoturvan parantamiseen teollisten automaatiojärjestelmien suunnittelussa, kehittämisessä, käyttöönotossa, käytössä ja ylläpidossa eli järjestelmän koko elinkaaren aikana. Kirjassa tuodaan esille havaittuja tärkeitä ongelmakohtia ja näkökulmia sekä esitetään tilanteen parantamiseksi periaatteita ja ratkaisuvaihtoehtoja. Esitetyt ratkaisumallit eivät ole välttämättä ainoita oikeita, mutta ne antavat kuitenkin käsityksen tämän päivän tilanteesta.

Kirjan tarkoituksena on kiinnittää huomiota teollisuusautomaation tietoturvaan ja sen tärkeään rooliin tuotannon jatkuvuuden ja turvallisuuden varmistamisessa. Kirja on tarkoitettu teollisuuden tuotantolaitoksille, automaation henkilöstölle, teollisuusautomaation valmistajille, automaatiotoimittajille ja -integraattoreille, tietoturvan asiantuntijoille sekä automaatioalan opiskelijoille.

Kirja on koostettu eri asiantuntijoiden kirjoituksista. Esitetyissä näkökohdissa on erilaisia painotuksia, mikä osoittaa, että keskustelu teollisuusautomaation tietoturvasta on alkanut. Kirjan kirjoittajat ovat:

Antti Ala-Tala, toimitusjohtaja, Remion Oy
tietoturvaratkaisut PK-yrityksessä
Annika Havaste, lakimies, If Vahinkovakuutusyhtiö Oy
vakuutustoiminta
Harri Heimbürger, tutkimuskoordinaattori, Säteilyturvakeskus STUK
ydinvoimalaitosten turvallisuustutkimus
Marko Helenius, yliassistentti, Tampereen yliopisto
haitalliset ohjelmat ja niiden torjunta
Markku Henttu, tuotepäällikkö, Metso Automation Oy
tietoturvapalvelut
Pasi Hänninen, tietoturva-asiantuntija, Viestintävirasto
tietoturvan hallinnointi
Jorma Kajava, lehtori, Oulun yliopisto
tietoturvan hallinta organisaatiossa ja mittaaminen
Pekka Koponen, erikoistutkija, VTT
sähköverkot
Tuija Kyrölä, yritysturvallisuusjohtaja, Neste Oil
riskienhallinta, yritysturvallisuus ja tietoturva
Terho Riipinen, järjestelmäasiantuntija, Outokumpu Stainless Oy
aktiivihakemistot
Reijo Savola, tietoturvatutkimuksen koordinaattori, VTT
tietoturvan mittaaminen, testaaminen ja sertifiointi sekä hallinta organisaatiossa
Jari Seppälä, erikoistutkija, Tampereen Teknillinen Yliopisto, Automaatio- ja säätötekniikan laitos
tietoturvaratkaisut ja -käytännöt, tulevaisuuden kehitystrendit
Matti Sundquist, ylitarkastaja, Uudenmaan työsuojelupiiri
koneiden ohjausjärjestelmät
Veli Taskinen, laatupäällikkö, Ramse Consulting Oy
vaatimusmäärittely
Esa Tuovinen, tietoturva-asiantuntija, Honeywell Oy
tietoturva ja verkkoratkaisut
Markku Tyynelä, ohjelmapäällikkö, Metso Automation Oy
automaation tietoturva ja verkkoratkaisut

Lisäksi useat asiantuntijat ovat antaneet tärkeitä kommentteja ja lisäyksiä kirjaan. Heistä mainittakoon erityisesti:

Ari Meldo, johtaja, Information Risk Management, Metsäliitto Group
Mikko Salmenperä, tutkija, Tampereen Teknillinen Yliopisto, Automaatio- ja säätötekniikan laitos
Juha Viljamaa, teknologiapäällikkö, Metso Automation Oy

Sisällys

Lyhenteitä

BIOS (Basic Input/Output System) = ROM-muisti, joka sisältää laitteiston perustason tiedot, kuten käynnistys- ja asetusohjelmat. BIOS huolehtii keskusyksikön ja oheislaitteiden välisestä tiedonsiirrosta.
CERT-FI (Computer Emergency Response Team-Finland) = Viestintäviraston CERT-ryhmä, jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisut sekä tietoturvauhkista tiedottaminen.
DCOM (Distributed Component Object Model) = Integraatioarkkitehtuuri, joka käyttää ActiveX-teknologiaa, joka on Windows-käyttöjärjestelmän laajennus, ja joka on käyttöjärjestelmässä täysillä oikeuksilla suoritettava ohjelma.
DCS (Distributed Control System) = Hajautettu ohjausjärjestelmä.
DMZ (Demilitarized zone) = Harmaa alue, suoja-alue, ”ei-kenenkään-maa”.
DoS (Denial of Service) = Palvelunestohyökkäys, ylikuormitushyökkäys.
HTTP (Hyper Text Transfer Protocol) = Internet-sivujen välittämiseen käytettävä protokolla.
IDS (Intrusion Detection System) = Verkko- tai laitetasolla toteutettu tunkeutumisen havaitsemisjärjestelmä (tunnistamisjärjestelmä).
ICS (Industrial Control Systems) = Teollisuuden ohjausjärjestelmä.
IP (Internet Protocol) = Internet-verkkoprotokolla. IP-osoite yksilöi jokaisen Internetissä olevan laitteen.
IPS (Intrusion Prevention System) = Verkko- tai laitetasolla toteutettu tunkeutumisen estojärjestelmä.
IPv6 (Internet Protocol version 6) = Internet-protokollan versio 6.
IT (Information Technology) = Informaatioteknologia. Tätä suppeampaa lyhennettä korvaamaan käytetään yleisesti lyhennettä ICT (Information and Communication Technology) = Tieto- ja tietoliikenneteknologia.
LAN (Local Area Network) = Lähiverkko.
LSASS (Local Security Authority Subsystem) = Microsoft Windows-käyttöjärjestelmissä oleva alijärjestelmä käyttäjän tunnistamiseen ja käyttäjän oikeuksien hallintaan.
MS Windows (Microsoft Windows) = Yleisnimike Microsoft Corporationin käyttöjärjestelmäversioille, kuten Windows NT, Windows 2000, Windows XP ja Windows Server 2003.
OPC (OLE for Process Control) = Microsoft Windows -teknologiaan perustuva standardi ja joukko määrittelyjä, joilla voidaan liittää erilaisia ohjelmistoja samaa rajapintaa hyväksikäyttäen eri valmistajien laitteisiin (OLE = Object Linking and Embedding).
OSI (Open Systems Interconnection) = ISO:n (International Standardization Organization) kehittämä OSI-malli, jonka mukaisesti eri tietoliikennejärjestelmät tulisi suunnitella (ks. luku 5.4.4).
PLC (Programmable Logic Control) = Ohjelmoitava tai ohjelmoitu logiikkayksikkö.
RFID (Radio Frequency Identifier) = Radiotaajuinen tunnistus.
RTU (Remote Terminal Unit) = Etäasema (etäohjausyksikkö).
RTOS (Real Time Operating System) = Tosiaikainen ohjausjärjestelmä.
SCADA (Supervisory, Control and Data Acquisition System) = Käytönohjaus- ja valvontajärjestelmä.
USB (Universal Serial Bus) = Sarjaliikennestandardin mukainen liitin, jolla lisälaitteet saadaan liitettyä tietokoneeseen.
VLAN (Virtual LAN) = Virtuaalinen lähiverkko.
VPN (Virtual Private Network) = Tekniikka, jolla organisaation sisäverkko levitetään turvallisesti julkisen verkon yli.
WAN (Wide Areal Network) = Laaja lähiverkko, joka teollisuusautomaatiossa mielletään tehtaiden välisenä verkkona.
WLAN (Wireless Local Area Network) = Langaton lähiverkko.

Käsitteitä

AAA = Tunnistus (myös autentikointi, Authentication), valtuutus (Authorisation) ja seuranta (Accounting) vaaditaan tietoturvalliseen käytönhallintaan (ks. luku 5.5 ja liite 3).

CIA = Luottamuksellisuuden (Confidentiality), eheyden (Integrity) ja saatavuuden (Availability, myös käytettävyys) varmistaminen on ISO/IEC 17799 [2] standardin mukaan tietoturvan (Information Security) ominaispiirre (ks. luku 3.1).

Haavoittuvuus (Vulnerability) = Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää hyväksi vahingon aiheuttamisessa (ks. luku 3.7.2).

Haittaohjelma (Malicious Software, Malware) = Ohjelma, ohjelman osa tai muu käskyjoukko, joka tarkoituksellisesti aiheuttaa ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Haittaohjelmia ovat esimerkiksi tietokonevirukset ja -madot sekä näiden yhdistelmät (ks. luku 2).

Hyökkäys (Attack) = Toimenpiteet, joilla pyritään vahingoittamaan tai käyttämään oikeudettomasti tietojärjestelmää tai tietoverkkoa. Hyökkäys voidaan toteuttaa esimerkiksi verkkohyökkäyksenä tietoverkon kautta (ks. luku 2).

Kiistämättömyys (Non-repudiation) = Tietoverkossa eri menetelmin saatava varmuus siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi (ks. luku 3.1).

Koventaminen, ”hardenointi” (Hardening) = Koventamisella tarkoitetaan sellaisten perusominaisuuksien, ohjelmistojen, palvelujen ja osuuksien poistoa tai niiden käytön estämistä (sulkemista), joita ei automaatiojärjestelmän toiminnassa välttämättä tarvita (ks. luku 5.2.1).

Palomuuri (Firewall) = Tekninen järjestely, jonka tarkoituksena on hallita tietoliikennettä verkosta toiseen tai verkon ja yksittäisen järjestelmän välillä. Palomuuri voi olla ohjelmisto tai laite (ks. luku 5.4.2).

Pääsyn valvonta (Access Control) = Toiminnot ja menettelyt, joiden avulla tietojärjestelmään pääsy tai tiedon saanti sallitaan vain valtuutetuille henkilöille tai sovelluksille (ks. luku 5.5 ja liite 3).

Varmenne (certificate, digital certificate) = Sähköinen todistus, jolla vahvistetaan, että todistuksen haltija on tietty henkilö, organisaatio tai järjestelmä. Varmenne on yleensä ulkopuolisen varmentajan myöntämä (ks. luku 5.5).

1
Johdanto

Sasser-mato sulki tehtaita

Keväällä 2004 levinnyt Sasser-mato on eräs laajalti teollisuusautomaatioon vaikuttaneista haittaohjelmista. Sasser on Internetin kautta leviävä mato, joka käyttää Microsoftin huhtikuun 13. 2004 julkistamaa, MS Windows -käyttöjärjestelmässä olevaa LSASS (Local Security Authority Subsystem Service) -haavoittuvuutta.

Ensimmäinen havainto Sasser-madosta tehtiin vain 18 päivää haavoittuvuuden julkistamisen jälkeen, joten se on myös yksi nopeimmin toteutetuista tiedossa olevia haavoittuvuuksia hyödyntävistä haittaohjelmista. Johtuen leviämisen ajankohdasta (lauantaina 1.5) viikonlopun aikana ei havaittu suuria häiriöitä. Maanantaina työntekijöiden saapuessa työpaikoille mato aloitti rajun leviämisen, leviten ensin toimistoverkkoihin ja sen jälkeen suojaamattomiin automaatioverkkoihin.

Huomion arvoista oli, että mato ei levinnyt toimistoverkkoihin suoraan Internetistä yritysten palomuurien läpi, vaan nimenomaan oman henkilöstön kannettavien tietokoneiden kautta, joihin se oli viikonlopun Internetkäytön yhteydessä tarttunut. Sasser-mato saattoi myös leviämisyrityksensä seurauksena aiheuttaa kohteen käyttöjärjestelmän uudelleenkäynnistymisen, mikä puolestaan sai aikaan palvelunesto-tilanteen. Kohteen kriittisyydestä riippuen tämä saattoi aiheuttaa hyvinkin suurta haittaa ja vahinkoa kun järjestelmien käyttö estyi.

Vaikka mato ei sinällään saanut aikaan varsinaista tuhoa, kuten esimerkiksi tuhonnut tiedostoja, sen leviämismekanismi kuormitti verkkoja aiheuttaen liikenteen hidastumista ja pahimmillaan ylikuormitti verkkoa niin paljon, että tietoliikenne estyi lähes kokonaan. Tämä puolestaan aiheutti erilaisten turvallisuuslukitusten laukeamisia ja varatoimintojen käynnistyksiä. Maanantaina työpäivän loppuessa Sasser-mato oli aiheuttanut teollisuusautomaatioympäristöissä lukuisia häiriöitä ja pahimmillaan tuotantolaitosten alasajoja ja siten tuotannon keskeytymisiä.

Aiheutuneista haitoista ei ole saatavissa tarkkoja lukuja, mutta Sasser-madon on arvioitu aiheuttaneen maailmanlaajuisesti yli 400 M€:n kustannukset. Niissä automaatiojärjestelmissä, joissa tietoturvasta ja Microsoftin tietoturvapäivityksistä oli huolehdittu asianmukaisesti, ei merkittäviä häiriöitä havaittu.

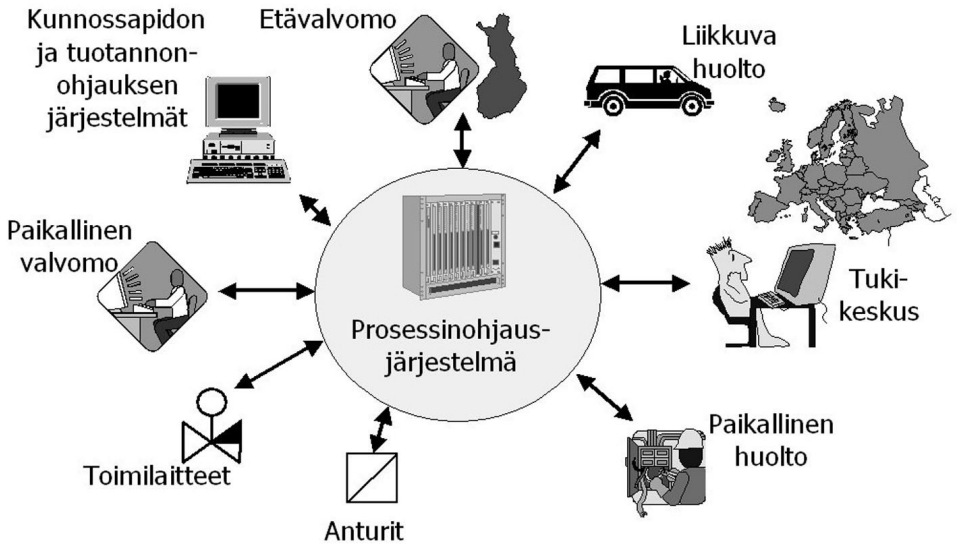
1.1 Verkottuminen

Uusien ohjelmoitavien valmistusjärjestelmien kehittämisen ja käyttöönoton seurauksena teollisuudessa käytössä oleva tekniikka muuttuu nopeasti. Mahdollisuudet erilaisten laitteiden ja ohjelmistojen yhdistämiseen lisääntyvät, mutta samalla tuotantojärjestelmien monimutkaisuus kasvaa.

Tarve informaation laaja-alaiseen hyödyntämiseen sekä yritysten sisällä että yritysten kesken lisää paineita tietoverkkojen entistä laajempaan käyttöön. Yhtenäiset, sovellusaluekohtaiset standardit ja ohjeet tietoturvasta sekä sen käytännön toteutuksesta kuitenkin puuttuvat. Monilla yrityksillä ole kokonaisuuden hallintaan tarvittavaa osaamista tai selkeitä käytäntöjä.

Joissakin tapauksissa myös itse ohjaukseen liittyvät mittaukset ja jopa prosessiohjaus tehdään yleisten tietoliikenneverkkojen välityksellä. Tietoturvan kannalta tämä ei ole hyvä käytäntö, koska yleisissä tietoliikenneverkoissa ei tietoturvaa aina voida varmistaa. Eräillä aloilla (esimerkiksi lääketeollisuus, voimalaitokset, ydinvoimalaitokset) viranomaiset asettavat vaatimuksia automaatiojärjestelmien tietoturvaratkaisuille.

Kuvassa 1 on havainnollistettu automaatiojärjestelmän toimintaympäristöä. Prosessinohjauksen tietovirrat tapahtuvat anturien, toimilaitteiden ja valvomon välillä. Kunnonvalvonnan tietovirrat tuovat kokonaisuuteen mukaan koko ohjausjärjestelmän ja lisäksi teknisen tukikeskuksen. Automaation kunnossapito tuo mukaan ainakin paikallisen ja liikkuvan huollon tarpeet.



Kuva 1. Automaation liityntöjä tietoverkkoihin.

1.2 Tietoturvauhkat ja haitat

Tietoturvaongelmat nykyisessä tietoyhteiskunnassa ovat laajentuneet ja kohdistuvat myös uusiin järjestelmäympäristöihin sekä tietoliikennetekniikoihin. Tietoturvauhkat yleisissä käyttöjärjestelmäympäristöissä, sovelluksissa ja protokollissa vaikuttavat laajamittaisesti koko yhteiskuntaan. Erityisesti tietoliikenneverkkoon liitetyt tietojärjestelmät lisääntyvät, jolloin verkkoon tunkeutumisen uhkat kasvavat ja asettavat entistäkin suurempia haasteita tietojärjestelmien suojaamiseen. Uusimpina uhkina voidaan todeta langattomiin verkkoihin liittyvät haavoittuvuudet sekä matkapuhelinverkossa leviävät virukset.

Järjestelmän tietoturvan voi vaarantaa yrityksen oman henkilöstön (tahallinen tai tahaton) väärinkäyttö tai ulkopuolisen tunkeutuminen järjestelmään tietoverkkojen kautta. Tietoverkkoja ja palvelimia ylikuormittamalla voidaan häiritä tuotantoa ja aiheuttaa tuotantokatkoja. Vahingollista toimintaa ovat myös ohjelmistojen laiton kopiointi ja osaamisen vuotaminen kilpailijalle.

Tarve suojata tietojärjestelmiä niihin kuuluvine automaatiojärjestelmineen ja verkkoineen kasvaa nopeasti. Pelkästään tunkeutumisen estäminen ja viruskuvaustiedostojen päivitys ei riitä, vaan kaikki tietojärjestelmien komponentit ja järjestelmien käyttötavat on otettava huomioon.

Liikesalaisuudet unohtuvat taksin takapenkille – suojaamattoman kannettavan tietokoneen riskit

Tammikuussa 2005 kerrottiin Tietokone-lehden verkkosivuilla, että yksistään pääkaupunkiseudulla unohdettiin takseihin viimeisen puolen vuoden aikana yhteensä yli 3700 matkapuhelinta, kannettavaa tietokonetta ja kämmenmikroa. Kansainvälisesti ongelma on huomattavasti laajempi. Suojaamaton kannettava tietokone voi väärissä käsissä mahdollistaa suoran pääsyn yrityksen automaatioverkkoon. Tällainen uhkakuva toteutuu esimerkiksi seuraavasti:

- Automaatioverkon ylläpito-oikeuksiin valtuutettu henkilö on liikematkalla ulkomailla ja unohtaa kannettavan tietokoneen taksiin.
- Kannettavassa tietokoneessa on käyttöjärjestelmän (esimerkiksi Windows XP) automaattinen sisäänkirjautumistoiminto päällä. Varas saa siis automaattisesti käyttäjän oikeudet käynnistäessään koneen. Usein käyttäjillä on myös ylläpito-oikeudet, jolloin nämäkin ovat suoraan varkaan käytössä.
- Yrityksen VPN (Virtual Private Network) käyttää selainpohjaista tunnistusta, ja käyttäjällä on selaimen (esimerkiksi Internet Explorer) salasanojen tai lomakkeiden automaattinen täyttötoiminto käytössä. Varas voi tällöin oikean linkin löydettyään muodostaa VPN-yhteyden yrityksen automaatioverkkoon.

- Tämän jälkeen varkaan on helpompaa etsiä mahdollisia heikkouksia automaatioverkosta, sillä usein sisäverkon palvelimet on hyvin suojattu ulkoisia uhkia vastaan, mutta heikosti suojattu sisäverkon kautta tulevilta tunkeutumisilta.

- Automaattinen sisään kirjautuminen antaa myös pääsyn tietokoneen levyllä oleviin luottamuksellisiin tietoihin, esimerkiksi tarjouksiin, sopimuksiin ja automaatiojärjestelmän konfiguraatiotietoihin, jos kyseisiä tietoja ei ole salattu. Salaus voidaan tehdä joko laitteistopohjaisesti tai ohjelmistolla, kunhan salasana tai muu avain on erotettu käyttöjärjestelmän käyttäjätilistä.

Haittaohjelmien vaikutus voi kohdistua myös yhteiskunnan toiminnan kannalta kriittisiin infrastruktuurin ohjausjärjestelmiin, vaikka haittaohjelman tekijöillä ei tällaista tarkoitusta olisikaan.

Turvallisuusriskit yksittäisissä tuotantolaitoksissa kohdistuvat ihmisten turvallisuuteen ja terveyteen. Tietoturvahyökkäykset energiantuotanto- ja jakelujärjestelmiin mukaan lukien sähkön-, öljyn- ja kaasunjakeluverkot, jätevedenkäsittely, vedenjakelujärjestelmät sekä kemianlaitokset, joissa käsitellään vaarallisia aineita, voivat vaarantaa yleisön terveyden ja turvallisuuden sekä olla uhkana ympäristölle. Lisäksi näistä haitoista tulee merkittävää taloudellista häviötä vahinkojen, tuotannon menetysten, jakeluketjujen katkeamisen, salassa pidettävien tietojen leviämisen, luottamuksen menettämisen, kielteisen julkisuuden ja oikeusprosessien muodossa.

1.3 Tietoturvaperiaatteiden soveltaminen verkottuneeseen automaatioon

Tietotekniikan yleiset lähestymistavat ovat sovellettavissa myös tuotannollisiin tietojärjestelmiin sekä erilaisiin automaatio- ja ohjausjärjestelmiin, mutta näitä menettelyitä ja ratkaisuja on sovellettava oikealla tavalla ja ottaen huomioon automaation erityispiirteet. Näitä erityispiirteitä ovat esimerkiksi tosiaikaisuus, rajalliset laskentaresurssit sekä tuotannon jatkuvuus- ja turvallisuusvaatimukset. Laajasta erilaisten menetelmien valikoimasta on valittava sopivimmat sen mukaan, mitä tietoturvan tasoa automaatiojärjestelmässä vaaditaan ja mitä menetelmää voidaan tällä vaaditulla tietoturvan tasolla käyttää. Tavoitteena on yhdistää tietotekniikkaan liittyvät toimenpiteet muihin riskien vähentämisen menetelmiin tavoitteena riskin vähentäminen hyväksyttävälle tasolle.

Tietotekniikkaan liittyvien riskien hallinta on osa automaatiojärjestelmän riskien hallintaa. Riskinhallinnan toimenpiteillä pyritään vähentämään eitoivottujen tapahtumien toteutumista ja pienentämään niiden haitallisia seurauksia. Riskinhallinnan lähtökohtana on automaatiojärjestelmän riskien arviointi ja sen perusteella tunnistetaan tietoturvan tarpeet. Tässä on otettava huomioon automaation erityispiirteet, kuten tosiaikaisuus, rajalliset

laskentaresurssit sekä tuotannon jatkuvuus- ja turvallisuusvaatimukset. Tietoturvatarpeet määrittävät sen, mitä eri tietoturvatoimenpiteitä ja teknisiä ratkaisuja sekä toimintaympäristön suojauskeinoja on käytettävä varmistettaessa toiminnan häiriöttömyys ja jatkuvuus.

Tietoturvan hallinta edellyttää tietoturvatyön organisointia sekä eri henkilöstöryhmien ohjeistamista ja kouluttamista. Teknisiä tietoturvaratkaisuja ovat muun muassa tietoliikenteen suojaamiseen tarkoitetut palomuurit ja virustorjuntaohjelmat. Teknisen toimivuuden takaaminen edellyttää myös selkeitä vastuita muun muassa palvelu-, ohjelmisto- ja laitteistotoimittajien kanssa, jolloin toimitus- ja ylläpitosopimuksien tietoturvakäytännöt nousevat tärkeiksi. Automaatioympäristön fyysisellä suojaamisella ja valvonnalla estetään asiattomien pääsy työtiloihin.

Automaatioympäristössä on tavoitteena painottaa tietoturvatyössä ennaltaehkäisevää toimintaa, mikä on mahdollista vasta kun tietoturvan perusasiat ja käytännöt on luotu ja otettu käyttöön. Automaatiojärjestelmien tietoturvaperiaatteita ovat muun muassa:

- Suora yhteys automaatiojärjestelmiin yleisistä tietoliikenneverkoista estetään.
- Tietojärjestelmäpalvelut määritetään tarkasti vain tarvittavaan käyttöön ja muut toiminnot rajataan pois.
- Kriittisten tietojärjestelmien toimintaa seurataan jatkuvasti.
- Toimintahäiriöiden varalle laaditaan toipumissuunnitelmat.
- Tietojärjestelmämuutosten ylläpito ja laite- ja ohjelmistoversioiden päivitys organisoidaan, koska laite- ja ohjelmistoversiot uusiutuvat nopeasti.

Järjestelmäkomponenttien päivittäminen voi olla hankalaa. Käyttöjärjestelmät saattavat olla niin vanhoja, että tietoturvapäivityksiä ei ole saatavilla. Myös eri tietojärjestelmien yhdistäminen saattaa aiheuttaa vaikeuksia tietoturvapäivityksiin.

Ensiarvoisen tärkeää on varmistaa, että tarpeeton tietoliikenne on estetty yrityksen omiin palveluihin yleisistä tietoliikenneverkoista. Lisäksi tietojärjestelmissä ei saisi tarjota sellaisia palveluita, jotka eivät ole järjestelmän toiminnan ja käytön kannalta tarkoituksenmukaisia.

Tietoturvan varmistamiseksi järjestelmien ylläpito on entistä tärkeämpää. Tietotekniikan nopea kehittyminen kärjistää näitä ongelmia: muutaman vuoden ikäiset automaatiojärjestelmät, -laitteet ja niihin liittyvät ohjelmistot saattavat olla jo tänä päivänä vanhentuneita. Eri ohjelma- ja laiteversioiden hallinta edellyttää muutostöiden ja päivitysten asianmukaista organisointia.

1.4 Tietoturvan hallinnointi Suomessa

Hallitus teki vuoden 2003 syyskuussa merkittävän periaatepäätöksen kansallisesta tietoturvallisuusstrategiasta. Päätöksen visiona on rakentaa Suomesta nykyistä tietoturvallisempi tietoyhteiskunta. Strategian toimeenpanon edel-

lyttämien toimien yhteensovittamista sekä strategian toteutumista seuraa kansallinen tietoturvallisuusasioiden neuvottelukunta.

Tietoturvastrategian tavoitteena on

– edistää kansallista ja kansainvälistä tietoturvayhteistyötä,
– edistää kansallista kilpailukykyä ja suomalaisten tieto- ja viestintäalan yritysten toimintamahdollisuuksia,
– parantaa tietoturvariskien hallintaa,
– turvata perusoikeuksien toteutuminen ja kansallinen tietopääoma ja
– lisätä tietoturvatietoisuutta ja -osaamista.

Koko yhteiskuntaan kohdistuvat uhkat on tiedostettu ja Suomen hallitus päätti vuonna 1999 selvittää, miten tietoliikenteen ja tietoverkkojen turvallisuus ja suojaustekniset kysymykset tulisi hallinnollisesti järjestää Suomessa. Selvityksen pohjalta nimitettiin tietoliikenneturvallisuudesta vastaavaksi viranomaiseksi Suomessa silloinen Telehallintokeskus eli nykyinen Viestintävirasto.

Selvityksessä todettiin muun muassa, että tietoteknisten laitteiden ja ohjelmistojen tietoturvan testausta, sertifiointia ja valvontaa varten ei ollut tarkoituksenmukaista perustaa Suomeen erillistä viranomaisorganisaatiota, vaan tietoturva päätettiin hoitaa hyödyntämällä kaupallisia palveluja ja kansainvälistä yhteistyötä. Erityisesti yhteiskunnan toimintaa vakavalla tavalla uhkaavien tietoturvaloukkausten ja tietoturvauhkien havaitsemiseksi ja ratkaisemiseksi perustettiin Viestintävirastoon CERT-FI-ryhmä (Computer Emergency Response Team – FICORA) [3].

Yhtenä merkittävänä kansallisen tietoturvallisuusstrategian hankkeena on edellä mainitun Viestintäviraston CERT-FI-ryhmän ylläpitämä kansallinen tietoturvariskien tilannekuva. CERT-FI seuraa jatkuvasti kansallista ja kansainvälistä tietoturvaa vaarantavia uhkia ja ilmiöitä sekä laatii tilannekatsauksia. Tarkoituksena on tarjota yrityksille, yhteisöille ja yksityisille henkilöille tietoturvariskien tilannekuva, joka antaa edellytyksiä arvioida tietoturvariskejä sekä kohdistaa tarvittavat vastatoimenpiteet oikealla tavalla.

Tietoverkkorikosten tutkinta Suomessa kuuluu poliisiviranomaiselle. Tutkinta on pääosin keskitetty keskusrikospoliisin (KRP) tietotekniikkarikosyksikköön. Kansallisen tietoliikenneturvallisuuden yleisestä ohjauksesta ja kehittämisestä vastaava ministeriö on Liikenne- ja viestintäministeriö (LVM) ja sen alainen viestintävirasto. Valtionvarainministeriö (VM) vastaa valtionhallinnon tiedonkäsittelyn tietoturvatoiminnan ohjauksesta ja yhteensovittamisesta sekä antaa valtionhallinnolle siihen liittyviä ohjeita ja suosituksia. Muita tietoturvasta huolehtivia viranomaisia omalla hallinnonalallaan ovat muun muassa sisäasiainministeriö ja huoltovarmuuskeskus.

2
Tietotekniset riskit

Automaatiojärjestelmään tunkeutuminen on tietoturvan kannalta tärkeä esimerkki ei-toivotusta tilanteesta ja uhkasta, joka tulee estää ennalta ja paljastaa. Tässä luvussa keskitytään niihin tietoteknisiin riskeihin, jotka liittyvät tietoverkkoon tunkeutumiseen, kuten haittaohjelmiin, puskuriylivuotoon, sähköpostin riskeihin sekä palvelunestohyökkäyksiin ja käyttöjärjestelmän valinnan arviointiin.

2.1 Järjestelmään tunkeutuminen

Arvioitaessa järjestelmään tunkeutumisen mahdollisuutta ja seurauksia on tiedettävä, minkälaisia ovat yrityksen tietoliikenne- ja tietoturvaratkaisut ja miten tunkeutuminen tietoverkkoon voi tapahtua. Tietoverkko voi ulottua fyysisesti suojatun alueen ulkopuolelle tai ylittää sen. Tietoverkkoa voidaan käyttää valmistukseen, valvontaan ja muihin toimintoihin samanaikaisesti. Tietoverkon tietoturvaratkaisuissa voi olla haavoittuvuuksia, heikkouksia tai puutteita. Tietoverkkoon voi olla liitettynä monenlaisia laitteita, kuten radiolaitteita ja telemetrisiä laitteita sekä ulkoisia palveluita, joita käytetään maantieteellisesti erillisten alueiden väliseen kommunikointiin.

Järjestelmään tunkeutuminen voi tapahtua fyysisesti tai tietoverkon kautta [4]:

- Ilman valtuuksia oleva henkilö pääsee luottamuksellisiin tietoihin: tietoja paljastuu henkilöille, joille ei ole annettu valtuuksia niiden käyttöön.
- Pääsy väärentämällä tunnistamista: lavastetaan käyttäjän tunnistustiedot, kuten käyttäjän tunnus- ja salasana (järjestelmään tunkeutumisen jälkeen väärillä tunnuksilla esiintyvä voi ottaa järjestelmän haltuunsa ja antaa ei-toivottuja käskyjä ohjausjärjestelmään).
- Valtuutetun henkilön kielletty tai sopimaton toiminta: tarkoituksella tai vahingossa toteutettu tiedostojen tai tietoliikenteen tietojen muuttaminen käyttökelvottomaksi.
- Käytönesto: normaalin käytön estäminen tekemällä verkkopalvelin käyttökelvottomaksi (DoS).

Tietoverkon haavoittuvuuksia ja heikkouksia ovat esimerkiksi [4]:

- Internet- ja intranet-yhteydet.
- Modeemiyhteydet, erityisesti modeemit, joissa ei ole takaisinsoittoa eikä salausta.
- Langattoman yhteyden kytkentäkohdat.

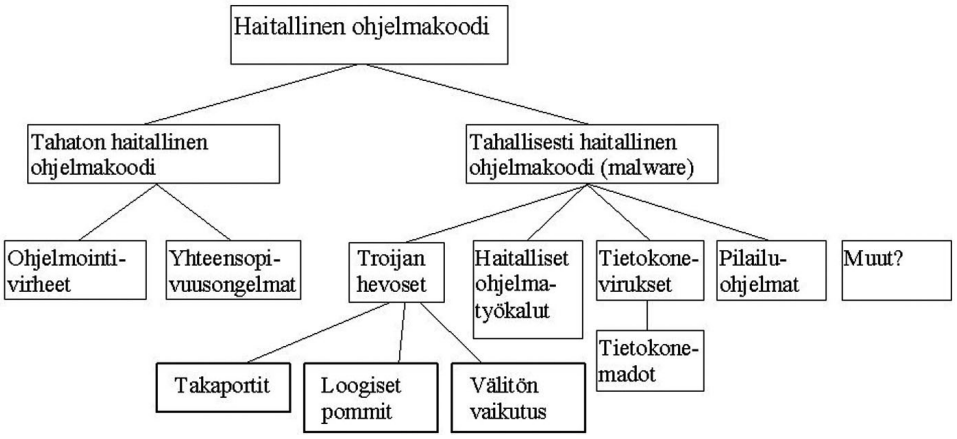
- Etätyöpisteen ohjelmistot, joita asiantuntijat käyttävät järjestelmän ylläpitämiseen (näissä yhteyksissä on järjestelmiin pääsyä valvottava ja estettävä luvattomilta järjestelmän käyttö).
- Järjestelmien etäkäyttö.
- Kaukovalvontaverkot ja mittausten etäluku.
- Kaikki verkkoyhteydet järjestelmiin, jotka eivät ole osana valmistus- ja ohjausjärjestelmiä.
- Kaikki verkkoyhteydet, joita käytetään kytkemään SCADA-verkkoja tai ohjausjärjestelmiä yhteen ja jotka eivät ole osana fyysisesti varmistettua tuotanto- ja ohjausjärjestelmäverkkoa.

Ulkoisista verkoista on verkkoyhteyksien kautta mahdollista tunkeutua automaatioverkkoon. Seuraavassa on esimerkkejä tunkeutumisen seurauksista ja tunkeutumisen todennäköisyydestä:
- Jos yhteys ulkoiseen verkkoon on suojaamaton, järjestelmään tunkeutuminen on todennäköistä ja jatkuvaa, ja toiminnan seuraukset automaatiojärjestelmän toimivuudelle voivat olla erittäin haitallisia.
- Jos yhteys ulkoiseen verkkoon on hyvin suojattu, tunkeutuminen on hyvin epätodennäköistä eikä tästä aiheudu haittaa toiminnalle.
- Jos automaatiojärjestelmä on erotettu muista yrityksen verkoista, tunkeutuminen on hyvin epätodennäköistä eikä tästä aiheudu haittaa toiminnalle.
- Jos Internet-verkkoon on suojattu yhteys, on tunkeutuminen silti mahdollista. Mahdollisen tunkeutumisen seuraukset riippuvat siitä, kuinka kriittiseen verkkoon tai järjestelmään vaikutetaan tai aiheutetaan häiriötä, ja seuraukset voivat haitata toimintaa suurestikin.
- Jos Internet-verkkoon on suojaamaton yhteys, esimerkiksi langaton yhteys tai modeemi, on tunkeutuminen erittäin todennäköistä.

2.2 Haittaohjelmat

Haitallisilla ohjelmilla aiheutetut hyökkäykset voidaan jaotella seuraaviin luokkiin: virukset, troijanhevoset ja roskaposti (spam). Tietokonevirusten alijoukkona ovat tietokonemadot ja troijanhevosten alijoukkona ovat takaportit sekä loogiset pommit. Myös vakoiluohjelmat voidaan nähdä määrätynlaisina troijanhevosina. Haitallisilla ohjelmatyökaluilla voidaan muun muassa tehdä hyökkäyksiä, esimerkkinä palvelunestohyökkäykset.

Haitallinen ohjelmakoodi voidaan luokitella seuraavasti (kuva 2):
- Haitallinen ohjelmakoodi: Ohjelmakoodi, joka on toimii vastoin järjestelmän määrityksiä tai tarkoitettua toimintaa. Haitallinen ohjelmakoodi voidaan jakaa tahalliseen ja tahattomaan haitalliseen ohjelmakoodiin.
- Tahaton haitallinen ohjelmakoodi: Ohjelmakoodi, joka on tehty tahattomasti haitalliseksi.



Kuva 2. Haitallisen ohjelmakoodin luokitus.

- Tahallinen haitallinen ohjelmakoodi: Ohjelmakoodi, joka on tehty tarkoituksella haitalliseksi.
- Troijanhevonen: Ohjelmakoodi, joka on naamioitu tekemään jotakin hyödyllistä, mutta joka sisältää piilotetun ja tarkoituksella tehdyn haitallisen toiminnon. Troijanhevonen voi aiheuttaa haitallisen vaikutuksen välittömästi (välitön vaikutus) tai tiettyjen ehtojen ollessa voimassa (loogiset pommit).
- Looginen pommi: Troijanhevonen, jonka haitallinen toiminto aktivoituu vasta jonkin ehdon ollessa voimassa. Ehto voi olla aika, asetus, levytila, näppäinkoodi, laite, asennettu ohjelma tai mikä tahansa muu mahdollinen järjestelmän tila mukaan lukien erilaisten tilojen yhdistelmät.
- Takaportti: Troijanhevonen, joka on tarkoituksella suunniteltu ohittamaan järjestelmän tai sovelluksen suojaustoimintoja.
- Tietokonevirus: Ohjelmakoodi, joka kykenee leviämään monistamalla itseään.
- Tietokonemato: Ohjelmakoodi, joka kykenee leviämään ilman ihmisen toimenpiteitä. Tietokonemadot ovat tietokonevirusten osajoukko.
- Haitallinen ohjelmatyökalu: Ohjelma, joka on suunniteltu helpottamaan tietojärjestelmiä vastaan tehtäviä hyökkäyksiä. Tällaisia ohjelmia ovat muun muassa haitallisten ohjelmien luontiohjelmat, tiedonkaappaajat ja hakkerointiohjelmat.

2.2.1 Tietokonevirukset ja -madot

Tietokonevirus on ohjelmakoodi, joka kykenee tekemään itsestään leviämiskelpoisen ohjelmakoodin. Tämä toiminto on helppo toteuttaa ohjelmallisesti ja valitettavasti se on myös varsin tehokas tapa kuluttaa järjestelmien ja tietoliikenteen resursseja.

Tietokonemato on tietokonevirus, joka on toteutettu leviämään tietoverkkoja pitkin. Nopeasti leviävät Internet-madot nähdään yhtenä merkittävimmistä uhkista Internet-infrastruktuurille sekä muille pakettivälitteisille TCP/IP-verkoille. Siten myös tätä teknologiaa käyttävät automaatioverkot ovat alttiita näille uhkille. Toistaiseksi madot ovat käyttäneet ennalta tunnettua tietoturva-aukkoa hyväkseen, mutta suurempi uhka syntyy kun mato käyttää toistaiseksi tuntematonta tietoturva-aukkoa.

Merkittävänä uhkana on erilaisten kannettavien tietolaitteiden siirtäminen paikasta toiseen sekä luvattomat yhteydet ulkoverkkoon. Kannettavan tietolaitteen, kuten USB-muistin ja kannettavan tietokoneen tai luvattoman verkkoyhteyden kautta virus voi päästä eristettyyn sisäverkkoon. Huonosti suojatussa sisäverkossa yksikin vuotokohta riittää viruksen leviämiseen. Seurauksena voi olla esimerkiksi verkon tietoliikenteen tukkiutuminen ja tiedon tuhoaminen. Pelkkä sisäisen verkon eristäminen ulkomaailmasta ei siis riitä.

Yleisesti ottaen automaatiojärjestelmien kannalta suurimmat uhkat liittyvät nimenomaan haittaohjelmiin, joiden tarttuminen järjestelmään ei edellytä kohteen käyttäjältä mitään vuorovaikutusta

2.2.2 Troijanhevoset

Troijanhevosten määrittely vaihtelee ja myös ohjelmiin ja käyttöjärjestelmiin tarkoituksella piilotetut haitalliset toiminnot ovat troijanhevosia. Troijanhevoset eivät leviä itsekseen toisin kuin tietokonevirukset, mutta ne voivat viruksia helpommin aiheuttaa kohdistettuja hyökkäyksiä tai ottaa yksittäisiä tietolaitteita haltuun. Kohdistetuissa hyökkäyksissä on ongelmana se, että virustentorjuntaan suunnitellut ohjelmat eivät tyypillisesti tunnista muokattuja, haitallista tarkoitusta varten kirjoitettuja ja järjestelmiin upotettuja ohjelmia. Troijanhevosten torjunnassa järjestelmien ja tietoverkkojen suunnittelu, tietoliikenteen suodatus, tietoturvasäännöt ja -käytännöt sekä koulutus ovat tärkeitä.

Vakoiluohjelmiksi (Spyware, myös Spybot ja Tracking Software) kutsutaan ohjelmia, jotka keräävät tietoa henkilöstä tai yrityksestä niiden tietämättä. Ne voivat asentua kohdekoneelle joko viruksen muodossa tai uuden ohjelman asennuksessa. Jälkimmäisessä tapauksessa asennettava ohjelma sisältää halutun toiminnallisuuden lisäksi myös tämän piilotetun ominaisuuden.

2.3 Puskuriylivuodot

Puskuriylivuodolla tarkoitetaan ohjelmassa olevaa virhettä, jonka seurauksena ohjelman keskusmuistista varaama muistitila vuotaa yli virheelliselle muistialueelle. Tällöin on vaarana, että hyökkääjä pääsee muokkaamaan tietokoneen keskusmuistissa olevaa aluetta. Jo yhdenkin luvattoman muistiosoitteen muokkaaminen voi olla vaarallista. Osaava hyökkääjä saattaa pystyä

syöttämään haluamaansa ohjelmakoodia järjestelmään sekä siirtämään ohjelman suorituksen syöttämälleen koodille. Tällöin hyökkääjä saattaa ohittaa kaikki normaalit turvamekanismit ja pystyy ottamaan järjestelmän haltuun. Jos järjestelmän haltuun ottaminen ei onnistu, puskuriylivuodolla voi olla mahdollista aiheuttaa palvelunestohyökkäys.

Puskuriylivuotojen hyväksikäyttö voidaan myös automatisoida. Esimerkiksi useat nopeasti levinneet tietokonemadot ovat käyttäneet hyväkseen puskuriylivuotoja ja erilaisissa hyökkäysohjelmissa voi olla valmiiksi ohjelmoituna puskuriylivuotojen hyväksikäyttö.

Kuvassa 3 on esimerkki pienestä, mutta vakavasta ohjelmointivirheestä C/C++-kielisessä ohjelmakoodin osassa. Taulukolle on varattu tilaa 200 merkille, mutta taulukkoon asetetaankin 201 merkkiä. Virheen seurauksena järjestelmän haltuun ottaminen on mahdollista edellyttäen, että syöte-taulukko sisältää käyttäjän ohjelmalle antamaa syötettä eikä puskuriylivuotoja vastaan ole muuten suojauduttu.

```
char taulukko[200];
int i;
...
for (i=0; i<=200; i++) //Käsitellään yksi taulukon alkio
liikaa
   taulukko[i]=syote[i];
```

Kuva 3. Esimerkki vakavasta ohjelmistokoodin puskuriylivuodosta.

2.4 Sähköposti

Sähköpostin käyttö sallitaan toisinaan myös automaatiojärjestelmien yhteydessä valvomoissa. Tämä ei ole tietoturvan kannalta hyvä käytäntö, koska sähköpostiin liittyy useita tietoturvaongelmia. Tärkeintä automaatiojärjestelmien yhteydessä on estää asiaton liikenne ja ylimääräisten ohjelmistojen pääsy automaatiojärjestelmään, oli sitten kyse roskapostista tai sähköpostin avulla leviävistä haittaohjelmista.

> Valvomossa oli estetty Internet-käyttö, mutta henkilökohtaisen sähköpostin käyttö oli sallittu. Erästä ongelmaa selvitellessä huomattiin, että eräs valvomossa työskentelevä henkilö oli asentanut sähköpostin kautta lähettämänsä pelin valvomokoneeseen.

Roskaposti on muodostunut merkittäväksi Internet-verkkoon liittyväksi ongelmaksi. Ongelman laajuutta kuvaa roskapostiliikenteen määrä. Spamhaus-projektin (2004) arvion perusteella 62 % Internetin sähköpostiliikenteestä on roskapostia. Kyseessä on siis merkittävä resurssien tuhlaus, kun verkkoliikenne

kuormittuu, jolloin käyttäjät ja ylläpito joutuvat huolehtimaan roskapostin poistamisesta ja lisäksi tärkeää sähköpostia häviää roskapostin sekaan. Automaatiojärjestelmän kannalta roskapostin ei tulisi koskaan olla suoranaisesti ongelmana. Jos näin kuitenkin on, tarvitaan välittömästi korjaavia toimenpiteitä ja koko yrityksen tietoturvaratkaisujen kuntoon saattamista.

Roskapostin perusongelmana on luotettavan autentikoinnin puuttuminen sähköpostiliikenteestä. Jos sähköpostiliikenteen alkuperä pystyttäisiin luotettavasti määrittämään, ei roskapostin lähettämisessä olisi enää mieltä, koska haitalliset viestit pystyttäisiin suodattamaan ja alkuperäinen lähettäjä saisi vastauksena virheviestejä. Valitettavasti kansainvälisen julkisen avaimen (PKI) salausstandardin käyttöönotto ja salausavainten varmentaminen on vaikeaa.

Organisaation sisällä sekä haluttaessa myös yhteistyökumppanien kanssa on kuitenkin mahdollista toteuttaa sähköpostin autentikointi, jolloin voidaan olla varmoja viestin alkuperästä ja sisällöstä. Tarkalleen ottaen turvallinen autentikointi edellyttäisi, että salausavaimet ja -ohjelmat pidettäisiin eristettyinä esimerkiksi toimikortilla. Lisäksi avainten varmentaminen tulisi tehdä oikeaoppisesti. Roskapostiongelmaa pyritään ratkaisemaan myös lainsäädännön avulla, mutta tällöin tulee vastaan lainsäädännön monimutkaisuus ja valvonnan vaikeus.

Jos automaatiojärjestelmässä sallitaan sähköpostin lukeminen, olisi sähköpostin oltava mahdollisimman hyvin suodatettua ennen sen pääsyä automaatiojärjestelmän puolelle. Suodatus voi sisältää paitsi virustarkistuksen ja roskapostisuodatuksen myös liitetiedostojen suodatuksen. Lisäksi sähköpostisovelluksen valinnalla ja rajoituksilla voidaan saavuttaa lisäturvaa. On myös huolehdittava siitä, että sähköpostilla ei voi kuormittaa järjestelmää.

2.5 Palvelunestohyökkäykset

Palvelunestohyökkäyksellä tarkoitetaan tilannetta, jossa tahallisesti tai tahattomasti estetään jonkin tietojärjestelmän tarjoaman palvelun saatavuus. Hajautetulla palvelunestohyökkäyksellä tarkoitetaan tilannetta, jossa palvelun estäminen tapahtuu useasta eri lähteestä käsin.

Tyypillisesti hajautettu palvelunestohyökkäys saadaan aikaan ottamalla Internet-verkosta haltuun heikosti suojattuja tai takaportin sisältäviä tietokoneita. Tietokoneisiin asennetaan ohjelma, joka mahdollistaa tietokoneiden käytön haluttuun tarkoitukseen tietokoneen käyttäjän huomaamatta. Hyökkääjän on helppo saada haltuun tuhansia koneita eri puolelta maailmaa, ja joidenkin arvioiden mukaan on mahdollista ottaa haltuun jopa miljoonia tietokoneita. Nämä ns. zombit käynnistävät palvelunestohyökkäyksen tietomurtautujan käskystä.

Internetissä levinnyt tietokonemato voi käynnistää myös hajautetun palvelunestohyökkäyksen, esimerkkinä W32.Blaster-mato, joka pyrki tekemään hajautetun palvelunestohyökkäyksen Microsoftin sivustoa vastaan. Palvelun-

estohyökkäyksen kohteen on oltava ohjelmoitu matoon sisälle tai madon on haettava jostain tietoja kohteesta. Mato voi myös jättää järjestelmiin takaportin, jolloin hyökkääjät pääsevät käsiksi tartutettuihin koneisiin.

Kriittiset järjestelmät ovat houkuttelevia kohteita palvelunestohyökkäyksille ja hyökkäyksiä on käytetty muun muassa kiristämiseen. Yleisesti voidaan todeta suojautumisesta, että aukoton suojautuminen hyökkäystä vastaan on nykytietämyksen mukaan mahdotonta. Hyökkääjällä on käytännössä rajattomat resurssit hyökkäysten toteuttamiseen, kun taas suojautujalla ei niitä ole.

Hyökkäystilanteen torjunnassa on tärkeää tietojärjestelmien ylläpitohenkilöstön osaaminen sekä varautuminen etukäteen tilanteeseen. Ylläpitohenkilöstö on yleensä se, joka kriisitilanteessa pystyy puuttumaan tilanteeseen. Yhteydet Internetin palveluntarjoajiin sekä viranomaisten yhteistyö on myös tärkeää. Hyökkäystilanteessa pyritään tallentamaan ja tutkimaan Internet-liikenteen sekä eri järjestelmien lokitiedot, pyritään suodattamaan haitallinen tietoliikenne yhteistyössä palveluntarjoajan kanssa ja tehdään mahdollisuuksien mukaan tutkintapyyntö poliisille.

Eräänä ennaltaehkäisevänä suojautumiskeinona julkisen verkon palveluille on segmentointi ja kuormantasaus, jolloin Internetistä tuleva tietoliikenne ohjataan käsiteltäväksi usealle eri tietokoneelle. Tämä auttaa siihen asti, kunnes hyökkääjä pystyy saamaan aikaan vielä suuremman tietoliikennemäärän kuin mitä järjestelmä pystyy käsittelemään. Voidaan myös pyrkiä suojautumaan ottamalla käyttöön vaihtoehtoisia osoitteita siinä vaiheessa, kun hyökkäys on käynnissä. Automaatiojärjestelmissä on lähtökohtana oltava, että Internet-yhteys ei ole käytössä. Tästä huolimatta ainakin Windows-pohjaisissa automaatiojärjestelmissä on varauduttava hajautetun palvelunestoon uhkaan, koska palvelunestohyökkäys voi tulla myös tehdasverkosta.

2.6 Haittaohjelmien torjunta

Toimiva virustorjuntaohjelmisto on tärkeää järjestelmän suojaamiseksi erilaisilta haittaohjelmilta kuten madoilta, viruksilta ja troijanhevosilta. Joskus prosessiympäristön vaatimukset, esimerkiksi käytettäessä kriittistä tosiaikaohjelmistoa, voivat estää virustorjuntaohjelmiston käytön, mutta yleensä virustorjuntaohjelmiston käyttö on kuitenkin mahdollista. Käytettävän virustorjuntaohjelmiston toimivuus automaatiojärjestelmässä on oltava testattu ja ympäristön muuttumisen vuoksi myös testauksen tulee olla jatkuvaa.

Virustorjuntaohjelmiston käytössä on tärkeää huolehtia siitä, että ohjelmisto pidetään ajan tasalla, sillä muutoin ohjelman käytöstä saatava hyöty jää kyseenalaiseksi. Tämä tarkoittaa, että on oltava menetelmä, jolla virustorjuntaohjelmisto pidetään ajan tasalla, ja että tämä menetelmä on myös tietoturvallinen. Virustorjuntaohjelmisto on syytä pitää aktiivisena, ja on huolehdittava siitä, että sitä ei voi tavanomaisen käytön yhteydessä kytkeä pois päältä.

Jotta kaikki tietoturvan perusperiaatteet (vakiointi, testaus, asiantunteva asennus, ks. luku 5.2) toteutuisivat, on myös virustorjuntaohjelmiston sekä ohjelmiston viruskuvaustiedostojen päivitykset testattava asianmukaisesti. Tiedetään tapauksia, joissa virustorjuntaohjelmistojen päivitykset ovat aiheuttaneet häiriöitä. Toisaalta päivitysten nopea käyttöönotto on välillä tarpeen. Näin ollen lopullinen ratkaisu on aina jonkinlainen kompromissi näiden näkökohtien välillä. On kuitenkin tärkeää, että päivitysperiaate toimii käytännössä sovitulla tavalla. Teollisuuslaitoksen omat periaatteet voivat vaikuttaa oleellisesti virustorjuntaohjelmiston viruskuvaustiedostojen päivityksen toteutustapaan.

Myös virustorjuntaohjelmisto joudutaan joskus päivittämään. Tällöin ohjelman oikea toiminta on testattava ennen sen käyttöönottoa ja käyttöönoton ajankohta on varmistettava.

Vakava virhe viruskuvaustiedoston päivityksessä

Vakava virhe Trend Micron virustorjuntaohjelmiston viruskuvaustiedoston päivityksessä aiheutti päivitetyn järjestelmän ylikuormituksen. Trend Micro myönsi, että oli saanut yli 370 000 kyselyä asiakkailtaan ja että häiriöt koskivat yli 650 yritystä (Infoworld, 28. Huhtikuuta, 2005).

Yllä mainitussa tapauksessa oli oleellista, että ongelmia aiheutti virustorjuntaohjelmiston viruskuvausten päivitys eli se toimenpide, jota käytännössä tehdään jatkuvasti.

Haittaohjelmia vastaan voidaan käyttää muitakin menetelmiä kuin varsinaista virustorjuntaohjelmistoa. Käyttöjärjestelmien ja ohjelmistojen tietoturvapäivitysten seuranta ja käyttöönotto estävät tehokkaasti myös virusten leviämistä. Erityisesti kriittisissä järjestelmissä on tärkeää myös alustojen valinta, verkkojen ja järjestelmien suunnittelu, pyrkimys yksinkertaisuuteen, eristäminen, tietoturvasäännöt sekä koulutus osana torjuntaa. Palomuurit auttavat tietoturva-aukkoja hyväksikäyttäviä viruksia vastaan.

Paras suoja haittaohjelmia vastaan saavutetaan, jos virusten aiheuttama uhka otetaan huomioon jo järjestelmien suunnittelun aikana. Tällöin verkon segmentointi, eheystarkistukset, ohjelmisto- ja laitteistoalustojen valinnat, varajärjestelmät, käyttöoikeuksien hallinta sekä tiedon varmennus ja -palautustoiminnot ovat mukana suunnittelussa. Kriittisissä järjestelmissä tulee tarkoin harkita, mitkä osat on tarpeen verkottaa ja millä tavalla.

2.7 Virustorjuntaohjelmien erot

Virustorjuntaohjelmien vertailu on vaikeaa johtuen tuotteiden jatkuvasta vaihtumisesta sekä testaamisessa käytettävien menetelmien vaativuudesta. Jokainen virusnäyte tulisi todistaa oikeaksi ja testikannan olisi oltava kattava

sekä vinoutumaton, jotta se ei suosisi jotakin tiettyä tuotetta. Lisäksi torjuntaohjelmien reagointinopeus ja tukipalvelut ovat nykyisin tärkeä osa tuotteita. Ammattimaisia vertailuja tehdään tällä hetkellä esimerkiksi Hampurin yliopiston virustestikeskuksessa sekä ”Virus Bulletin” -lehdessä. Ei-ammattimaisten lehtien vertailuihin kannattaa suhtautua varauksella, koska lehdillä ei tavallisesti ole resursseja eikä osaamista pätevien vertailujen tekemiseen.

Teollisuusautomaatiossa on otettava huomioon, että automaatiossa käytettävien virustorjuntaohjelmistojen tärkein ominaisuus on niiden toiminnan luotettavuus ja se, että ne häiritsevät mahdollisimman vähän toimintaympäristöään normaaliolosuhteissa. Viruksen tunnistuksen kattavuus voi tähän nähden olla toissijaista.

2.8 Käyttöjärjestelmät ja tietoturva

Käyttöjärjestelmiä valittaessa joudutaan pohtimaan useita erilaisia tekijöitä. Valinnassa on syytä pohtia paitsi lyhyen aikavälin kustannustehokkuutta myös pitkän aikavälin säästöjä. Samoin on otettava huomioon järjestelmän kriittisyys sekä valintojen vaikutukset järjestelmän turvallisuudelle.

Käyttöjärjestelmän yleisyys vaikuttaa toisaalta kustannustehokkaasti siten, että käyttöönottoon tarvittava työmäärä jää vähäiseksi. Alustat on jo testattu ja niistä on karsittu pahimmat virheet. Toisaalta yleisyydellä on se haitallinen puoli, että yleinen järjestelmä on myös hyökkäysten kohteena suosittu ja löydetyille haavoittuvuuksille löytyy nopeasti hyväksikäyttäjiä. Mitä yleisempi alusta on, sitä alttiimpi se on haitallisilla ohjelmilla aikaan saaduille hyökkäyksille ja tietomurroille.

Kysymykseen onko avoin lähdekoodi turvallisempi kuin suljettu lähdekoodi ei ole olemassa yhtä oikeaa vastausta. Paljon riippuu ohjelmistovalmistajien suhtautumisesta tietoturvaan ja reagointinopeudesta. Lähdekoodin tarkastelu mahdollistaa koodin oikeellisuuden toteamisen. Koodista on mahdollista myös karsia toiminnan kannalta turhia osia pois. Toisaalta haavoittuvuuksia on helpompi löytää koodista, jolloin voidaan ajatella, että riski toistaiseksi tuntemattoman tietoturva-aukon hyödyntämiselle on suurempi. Avoimen lähdekoodin järjestelmien ongelmana on se, että ohjelman ylläpitoa ja tietoturvan toteutusta ei ole keskitetty.

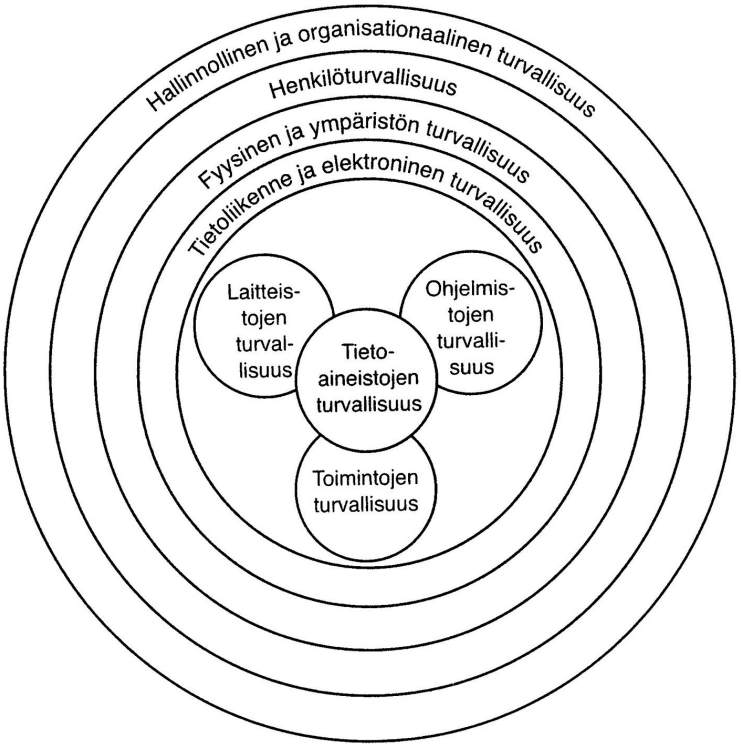
Yhtenä vaihtoehtona on kehittää käyttöjärjestelmä itse tai käyttää teollisuusympäristöihin räätälöityä laitteisto- ja ohjelmistokokoonpanoja. Tällöin tietoturvassa päästään hyvään tulokseen, kun järjestelmistä on karsittu turhat osat pois ja järjestelmä voidaan suunnitella alusta alkaen ympäristöön sopivaksi.

3

Tietoturvan hallinnan periaatteet

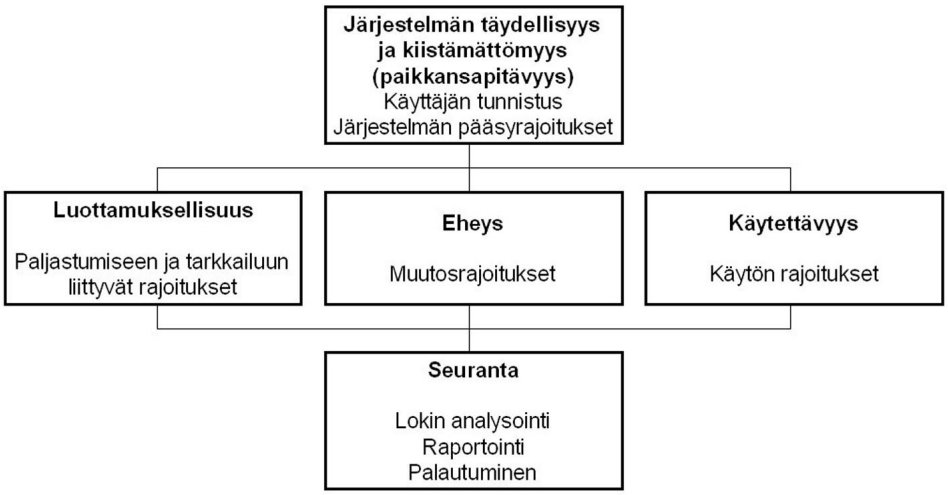
3.1 Tietoturvan käsitteet

Yhteiskunnan perusturvallisuuden edellytyksenä on yhteisöjen ja organisaatioiden tietojen, järjestelmien sekä palvelujen varmistaminen. Tietoturvan tavoitteena on tehokkaan tietojenkäsittelytavan ja asianmukaisen perusturvallisuustason luominen, joiden mukaisesti suojaudutaan yhteiskunnan ja yritysten toimintaa uhkaavilta vahingoilta, kuten käyttäjävirheiltä, tahallisilta vahingonteoilta ja laitteistojen vikaantumisilta sekä ohjelmistovirheiltä [5].



Kuva 4. Tietoaineistojen turvallisuus on kaikkien tietoturvan kerrosten ytimenä [5].

Tietoturvan kehittämisen päätavoite on luoda turvallinen tapa käsitellä tietoja. Tietoturva on käsitteenä laaja eikä sen kattavuutta voi aina määrittää (kuva 4). Tietoturvan osa-alueet voidaan määrittää muun muassa soveltamalla kansainvälisiä standardeja ja yleisiksi muodostuneita käytäntöjä.



Kuva 5. Tietoturvan tavoitteet.

Tietoturvatoiminnan tavoitteena on varmistaa (kuva 5):

- Luottamuksellisuus – tiedot ovat vain käyttöön oikeutettujen saatavissa, eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön.
- Eheys – tiedot ja järjestelmät ovat luotettavia, oikeita ja ajantasaisia, eivätkä ne ole laitteistovikojen tai ohjelmistovirheiden, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.
- Saatavuus – järjestelmien tiedot ja niiden muodostamat palvelut ovat tarvittaessa niihin oikeutettujen käytössä riittävän lyhyen ajan kuluttua. Tietoliikenneympäristössä ja nimenomaan verkkopalvelujen tarjoajan ja käyttäjän kannalta tärkeä peruskäsite on palveluvarmuus.

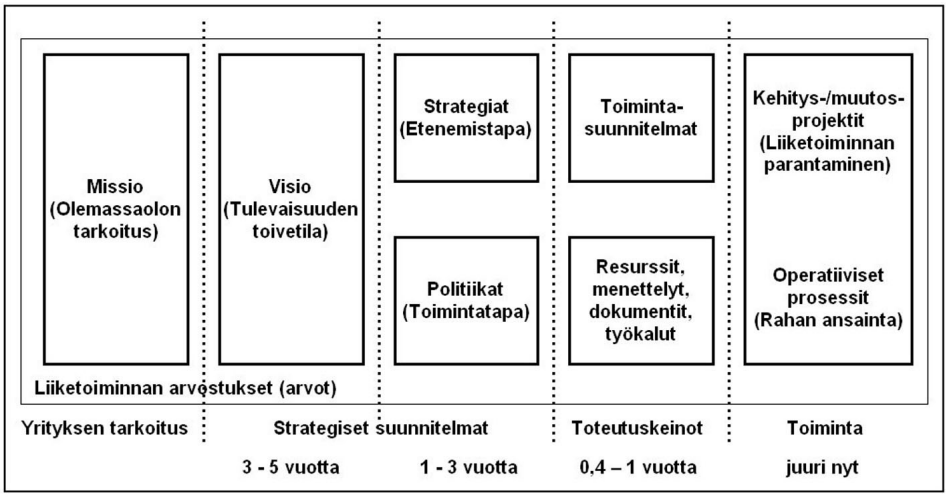
Lisäksi tietojen kiistämättömyyttä tarvitaan aina kun tietojärjestelmän käytössä tehtyjen tapahtumien todentaminen ja niiden tekijöiden paikkansa pitävyys on tärkeää.

3.2 Tietoriskien hallintajärjestelmä

Tietojärjestelmiä, sovelluksia ja tietoliikenneyhteyksiä käytetään työpaikan työasemilta ja työpaikan ulkopuolelta kannettavien tietokoneiden tai kotikoneiden avulla. Sähköpostijärjestelmällä lähetetään ja vastaanotetaan viestejä, kuten teksti-, ohjelma-, kuva- ja äänitiedostoja. Sovellusten ja tietojärjestelmien käytössä haetaan, muokataan, talletetaan ja arkistoidaan dataa tietokantoihin, jotka sijaitsevat tietokoneen kovalevyllä, palvelimilla tai muilla tietovälineillä. Työryhmien käyttöön on olemassa monenlaisia ohjelmistoja,

joiden avulla työryhmän jäsenet voivat olla toisiinsa yhteydessä sijaintipaikasta riippumatta (esimerkiksi puhelin- ja videokonferenssiohjelmistot). Virtuaaliset foorumit ja keskustelupalstat tukevat tiedon kulkua osallistujien kesken. Kaikessa tiedon siirrossa on otettava huomioon tiedon häiriötön kulku ja sen suojaaminen, esimerkiksi Internet-verkon välityksellä kulkevan tiedon suojaaminen ja salaaminen.

Tietoriskien hallinta kattaa tieto-omaisuuteen, tietotekniikan käyttöön ja ratkaisuihin liittyvien riskien kartoittamisen ja analysoinnin sekä tietoturvan osa-alueisiin liittyvät toimintatavat ja tietotekniset ratkaisut. Tietoriskien hallintaan kuuluvat myös tietoturvan johtaminen ja vakuutustoiminta. Kuten kuvassa 6 on esitetty, tietoturvatoimenpiteiden sulauttaminen yrityksen johtamisjärjestelmään ja sen eri osiin luo perustan tietoturvan toimivalle hallinnalle [6]. Hyvä tietoturva syntyy täten toimintaprosessien luonnollisella ja johdetulla toiminnalla, ja tästä vastaa yrityksen johto.

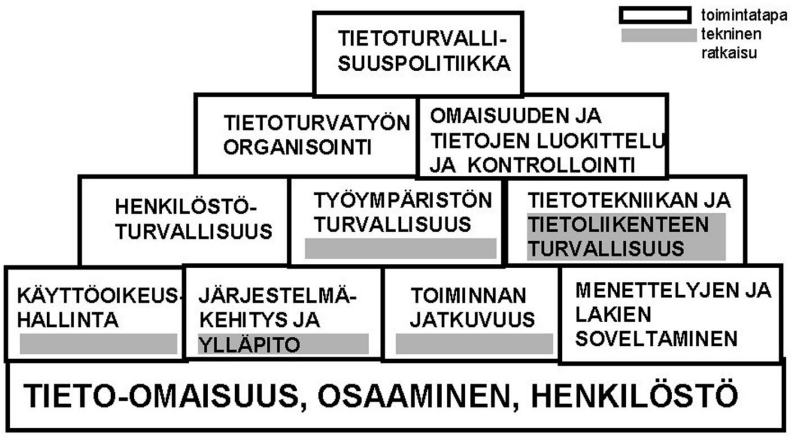


Kuva 6. Tietoturvan liittäminen johtamisjärjestelmään ja sen osiin.

Tietoriskien hallinta ulottuu tietojen sisältöihin, niiden käsittelytapojen riskien tunnistamiseen ja vaikutusten analysointiin. Riskeinä ovat muun muassa tietovuoto, tietojen urkkiminen, tietojen vastikkeeton omiminen ja hyväksikäyttö, luvaton tiedon siirto ja tietojen vakoilu. Lisäksi tietoriskien hallinta ulottuu oleellisesti tietoteknisten ratkaisujen hallintaan liittyvien riskien tunnistamiseen ja vaikutusten analysointiin. Tietoteknisiä riskejä ovat usein tietoverkkojen ja ohjelmistojen käyttöä haittaavat tilanteet, kuten ohjelmistovirheet, tietoverkon toimimattomuus, roskaposti, tietokonevirus ja tietomurto. Riskien analysoinnin perusteella kehitetään ja otetaan käyttöön niitä estäviä, paljastavia ja toimintaa korjaavia toimenpiteitä ja ratkaisuja.

Huolellinen tietojenkäsittely edellyttää tietojärjestelmän käyttöön, sovelluksiin ja tietojärjestelmäympäristön hallintaan soveltuvia valvontamenetelmiä, kuten ohjeita, käytäntöjä, menetelmiä, ohjelmoituja proseduureja ja laitteita.

Tietoturvan edellyttämien keinojen ja ratkaisujen suunnittelussa on syytä noudattaa yleisesti hyväksyttyjä toimintatapoja. Standardi ISO/IEC 17799 [2] on yksi käytetyimmistä standardeista tietoturva-alalla ja se tukee tietoturvan suunnittelua, toteutusta ja toimeenpanoa. Sitä voidaan soveltaa laajalti yrityksen koosta riippumatta. Sen osa-alueet esitetään kuvassa 7.



Kuva 7. Tietoturvan hallintajärjestelmä.

3.3 Liiketoiminnan vaatimukset tietoturvalle

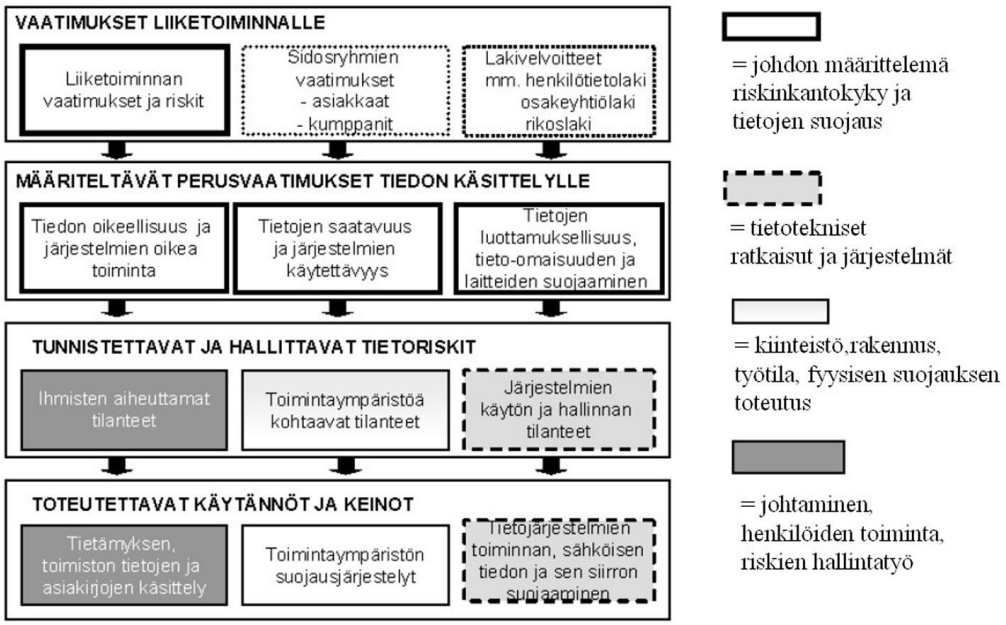
Tietotekninen järjestelmä toteutetaan liiketoiminnan tarpeisiin. Liiketoiminnan riskien hallinta kohdistetaan tulovirtojen varmistamiseen, tulevaisuuden tuotteiden ja palveluiden kehittämiseen sekä omaisuuden suojaamiseen. Tietoriskien näkökulmasta nykyisen liiketoiminnan tulovirtojen varmistaminen edellyttää huolellisuutta käsiteltäessä toiminnassa tarvittavia tietoja ja käytettäessä tietojärjestelmiä. Häiriöiden hallinta on osa liiketoiminnan jatkuvuussuunnittelua.

Tietoturvariskien merkityksen ymmärtäminen ja vaadituista toimenpiteistä huolehtiminen kuuluu kaikkien työntekijöiden jokapäiväiseen toimintaan. Uusien tuotteiden ja palveluiden kehittämisessä on erityisen tärkeää kehitystyön aikaisten kirjallisten tietojen huolellinen käsittely ja se, että suojataan tekijänoikeuksilla toiminnan tuloksena syntyvät tietoaineistot ja muu aineeton omaisuus, kuten patenttien valmistelu ja patentit.

Tiedon käsittely kuvaa yrityksen kulttuuria ja tapaa toimia. Tietoinen tietoriskien hallinta liittyy jokapäiväiseen työntekoon ja ihmisten johtamiseen eli tuotteiden ja palveluiden tarjontaan ja hallintaan sekä näitä tukevien teknisten ratkaisujen hallintaan. Jotta liiketoiminnan jatkuvuus voitaisiin varmistaa, on jo ennakolta varauduttava virhe-, häiriö- ja katastrofitilanteisiin. Toiminta-ohjeet ja varajärjestelyt on suunniteltava liiketoimintayksikkökohtaisesti. Tietojen oikeellisuus, eheys ja aitous on pystyttävä takaamaan ennalta suunnitelluilla järjestelyillä, osapuolten kesken sovituilla menettelyillä ja toiminta-ohjeilla. Tietojen luottamuksellisuus on pystyttävä tarvittaessa osoittamaan myös asiakkaille ja muille sopimuskumppaneille.

Tietoturvatoimintaan vaikuttavat monet lait, kuten osakeyhtiölaki, työsopimuslaki, arvopaperimarkkinalaki, henkilötietolaki ja sähköisen viestinnän tietosuojalaki sekä hyvän hallintotavan ohjeet, kuten esimerkiksi ”Corporate Governance” ja alan standardit. Yritysjohdolla on osakeyhtiölain mukaan vastuu liiketoiminnan jatkuvuuden varmistamisesta, toiminnan turvaamisesta ja valvonnan organisoinnista, johon tietoturvakin kuuluu.

Riskienhallinta ulottuu yrityksen sisäisen toiminnan lisäksi myös yrityksen ulkoistettuun toimintaan ja ulkoiseen yhteistoimintaan. Asiakkaat, kumppanit ja muut sidosryhmät asettavat myös vaatimuksia omaisuutensa ja tietojensa käsittelylle ja säilyttämiselle. Monet lait ja säädökset velvoittavat yritystä huolelliseen tiedon käsittelyyn. Tietojen käsittelytapojen ja -ratkaisujen luominen edellyttää sekä suojattavien yritystietojen että niiden suojaustason määrittämistä (kuva 8).



Kuva 8. Tietoturvavaatimusten määrittely.

3.4 Tietoriskien hallinnan organisointi ja kehittäminen

Tietoriskien hallinta vaatii riskienhallinnan tehtävien täsmentämistä. Liiketoiminnan kriittisyys ja tietojen turvaamisen tarve määrittävät toimintamenettelyjen ja suojausratkaisujen tason. Suojauksen kustannukset suhteutetaan kohteen rahalliseen tai muuhun arvoon.

Käytännön tietoturvatyössä voidaan erottaa seuraavat näkökulmat:

– toimintamallit ja -ohjeet
– tietotekniset ratkaisut
– toimitilasuojauksen tekniset järjestelmät
– sidosryhmäyhteistyössä noudatettavat sopimukset ja toimintaohjeet.

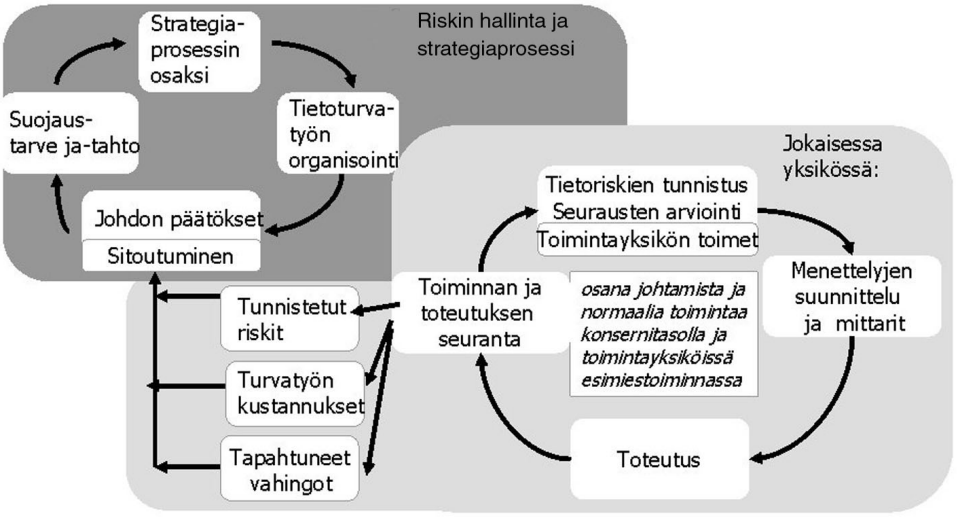
Useissa yrityksissä keskitytään vain laite- ja ohjelmistokohtaisiin tietoturvaratkaisuihin, mutta samanaikaisesti on otettava huomioon henkilöstön, niin teknisten asiantuntijoiden kuin järjestelmien käyttäjien, mahdollisuudet aiheuttaa vahinkoja ja ulkoisten toimittajien mahdolliset virhetoiminnot. Tärkeää on tunnistaa myös se, että teknisten ratkaisujen laatu ja turvallisuus riippuvat osaavien ja tietoturvanäkökulman huomioon ottavien henkilöiden toiminnasta.

Tietoriskien hallinnassa voidaan erottaa tiedon sisältöön ja tietotekniikan hallintaan liittyvät riskit, tiedon huolellinen käsittely sekä tietoteknisen järjestelmän ratkaisut (kuva 9).

Kuva 9. Tietoriskien hallinta liiketoiminnassa.

Osa tietoturvaan liittyvistä asioista ovat luonteeltaan arkaluonteisia ja niiden taitamaton käsittely voi vaikuttaa yrityksen maineeseen ja luotettavuuteen toimijana. Tämän vuoksi yrityksen tietoturvan koordinoinnista ja johtami-

sesta vastaavan henkilön on oltava ammatillisesti pätevä. Tietoturvahenkilöstöllä on oltava riittävät toimivaltuudet erilaisten tilanteiden käsittelyyn. Esimiesten osaamista tarvitaan tietoriskien arvioinnissa ja erityisesti häiriöiden varalle luotavien toimintaohjeiden laatimisessa.



Kuva 10. Tietoriskien hallinnan strateginen ja operatiivinen taso.

3.5 Johdon ja henkilöstön sitoutuminen tietoturvaan

Tietoturvasta vastaavien henkilöiden on saatava yritysjohto sitoutumaan tietoturvaan (kuva 10). Johto voi osoittaa sitoutumisensa muun muassa siten, että se osallistuu tietoturvatilaisuuksiin muun henkilökunnan kanssa viestittäen osallistumisellaan sitä, että tietoturva on tärkeää jokaiselle organisaation jäsenelle. Johdolle tärkeitä asioita ovat esimerkiksi tietoturvallisen toiminnan tai sen puutteen vaikutus yrityskuvaan sekä tietoturvatoimintojen organisointi ja vastuunjako.

Tietoturvapolitiikka on yrityksen ylimmän johdon kannanotto tietoturva-asioihin. On suositeltavaa, että joku yrityksen johtoon kuuluva ottaa päävastuun tietoturvapolitiikan koordinoinnista. Yrityksen tietoturvan hallinta on yrityksen oma sisäinen tehtävä, mutta yrityksen on kyettävä osoittamaan myös sidosryhmilleen, miten asiat ovat hallinnassa. Tällainen luottamuksen synnyttäminen ja sen jatkuva tosiasioihin perustuva vahvistaminen ovat perusedellytyksiä pitkäjänteiselle yhteistoiminnalle.

Johdon ja henkilöstön tietoturvatietoisuuden kehittäminen voidaan aloittaa siitä, että ensin kiinnitetään ihmisten huomio tietoturva-asioihin ja haetaan käytännöille heidän hyväksyntänsä. Näin heidät saadaan oppimaan ja

sisäistämään tietoturvatoimenpiteiden välttämättömyys, jolloin he haluavat käyttää turvallisia ja luotettavia menetelmiä.

Tietoturvan johtamisen kehittämisessä tulee vastata muun muassa seuraaviin kysymyksiin:

- Miten strateginen johtaminen takaa riittävän tietoturvan kehittymisen?
- Miten tietoriskien hallinnan tehtävät on organisoitava?
- Mikä on liiketoimintayksiköiden vetäjien vastuu tietoturvatyössä?
- Millaisissa tilanteissa liiketoiminta häiriintyy?
- Mitkä toiminnot ovat liiketoiminnalle kriittisiä?
- Miten varmistetaan tärkeiden tietojen käyttö häiriötilanteissa?
- Millaisissa tilanteissa tiedot saattavat tuhoutua tai joutua asiattomille?
- Mitkä ulkoiset tahot ovat kiinnostuneita yrityksen liiketoiminnan tiedoista?
- Miten rajataan ja valvotaan järjestelmien käyttöä?
- Miten ohjataan toimintayksikön henkilöitä tunnistamaan toimintaan liittyviä häiriöitä?
- Millaisin säännöin toimitaan liikesuhteissa?
- Miten jatketaan toimintaa esimerkiksi tulipalon aikana ja sen jälkeen?

3.6 Tietoturvan kehittäminen

Tietoturvatoiminnan kehittämisen on oltava järjestelmällistä ja osana yrityskulttuurin kehittymistä. Tietoturvanäkökulmat ja -toimenpiteet on nivottava asiaan liittyviin kriittisiin toimintoihin. Tietoturvan hallinta saavutetaan, kun se on yhdistetty osaksi yrityksen toimintaa ja sen eri prosesseihin (ks. kuva 6). Tämä voidaan tehdä toiminnan tai toimintaprosessin suunnittelu- tai kehittämisvaiheissa. Oleellista on, että ko. toiminnan tai prosessin riskit ja tietoturvatarpeet tiedostetaan, jolloin tarvittavat tietoturvatoimenpiteet saadaan yhdistettyä muuhun toimintaan. Tietoturvan nivominen toimintaprosesseihin kehittää muutoinkin yrityskulttuuria.

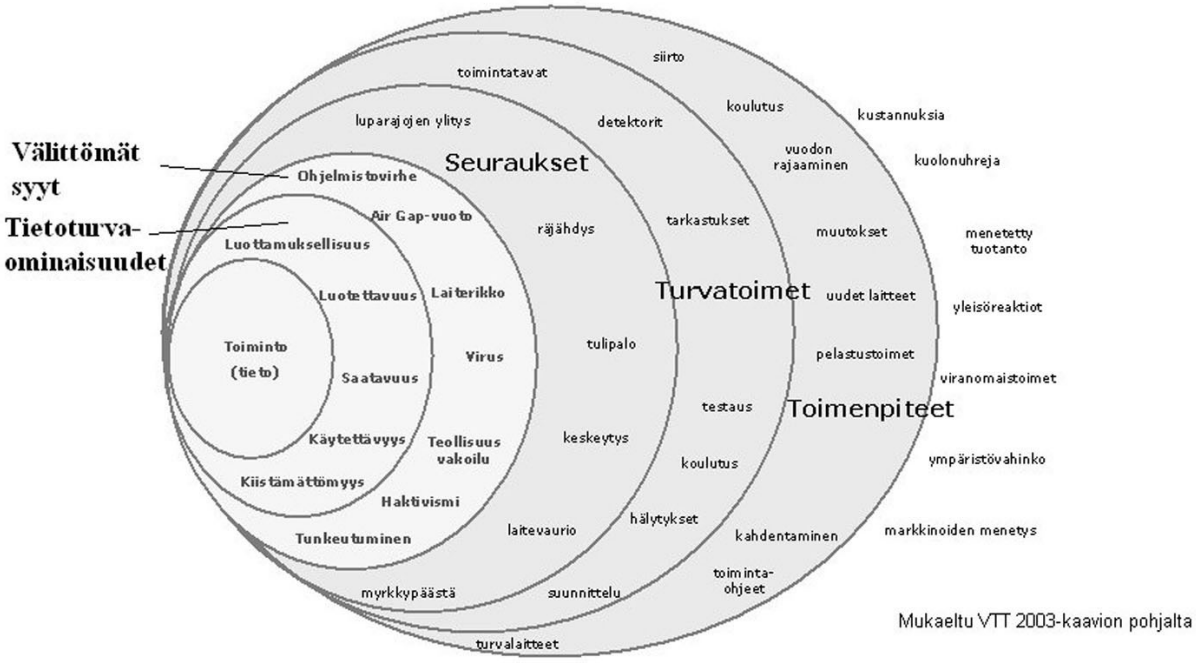
Yrityksen toimintaprosessien kehittämisessä on huomioitava prosessin omistajan ja henkilöresurssien ohella sen asiakkaat, prosessin toiminta, tuotteet ja liitynnät sekä näitä tukeva tietojärjestelmäympäristö. Tärkeää on suunnitella toimintaa tukeva raportointi, seuranta ja mittarit. Toiminnan kehittämiseksi tarvitaan myös seurantaa ja siihen liittyvä palautemenettely.

Keskittyminen vain tekniseen suojaukseen tai riskien kartoittamiseen voi olla hukkainvestointi, mikäli vastuuta tiedon huolellisesta käsittelystä ei työyksiköissä saada yhdistettyä osaksi operatiivisten riskien hallintaa (ks. kuva 9). Tietotekniikan ammattilaiset tai tietoturvan koordinaattori eivät yksin takaa riittävää toimintamallia. On jopa esitetty käsitys on, että tietoturva voitaisiin hoitaa ulkoistetulla ohjelmistoratkaisulla. Tietoriskien hallinta on kuitenkin laaja-alainen yhteistyöprosessi, jossa jokaisen esimiehen ja työn-

tekijän on tunnistettava ne muuttuvat riskit, joiden hallinnasta he ovat itse vastuussa.

3.7 Riskien hallinta

Verkottuneessa toiminnassa riskienhallinnan on katettava yritysten ja toimittajien välinen yhteistoiminta, jossa on kiinnitettävä huomio muun muassa osapuolten vastuiden selkiyttämiseen ja teknisten ratkaisujen käyttöön sekä näistä sopimiseen. Tietoturvavaatimukset sisältyvät toiminnan turvallisuusvaatimuksiin. Kuvassa 11 on esimerkki prosessiteollisuuden tietoturvavaatimuksien määrittämisestä.

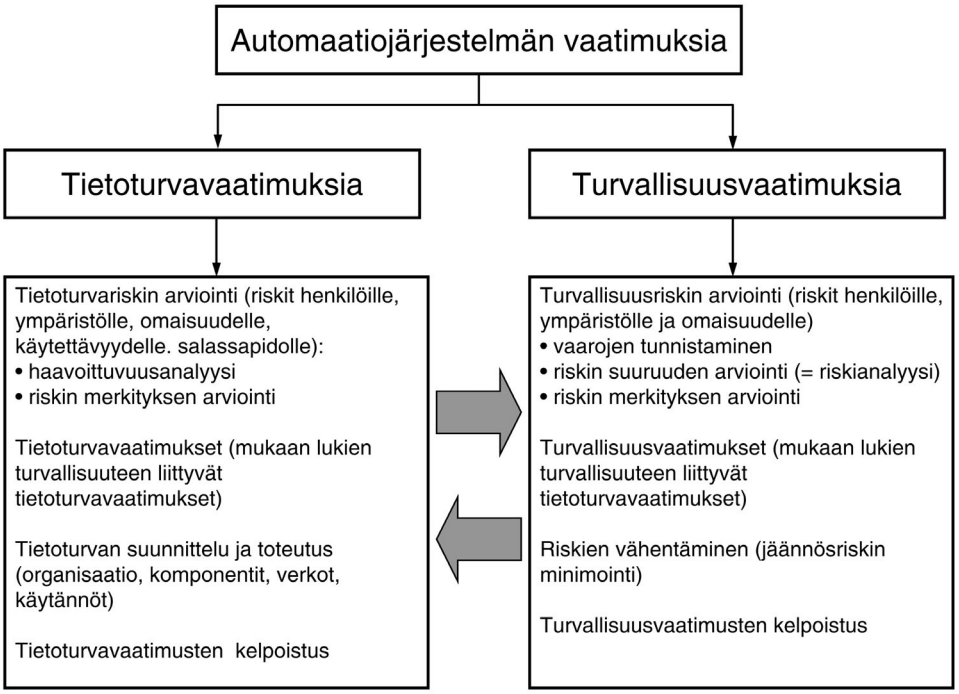


Kuva 11. Tietoturvavaatimukset ovat prosessiteollisuuden turvallisuuden ytimessä. Toteutuessaan tietoturvariskit aiheuttavat samanlaiset seuraukset ja liiketoimintaan kohdistuvat menetykset kuin perinteiset tuotantoprosessin riskit. Myös turvatoimet ja toimenpiteet ovat samanlaisia.

Riskillä tarkoitetaan riskin toteutumisen seurauksena syntyvän haitan ja sen esiintymisten todennäköisyyden funktiota. Automaatioympäristössä haitta tai muu ei-toivottu tapahtuma voi syntyä ohjattavan kohteen virheellisestä toiminnasta tai turvallisuuteen liittyvän ohjausjärjestelmän vikaantumisen seurauksena, esimerkiksi kone toimii vaarallisesti ja aiheuttaa työtapaturman, tai kemiallisen prosessin hallinta menetetään ja syntyy haitallisia päästöjä.

Riskien hallinta on osa turvallisuustoimintaa, jossa tavoitteena on kokonaisturvallisuus. Tietoriskien hallinnan tavoitteena on, että teollisuusautomaation ja siihen liittyvien tietoverkkojen ja niiden komponenttien toiminta täyttää tuotannon käytettävyyden ja laadun kriteerit sekä turvallisuus- ja ympäristövaatimukset. Tietoliikenteen häiriöt ja keskeytykset voivat aiheuttaa häiriöitä turvallisuuskriittisissä toiminnoissa. Ne voivat aiheuttaa myös tuotannon keskeytyksiä vaikuttamalla perus- ja käyttöjärjestelmiin. Näin ollen tietoturvan aiheuttamia ongelmia on tarkasteltava sekä turvallisuuskriittisten järjestelmien että perus- ja käyttöjärjestelmien osalta (ks. kuva 18). Tietoturvaan liittyvillä suojausmenetelmillä voidaan parantaa molempien järjestelmien tietoturvaa, mutta turvallisuuskriittisissä järjestelmissä vaatimustaso on korkeampi ja siksi niissä käytetään monia lisätoimenpiteitä ja tekniikoita turvallisuuden varmistamiseksi. Myös automaatioympäristössä tietoturvaan kuuluu luottamuksellisten tietojen salassapito ja yksityisyyden suoja.

Vaikka automaatiojärjestelmissä toteutuvat haitat johtuvat pääosin muista kuin tietoturvatoimenpiteistä tai -ratkaisuista, se ei saa vaikuttaa siihen, että tietoturvatoimenpiteiden ja -ratkaisujen laatu kärsii tai ne laiminlyödään. Saavutettu toiminnan tila, jossa tietoturva on otettu huomioon, merkitsee sitä, että ollaan tietoisia tietoverkkoihin liittyvistä riskeistä ja ehkäistään niitä ennalta aktiivisilla toimenpiteillä ja ollaan valmiita toimimaan yllättävissä vikatilanteissa.



Kuva 12. Turvallisuusvaatimusten ja tietoturvavaatimusten vuorovaikutus.

Teollisuusautomaation tietoturvan varmistamiseksi voidaan käyttää vastaavia lähestymistapoja kuin muunkin turvallisuuden varmistamiseksi eli järjestelmällistä, toiminnallista ja elinkaaritarkasteluun perustuvaa lähestymistapaa ottaen erityisesti huomioon ihmisen ja teknologian vuorovaikutus. Toiminnallisen turvallisuuden varmistaminen tehdään järjestelmän kaikissa elinkaaren vaiheissa lähtien niiden suunnittelusta, toteutuksesta, kelpuutuksesta ja käyttöönotosta edelleen järjestelmien käyttöön, kunnossapitoon ja järjestelmän muutoksiin. Kaikkien näiden toimintojen hallintaan tarvitaan turvallisuuden hallintajärjestelmää.

3.7.1 Turvallisuusriskit

Riskien kartoituksen ja arvioinnin vaiheita ovat esimerkiksi:
– ei-toivottujen tilanteiden tunnistaminen, kuten vaarat ja uhkat käytettävyydelle, henkilöille, omaisuudelle ja ympäristölle
– ei-toivotun tilanteen toteutumisen haittojen ja seurauksien arviointi
– ei-toivotun tilanteen toteutumisen todennäköisyyden arviointi
– riskien analysointi ja kehittämistoimenpiteiden suunnittelu
– kehittämiskohteista päättäminen ja kehittämisen toteutus sekä niiden valvonta ja seuranta.

Ei-toivottujen tilanteiden todennäköisyyttä ja seurauksien merkitystä voidaan arvioida esimerkiksi asteikolla: vähäinen – siedettävä – kohtalainen – merkittävä – sietämätön (kuva 13). Kukin arvioitu ei-toivottu tilanne sijoitetaan arvioituun kohtaan, jolloin tarkempi riskien analysointi ja kehittämistoimenpiteiden suunnittelu voidaan keskittää ensisijaisesti pahimpiin ei-toivottuihin tilanteisiin.

Ei-toivutun tapahtuman todennäköisyyksien luokittelu:
- Epätodennäköinen: haitta, joka esiintyy satunnaisesti ja epäsäännöllisesti.
- Todennäköinen: haitta, joka esiintyy toistuvasti, mutta ei säännöllisesti.
- Erittäin todennäköinen: haitta, joka esiintyy jatkuvasti ja säännöllisesti.

Ei-toivotun tapahtuman seurausten vakavuuden arviointi:
- Lievästi haitallinen: ohimenevä sairaus tai haitta, joka ei aiheuta pysyvää vahinkoa, palautuva lievä ympäristövahinko tai pieni omaisuusvahinko tai lyhyt toiminnan keskeytyminen.
- Haitallinen: suurempia tai pitkäkestoisempia vammoja, esimerkiksi palovammoja tai murtumia, tai pysyviä, vaikutukseltaan lieviä haittoja, esimerkiksi kuulon heikkeneminen tai astmaa, merkittävä ympäristö- tai omaisuusvahinko tai pitkällinen toiminnan keskeytyminen.
- Erittäin haitallinen: pysyviä ja palautumattomia vammoja, esimerkiksi raajojen menetys tai työperäinen syöpä, palautumaton suuri ympäristövahinko, liiketaloutta horjuttava omaisuusvahinko tai toiminnan loppuminen.

Seuraukset / *Todennäköisyys*	*Lievästi haitallinen*	*Haitallinen*	*Erittäin haitallinen*
Epätodennäköinen	VÄHÄINEN RISKI	SIEDETTÄVÄ RISKI	KOHTALAINEN RISKI
Todennäköinen	SIEDETTÄVÄ RISKI	KOHTALAINEN RISKI	MERKITTÄVÄ RISKI
Erittäin todennäköinen	KOHTALAINEN RISKI	MERKITTÄVÄ RISKI	**SIETÄMÄTÖN RISKI**

Kuva 13. Esimerkki riskien luokittelusta ja riskitekijöiden yhdistämisestä.

Turvallisuuteen liittyvien järjestelmien riskin arvioinnin periaatteita ja menetelmiä esitetään kattostandardin IEC 61508 osassa 5 [7]. Prosessiteollisuuden riskin arvioinnista on laadittu standardi IEC 61511-3 [8] ja konejärjestelmien riskin arvioinnista standardi ISO 14121 [9]. Lisäksi useilla muilla aloilla on standardeja tuotekohtaisista riskinarvioinnin menetelmistä, mutta niissäkään ei toistaiseksi ole erikseen käsitelty tietoturvan puutteista aiheutuvia riskejä.

Sekä turvallisuusriskien että tietoturvariskien kartoittamiseen ja arviointiin sopivia menetelmiä ovat muun muassa:

– viottumis- ja vaikutusanalyysi Failure Mode and Effect Analysis (FMEA) [10] ja sen ohjelmistot mukaan ottava menetelmä Software FMEA (SW-FMEA) [11]
– vikapuuanalyysi Fault Tree Analysis (FTA) [12]
– poikkeamatarkastelu Hazard and Operability Study (HAZOP) [13]
– As Low As Reasonably Practicable (ALARP) [14].

3.7.2 Tietoriskit ja haavoittuvuuksien analysointi

Tietoriskien kartoittaminen sisältää tavallisesti tietojärjestelmien, sovellusten ja laitteiden haavoittuvuuksien ja niiden puutteiden tai virheiden tunnistamisen. Esimerkiksi ohjelmistossa voi olla haavoittuvuus, joka mahdollistaa järjestelmän väärinkäytön. Haavoittuvuus -termiä käytetään toisinaan tietoturva-aukon merkityksessä. Haavoittuvuusanalyysit voidaan tehdä laite- ja ohjelmistokohtaisesti tai uhkakohtaisesti, mutta molempien tulisi johtaa samaan tulokseen.

Usein vaarallisimmat tilanteet syntyvät siten, että tekniset ongelmat ja inhimilliset virheet esiintyvät samanaikaisesti. Tämä on erityisen tärkeää tietoturvariskien tunnistamisessa ja arvioinnissa, koska riskin arvioinnissa teknisten häiriöiden tarkastelun (FMEA) lisäksi tietojärjestelmiin tunkeutumisella on erittäin suuri merkitys. Vikapuu-menetelmässä (FTA) voidaan käsitellä yhtä aikaa sekä teknisiä että inhimillisiä tekijöitä. Toimintovirheanalyysillä voidaan vielä tarkemmin kartoittaa inhimillisiä tekijöitä. Vikapuun huipputapahtumaksi valitaan riskin arvioinnin perusteella määritetyt pahimmat tilanteet, esimerkiksi vaaraa aiheuttavat viiveet, palvelun esto, parametrien tai konfiguraation muutokset ym., jotka aiheuttavat toteutuessaan vaaratilanteen, omaisuusvahingon, ympäristövahingon tai muun merkittävän toiminnan keskeytyksen.

Tietoriskien kartoituksen avulla saadaan selville toimintaa uhkaavat tilanteet, suojattavat kohteet ja niiden tärkeys toiminnalle. Kartoituksessa hyödynnetään järjestelmädokumentaatiota ja tarkistetaan muun muassa dokumentoimattomat verkkoyhteydet, kuten modeemit ja langattomat yhteydet. Kaikki järjestelmään tehdyt muutokset, lisäykset ja väliaikaiset yhteydet olisi testattava samalla tarkkuudella kuin muutkin järjestelmän osat. Lisäksi on huolehdittava, että väliaikaiset yhteydet poistetaan kun niitä ei enää tarvita.

Suojattavia kohteita ovat tietokannat ja dokumentaatiot sekä laitteet. Automaatioympäristössä suojattavat tiedot ovat sähköisinä ja paperiversioina. Suojattavia tietoja ovat muun muassa ohjausalgoritmit, tuotantoprosessin muuttujat, asetusarvot, säätöön liittyvät tiedot, salasanat, tiedostojen nimet, isäntäkoneiden nimet, valvonnan konfiguraatiot sekä prosessidokumentaatio, esimerkiksi järjestelmiä koskevat toimituslistat. Suojattavia laitteita ovat muun muassa

– operaattorien valvonta-asemat
– työaseman fyysiset liityntäportit
– tuotantoprosessin ohjausjärjestelmät ja ohjausyksiköt
– ohjelmoitavat kenttälaitteet
– Internet-työasema sekä verkkolaitteet, esimerkiksi kytkimet ja reitittimet.

Toimintaa uhkaavien tilanteiden mahdolliset seuraukset on arvioitava. Uhkatilanteet voivat toteutuessaan aiheuttaa haittaa tuotantoprosessille tai muulle järjestelmälle, esimerkiksi aiheuttaa vakavan vahingon tärkeälle laitteelle, jolloin laiterikko saattaa aiheuttaa normaalia pidemmän tuotannon keskeyttämisen. Tilanteen korjaaminen aiheuttaa selvitys- ja korjauskustannuksia. Arviointi sisältää useita vaiheita eri tapahtumien ja kohteiden kartoittamisessa. Seuraavassa esitetään esimerkinomainen etenemistapa:

- Toiminnan uhkatilanteiden ja suojattavien kohteiden tunnistaminen ja priorisointi:
  – Mitkä tilanteet uhkaavat toimintaa?
  – Miten kohteet priorisoidaan toiminnan jatkuvuuden kannalta?
  – Mitä tietoturvavaatimuksia sidosryhmät esittävät?

- Analysointi:
  - Millaista vahinkoa todennäköisimmät tilanteet aiheuttavat toiminnalle?
  - Mitkä kontrollit suojaavat kohteita ja niiden toimintaa?
  - Mitä kontrolleja täytyy lisätä? Mitä kontrolleja pitää kehittää?

- Tietoturvatoiminnan arviointi:
  - Miten tietoturvavaatimuksia tarkennetaan?
  - Miten kehittäminen organisoidaan?
  - Miten toimintaohjeista tiedotetaan? Miten toimintaohjeiden noudattamista seurataan?
  - Miten eri asiantuntijatoimia arvioidaan muun muassa ongelmien-, muutosten- ja konfiguraation hallinnan yhteydessä?

Tuloksia analysoimalla määritetään korjaavat toimenpiteet, jotka priorisoidaan, jonka jälkeen tärkeimmät niistä organisoidaan kehittämishankkeiksi.

3.8 Tietoturvavaatimusten hallinta

Järjestelmän tietoturvavaatimukset ovat osa kokonaisuutta, ja niitä hallitaan periaatteessa samalla tavalla kuin muitakin vaatimuksia järjestelmän hankinta-, käyttö- ja ylläpitovaiheissa. Käytännössä vielä nykyisinkin tietoturvavaatimukset on usein jätetty kokonaan määrittämättä.

Tietoturvavaatimusten hallinta on avainasemassa tietoturvan hallinnassa. Vaatimukset ohjaavat toimenpiteitä ja toimivat myös referenssinä, kun halutaan seurata tai mitata miten hyvin tietoturvan hallinta toteutuu. On oleellista, että tietoturva-asioita analysoidaan jo elinkaaren varhaisissa vaiheissa.

Systemaattinen tietoturvavaatimusten hallinta auttaa järjestelmän suunnittelussa luomaan tietoturvallisen järjestelmän. Tietoturvariskien hallintakäytännöt on määritettävä ja niiden on oltava mukana järjestelmän kehittämis-, käyttöönotto- ja käyttövaiheissa. Tietoturvavaatimusten määrityksessä on otettava huomioon järjestelmän elinkaaren kaikki vaiheet. Tässä suhteessa kriittisiä voivat olla esimerkiksi järjestelmän tai sen sisältämän ohjelmiston käyttöönotto-, konfigurointi- ja päivitysvaiheet.

Ennen järjestelmän hankintaa ja toteutusta järjestelmän keskeisille tietoturvaominaisuuksille, kuten luottamuksellisuus, saatavuus, eheys, on määritettävä toiminnalliset suorituskykyvaatimukset sekä reunaehdot, joista järjestelmän suunnittelija johtaa suunnitteluratkaisut järjestelmän eri tasoille. Järjestelmän rakentamis- ja käyttöönottovaiheissa tietoturvavaatimukset todennetaan ja lopuksi järjestelmä kelpuutetaan näiden vaatimusten perusteella.

Liitteessä 1 esitetään tarkemmin vaatimustenhallinnan (Requirements Management) systemaattinen lähestymistapa, jolla tunnistetaan, määritetään, organisoidaan ja dokumentoidaan järjestelmälle asetettavat vaatimukset, ylläpidetään niitä sekä hallitaan vaatimustietoja ja niiden muutoksia järjestelmän tai toiminnan koko elinkaaren ajan.

3.9 Teollisuusautomaation palveluliiketoiminta

3.9.1 Palveluliiketoiminnan kehittyminen

Automaatioalan liiketoiminnassa on viimeisen viiden vuoden aikana ollut nähtävissä selkeä trendi siirtymisestä palveluliiketoimintaan, jossa pelkkien automaatiolaitteiden ja -järjestelmien myyminen on vaihtumassa elinkaariajattelun mukaiseen käytettävyyden toimittamiseen. Entistä harvempien erityisasiantuntijoiden sekä asiantuntijakeskusten on saatava yhä tosiaikaisempaa tietoa käytettävyyssopimusten piiriin kuuluvista laitteista ja järjestelmistä. Asiantuntijoiden päätelaite- sekä tietoliikenneyhteyksien valikoima on myös kasvamassa.

Nähtävissä on käytettävyystoimittajien palvelujen laajentuminen koskemaan muidenkin laite- ja järjestelmävalmistajien toimitusten hallintaa. Käytettävyyden ostot tullaan tulevaisuudessa kilpailuttamaan erikseen automaatiotoimitusten kanssa. Toimittajien kilpailussa tulee voittaja olemaan se käytettävyysverkon hallitsija, jonka asiantuntijat saavat kustannustehokkaimmin oikean informaation oikeaan aikaan ja oikeaan paikkaan ilman tietoturvariskejä, ja joka voi osoittaa, että asiakkaiden tiedot eivät pääse missään vaiheessa vuotamaan ei-toivotuille tahoille.

Esimerkiksi sähkönjakelun ja -kaupan aloilla, joilla ulkoistaminen on yleistä, melkein mikä tahansa voi olla ulkoistettua:

- energian kulutuksen ja sähkön laadun mittaustietojen keruu
- kulutustietojen ja sähkönlaatutietojen analysointi ja jatkojalostus
- sähkömarkkinoiden ennustaminen
- verkon rakennus ja korjaus
- vikapartiot
- päivystys
- valvomot
- verkon hallinta
- automaatiojärjestelmä
- laskutus.

Uusi palveluliiketoiminta tuo mahdollisuuksia myös asiakkaalle. Esimerkkinä voidaan mainita metsäkoneurakoitsijan tarve nähdä omien metsäkoneiden tilatietoja. Tälle teollisuusalalle on tyypillistä erittäin hajautettu automaatiojärjestelmä, jossa tuotantolaitteet ovat liikkuvia ja maantieteellisesti

hajautettuja. Automaatiojärjestelmän toimittaja (metsäkonetoimittaja) voi tarjota tilatietoja oman käytettävyysverkkonsa kautta ja myydä tilatietopalvelun osana käytettävyyssopimusta.

Palveluliiketoiminnan hyödyntäminen näkyy myös asiakkaille erilaisten palvelujen ulkoistamisena. Kohteena ovat erityisesti IT-palvelut, kuten tietotekniset laitteistot, joihin automaatiojärjestelmätkin osittain kuuluvat, sekä näiden hallintapalvelut. Automaation käytettävyyden ostaminen on asiakkaan näkökulmasta katsoen automaatiojärjestelmän osittaista ulkoistamista. Myös tietoturvatoimintojen ulkoistamista suunnitellaan. Tämä muodostaa suuren haasteen eri palvelutoimittajien yhteistyölle, erityisesti testausten järjestämisestä tietoturvapäivitysten aiheuttamien katkojen eliminoimiseksi sekä vastuiden selkeyttämiseksi.

Palveluliiketoimintaan liittyy usein kiinteästi kolmansien osapuolten tekemien ohjelmistokomponenttien käyttö. Tällaisten komponenttien käyttö voi aiheuttaa tietoturvauhkia ja ne mahdollistavat liityntöjä, joiden tietoturvatasoa ei tunneta. Uusien ohjelmistokomponenttien käytössä ovat uhkana mahdolliset ohjelmointivirheet ja vääränlaiset kytkennät. Uutena haasteena ovat vastuiden määrittäminen sekä ongelmat osapuolten välisessä kommunikoinnissa. Myös käytetyt ohjelmistokehitys- ja tukijärjestelmät sisältävät uhkia, jotka liittyvät tietoturvan kannalta heikkoihin ohjelmointikieliin ja huonoihin kehitystyökaluihin.

Siirryttäessä käyttämään uusia tai päivitettäessä olemassa olevia järjestelmiä niihin liittyvät tietoturvauhkat ovat merkittäviä. Myös järjestelmien käytöstä poistamiseen liittyy uhkia, kuten järjestelmän osien liian aikainen alasajo tai piilossa oleva riippuvuus vanhasta järjestelmästä tai versiosta, joka ei enää ole aktiivisena [15].

3.9.2 Palvelujen yhdentyminen

Tietoturvan kannalta palvelujen yhdentymisen (digitaalinen konvergenssi) pääongelmana voidaan pitää integroituvien verkkojen erilaista peruslaatua eli palvelujen yhdentyminen korostaa avoimen verkon käyttöä, esimerkiksi Internet-verkko, kun taas yhdentymisen myötä siihen liittyvät perinteisesti suljetut järjestelmät, kuten tuotannonohjausjärjestelmät, ovat olleet yksittäisen organisaation hallussa. Integroituvien järjestelmien tietoturvan hallinta on siis lähtökohtaisesti eri tasolla.

Palvelujen yhdentymisen myötä avoimiin verkkoihin verkottuneet teollisuusautomaatiojärjestelmät voivat olla haluttuja hyökkäyskohteita Internet-verkosta lähtöisin oleville hyökkäyksille siinä missä muutkin verkon järjestelmät.

Palveluja tarjoava operaattoriverkko alkaa saada enemmän avoimen Internet-verkon piirteitä, poiketen yrityksen sisäverkoista, joissa tietoliikenne on tarkoin määritettyä. Operaattoriverkot perivät tällöin myös Internet-verkkojen uhkia, ja niiden palvelimia uhkaa epäkelpo ja haitallinen verkkoliikenne.

3.9.3 Tekniikan ja tietotekniikkapalvelujen hankinta

Tietotekniikan kehittyminen ja teollisuusautomaation verkottuminen osaksi tehdasverkkoa on saanut aikaan tilanteen, jossa automaatiojärjestelmää hankittaessa on oltava tarkoin selvillä tarvittavista tietoturvatoimenpiteistä ja -ratkaisuista. Tämä vaatii ymmärrystä automaatiojärjestelmien erityisvaatimuksista varsinkin, kun käsitellään niiden liittämistä tehdasverkkoon.

Käytännön toiminnassa on tullut esiin, että kaikkia tietotekniikkaan ja tietoturvaan liittyviä asioita ei useinkaan sovita. Tämä voi olla vastuiden kannalta ongelmallista, ja siksi sopimukset on tehtävä riittävän kattaviksi. Teollisuusautomaatiotoimituksista sovittaessa on selvennettävä ainakin

– osapuolten vastuut
– toimintaprosessit, tiedotus ja tiedonvaihto
– verkkotopologia ja liityntä tehdas(toimisto)verkkoon
– virustorjuntaohjelmisto ja sen viruskuvaustiedostojen päivitykset
– tietoturvapäivitykset
– kovennus (hardenointi)
– tietoliikenteen dokumentointi
– käyttäjätunnukset ja salasanapolitiikka
– yrityksen ja toimittajan väliset tietoliikenneyhteydet (etäyhteydet)
– varmuuskopiot ja palautus
– yrityksen muiden IT ratkaisujen käyttö
– langaton liikenne (esimerkiksi WLAN).

Edellä esitetyt seikat on käytävä läpi yhdessä toimittajan kanssa ja kirjattava sopimukseen. Seuraavassa luvussa ja liitteessä 9 käsitellään sopimusasioita laajemmin.

3.10 Sopimukset

Sopimuksia tehdään eri tavoin. Usein tehdään asiakirja nimeltä ”Sopimus”, jonka osapuolet allekirjoittavat. Toisaalta kaupankäynnissä ei aina tarvitse luoda erillistä sopimusasiakirjaa, vaan sopimus syntyy asiakirjaketjun tai puhelun seurauksena. Tämä voi tapahtua siten, että tehdään tarjous, jonka vastapuoli hyväksyy tai siten, että tilauksen jälkeen lähetetään tilausvahvistus ja tilattu tavara tai palvelu. Myös sähköpostikirjeenvaihdossa syntynyt sopimus on pätevä. Eri asia on, mitä riitatilanteessa pystytään näyttämään sovitun tai katsotaanko esimerkiksi jommankumman osapuolen lähettämien yleisten sopimusehtojen tulleen osaksi sopimusta.

Sopimusvapauden periaatteen mukaisesti elinkeinonharjoittajat voivat varsin vapaasti sopia kaupan ehdoista. Irtaimen tavaran kauppaan sovelletaan Suomessa kauppalakia ja pohjoismaiden ulkopuoliseen kauppaan usein kansainvälistä kauppalakia. Jälkimmäinen perustuu kansainväliseen CISG-

sopimukseen [16]. Osapuolten välinen sopimus on ensisijainen, mutta kauppalaki ja joskus myös kauppatapa, toimivat oikeusohjeina, jos jostain asiasta ei ole sovittu. Myyjä ja ostaja haluavat usein täsmentää kauppalain velvoitteita ja menettelytapanormeja, kuten määräyksiä ostajan velvollisuuksista reklamoida virheestä ”kohtuullisessa ajassa siitä, kun hän on tai hänen olisi pitänyt havaita virhe”.

Sopimusten avulla luodaan pelisäännöt yritysten väliselle kaupankäynnille eli tavaroiden ja palveluiden ostamiselle ja myymiselle. Sopimus määrittelee kustannusten, tehtävien ja vastuiden jaon kaupan osapuolten kesken.

3.10.1 Sopimusriskien hallinta

Keskeisimmät sopimuksiin liittyvät riskit ovat [17]:

- Sopimusta ei täytetä lainkaan.
- Sopimusta ei täytetä oikeaan aikaan (viivästys).
- Sopimus täytetään puutteellisesti tai virheellisesti.
- Sopimuksen kohde aiheuttaa vahinkoa tilaajalle tai kolmannelle osapuolelle.
- Sopimuksen täyttäminen tulee odotettua kalliimmaksi.

Sopimuksissa sovitaan muun muassa vastuiden jaosta. Tämä voi tarkoittaa esimerkiksi toimittajan vastuun rajoittamista kaupan kohteen tai palvelun aiheuttaessa tilaajalle omaisuusvahingon tai toiminnan keskeytyksen. Samoin voidaan sopia seuraamukset toimituksen viivästymisen varalta ja tässä yhteydessä rajata vastuu tiettyyn rahamäärään sopimussakkolausekkeen avulla.

Sopimukset on kuitenkin syytä tehdä kirjallisina ja kattavina, koska suullisen tai puutteellisen sopimuksen ristiriitoja voi olla vaikea ratkaista. Sopimusta tehdessä kannattaa kiinnittää huomiota kieleen ja sanamuotoon sekä välttää monimerkityksisiä tai tulkinnanvaraisia sanoja ja ilmaisuja. Sopimuksen kohde on yksilöitävä mahdollisimman tarkasti ja sopijapuolen kanssa on syytä keskustella vaikeaksikin koetuista asioista. Paras sopimus syntyy, kun molempien osapuolten edut otetaan huomioon tasavertaisesti. Esimerkiksi vastuurajoitusten tulisi olla kohtuullisia molemmille osapuolille.

Sopimukseen sovellettava laki ja mahdollisen riidan ratkaisutapa (tuomioistuin – välimiesmenettely – sovintomenettely) on syytä sopia. Tärkeää on käyttää tilanteeseen sopivia yleisiä sopimusehtoja sekä osata käyttää niitä siten, että ne saadaan osaksi sopimusta.

3.10.2 Sopimusrikkomuksen seurauksista

Hyvin yleisellä tasolla voidaan todeta, että myyjällä on erittäin pitkälle menevä velvollisuus korvata ostajalle kaupan johdosta aiheutuva vahinko. Myyjällä on lain mukaan velvollisuus korvata välittömien kustannusten lisäksi välil-

liset vahingot, mikäli tuottamus havaitaan myyjän puolella. Tämä tarkoittaa muun muassa vastuuta alihankkijoiden toimista. Välillisen vahingon tyyppiesimerkki on kauppavoiton menettäminen, joka aiheutuu helposti tilaajalle toimittajan virheen johdosta.

Mikäli sopimuksen kohteena on ensisijaisesti palvelu, ei kauppalaki sovellu siihen. Tällöinkin vastuu sopimusrikkomustilanteissa määräytyy ensisijaisesti solmitun sopimuksen perusteella. Jos sopimus ei sisällä määräyksiä esimerkiksi virheen tai viivästyksen seurauksista, ratkaistaan kysymys nk. yleisten sopimusoikeudellisten periaatteiden mukaan. Pääsääntönä on täyden korvauksen periaate, joka tarkoittaa, että vahingonkärsinyt saatetaan asemaan, jossa hän olisi, jos vahinkoa ei olisi sattunut. Vastuu edellyttää yleensä huolimattomuutta tai laiminlyöntiä. Palveluntarjoaja vastaa myös käyttämiensä avustajien toimista, vaikka tuottamusta ei voitaisikaan osoittaa hänen viakseen.

3.11 Tietoturvatilan todentaminen

Tietoturvan hallinta helpottuu, jos voidaan kehittää sopivia mittareita tarjoamaan näyttöä hallittavan järjestelmän tietoturvasta. Myös järjestelmän toiminnan tietoturvaa voidaan testata sen todellisessa käyttöympäristössä. Tietoteknisten tuotteiden tietoturvan sertifiointiin on käytettävissä standardisoituja menetelmiä.

3.11.1 Tietoturvatason arviointi

Liiketoiminta- ja tietoturvanhallintaprosessien tietoturvan arvioimisessa voidaan käyttää tietoturvamittareita. Mittaamisessa voidaan käyttää apuna standardeja, kuten esimerkiksi järjestelmän tietoturvahallinnan ohjelmiston suorituskyvyn mallistandardi ISO/IEC 21827 [18]. Mittaustulosten avulla voidaan reagoida mahdollisiin puutteisiin ja varmistaa, että vaadittu tietoturvataso saavutetaan. Näitä mittareita voidaan kutsua tietoturvamittareiksi, joilla voidaan mitata esimerkiksi teollisuuden liiketoimintaprosesessien tai automaatiojärjestelmien tietoturvan hallintaa.

Yrityksissä voidaan soveltaa erilaisia tietoturvan hallinnan arviointi- ja mittaustapoja. Tarkoituksena on tuottaa tietoa tietoturvan tilasta ja puutteista sekä tukea tietoturvan kehittämistä. Verkottuneessa ja integroidussa toiminnassa, on tietoturvan hallintaa arvioitava myös ostettaessa palveluita. Tietotekniikkatoimittajille tietoturvan mittaaminen voi tuoda kilpailukykyä. Mittaustulokset osoittavat myös yrityksen sisäisen tietoturvatoiminnan laatua.

Järjestelmältä vaadittavan tietoturvatason tai tietoturvan suorituskyvyn on oltava vähintään tietoturvan vaatimusmäärittelyn mukainen. Tietoturvavaatimukset riippuvat suuressa määrin järjestelmään liittyvistä uhkista ja

niiden todennäköisyyksistä. Niiden perusteella voidaan määrittää asteikko tietoturvan mittaamiselle. Tietoturvan mittarit on määritettävä kohteen tietoturvavaatimusten mukaisesti, joten erilaisissa toimintaympäristöissä mittarit ovat erilaisia. Näin ollen tietyn tietoturvakohteen arviointi asteikolla 1–5 ei yksittäisenä kuvaa mitään, vaan arvioitavat kohteet ja mittarit on suunniteltava kuhunkin toimintaan soveltaen.

Yrityksen tai sen osaston tietoturvaa voidaan arvioida tietoturvatarkastuksella (auditointi), joka tavallisesti perustuu tarkastajan (usein konsulttiyritys) tätä tarkoitusta varten kehittämiin mittareihin. Tarkastuksella selvitetään tarkastettavan kohteen toiminta ja vaatimustenmukaisuus. Vaatimuksia voivat olla esimerkiksi oikeellisuusvaatimukset, säädösten ja sopimusten vaatimukset, taloudellisuuden, tuloksellisuuden ja sidosryhmien vaatimukset. Tarkastavan tahon riippumattomuus on tarpeen, koska tarkastuksen tulokset voivat vaikuttaa eri tahojen vastuisiin.

Tietoturvatarkastuksen tulokset kootaan yhteenvedoksi esimerkiksi tietoturvan eri osa-alueiden mukaisesti. Kunnollinen yhteenveto sisältää myös parannusehdotuksia. Tietoturvatarkastuksen tulokset kuvaavat järjestelmän nykytilaa. Käytännössä tietoturvan tila ei kuitenkaan ole vakaa, koska muun muassa toimintajärjestelmät, tietoturvaratkaisut ja -prosessit muuttuvat lyhyessäkin ajassa. Tietoturva on monien tekijöiden summa, joka vaihtelee järjestelmän koko elinkaaren ajan. Prosessimuotoisuus edellyttää ennalta määritettyjä toimintatapoja, joita voidaan tietoturvatarkastuksessa toistaa ja parantaa.

Irralliset tietoturvatarkastukset eivät riitä tietoturvan arviointiin ja on suositeltavaa, että kehitetään tietoturvan mittausprosesseja, jotka on räätälöity tarpeen mukaan. Tietoturvan arvioinnin on oltava jatkuvaa, prosessimuotoista ja muuttuviin tilanteisiin reagoivaa. Tietoturvan hallinnan arvioinnin on oltava kattavaa ja siihen tulisi kuulua esimerkiksi tunkeutumisen estäminen ja toimintaprosessien tietoturvan arviointi. Tuotteen tietoturvaan vaikuttaa paitsi itse tuotteen ominaisuudet myös sen käyttöympäristö, käyttäjät sekä ulkopuoliset tekijät.

3.11.2 Tietoturvan mittaaminen

Tietoturvatuotteen tai -järjestelmän toiminnallisuus voi perustua erilaisille tietoturvamittareille, esimerkkinä tunkeutumisen havaitsemisjärjestelmät (IDS, Intrusion Detection Systems), virustorjuntaohjelmistot sekä palomuurit. Käytettävissä on siis mittareita, jotka mittaavat tavanomaisia toimintoja ja pystyvät havaitsemaan ko. tilanteeseen nähden poikkeuksellisia tilanteita.

Erilaisia tietoturvaratkaisuja voidaan vertailla jo järjestelmän suunnitteluvaiheessa. Käytettäviä tietoturvamittareita voivat tällöin olla algoritmien vahvuuksien mittarien lisäksi tietoturvaratkaisujen käytettävyys-, suorituskyky- ja toteutettavuusmittarit.

Tietoturva voidaan nähdä myös yhtenä tuotteiden laatuun vaikuttavana tekijänä, jolloin käytetään tietoturvaominaisuuksia painottavia laatumitta-

reita. Ne perustuvat tavallisesti laadunhallinnan standardeihin, kuten esimerkiksi ISO 9001 ja ISO 9003.

Etäyhteyksiä käytetään laajalti teollisuusautomaatiossa tuotantoprosessien ohjaukseen ja monitorointiin. Tällaisissa yhteyksissä korostuu tosiaikaisen tietoturvan mittauksen tarve ja siksi tarvitaan hyviä IDS-, antivirus- ja palomuurituotteiden tietoturvamittareita.

Esimerkkejä teknisten tietoturvamittareiden käytöstä ovat
– tavoitteiden määritteleminen
– tietoturvatason ennustaminen tehtyjen valintojen pohjalta
– teknisten kohteiden vertailu
– tietoturvan valvonta(monitorointi)
– järjestelmäanalyysi tietoturvan näkökulmasta.

Teknisillä tietoturvamittareilla voidaan helpottaa tietoturvatavoitteiden määrittelyä, erilaisten tietoturvaratkaisujen vertailua, tuotteen kelpuutusta ja tietoturvatason ylläpitoa ohjelmisto- tai laitteistopäivitysten yhteydessä. Tietoturvatavoitteiden määrittelyssä voidaan käyttää teknisiä mittareita ilmaisemaan haluttu tietoturvataso esimerkiksi käytettävien algoritmien salausvahvuuden (Cryptographic Strength) tai läheisesti järjestelmään liittyvien teknisten parametrien avulla.

Myös tuotteen kelpuutuksessa voidaan käyttää tietoturvamittareita, jotka on suunniteltu vertaamaan tuotteen toteutusta tuotteen yleisiin vaatimuksiin. Tietoturvatason ylläpitoa varten suunniteltujen mittareiden on pystyttävä vertaamaan päivityksen yhteydessä entisen järjestelmän ja uuden järjestelmän oleellisia tietoturvanhallintaan liittyviä asioita. Tuotteen tietoturvaominaisuuksia voidaan myös ennustaa mittareiden avulla ennen valmistusvaihetta.

3.11.3 Tietoturvamonitorointi

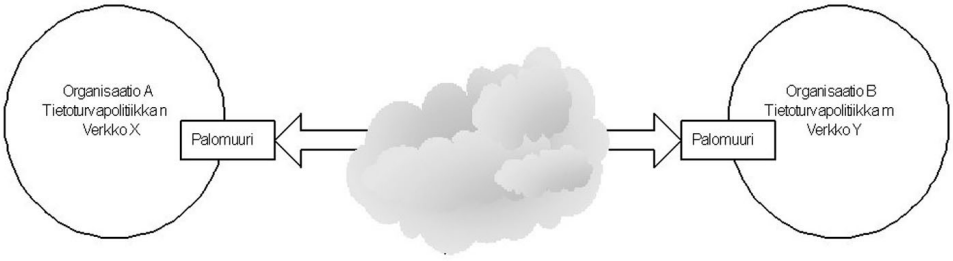
Tietoturvamonitorointi pohjautuu erilaisten tietoturvamittareiden käyttöön ja niiden tulosten yhdistämiseen. Tulevaisuudessa voi olla mahdollista valvoa verkon tietoturvatasoa ja tehdä sen perusteella päätöksiä esimerkiksi verkon liittämisestä toisiin verkkoihin, joilla voi olla täysin erilaiset tietoturvapolitiikat ja jotka voivat lisäksi sijaita eri organisaatiossa. Verkon hallinnolliset ja organisatoriset rajat on yleensä suojattu hyödyntämällä erilaisia palomuuritekniikoita. Tällainen suojaus on välttämätön, jotta voidaan estää hyökkäykset verkoista, joiden pohjana ei ole selkeitä tietoturvapolitiikoita, esimerkkinä Internet-verkko (kuva 14).

Verkkoliikennettä rajoittava palomuuri on usein yhdistetty tunkeutumisen havaitsemisjärjestelmään (Intrusion Detection System, IDS), joka on eräs mittareita hyödyntävä tietoturvamonitoroinnin työkalu. Tunkeutumisen havaitsemisjärjestelmän toiminta perustuu tyypillisesti sen kykyyn tunnistaa epänormaali liikenne verkossa, joka perustuu tietoon tunnetuista hyökkäystyypeistä, virusten toimintatavoista ja tunnetuista haavoittuvuuksista. Tämän

lisäksi on mahdollista mallintaa normaalista poikkeavaa käyttäytymistä. Tämäntyyppinen lähestymistapa sopii erityisen hyvin ennalta tuntemattomien hyökkäysten tunnistamiseen.

Tunkeutumisen havaitsemisjärjestelmät voidaan jakaa verkkokohtaisiin ja konekohtaisiin järjestelmiin. Verkkokohtaiset havaitsemisjärjestelmät kuuntelevat ja ”kaappaavat” kaiken verkkoliikenteen analysointia varten. Konekohtaiset havaitsemisjärjestelmät sen sijaan tarkkailevat yksittäiseen verkossa olevaan koneeseen kohdistuneita tapahtuneita hyökkäysyrityksiä tai muuta epäilyttävää verkkoliikennettä.

Erilaiset yhteistoimintamallit organisaatioiden välillä vaativat usein verkkoresurssien yhteiskäyttöä. Suojattujen verkkojen liittäminen yhteen sisältää merkittäviä tietoturvahaasteita, mutta ne ovat hallittavissa mittausten avulla. Tietoturvan mittaaminen antaa kokonaiskuvan toimintaympäristöstä ja auttaa arvioimaan riskejä, joita verkkojen ja organisaatioiden yhteistoiminnassa on erilaisten tietoturvakäytäntöjen ja teknisten ratkaisujen johdosta. Tekniset mittausjärjestelmät on syytä rakentaa siten, että mittaustiedon tallentamiseen, analysointiin ja tallennetusta historiatiedosta oppimiseen kiinnitetään riittävästi huomiota, jotta järjestelmiä voitaisiin kehittää ja pitää ajan tasalla uusien uhkien ja haavoittuvuuksien osalta.



Kuva 14. Suojattujen verkkojen yhteen liittäminen ja tietoturvamonitorointi.

3.12 Ohjelmisto- ja tietoliikennejärjestelmien ja -tuotteiden tietoturvan testaus

Teollisuusautomaatiossa testattavia järjestelmän osia ovat lähinnä ohjaus- ja tietoliikennejärjestelmät sekä kriittiset automaatiojärjestelmät. Teollisuusautomaatiojärjestelmä tai sen muutos testataan monella eri tavalla ja useassa eri vaiheessa järjestelmän elinkaaren aikana. Tyypillisiä testausvaiheita ovat valmistuksenaikaiset järjestelmä-, toipumis- ja tehdastestaukset sekä vastaanottajan hyväksymistestaukset. Lopullisessa sijoituspaikassa tehdään ensin ”kylmät” ja myöhemmin ”kuumat” testaukset. ”Kylmissä” kokeissa testataan

asennukset ja laitteiden toiminta ilman prosessiaineita, esimerkiksi kemian teollisuuden vesiajot. ”Kuumissa” kokeissa on mukana todelliset prosessiaineet. Ennen käyttöönottoa tehdään käyttöönottotestaus. Käytön aikana voidaan joutua testaamaan ohjelmiston muutostöitä (regressiotestaus).

Teollisuusautomaatiojärjestelmän osana olevat ohjelmistot ja tietoliikenne testataan edellä kuvatun vaatimustenmukaisuuden testauksen mukaisesti. Tietoturvan hallinnan toteutumisen näkökulmasta testaukseen kuuluu ainakin tietoturva-analyysit ja tuotteen kestävyysanalyysit. Tietoturva-analyysissä tuotteeseen liittyvää tietoturvavaatimusmäärittelyä verrataan tuotteen ominaisuuksiin ja todennetaan vaatimusten täyttyminen. Tietoturva-analyysi keskittyy lähinnä tahallisesti aiheutettujen ongelmatilanteiden esiintymisen mahdollisuuden selvittämiseen.

Tuotteen kestävyysanalyysillä varmistutaan siitä, että tuotteen kestävyys (Robustness) on riittävä tuotteen tietoturvavaatimuksiin nähden. Kestävyysanalyysi keskittyy lähinnä tahattomien ongelmatilanteiden etsintään. Kestävyysanalyysi on olennainen osa tietoturvatestausta, koska sen avulla voidaan selvittää, onko tuote riittävän kestävä tietoturvan hallinnan kannalta.

Tietoturva on ajan suhteen varsin dynaamista. Tietoturvatestauksiin liittyy jatkuva tarve tietoturvatestausprosessin päivityksiin. Testattavien kohteiden joukko muuttuu koko ajan, ja kun löytyy uusia haavoittuvuuskohtia, otetaan käyttöön uusia järjestelmiä sekä verkotetaan olemassa olevia järjestelmiä.

Teollisuudessa toteutettu tietoturva on perustunut perinteisesti siihen, että oma asiantuntijaryhmä tekee tunkeutumistestauksen. Testauksen kohteena olevaa järjestelmää testataan altistamalla se kokoelmalle tunnettuja hyökkäystapoja ja arvioidaan hyökkäysten onnistumisen mahdollisuuksia. Jos hyökkäys johtaa tunkeutumiseen, tarvitaan korjaavia toimenpiteitä. Asiantuntijaryhmät käyttävät erilaisia menetelmiä, joita he ovat itse kehittäneet.

Tunkeutumisen testaustapoja:

- Suora tunkeutumistestaus: kohdejärjestelmän palomuurit läpäisevän ohjelmiston käyttö.
- Epäsuora tunkeutumistestaus: vikatilanteiden aiheuttaminen, joiden aikana voi yrittää tunkeutua kohdejärjestelmään.
- Palvelunestotestaus: kohdejärjestelmän ylikuormitus, jolloin kohdejärjestelmä ei voi vastata palvelupyyntöihin muualta.
- Testaus hankitulla luottamuksellisella tiedolla: menetelmien käyttö, joilla voidaan yrittää tunkeutua kohdejärjestelmästä hankitun turvattoman tiedon avulla.
- Poisto- tai muuntohyökkäystä simuloiva testaus.
- Takaportteja hyväksikäyttävä simuloiva testaus.

Teollisuuden tietoturvan testauksen lisäksi on kehitetty lukuisia tietoturvan testausmenetelmiä, jotka pohjautuvat muodolliseen todentamiseen. Nämä menetelmät ovat matemaattisia ja vaikeasti sovellettavissa käytännön testausprosesseihin.

3.13 Tuotteiden tietoturvan sertifiointi

Tuotteiden tietoturvan sertifiointiin on kehitetty lukuisia menetelmiä. Useimmat niistä perustuvat tunnettuihin tietoturvan arviointikriteereihin, joita ovat erityisesti eurooppalainen ITSEC [19] ja yhdysvaltalainen TCSEC (”Orange Book”) [20].

Tietoturvasertifiointijärjestelmistä yleisimmin käytössä oleva menetelmä on Common Criteria (CC) [21], joka on standardoitu (ISO 15408). Common Criteria -järjestelmässä sertifioijia ovat tähän toimintaan valtuutuksen saaneet yritykset tai tutkimuslaitokset. Se perustuu suuressa määrin muun muassa ITSECiin ja TCSECiin.

Common Criteria -sertifioinnissa asetetaan tuotteelle tavoitteeksi jokin kahdeksantasoisen järjestelmän EAL (Evaluation Assurance Level) -sertifiointitaso, jonka mukaan sertifiointiprosessin vaativuus määräytyy. EAL0 on alin taso ja EAL7 vaativin taso. Common Criterian EAL-tasot on kuvattu oheisessa taulukossa (kuva 15). EAL4 edustaa jo varsin hyvää tietoturvan tasoa. EAL7-tason saavuttaminen on erittäin harvinaista.

Common Criteria -sertifiointi määrittelee potentiaalisen joukon tietoturvavaatimuksia, jotka on jaettu toiminnallisiin ja vakuutusvaatimuksiin. Common Criterian sertifiointiprosessi käyttää kahdenlaisia dokumentteja, joihin ko. vaatimuksia voidaan heijastaa:

- Suojausprofiilit (Protection Profiles, PP): dokumentti, joka on kehitetty käyttäjäkunnan toimesta kuvaamaan käyttäjien tietoturvavaatimuksia.
- Tietoturvakohdekuvaukset (Security Targets, ST): dokumentti, jossa järjestelmän kehittäjä kuvaa järjestelmänsä tietoturvaominaisuudet. ST:n voidaan väittää toteuttavan yhden tai useamman PP:n.

EAL	Kuvaus
0	ei testattu
1	toiminnallisesti testattu
2	rakenteellisesti testattu
3	menetelmällisesti testattu ja tarkistettu
4	menetelmällisesti suunniteltu, testattu ja tarkistettu
5	puolimuodollisesti suunniteltu ja testattu
6	puolimuodollisesti todennettu ja testattu
7	muodollisesti todennettu ja testattu

Kuva 15. Common Criterian EAL -tasot.

Process Control Security Requirements Forum (PCSRF) on kehittänyt edellä mainittua Common Criteria -standardia soveltaen yleiskäyttöisen teollisuuden ohjausjärjestelmien suojausprofiilin (ks. luku 9).

4

Teollisuusautomaatio, verkottuminen ja tietoturva

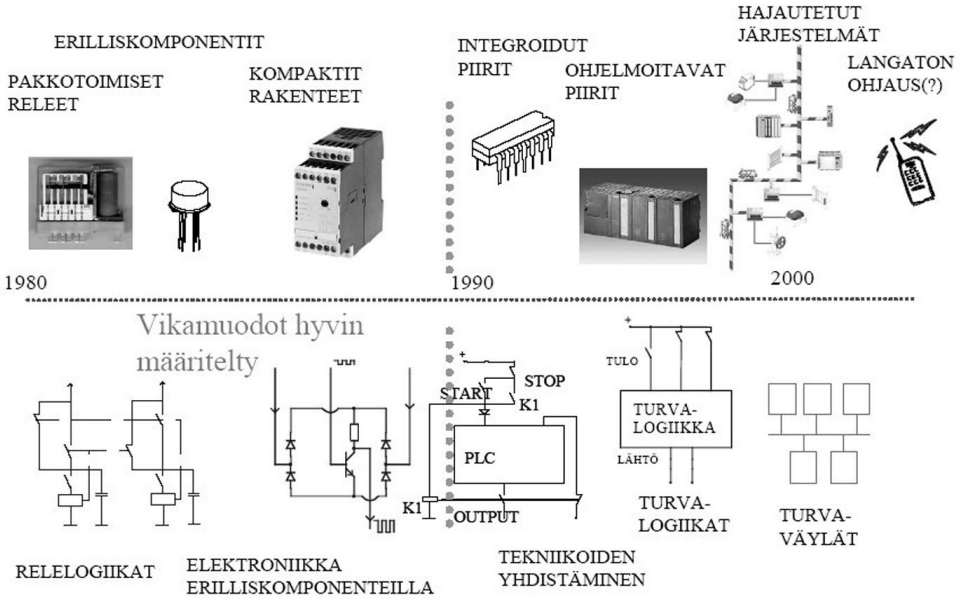
4.1 Historiasta nykypäivään

Perinteisesti automaatio on määritelty järjestelmäksi, jossa automaattisilla laitteilla vähennetään ihmisen tekemiä ohjaustoimintoja. Tämä ei kuitenkaan kuvaa nykyistä teollisuusautomaatiota, koska tänä päivänä teollisuusautomaatiolla ohjataan, seurataan ja muutoinkin hallitaan tuotantoprosessin etenemistä niin tarkasti ja luotettavasti, että ihminen ei siihen pysty. Teollisuusautomaatio mahdollistaa nykyisin sellaisetkin toiminnat, joista aikaisemmin ei edes haaveiltu [22].

Suomalainen teollisuus aloitti 1940–1950-lukujen vaihteessa säätäjien, mittauslähettimien, antureiden ja toimilaitteiden tuonnin USA:sta. Tästä voidaan verkottuneen automaation käytön katsoa alkaneen, sillä automaattinen säätö vaatii tuotantoprosessista saatavien mittaus- ja asetusarvojen siirtämisen säätöyksikköön.

Alussa automaatioverkon muodosti 4-20 mA (”elävän nollan periaatteella”) toimiva mittaussignaalin siirto. 1960-luvun aikana digitalisointi valtasi alaa ja tietokonepohjaisia ratkaisuja alettiin ottaa käyttöön. 1960-luvun lopulla releohjauksien rinnalle tulivat vähitellen binääriset ohjauslogiikat sekä mekaanisesti ohjelmoitavat logiikat. Nämä perinteiset logiikat (PLC) on korvattu mikroprosessoreihin perustuvilla ohjelmoitavilla logiikoilla (SoftPLC) vasta viimeisten parin vuosikymmenen aikana (kuva 16).

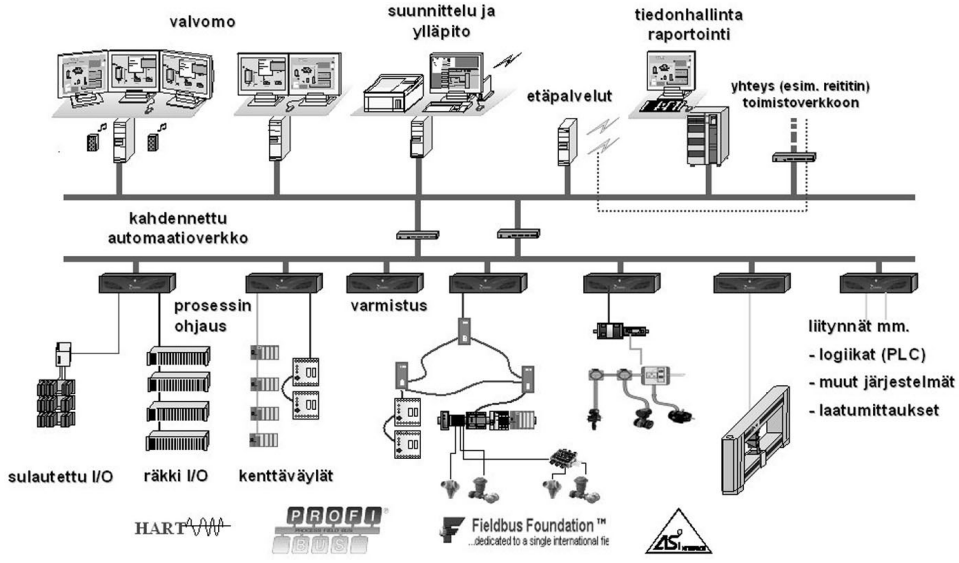
Standardisointi massamarkkinoilla säästää kustannuksia. Tämä trendi on ollut nähtävissä automaatiomarkkinoilla: asiakkaat haluavat käyttää mahdollisuuksien mukaan standardituotteita ja -komponentteja niin valvomoissa kuin tuotantoprosessien ohjauksessa. Sama suuntaus on nähtävissä myös verkkojen osalta: suljetuista valmistajakohtaisista verkoista halutaan siirtyä standardiverkkoihin, kuten Ethernet-verkon ja Internet-verkon teknologioiden käyttöön. Automaation viimeiset viisi vuosikymmentä voidaankin kuvata siirtymisestä tiettyyn tarkoitukseen erikseen suunnitelluista laitteista standardilaitteistoilla, -ohjelmistoilla ja -tiedonsiirtoteknologioilla toteutettuihin automaatioympäristöihin, joissa automaatio on toteutettu sulautetuilla ohjelmistoilla.



Kuva 16. Turvapiireissä käytetyt tekniikat eri aikoina [23].

4.2 Nykyaikaiset teollisuuden automaatiojärjestelmät

Kuvassa 17 on esitetty yksi malli nykyaikaisesta automaatiojärjestelmästä, joka sisältää liitynnät kenttälaitteisiin ja kenttäväyliin, joissa sijaitsevilla laitteilla hoidetaan valvomossa olevien prosessinohjausasemien avulla tuotantoprosessin ohjausta ja ylläpitoa.



Kuva 17. Nykyaikainen automaatiojärjestelmä.

Teollisuuden automaatiojärjestelmät voidaan luokitella niiden ohjausjärjestelmien ja verkkorakenteen perusteella karkeasti seuraaviin ryhmiin:

1. Hajautetut automaatiojärjestelmät (Distributed Control Systems, DCS).

2. SCADA-käytönvalvontajärjestelmät (Supervisory Control and Data Acquisition Systems).

3. Ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC).

Ohjausjärjestelmät voidaan jakaa myös jatkuviin ja panosprosessia ohjaaviin automaatiojärjestelmiin, mutta tietoturvan kannalta näillä järjestelmillä ei ole merkittäviä eroja.

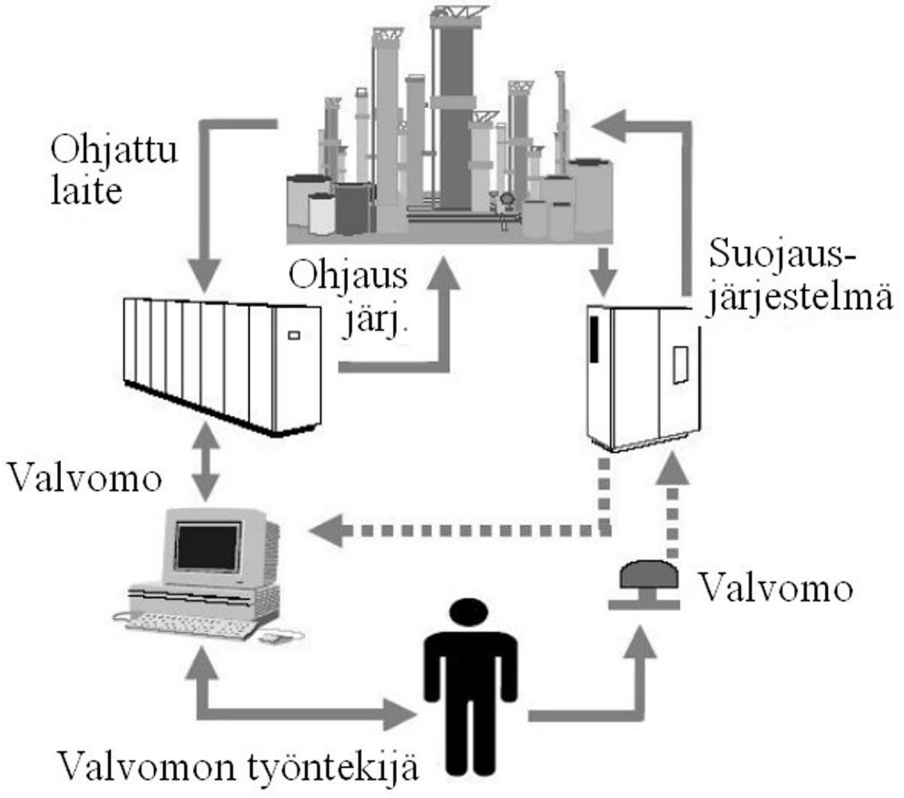
4.2.1 Hajautettu ohjausjärjestelmä

Hajautettuja järjestelmiä käytetään ohjaamaan laajoja ja monimutkaisia prosesseja, kuten voimalaitoksia, kemianlaitoksia ja öljynjalostuslaitoksia sekä terästeollisuuden, elintarvikealan, panimoalan, lääketeollisuuden, selluja paperiteollisuuden, metalliteollisuuden ja kaivosten laitoksia, jotka sijaitsevat tavallisesti yhdellä alueella (kuva 18).

Hajautettu ohjausjärjestelmä (DCS) käsittää ohjaustason ja yhden tai useampia hajautettuja ohjausyksiköitä samassa tehdaslaitoksessa. Valvontayksikkö toimii ohjauspalvelimessa ja kommunikoi sen ala-asemissa oman aliverkon kautta. Ohjausyksikkö antaa asetusarvoja ja hankkii tietoja hajautetuilta ohjausyksiköiltä. Hajautetut ohjausyksiköt ohjaavat tuotantoprosessien toimintoja ohjausyksikön antamien käskyjen mukaisesti käyttämällä anturien palautetta tuotantoprosessiin sijoitetuista antureista. Nämä ohjausyksiköt käyttävät tyypillisesti paikallista kenttäväylää kommunikointiin toimilaitteiden ja anturien kanssa. Näin vältetään pisteestä toiseen tehtävää langoitusta ohjausyksikön ja ohjattavan laitteen välillä.

Hajautetun järjestelmän ohjausyksikköinä käytetään erityyppisiä laitteita, kuten koneiden ohjauslaitteita, ohjelmoitavia logiikkoja, tuotantoprosessien ohjausyksiköitä ja yksinkertaisia palautteeseen perustuvia ohjaimia sovelluksesta riippuen. Hajautetun ohjausjärjestelmän yksiköihin on usein pääsy suoraan modeemin kautta. Tällöin diagnostiikkaa ja huoltotoimenpiteitä voivat tehdä laitetoimittajien tai teollisuuslaitoksen työntekijät.

Prosessiautomaatiossa turvallisuus perustuu tyypillisesti perusjärjestelmän toimintaan, ja turvajärjestelmiä tarvitaan vain poikkeustilanteiden hallintaan (harvojen vaateiden tapaus, IEC 61508-1 ja kuva 18). Siten näille turvajärjestelmille kohdistetaan suuremmat vaatimukset kuin perusjärjestelmälle.

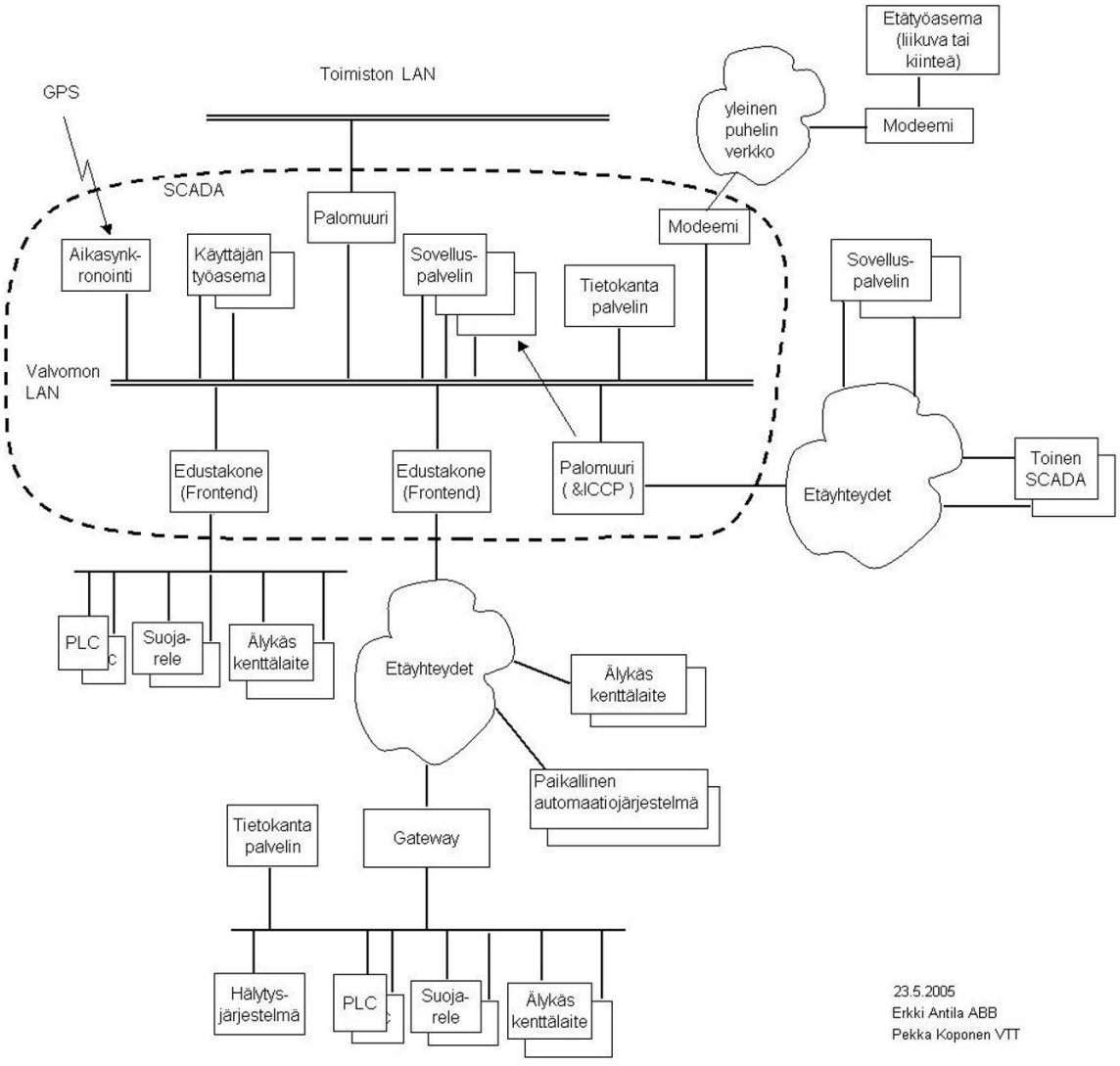


Kuva 18. Prosessiteollisuuden ohjausjärjestelmä (perusjärjestelmä ja turvajärjestelmä).

4.2.2 SCADA-käytönvalvontajärjestelmät (infrastruktuuri)

SCADA-tyyppisiä järjestelmiä käytetään pääasiassa maantieteellisesti hajautettujen järjestelmien ohjaukseen, joissa hankitaan keskitetysti tietoja eri yksiköistä ohjaustoimintoja varten. Tyypillisiä hajautettuja toimintoja, joissa käytetään SCADA-järjestelmiä, ovat infrastruktuurijärjestelmät, kuten energianjakeluverkot, kaasulinjat, vesijärjestelmät, jätevesijärjestelmät sekä muut vastaavat yleiset verkot ja teollisuusverkot.

SCADA-järjestelmät ovat tyypillisesti hajaantuneempia kuin DCS-järjestelmät, ja niissä keskitetty tietojen hankinta on tärkeää. Käytännössä sähkön siirrossa ja jakelussa käytettävien SCADA-järjestelmien tärkeä tehtävä on alajärjestelmien etäohjaus, mikä tapahtuu tavallisesti automaattisesti. Yritysten liiketoimintoja varten voi olla pääsy tehtaan tietojärjestelmiin Internetverkon kautta ja joskus laajan lähiverkon (Wide Area Network WAN) kautta. Teollisuuslaitoksen toimintoja voidaan ohjata palveluilla paikallisverkon (Local Area Network, LAN) kautta, mutta varsinainen laitoksen ohjausjärjestelmä on erotetussa verkossa.



Kuva 19. Maantieteellisesti hajautettu SCADA-tyyppinen järjestelmä (Erkki Anttila ABB, Pekka Koponen VTT).

Erityisesti sähkönsiirron ja -jakelun uudet SCADA-järjestelmät ovat kuvassa 19 esitetyn kaltaisia. Laajan infrastruktuurin eri osia palvelevien järjestelmien on kyettävä keskustelemaan keskenään. Tähän SCADA-järjestelmä voi käyttää tarkoitukseen soveltuvia tietomalleja, kuten kuvassa ICCP (Inter Control Center Protocol), jotka on tarkoitettu toimimaan TCP/IP -verkoissa. Yhteydet yrityksen muihin liiketoimintoihin ja sovelluksiin hoidetaan siten, että SCADA -järjestelmän valvomon lähiverkko on palomuurin kautta yhtey-

dessä toimiston paikallisverkkoon ja usein myös laajaan lähiverkkoon (Wide Area Network, WAN). Teollisuuslaitoksen tai muun kohteen toimintoja voidaan ohjata palveluilla paikallisverkon (Local Area Network, LAN) kautta, mutta varsinainen laitoksen ohjausjärjestelmä on erotetussa verkossa. SCADA-järjestelmä ja sen ala-asemat on aikasynkronoitava esimerkiksi GPS-ajan (Global Positioning System, GPS) perusteella. Yhteyksiä etätyöasemiin toteutetaan varsin usein joko Internet-verkon tai yleisen puhelinverkon kautta.

SCADA-tyyppisiin järjestelmiin kuuluvat keskusvalvontayksikkö (Central Monitoring System, CMS) sekä yksi tai useampia etäasemia (Remote Terminal Unit, RTU). Keskitetty ohjausjärjestelmä sijaitsee ohjauspalvelimessa ja kommunikaatio reititetään oman suojatun aliverkon kautta. Keskitetty ohjausjärjestelmä kerää ja tekee lokit tiedoista, joita saadaan etäasemista, ja tuottaa tarvittavat toimenpiteet etäasemien tekemien havaintojen ja mittausten perusteella.

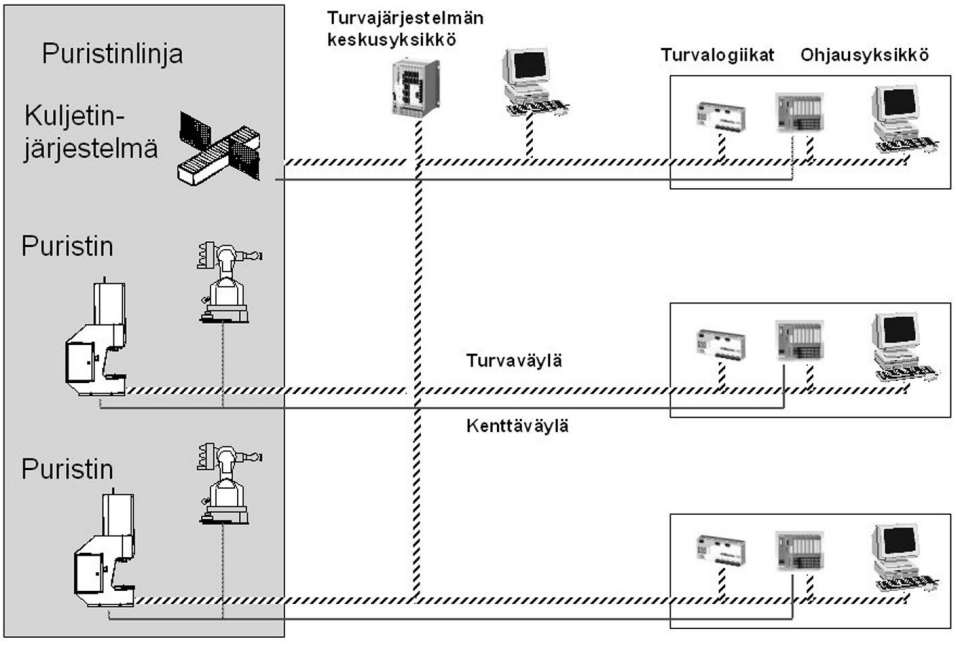
Etäasemaan kuuluu joko etäasema tai ohjelmoitava logiikkayksikkö, joka ohjaa toimilaitteita ja valvoo antureita. Etäasemilla on tyypillisesti lisäkapasiteettia kenttäoperaattorien liitäntöjä varten, jotka tekevät kannettavilla laitteilla diagnostiikka- ja korjaustoimenpiteitä. Kommunikaatioverkkoa käytetään tietojen siirtämiseen etäasemien ja keskusohjausyksikön välillä. Alajärjestelmät kommunikoivat LAN- ja WAN-verkkojen, Internetin, puhelinlinjojen ja radiotaajuisten siirtoyhteyksien kautta alajärjestelmien fyysisestä läheisyydestä riippuen. Jos etäasema on liian eristyksissä, jotta se voitaisiin tavoittaa suoraan radiosignaalilla, käytetään radiolinkkiä asemien välillä.

4.2.3 Ohjelmoitavat logiikkajärjestelmät

Ohjelmoitavia logiikoita käytetään ohjaamaan erillisiä prosesseja sekä hajautettujen ohjaus- ja SCADA-järjestelmien alajärjestelmiä sekä erillisiä turvatoimintoja. Tyypillisiä järjestelmiä ovat kappaletavarateollisuuden valmistusjärjestelmät. Toteutus tehdään ohjelmoitavilla logiikoilla, joissa on jatkuvaaikainen säätö yhdistettynä logiikalla ohjelmoituun työkiertoon, esimerkiksi harvesterissa voi olla viisi erillistä tietokonetta ohjaamassa konetta CAN-väylän kautta.

Ohjelmoitavat logiikat (PLC) ovat tyypillisesti modulaarisia laitteita tai piirikortteja, joita käytetään prosessinohjaukseen, digitaalisiin binäärituloihin ja -lähtöihin sekä analogisiin tuloihin ja lähtöihin, ihminen–kone-vuorovaikutukseen sekä tietoliikenteen liitäntöihin (kuva 20).

Koneautomaatiossa turvatoimintoja tarvitaan tyypillisesti usein tai jatkuvasti. Siten kaikki järjestelmät, joiden puutteet tai vikaantumiset voivat aiheuttaa turvallisuuden heikentymisen, kuuluvat turvallisuuteen liittyviin järjestelmiin ja niiden on oltava turvallisuusvaatimusten eritelmien mukaisia.



Kuva 20. Koneiden turvallisuuteen liittyvä ohjausjärjestelmä, jossa on yhdistetty turvaväylä (SafeEthernet) ja tavallinen kenttäväylä sekä PC-työasemia. Puristimien ja kuljetinjärjestelmän turvatoimintoja ohjataan turvaväylällä (paksu viiva), ja muut ohjaukset on toteutettu tavallisella logiikalla. PC on yhteydessä turvaväylään, mutta se toimii lähinnä tiedonkeruutehtävissä [23].

4.2.4 Tosiaikajärjestelmät

Nykyinen automaatioverkoissa käytettävä verkkoteknologia perustuu alun perin liiketoimintaverkkojen rakentamiseen, joissa ajoitus ei ollut aina kriittistä, ja välitallennukset olivat tavanomaisia ja hyväksyttäviä. Kun näissä verkoissa lähetettiin tietoturvaa vaativaa luottamuksellista tietoa, tietoturva hoidettiin sovellustasolla, johon se otettiin mukaan jo sovellusten kehityksen varhaisessa vaiheessa.

Koska teollisten tuotantoprosessien ja kappaletavarateollisuuden automaatiojärjestelmissä vaadittiin tosiaikaista ohjausta, ne suunniteltiin alun perin erillisiksi järjestelmiksi. Näissä järjestelmissä tietoturva hoidettiin erottamalla ne fyysisesti muista verkoista ja toiminnoista, ja tarvittava pääsy hoidettiin hyvin rajoitetusti pääsyn valvonnan avulla.

Tosiaikaiset tietokonejärjestelmät eroavat monin tavoin perinteisistä tietoteknisistä järjestelmistä, joita käytetään muualla liiketoimintojen tukena. Tosiaikaiset ohjausjärjestelmät on suunniteltu tavoittelemaan tehokkuutta ja aikakriittistä vastetta (deterministisyys). Deterministisessä automaatiojärjestelmässä vasteajat eivät saa häiritä ohjaustapahtumaa, ja siten niillä on pienet vasteajat, jolloin esimerkiksi tietoturvaan liittyvien salausalgoritmien käsittely ei ole aina mahdollista. Tietoturvaa ei ole otettu useinkaan huomioon

suunnittelussa, jolloin tietoturvateknisiä toimenpiteitä on suoraan jätetty pois laitteiden suorituskyvyn takaamiseksi. Usein turvallisuuden ja tietoturvan tavoitteet ovat myös keskenään ristiriidassa automaatiojärjestelmän ja käyttötoimintojen suunnittelun kanssa.

Perinteisesti automaatiossa on pyritty kustannustehokkuuteen minimoimalla tietoliikennekapasiteettia sekä hajautettuja laskenta- ja muistiresursseja. Laskentakapasiteetti, joka on käytettävissä tietoturvatoimintoihin, on ollut hyvin rajoitettua muun muassa keskusyksikköjen ja muistien osalta. Nykyisin nämä ovat muuttuneet huomattavasti edullisemmiksi, mutta samaan aikaan entistä monimutkaisempien järjestelmien tietojen hallinta ja järjestelmien ylläpito, kuten asennukset ja konfigurointi ovat kallistuneet. Yksittäisten tietoliikenneyhteyksien kustannukset saattavat olla edelleen korkeat, mutta nykyisillä ratkaisuilla riittävä tietoliikennekapasiteetti sekä muistin ja laskentatehon hajauttaminen on suhteellisen edullista. Täten kustannustehokkaaseen ratkaisuun pyrkiminen johtaa aivan erilaiseen ratkaisuun kuin aikaisemmin.

Perinteiset yritysten toimistotason verkot eivät ole deterministisiä. Toimistojärjestelmissä palvelun vasteaika voi useita sekunteja. Verkot ovat aliverkotettuja ja reititettyjä, jolloin verkkoliikenteen jokaisessa solmussa (kytkin tai reititin) on oma käsittelyviiveensä. Tämän tyyppisessä verkossa voidaan käyttää salaukseen perustuvia algoritmeja ja tietoturvaa parantavia tekniikoita esimerkiksi pääsylistojen avulla.

4.3 Verkkoyhteydet

Tietoturvaa ei ole pidetty viime vuosituhannen vaihtumiseen asti merkittävänä tekijänä teollisten tuotantoprosessien ohjauksessa. Järjestelmät on yleensä suunniteltu toteuttamaan toiminnalliset vaatimukset sekä täyttämään niihin liittyvät luotettavuus-, turvallisuus- ja joustavuusvaatimukset. Järjestelmät ovat tyypillisesti olleet fyysisesti eristettyjä ja perustuneet niihin soveltuviin laitteisiin sekä tiedonsiirtovälineisiin.

Vuoden 2001 tapahtumat (esimerkiksi Code Red ja Nimda -virukset) herättivät useat verkottuneet yritykset suojaamaan toimistoverkkojaan. Automaatioverkot eivät tämän jälkeenkään ole olleet tarvittavassa erityisasemassa yritysten sisäverkoissa.

Vertailu eri tietojärjestelmien välillä osoittaa, että järjestelmän korkeimmalla tasolla verkoston arkkitehtuuri on yhtäläistä tuotantolaitoksen kaikkia toimintoja varten. Tältä tasolta alajärjestelmät jakautuvat paikallisiin verkkoihin. Järjestelmän osia ovat yleisessä käytössä olevat työasemat, tehtaan tietokannat, sovelluspalvelimet, käyttäjätunnusten hallintajärjestelmät, modeemit jne. Tietoliikenne tehtaasta ulospäin on tyypillisesti hoidettu palomuurin kautta Internet-verkkoon tai muuhun paikalliseen yleiseen tietoliikenneverkkoon.

Kaikkia tietoliikenneyhteyksiä pyritään hallitsemaan ja valvomaan asianmukaisesti, ja tämä parantaa myös tietoturvaa. Yleinen suuntaus on siirtyä hankalasti valvottavien modeemien käytöstä muiden ja paremmin hallittavien ratkaisujen käyttöön. Esimerkiksi modeemeja toki käytetään vielä yleisesti, mutta vain silloin kun niitä tarvitaan, ja tällöin niiden käyttöön ja käytöstä aiheutuviin tietoturvauhkiin on pyritty vastaamaan.

Internet-verkkoon perustuva teknologia on lisännyt teollisuuden tietojärjestelmien haavoittuvuutta. Internet-verkon syntyessä tietoturvaa ei ole otettu huomioon. Keskitetty ohjaus ja etäkunnossapito on siirtynyt yleisiin puhelin- ja muihin tietoverkkoihin, ja ne ovat sitä kautta uhkana kriittisille infrastruktuureille. Hajautetut järjestelmät toimivat kaupallisten laitteistojen ja ohjelmistojen varassa, joita on yhdistetty ulkoisiin tietoverkkoihin, jotka voivat tehdä mahdolliseksi yksinkertaisetkin tunkeutumiset järjestelmiin ja siten vaarantaa yrityksen tuotannon tai jakelujärjestelmien toimintaa.

4.4 Uhkakuvat

Tietomurron tai -hyökkäyksen takana on aina, suoraan tai epäsuorasti, ihminen tai joukko ihmisiä. Samalla on kuitenkin todettava, että hyökkäyksen alkuperän jäljittäminen voi olla vaikeaa ja usein jopa mahdotonta. Vaikka pääosa hyökkäyksistä tapahtuukin yleisen Internet-verkon puolelta, ne voivat yhtä hyvin tapahtua myös yrityksen sisäverkosta käsin. Ongelmia lisäävät teollisuusympäristöissäkin yhä enemmän käytetyn IP-protokollan, kuten muidenkin yleisten protokollien, tietoturvan puutteiden lisäksi Internet-verkonlaajuus ja kansainvälisyys. Internet-verkon käyttäjien joukossa on myös niitä, jotka haluavat aiheuttaa tavalla tai toisella haittaa. Valitettavasti suurenkin haitan aiheuttaminen yleisissä verkoissa, kuten Internet-verkossa, on suhteellisen helppoa.

Taustalla voi olla erilaisia motiiveja, joita perinteisesti ovat olleet ilkivalta, jännityksen ja kuuluisuuden etsiminen, tutkiminen, uteliaisuus, ystäväpiirin painostus, torjuntaohjelmien haastaminen, sosiaalinen arvostuksen etsiminen, turvallisuusaukkojen paljastaminen, ajattelemattomuus ja helppous. On kuitenkin havaittavissa, että taloudellisen hyödyn tavoitteleminen ja järjestäytynyt rikollisuus ovat yhä enenevässä määrin uhkien takana. Tietoturvatietämyksen ja -ymmärryksen lisääntyessä sekä ohjelmisto- ja laitevalmistajien jatkuvasti parantaessa tietoturvatasoaan, on toiminta siirtynyt enenevässä määrin harrastelusta ammattimaisempaan toimintaan.

Vaikka edellä mainitut uhkakuvat ovatkin varsin yleisiä, koskettavat ne kuitenkin yhä laajemmin myös teollisuusautomaatiota, koska automaatio on verkottunut osaksi yhteiskunnan järjestelmiä. Monet järjestelmät ovat lisäksi nykyyhteiskunnan toiminnan kannalta kriittisiä, kuten sähkön ja lämmön jakelu.

Automaatiota käyttävät yritykset, samoin kuin automaatiotoimittajatkin, ovat maailmanlaajuisia konserneja myös verkkojensa osalta, joten sisäverkkoon päässyt häiriö voi levitä välittömästi koko verkkoon. Globaalilla riskillä tarkoi-

tetaan tietojärjestelmien yhteydessä riskiä, joka voi toteutua useissa eri järjestelmissä samaan aikaan. Esimerkkeinä globaaleista riskeistä voidaan mainita verkkomadot, palvelunestohyökkäykset ja kansainvälinen tietovakoilu.

Internet-verkossa on miljoonia käyttäjiä, jolloin muodostuu ennalta-arvaamattomia ja satunnaisia riskejä. Yhtenä merkittävänä riskinä pidetään toistaiseksi tuntematonta tietoturva-aukkoa, jonka hakkeri voi löytää ja jota hän käyttää hyväkseen. Tällaista ei ole toistaiseksi tapahtunut laajassa mittakaavassa, mutta erityisesti kriittisissä järjestelmissä olisi syytä varautua myös tähän.

4.5 Toimistojärjestelmien ja teollisuuden automaatiojärjestelmien erot

Automaatiojärjestelmien tietoturva perustuu useimmiten olemassa oleviin kokemuksiin toimistojärjestelmien tietoturvaohjelmista ja -käytännöistä. Kuitenkin automaatiojärjestelmiltä vaaditaan tavallisesti korkeampaa tietoturvatasoa kuin yleisissä toimistojärjestelmien ympäristöissä. Siksi automaatiojärjestelmiä voidaan luonnehtia seuraavasti [4]:

- Automaatiojärjestelmät ovat vakiintuneempia kuin toimistojärjestelmät. Organisaatiossa tunnetaan laitteet paremmin ja niitä pidetään pidempään käytössä. Konfiguraatiota muutetaan lähinnä suurempien kunnossapito- tai muutostöiden yhteydessä.
- Automaatiojärjestelmissä ei useinkaan ole liiketoimintojen kannalta salassa pidettävää tietoa.
- Suoraa yhteyttä Internet-verkkoon ei tavallisesti tarvita.
- Automaatiojärjestelmän tietoteknisiä laitteita ei tavallisesti käytetä muihin tarkoituksiin ja useimmiten ne on hajautettu valmistusprosessin mittauksiin ja ohjauksiin sekä turvatoimintoihin.
- Pääsyn hallinta on useimmiten tarkasti järjestetty ja henkilöstö on koulutettu näihin tehtäviin.
- Automaatiojärjestelmien toimintojen ja henkilöstön valvonta on tiukempaa järjestelmälle asetettavien lisävaatimusten takia, esimerkiksi turvallisuusvaatimukset.

Teollisuusautomaatiolla on muusta tietotekniikasta eroavia erityispiirteitä. Näitä ovat muun muassa [4]):

- Tavoitteet
  Ihmisten terveyden ja turvallisuuden varmistaminen, laitteiston ja tehdaslaitosten suojaaminen vahingoilta, tuotteiden laadun varmistaminen ja tuotantotoiminnan jatkuvuuden ylläpitäminen.

- Järjestelmän kokoonpano
  Toimistojärjestelmissä tietoturvalla keskitytään suojelemaan palvelimeen tallennettuja tietoja. Tuotantojärjestelmissä toiminnallisia yksiköitä on hajautettu ja niiden oikea toiminta on tärkeämpää kuin palvelinkeskuksen toiminta. Molemmilla alueilla järjestelmät kehittyvät nykyistä hajautetumpaan suuntaan sekä tekniikan että verkottuneiden liiketoimintamallien kehityksen takia.

- Tiedon ja palvelujen saatavuus
  Useimmat tuotantojärjestelmät ovat jatkuvatoimisia, jolloin odottamattomat seisokit eivät ole hyväksyttävissä. Järjestelmiä ei voi aina pysäyttää helposti ilman, että siitä aiheutuu vahinkoa tuotannolle. Tavallisesti tuotteet ovat arvokkaampia kuin niihin liittyvä informaatio. Korkeat vaatimukset saatavuudelle, luotettavuudelle ja ylläpidettävyydelle vähentävät monien tietotekniikan menetelmien käyttöä ja esimerkiksi mahdollisuuksia toistuviin uudelleenkäynnistyksiin.

- Ei-toivotut seuraukset
  Toimistojärjestelmissä ei-toivotut seuraukset eivät aina ole vakavia. Tuotantojärjestelmissä seuraukset voivat olla tuhoisia. Tuotantojärjestelmät voivat olla hyvin monimutkaisia ja kaikki tietoturvatoiminnot, joita yhdistetään tuotantoprosessiin, on huolellisesti testattava ennen niiden käyttöönottoa, jotta estettäisiin ei-toivottuja seurauksia.

- Aikakriittisyys
  Monissa järjestelmissä vasteajat ovat kriittisiä, esimerkiksi ohjaustoimintoja ja varsinkaan turvallisuuteen liittyviä toimintoja (esimerkiksi hätäpysäytystoimintoa) ei voida ohjelmoida tekstiviestipohjaisten käyttäjätunnusten taakse. Tosiaikaisuutta vaativissa järjestelmissä ei voida hyväksyä poikkeuksellisia viiveitä.

- Ohjelmistot
  Tuotantojärjestelmien ohjelmistot ovat monimutkaisempia kuin tavallisissa tietoteknisissä järjestelmissä, ja niiden ylläpitoon vaaditaan erityisasiantuntemusta.

- Salaus
  Monissa järjestelmissä ei ole mahdollisuuksia salaukseen ja salasanasuojauksiin tai autentikoinnin virhelokeihin.

- Resurssit
  Automaatiojärjestelmät ja niihin liittyvät tosiaikajärjestelmät ovat resursseiltaan rajoittuneita, eikä niissä yleensä ole voitu käyttää tyypillisiä tietoturvateknologioita.

- Tiedon eheys
  Tiedon eheys on erittäin tärkeää ohjausjärjestelmien toiminnolle.

- Yhteydet
  Ohjausjärjestelmien protokollat ja tiedonsiirtotavat ovat yleensä erilaisia verrattuna yleisiin tietoteknisiin ympäristöihin, esimerkkinä radio-ohjaus , jossa käytetään asynkronista ja sarjamuotoista protokollaa.

- Ohjelmistojen ja laitteiden päivitykset
  Ohjelmistojen ja laitteiden päivittäminen on vaikeampaa, koska on tunnettava myös automaatiosovellus tai -järjestelmän toiminta ja käytettävien ohjelmistojen väliset riippuvuussuhteet. Tietoturvan korjaus- ja ylläpito-ohjelmia ei voida aina päivittää välittömästi, koska automaatiojärjestelmän toimittajan on ensin testattava ne. Muutosten hallinta on erittäin tärkeää automaatiojärjestelmien eheyden ylläpitämisessä.

Tietoturvan varmistamiseksi myös automaatiojärjestelmien osalta tarvitaan edellä kuvattujen eroavaisuuksien käsittelyä sekä automaatioasiantuntijoiden että tietotekniikan asiantuntijoiden yhteistyötä. Erityisesti kattavat testaukset ennen järjestelmien käyttöönottoa on suunniteltava yhteisesti. Tällöin myös molemminpuolinen vastuunjako on tehtävä selväksi.

Teollisuusautomaation tosiaikavaatimusten johdosta ohjattavan tuotantoprosessin tehtävät suoritetaan määrättyjen aikavälien ja prioriteettien mukaisesti. Priorisointeja voi tulla myös ohjattavasta tuotantoprosessista. Siten jokaisen tehtävän ajoitus on rajoitettu, ja tehtävät on saatettava loppuun ennen kuin niiden tuloksia tarvitaan eli ennen kuin niitä tarvitaan tosiaikaohjauksessa.

Esimerkiksi koneautomaatiossa ajoitus on kriittistä, ei ainoastaan koko ohjattavalle tuotantoprosessille vaan myös erikseen jokaiselle tehtävälle, jolloin

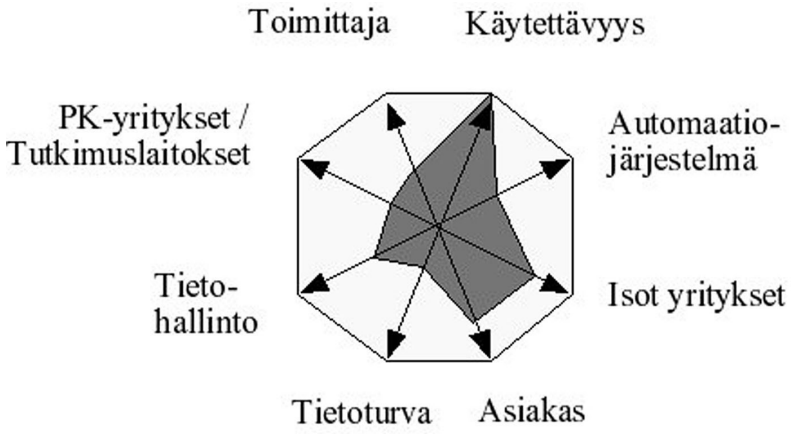
- on oltava mahdollista keskeyttää ja uudelleen käynnistää tehtävät ja tuotanto- sekä käyttöjärjestelmän prosessit
- poikkeuksellisia viiveitä ei voida hyväksyä
- tietojen käsittelyn resursseja on useimmiten rajoitetusti.

Tietyissä tapauksissa ajoitukset ja tehtävien keskeytykset tosiaikajärjestelmissä voivat estää perinteisten salausalgoritmien käytön, jolloin turvallisuuteen liittyvissä järjestelmissä voidaan tarvita turvallisuuden ja tietoturvan välistä kompromissiä. Vaikka tietojen eheys on ratkaisevan tärkeää ja salassapito yleensä toissijaista, on erityistapauksia, joissa myös salausta vaaditaan, esimerkiksi vaativia valmistusreseptejä ja laskenta-algoritmeja suojataan yleisesti salaamalla.

4.6 Tietoturvavaatimusten tasapainotus

Kuvassa 21 on esitetty ongelmakenttää ottaen huomioon eri osapuolien ja vaatimusten vastakkainasettelun:

- Tietotekniikka (IT) vs. automaatio.
- Käytettävyys vs. tietoturvataso.
- Asiakas vs. toimittaja.



Kuva 21. Kuvassa esitetään eri osapuolten ja vaatimusten väliset ristiriidat. Nuolten päissä on esitetty vastakkain kilpailevat osapuolet ja keskelle muodostuva alue kuvaa osapuolten tietoturvavaatimusten tasapainoa. Mitä lähempänä alue on ulkokehää, sitä parempi on kokonaisuus ja mitä lähempänä alue on muodoltaan ulkokehää, sitä tasapainoisempi on kokonaisuuden tietoturva.

4.7 Tietoturvaan ja turvallisuuteen liittyvät säädökset, standardit ja ohjeet

Turvallisuuteen ja terveyteen liittyvissä säädöksissä on vaatimuksia siitä, miten turvallisuus ja terveys on varmistettava erityyppisissä järjestelmissä. Euroopassa säädökset on annettu direktiiveillä, joiden vaatimukset otetaan sellaisenaan jäsenmaiden kansalliseen lainsäädäntöön. Suomessa direktiivit julkaistaan valtioneuvoston asetuksilla (aikaisemmin myös valtioneuvoston tai ministeriöiden päätöksillä). Tärkeimmät teollisuusautomaation turvallisuutta koskevat direktiivit [24] ovat pienjännitedirektiivi (sähkölaitteet), painelaitedirektiivi, konedirektiivi (koneet, laitteet ja koneyhdistelmät), ATEX-direktiivi (räjähdysvaarallisissa tiloissa käytettävät laitteet) ja SEVESO-direktiivi (suuronnettomuusvaarat).

Direktiivien ja niiden mukaisten kansallisten säädösten vaatimukset ovat pakottavia. Vaatimuksia tulkitaan niihin liittyvien eurooppalaisten yhdenmukaistettujen SFS-EN-standardien avulla, jotka osoittavat direktiivien mukaisen ja vähitellen kehittyvän turvallisuuden vaatimustason. Siten yhdenmukaistettujen standardien mukaisten ratkaisujen oletetaan täyttävän säädöksissä esitettävät vaatimukset. Toisaalta yhdenmukaistettujen standardien

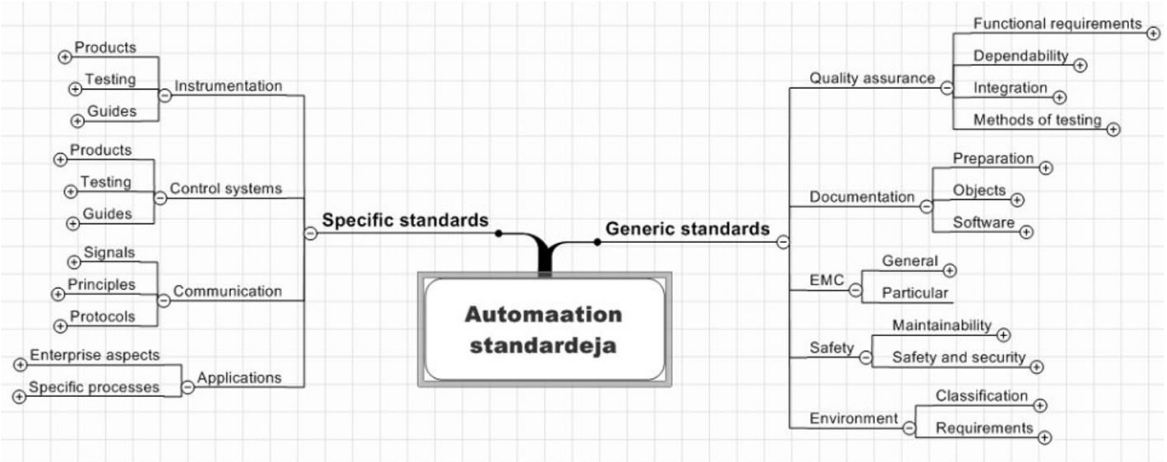
osoittaman turvallisuustason alittavat ratkaisut voivat antaa aihetta epäillä ratkaisun lainmukaisuutta.

Teollisuusautomaation eurooppalaiset standardit (CEN ja CENELEC) ja kansainväliset standardit (ISO ja IEC) esittävät standardisoituja menetelmiä riskien hallintaan, riskin arviointiin sekä teknisiin ja organisatorisiin toimenpiteisiin riskin vähentämiseksi (kuva 22). Erityisesti IEC:n ja CEN:n ohjausjärjestelmien suunnittelua ja turvallisuutta koskevat standardit antavat järjestelmällisen perustan turvallisuuden varmistamiseksi tuotantoprosessien ohjauksessa. Lisäksi eri alojen ammatilliset- ja asiantuntijajärjestöt (esimerkiksi IEEE, EWICS ja ISA) ovat laatineet omia turvallisuuteen liittyviä standardeja, teknisiä raportteja ja ohjeita oman alansa yritysten riskien hallintaan.

	SÄHKÖALA	TELEVIESTINTÄ	MUU TEKNIIKKA
MAAILMA	**IEC** IEC-standardit	**ITU** ITU-suositukset	**ISO** ISO-standardit
EUROOPPA	**CENELEC** EN-standardit	**ETSI** EN-standardit	**CEN** EN-standardit
SUOMI	**SESKO** **SFS-standardit**	VIESTINTÄVIRASTO SFS-standardit	**SFS** SFS-standardit

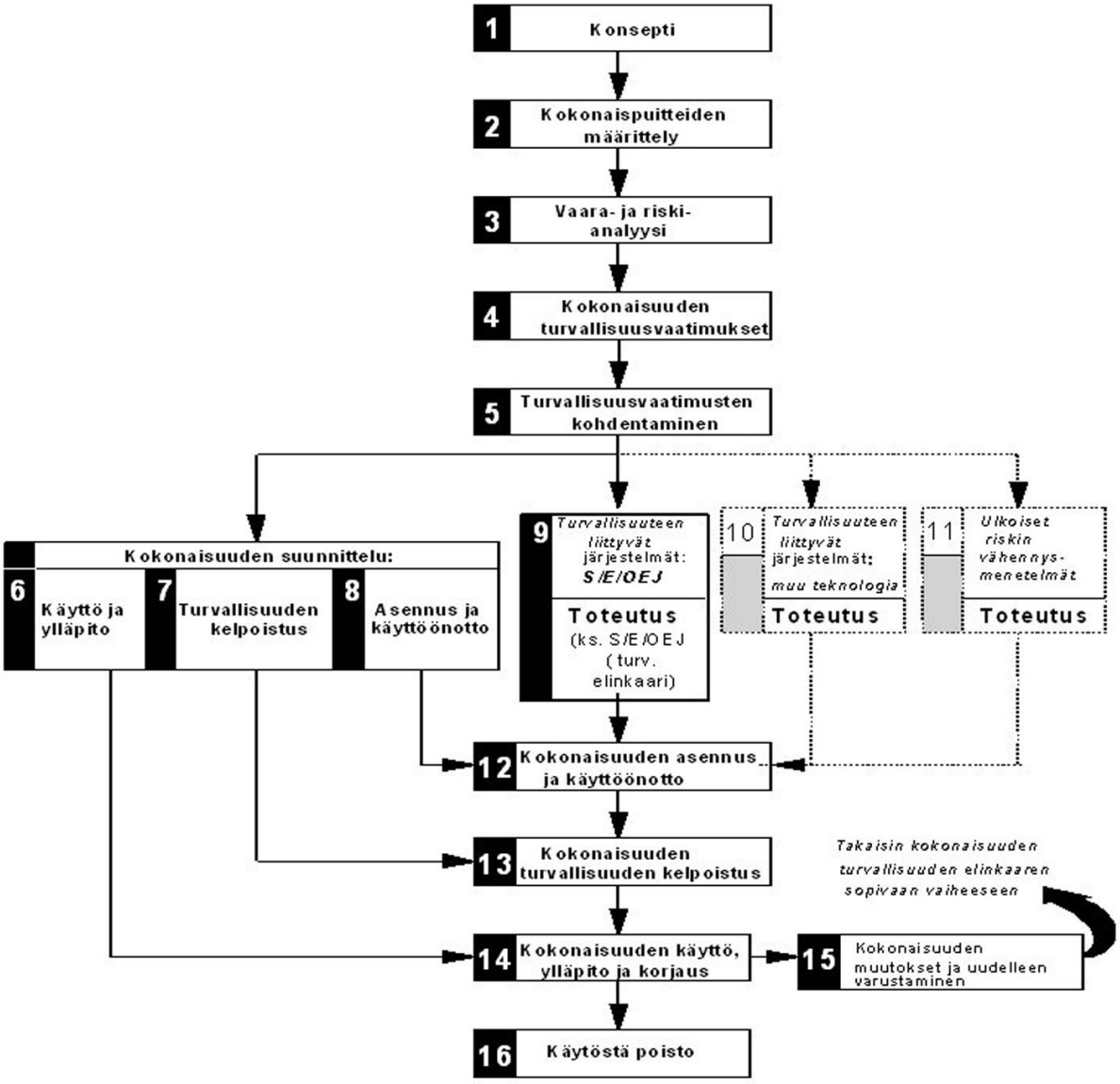
Kuva 22. Standardisoimisorganisaatioita.

Standardisoimisorganisaatiot ylläpitävät standardiluetteloita, joihin on pääsy verkkosivuilta. Standardeja voi hankkia paperimuodossa, sähköisenä tai edullisimmin standardikäsikirjoina. Standardisointi automaation alueella on hyvin hajanaista. Kuvassa 23 esitetään yksinkertaistettu jäsentely automaatioon liittyvistä standardisoimiskohteista, joista vastaavat IEC:n tekniset komiteat (Technical Committee TC) ja alakomiteat (Subcommittee SC).



Kuva 23. Automaation IEC standardien ryhmittely (Seppo Pyyskänen, Duocon Oy).

Teollisuusautomaation toiminnallisen turvallisuuden lähestymistapa (Functional Safety) on laajalti hyväksytty lähtökohdaksi teknisten järjestelmien turvallisuuden varmistamiseen. Ohjelmoitavien, elektronisten ja sähköisten järjestelmien toiminnallisen turvallisuuden elinkaarimalli esitetään standardisarjassa IEC 61508 1–7 [7]. Siinä esitettävä turvallisuuden elinkaarimalli voi olla perustana myös muiden toimintojen (tietoturva, ympäristönäkökohdat, käynnissäpito jne.) suunnittelussa (kuva 24).



Kuva 24. Elinkaarimallin vaiheet (IEC 61508-1).

Standardi IEC 61508 1–7 [7] on ns. kattostandardi, joka kattaa muun muassa prosessiteollisuuden ohjelmoitavat, elektroniset ja sähköiset automaatiojärjestelmät. Sen pohjalta on valmisteltu ja valmistellaan eri aloille sovellusstandardeja. Prosessiteollisuuden sovellusstandardi IEC 61511 [8] on kolmiosainen, ja sen ensimmäisessä osassa on vaatimukset, toisessa soveltamisohjeita ja kolmannessa prosessien riskin arviointia. Koneautomaatiojärjestelmien sovellusstandardi IEC 62061 [25] on julkaistu vuoden 2005 alussa.

Standardissa IEC 61508 ja sen sovellusstandardeissa on eri turvallisuuden eheyden tasoille (Safety Integrity Level, SIL) määritettyjä vaatimuksia, jotka ovat asiaankuuluvia myös tietoturvan kannalta suunnittelu-, käyttöönotto- ja ylläpitoprosessin elinkaaren eri vaiheissa. Vaikka tietoturvaa ei näissä standardeissa erikseen käsitellä, voidaan standardeja soveltaa osittain myös tietoturvan alueelle. IEC:ssä on aloitettu valmistelutyö uusien automaatiota koskevien tietoturvastandardien laatimiseksi. Uusia projekteja on käynnistetty muun muassa teknisten komiteoiden TC 65 (Industrial-Process Measurement and Control), TC 45 (Nuclear instrumentation) ja sen alakomitean SC 45A (Instrumentation and Control of Nuclear Facilities) vastuualueilla.

IEC:n komitean TC65:n alakomitea SC65C (Digital Communications) käsittelee muun muassa tietoturvaa ja sen työryhmä WG13 (Cyber Security) valmistelee teollisuusautomaation tietoturvastandardia ISA:n raporttien pohjalta. Standardi suuntautuu erityisesti valmistusteollisuuden tietoturvaan. Uusin versio on standardiehdotus 65/360/NP [26]. IEC:n standardeissa on vaatimuksia teknisten järjestelmien väliselle tietoliikenteelle (esimerkiksi kenttä- ja turvaväylät). Valmisteilla on muun muassa standardi 61784-4 [27], joka käsittelee kenttäväyliä ja siinä yhteydessä niiden tietoturvavaatimuksia.

Monet turvallisuusperiaatteet sopivat sellaisenaan myös tietoturvan käsittelyyn, esimerkiksi turvallisen vikaantumisen periaate, jonka mukaan myös tietoturvan aiheuttamien ongelmien (viiveet, katkot, virheelliset tiedot) olisi johdettava järjestelmä turvalliseen tilaan. Tällöin turvallisuus saadaan varmistettua, mutta toisaalta toiminnan pysähtyminen voi johtaa taloudellisiin menetyksiin. Ongelmana on, että tietoturvan häiriöt eivät aina ole niin yksikäsitteisiä, että niistä voitaisiin suoraan johtaa järjestelmä turvalliseen tilaan. Kysymys voidaan asettaa myös kuinka paljon epäkäytettävyyttä voidaan sallia tietoturvan häiriöiden johdosta.

Ensimmäinen ISO:n tietoturvastandardi ISO 17799 tähtäsi tietoturvan organisointiin ja muun muassa tietojärjestelmiin tunkeutumisen estämiseen. Standardi valmistui vuonna 2000 ja sen uusin versio on ISO/IEC 17799:2005 [2]. Standardissa kuvataan yrityksen toimenpiteitä ja esitetään ohjeita miten luodaan organisaatio tietoturvan kehittämiseen yrityksessä.

5

Teollisuusautomaation tietoturvaratkaisuja ja -käytäntöjä

Tässä luvussa keskitytään automaatioverkon sekä siihen liittyvien sovellusten tietoturvaan liittyviin asioihin. Koska automaatioverkko on osa koko tehdasverkkoa (toimistoverkkoa tai sisäverkkoa), lähdetään tässä yhteydessä siitä perusolettamuksesta, että tehdasverkon tietoturva on hoidettu asianmukaisesti. Samoin oletetaan, että myös yrityksen muut turvallisuuden osa-alueet, kuten fyysinen tietoturva ja tilaturva, on hoidettu asianmukaisesti. Tässä luvussa noudatetaan pääasiallisesti teknistä lähestymistapaa. Toimintaprosesseja on käsitelty tarkemmin jo edellisissä luvuissa, joten niitä käsitellään satunnaisemmin. Tästä huolimatta on korostettava, että oikeilla toimintaprosesseilla ja tietoturvapolitiikoilla varmistetaan tietoturva käytännössä, esimerkiksi tietoturvatilanteen seuranta.

5.1 Teollisuusautomaation tietoturvan hallinta

Kuten toimistojärjestelmissä myös teollisuusautomaatiossa tietoturvan perushaasteina ovat tietoturvan vaatima jatkuva ylläpito ja tietoturvauhkien jatkuva muutos. Nykyisessä verkottuneessa ympäristössä teollisuusautomaation kokonaisuuden ja sen tietoturvan hallinta on noussut yhä tärkeämmäksi tehtaan käytettävyyden varmistamisessa. Tietoturvan varmistamiseksi on saatava aikaan yhteinen ymmärrys monien eri tahojen kesken, tavallisesti ainakin laitoksen IT-organisaation, laitoksen automaatio-osaston sekä automaatiotoimittajan kesken. Käytännössä tätä haastetta voi lisätä esimerkiksi se, että mukana on yrityksen konsernitason IT-organisaatio, joka voi sijaita kokonaan eri maassa kuin kyseessä oleva laitos. Yhteinen ymmärrys ei valitettavasti läheskään aina toteudu käytännön tasolla, ja usein myös IT- ja automaatiomaailman erilaiset terminologiat aiheuttavat ongelmia keskinäisessä ymmärryksessä. Lisähaasteena on usein tehtävien hoidon ulkoistaminen tehtaan ulkopuolisille tahoille, tästä esimerkkinä prosessilaitteiden jatkuvan ylläpidon ulkoistaminen.

Tietoturva voidaan jakaa kahteen alueeseen:

- Ennakoiva tietoturva, jolla pyritään mahdollisimman kattavasti varautumaan ja ehkäisemään ennakolta mahdolliset häiriöt.

- Tietoturvahäiriöiden (Security Incidents) hallinta eli toimintaratkaisut, joilla varmistetaan toiminta häiriötilanteessa sekä korjaavien toimenpiteiden välitön toteutus ja nopea toipuminen.

Molemmat alueet vaativat teknisten ratkaisujen lisäksi hyvät ja toimivat toimintaprosessit, jotta tuotannon häiriötön toiminta voidaan varmistaa. Vaikka vaadittavat toimenpiteet mahdollisesti jakautuvatkin usealle taholle, lopullinen vastuu tehtaan toiminnasta on aina teollisuuslaitoksen johdolla. Siten myös johdon tasolla vaaditaan perusymmärrystä tietoturvan merkityksestä liiketoiminnan jatkuvuudelle.

5.1.1 Vaatimuksia automaatiojärjestelmän tietoturvalle

Yritykset vastaavat omien tehdasverkkojensa tietoturvasta. Yrityksillä on omat tietoturvapolitiikkansa, joiden mukaan toimitaan ja joiden avulla varmistetaan sisäinen tietoturva ja sen perusperiaatteet, kuten

– verkot on erotettu Internetistä palomuurien avulla, ja liikenne palomuurin läpi on tarkoin rajattua
– sisäverkossa käytetään virustorjuntaohjelmistoja ja ne pidetään ajan tasalla
– Internet-liikennettä tarkkaillaan, jolloin tyypillisiä toimenpiteitä ovat esimerkiksi selainliikenteen (HTTP) ja sähköpostiliikenteen tarkkailu sekä havaittujen virusten ja roskapostien poistaminen.

Korkeat käytettävyysvaatimukset sekä toimiminen tosiaikaisessa prosessinohjausympäristössä aiheuttavat automaatiojärjestelmien tietoturvalle lisävaatimuksia. Tämän vuoksi kaikki toimistoympäristöön tarkoitetut tietoturvapolitiikat ja -periaatteet eivät sellaisenaan sovellu automaatiojärjestelmiin.

Automaatiojärjestelmän tietoturva on, kuten tietoturva yleensäkin, riskien hallintaa, jota optimoidaan korkean käytettävyyden, tietoturvatason sekä käytettävien kustannusten kesken. Koska nykyisessä verkottuneessa maailmassa täydellistä tietoturvaa ei voida saavuttaa, on tietoturvaa arvioitava nimenomaan riskien hallinnan näkökulmasta. Tästä lähtökohdasta on määritettävä hyväksyttävä tietoturvataso tapauskohtaisesti ottaen huomioon muun muassa ohjattavan tuotantoprosessin kriittisyys, kuten ympäristövahinkojen ja henkilövahinkojen mahdollisuus, sekä tarvittavat tietoliikenneyhteydet. Valitut tietoturvaratkaisut ja se kuka varsinaisen työn suorittaa, vaikuttavat tietoturvatasoon ja oleellisesti myös siihen, kuka kantaa vastuun mahdollisen vahingon sattuessa.

Järjestelmien korkean käytettävyyden ja riittävän turvallisuuden varmistamiseksi kaikissa olosuhteissa on tietoturva-asiat hoidettava asianmukaisesti. Tämä asettaa erittäin suuret vaatimukset automaatio- ja informaatiojärjestelmille ja erityisesti niiden

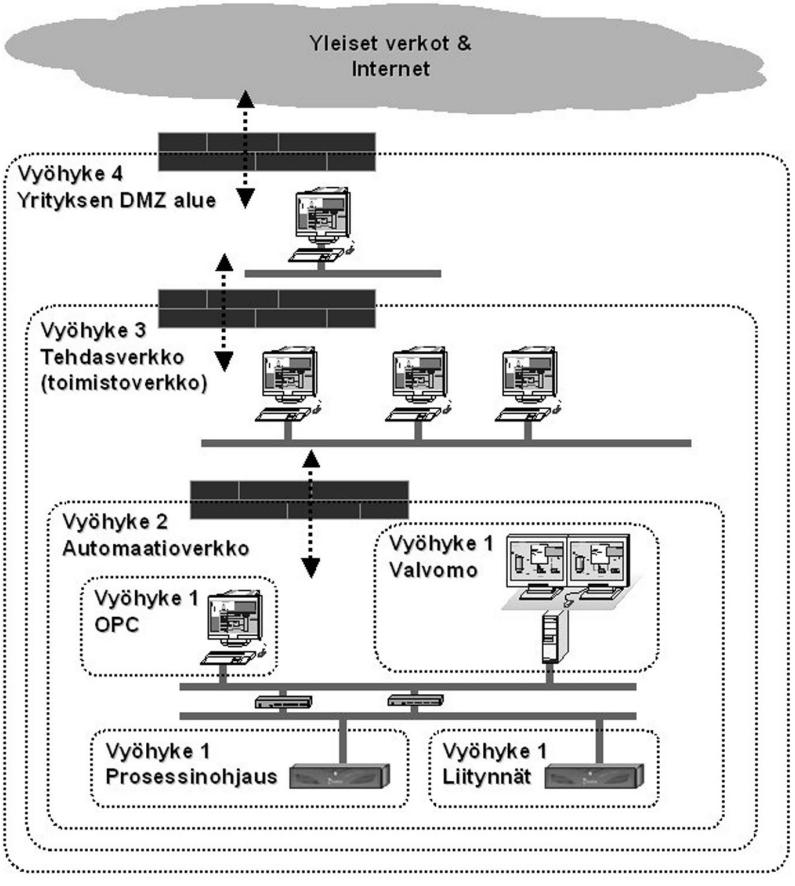
– verkkoarkkitehtuurille
– verkon suunnittelulle, mukaan lukien rajapinnat ja liitynnät automaatioverkosta muihin verkkoihin ja sovelluksiin

– tietoturva-ohjelmistojen käytölle
– tietoturvaparannusten määrittelylle ja toteutukselle
– tietoturvapäivitysten hallintaan.

Automaatiojärjestelmä tulee suunnitella siten, että se havaitsee ja sietää mahdollisimman hyvin virhetoimintoja ja että vikatilanteesta toipuminen on nopeaa. Koska kuitenkaan erilaisia ohjelmistovirheitä, käyttäjän virheitä ja hyökkäyksiä ei voida täysin estää, on mahdolliset vahingot syytä pyrkiä rajoittamaan mahdollisimman pieniksi.

5.1.2 Syvyyssuuntainen suojaus

Mikään yksittäinen ratkaisu ei takaa riittävää suojaa kaikkia erilaisia tietoturvauhkia vastaan. Tietoturvaa voidaan kuitenkin toteuttaa useilla toisiaan täydentävillä ratkaisuilla, joiden avulla voidaan saavuttaa riittävä suoja uhkia vastaan. Tietoturva on yhtä vahva kuin sen heikoin lenkki, joten kaikkien käytettävien ratkaisujen on oltava asianmukaisesti suunniteltu, toteutettu ja ylläpidetty.



Kuva 25: Syvyyssuuntainen suojaus.

Syvyyssuuntainen suojaus (Defense-in-Depth) tarkoittaa kuvassa 25 esitettyä mallia, joka perustuu siihen, että moneen eri vyöhykkeeseen sijoitetuilla tietoturvatoimenpiteillä saadaan aikaan huomattavasti tehokkaampi suojaus kuin mitä on mahdollista saavuttaa yhden ainoan suojausratkaisun käytöllä. Tässä mallissa on huomattavaa, että suojausmenetelmät voivat käsittää teknisten ratkaisujen (kuten kuvassa esimerkiksi palomuurit) lisäksi myös prosesseja, ohjeita, koulutusta sekä muita toimenpiteitä ja ratkaisuja joilla tietoturvaa parannetaan.

5.1.3 Automaatioverkon hallinta

Vaikka tehdasverkon tietoturva olisikin hoidettu asianmukaisesti, valvomatonta tietoliikennettä ei saa sallia ilman muuta, koska se on joka tapauksessa automaatiojärjestelmän kannalta tietoturvariski. Aina ei voida edes luottaa siihen, että sisäverkon tietoturva olisi hoidettu asianmukaisesti, ja lisäksi sisäverkossa voi toimia tahoja, joilla on sekä motiivi häiriön aiheuttamiseen että taito sen toteutukseen. Käytännössä tämä tarkoittaa, että automaation kannalta toimistoverkkoa, samoin kuin muita automaatioverkkoja, on pidettävä potentiaalisesti yhtä epäluotettavana kuin Internet-verkkoa. Tämä pitää paikkansa myös toisin päin, eli sisäverkon kannalta on automaatioverkkoja pidettävä yhtä epäluotettavana kuin Internet-verkkoa muun muassa siksi, että automaatioverkon kautta voi tunkeutua sisäverkkoon. Samalla tunkeutuja voi aiheuttaa automaatiojärjestelmälle haittaa käyttäessään sen resursseja toimistoverkon heikkouksien tutkimiseen.

Sisäverkon ja automaatioverkon tietoturvavastuut on syytä pitää erillään, koska sama taho ei tavallisesti voi vastata molemmista, mutta molempien verkkojen hallinnan on oltava mukana samassa tietoturvaorganisaatiossa. Automaatioverkkoja muodostettaessa kannattaa välttää myös tarpeettoman suuria tietoturvavyöhykkeitä. Automaation tietoliikenneverkkoja käsitellään tarkemmin luvussa 5.4.

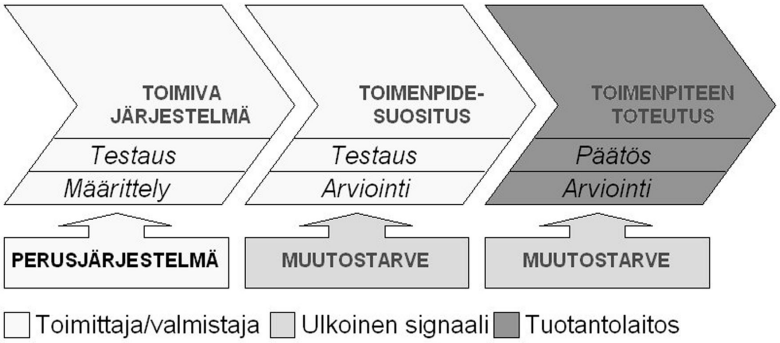
5.2 Tekniset menetelmät ja ratkaisut

Useat automaatiojärjestelmien toimittajat ovat luoneet toimitettaville automaatiojärjestelmilleen omat tietoturvapolitiikat ja -periaatteet, joilla määritetään järjestelmiin parhaiten sopivat tietoturvaratkaisut. Koska nämä politiikat ja periaatteet saattavat poiketa yritysten omista tietoturvapolitiikoista, on yrityksen oman IT-osaston tarpeellista olla mukana sopimassa tietoturvaan liittyvistä asioista. Automaatiotoimittajan ja teollisuuslaitoksen automaatio- ja IT-osastojen yhteistyönä voidaan varmistaa tietoturvaan liittyvien toimintaprosessien yhteensovittaminen, ja siten varmistaa automaation korkea käytettävyys, tuotantolaitoksen tuotannon jatkuvuus ja automaatiojärjestelmän korkea tietoturva. Yhteistyön laiminlyöminen ja yksinomaan toimittajan

politiikan noudattaminen voivat vaarantaa yrityksen oman tietoturvapolitiikan, ja vastaavasti vain yrityksen periaatteiden noudattaminen voi vaarantaa koko automaatiojärjestelmän toimivuuden (ks. luku 3.9 ja liite 9).

Yleiset perusperiaatteet, joilla voidaan huomattavasti rajoittaa teollisuusautomaation käytettävyysriskejä varsinkin kaupallisia komponentteja käytettäessä, ovat muun muassa

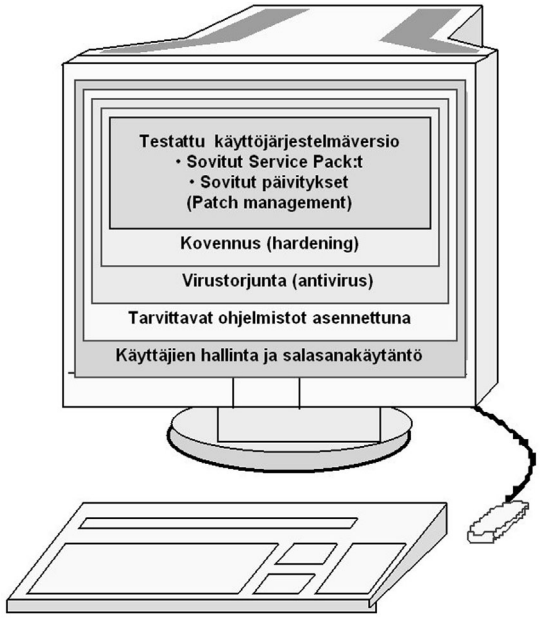
– ratkaisujen vakiointi
– muutosten arviointi ja testaus
– muutosten hallittu toteutus.



Kuva 26. Yleiset tietoturvan perusperiaatteet.

Jotta kuvassa 26 mainitut periaatteet saataisiin toimimaan käytännössä, tarvitaan ennalta suunnitellut ja harjoitellut toimintaprosessit, joilla tietoturva saadaan hyväksyttävälle tasolle.

Työasemat automaatioverkossa ovat hyvää suojausta vaativia komponentteja. Esimerkkinä esitetään kuvassa 27 työaseman tietoturvan parantamiseen liittyviä toteutuksia.



Kuva 27. Työaseman suojaaminen automaatioympäristössä.

Kaikkia olemassa olevia tietoturvan parantamistoimenpiteitä ei välttämättä voida toteuttaa vaarantamatta automaatiojärjestelmän käytettävyyttä. Joka tapauksessa ne toimenpiteet on toteutettava, jotka on mahdollista tehdä toimivuutta vaarantamatta. Jos laitetta ei voida tehdä tietoturvallisemmaksi, on tämä otettava huomioon sen käytössä.

Testaamattomien ohjelmistojen tai tietoturvapäivitysten asennus käynnissä olevaan tuotantolaitokseen on erittäin suuri käytettävyysriski, joten kaikki toimenpiteet ja käytettävät ratkaisut on huolellisesti testattava ennen niiden käyttöönottoa. Toisaalta puutteellinen tietoturva, kuten tietoturvapäivitysten laiminlyönti, voi saada aikaan käytettävyysriskin. Käytännön perusongelmana onkin arvioida parhaat toimenpiteet, joilla käytettävyys varmistetaan samalla kun tietoturvariskit minimoidaan.

5.2.1 Ratkaisujen vakiointi

Teollisuusautomaation yhteydessä puhuttaessa vakioinnilla tarkoitetaan sekä suunnittelun alussa tehtävien ratkaisujen ja niiden valintaan liittyvää osien vakiointia että valitun ratkaisun säilyttämistä muuttumattomana järjestelmän koko elinkaaren ajan. Tässä on periaatteellinen ongelma, sillä vakiointi teollisuuslaitoksen näkökulmasta on helposti ristiriidassa automaatiotoimittajan näkökulmaan ja päinvastoin. Tilannetta saattaa hankaloittaa vielä mahdollinen tietoturvaratkaisujen toimittaja, joka tuo oman näkemyksensä asiaan.

Nykyaikainen automaatiojärjestelmä on laaja ja monimutkainen kokonaisuus, johon kuuluu erilaisia laitteita ja ohjelmistoja. Osana kokonaisuutta käytetään myös komponentteja, joita ei ole alun alkaen suunniteltu käytettäväksi vaativissa teollisissa ympäristöissä. Tällaisen monesta osasta koostuvan järjestelmän toiminnan ja sen eri osien yhteensopivuuden todentaminen vaatii sekä syvällistä tietämystä että pitkäjänteistä ja jatkuvaa testausta. Lisäksi tarve liittää automaatiojärjestelmä muihin järjestelmiin voi aiheuttaa tilanteen, jossa kokonaisuus ei välttämättä ole tietoturvamielessä kenenkään hallinnassa.

Ohjelmistovirheet

Therac 25 -säteilyhoitolaitetta (Yhdysvallat ja Kanada, 1985–1987) käytettiin kasvainten säteilyhoitoon. Siirryttäessä laitteen edeltävästä mallista uuteen malliin siitä poistettiin osat, jotka estivät vaarallisen säteilyn. Laitteen valmistajat luottivat siihen, että laitetta ohjaava huolellisesti testattu ja loogisesti selkeä ohjelma toimii oikein. Laitteen ohjelmistossa oli kuitenkin useita vaikeasti havaittavia virheitä, jotka eivät paljastuneet testattaessa. Laite antoi suuria säteilyannoksia, jotka paljastuivat aluksi ainoastaan potilaiden reaktioista sekä myöhemmin säteilyvaurioista. Laitteen valmistaja ei aluksi myöntänyt virheitä. Vasta viranomaisten puuttuminen ja laitteen käyttäjien yhteistyö tuottivat tuloksia.

Opetuksia: Edes hyvin testatun ohjelmiston toimintaan ei voi välttämättä luottaa, ja lainsäädännön ja viranomaisten merkitys vastuiden asettamisessa ja valvonnassa on erittäin tärkeää. Kritiikitön luottaminen ohjelmistojen toimivuuteen ei riitä, vaan tarvitaan myös suojausjärjestelmät, jotka tässä tapauksessa oli poistettu.

Nykyisin monet ohjelmistot ovat niin laajoja, että niiden täydellinen testaaminen on mahdotonta. Esimerkiksi haittaohjelma saattaa käyttää tuntemaansa ohjelmavirhettä tunkeutumiseen tai haitan aiheuttamiseen, tai kuormittaa muisti- ja laskentakapasiteettia siten, että muutoin piilossa pysynyt ohjelmistovirhe alkaa vaikuttaa. Ohjelmistoihin tulisikin sisältyä menetelmiä, joilla ohjelmiston virheellinen toiminta havaitaan ajon aikana ja jotka rajoittavat virheiden vaikutusta ja auttavat vikatilanteista toipumisessa.

Jotta kokonaisuuden käytettävyys voitaisiin varmistaa teollisessa ympäristössä, on järjestelmän kokoonpano ympäristöineen pidettävä mahdollisimman muuttumattomana ja tämän kokoonpanon on oltava kattavasti testattu. Kaikkien muutosten, olivat ne sitten korjauksia tai lisäyksiä, on oltava hyvin perusteltuja. Siten hyväksytty ja yhteisesti noudatettu menetelmä muutosten hallinnassa on tarpeen. Muutostarpeeseen voi olla myös liiketoimintaan liittyviä syitä, kuten toiminnan tehostaminen tai yrityskaupat, joten vakioinnin säilyttäminen voi olla käytännössä haastavaa ja joskus lähes mahdotonta.

KOVENTAMINEN

Koventamisella (hardening) tarkoitetaan sellaisten perusominaisuuksien, ohjelmistojen, palvelujen ja osuuksien poistoa tai niiden käytön estämistä (sulkemista), joita ei automaatiojärjestelmän toiminnassa välttämättä tarvita. Se voi myös tarkoittaa jotain muutosta konfiguraatiossa, joka tekee ominaisuuden käytöstä vääriin tarkoituksiin hankalaa (esimerkiksi käyttöjärjestelmän tiettyjen hakemistojen pääsyoikeuksien rajoittaminen).

Lähes kaikkia järjestelmän osia voidaan koventaa, mutta tarkemmat toimenpiteet riippuvat kuitenkin koventamisen kohteesta. Seuraavassa on mainittu kaksi kohdetta, jotka ovat normaalisti koventamisen kohteena:

1. PC-työasemat ja -palvelimet ovat yleisin koventamisen kohde johtuen muun muassa käytettävien käyttöjärjestelmien laajoista ominaisuuksista. Sellaiset osuudet, kuten ohjelmistot, käyttöjärjestelmän palvelut, liikennöintiportit tms., joita ei automaatiojärjestelmän toimivuuden kannalta tarvita, voidaan poistaa tai sulkea.

   Yleisimpänä ongelmana on ollut MS Windows -käyttöjärjestelmä. Sen oletusarvoisen asennuksen jälkeen on aktiivisena paljon erilaista toiminnallisuutta, jota automaatiojärjestelmän normaalikäytössä ei tarvita. Uudemmissa MS Windows-versioissa koventamiselle on ollut vähemmän

tarvetta, koska niiden oletusarvoinen asennus on tietoturvaltaan aikaisempaa parempi (eräs merkittävä muutos tapahtui Windows Server 2003:n ja Windows XP SP2:n yhteydessä).

2. Toinen yleinen koventamisen kohde on itse automaatioverkko. Yleisinä periaatteina voidaan mainita rajapinnan liikenteen ja pääsyn rajoittaminen sekä automaatioverkon verkkolaitteiden konfigurointi häiriösietoisemmaksi (esimerkiksi reitittimet).

Koventaminen on tehtävä aina uudelle järjestelmälle ennen sen käyttöönottoa, ja tämä on normaali toimenpide useimpien automaatiojärjestelmien toimitusvaiheessa. Uusiin automaatiojärjestelmiin on myös usein saatavissa ratkaisuja ja palveluja, joilla niiden tietoturva varmistetaan myös jatkossa. Ongelman muodostavat jo käytössä olevat automaatiojärjestelmät ja niiden käyttöjärjestelmät sekä laitteistot, joihin ei välttämättä löydy tietoturvapäivityksiä tai niissä ei voida käyttää esimerkiksi virustorjuntaohjelmistoja joko niiden saatavuuden tai resurssien riittämättömyyden vuoksi. Koska tällaiset järjestelmät muodostavat valtaosan toiminnassa olevista automaatiojärjestelmistä, on olemassa olevien automaatiojärjestelmien tietoturva tarkastettava, suunniteltava mahdolliset korjaavat toimenpiteet ja huolehdittava niiden toimeenpanosta. Näitä tietoturva-arviointeja sekä niihin liittyviä toimenpideehdotuksia on saatavissa myös joiltakin automaatiotoimittajilta.

Tärkeä osa-alue on käytäntöjen luominen erilaisille liikuteltaville tallennusvälineille. CD- ja DVD-levyt sekä USB-muistit ovat erittäin laajalti käytettyjä, ja niiden mukanaan tuomat riskit on tiedostettava. Esimerkiksi CD-levyjen ja USB-muistien automaattisen käynnistyksen olisi oltava estetty automaatioverkon työasemissa.

Lisäturvaa voidaan saada aikaan muun muassa BIOS-salasanan aktivoimisella. Tämä on kuitenkin tehtävä harkitusti, ja suositeltu tapa on suojata ainoastaan käynnistysasetusten muuttaminen BIOS-salasanalla. BIOS-salasanaa ei ole normaalisti tarpeellista varmistaa aina työaseman uudelleenkäynnistyksessä.

Koventamisen onnistumiseksi tulisi ottaa huomioon, että
– automaatiojärjestelmän koventaminen tulisi tehdä ennen kuin järjestelmä kytketään verkkoon, ja tämä koskee myös sisäverkkoon kytkemistä
– peruskonfigurointi tulisi tehdä sellaiseksi, että oletuksena käyttäjällä ja laitteella on vain toiminnallisuudelle välttämättömät oikeudet
– koventaminen ei saa häiritä siinä ajettavien ohjelmistojen toimintaa.

Koventaminen vaatii käytännössä syvällistä käytettävien ohjelmistojen toiminnan tuntemusta. Esimerkiksi seuraavassa luettelossa esitetty palvelujen koventaminen edellyttää hyvää tietämystä siitä, mitä palveluja tarvitaan, jotta tarpeettomat palvelut voitaisiin kytkeä pois päältä. Seuraava periaatteellinen

luettelo on yleensä käytössä GNU/Linux-järjestelmien koventamisessa, mutta se on sovellettavissa myös muihin käyttöjärjestelmiin:

- Kovenna käynnistys (poista CD/USB/levyke-käynnistysmahdollisuus).
- Kovenna palvelut (tiedostonjaot, www/ftp-palvelut pois päältä).
- Kovenna paikallinen levyjärjestelmä (käyttäjät pääsevät vain tarpeellisiin tietoihin, estäminen esimerkiksi salauksella).
- Aseta levytilan käytölle rajat ja valvonta.
- Aseta pakotettu käyttöoikeuksien valvonta (Mandatory Access Control, MAC).
- Päivitä järjestelmän ohjelmistot ja käyttöjärjestelmä tietoturvallisiksi.

5.2.2 Muutosten arviointi ja testaus

Koska toimivaan järjestelmään tehtävät toimenpiteet voivat aiheuttaa riskejä, on jokainen toimenpide perusteltava ja hyväksyttävä. Toimenpiteet, jotka katsotaan välttämättömiksi, on testattava asianmukaisesti ja toimenpiteisiin mahdollisesti sisältyvät riskit on arvioitava. Siten kaikki vaadittavat lisäykset, muutokset ja päivitykset järjestelmään on testattava ennen niiden käyttöönottoa. Esimerkkinä toimenpiteistä ovat muun muassa käyttöjärjestelmätason päivitykset, jotka ovat normaalisti erittäin riskialttiita.

Oman ohjelmiston asennus

Automaatiojärjestelmän toiminnassa havaittiin ongelmia, jotka viittasivat liikenteen hidastumiseen valvomon työaseman ja automaatiojärjestelmän välillä. Asiaa tutkittaessa kävi ilmi, että tehtaan henkilökuntaan kuuluva oli asentanut valvomon työasemaan oman näytönsäästäjän, joka oltuaan hetken aktiivisena kuormitti konetta niin paljon, että tietoliikenne häiriintyi.

Aloite tietoturvaparannuksiin ja -toimenpiteisiin tulee yleensä automaatio-osaston ulkopuolelta, esimerkkeinä ilmoitus uudesta haavoittuvuudesta käyttöjärjestelmässä, uuden viruksen leviämisestä tai yrityksen uusista IT-vaatimuksista. Näitä tietoturvaan liittyviä asioita seurataan tällä hetkellä aktiivisesti usealla taholla (ks. esimerkiksi CERT-FI [3]).

Keskustelukanavan käyttö

Valvomotyöntekijä käytti työasemalta IRC-keskustelukanavaa, jossa tunnetun IRC-keskusteluun liittyvän tietoliikenneportin kautta kolmas osapuoli sai asennettua palvelun, joka kuormitti järjestelmää ja kasvatti verkkoliikennettä. Periaatteessa järjestelmästä oli estetty Internet-liikenne, mutta käyttäjän toimesta kyseinen liikenne tulikin sallituksi.

Opetuksia: Koska käyttäjä on yksi isoimmista riskeistä, on myös käyttäjien tietoturvatietämyksen varmistaminen tärkeää.

Automaatiojärjestelmän toimittajan on seurattava ja arvioitava, mitkä asiat voivat haitata automaatiojärjestelmän toimivuutta, määritellä näihin suositeltavat korjaus- ja parannustoimenpiteet, huolehtia toimenpiteiden testauksesta sekä riittävästä tiedottamisesta asiakaskunnalle. Teollisuuslaitosten on puolestaan vastaanotettava ja arvioitava eri tahoilta tulevat suositukset tietoturvan parantamiseen ja uhkien torjumiseen, sekä viime kädessä päätettävä suositusten toimeenpanosta ja toimeenpanojen aikatauluista. Koska kyse on verkottuneesta automaatiojärjestelmästä, jossa voi olla useiden toimittajien ratkaisuja, on tarpeettomien häiriöiden välttämiseksi yhteistyö osapuolten välillä suositeltavaa.

5.2.3 Muutosten hallittu toteutus

Verkon haavoittuvuus

Sonerassa 11.2.2005 Tampereella tehty reititysvirhe yksittäisessä runkoverkkoelementissä pysäytti hetkeksi tietoliikenteen koko Suomessa. Tulevan huollon valmisteluissa tehtiin konfigurointivirhe. Vika sai suuren osan suomalaisista yrityksistä putoamaan pois verkosta ja haittasi myös viranomaisten uuden VIRVE-verkon toimintaa ns. statusviesteissä, jotka siirtävät automaattisesti hälytyksiä hätäkeskusten välillä. Asetusvirheistä varoittava ohjelmisto olisi estänyt tapauksen. Myös tarkempi manuaalinen tarkistus olisi auttanut asiassa. IP-verkon vahvuus on myös sen heikkous: kun reititysprotokolla on hajautettu, myös vika voi hajautua.

Nykyaikainen automaatiojärjestelmä sisältää monia riippuvuussuhteita ja yhteen osaan tehtävät muutokset voivat vaikuttaa järjestelmän muihin osiin, joten väärin toteutettu toimenpide voi aiheuttaa vakavaa häiriötä koko järjestelmän toimintaan. Toimenpiteiden asianmukaisesta ja häiriöttömästä toteutuksesta voidaan ensisijaisesti varmistua valitsemalla sellainen järjestelmän toteuttava taho, joka tuntee kattavasti kyseisen järjestelmän toiminnan. Samalla varaudutaan siihen, että mahdollisiin ja yllättäviin ongelmiin voidaan nopeasti puuttua. Tämä periaate on toteutunut lähes luonnostaan aikaisemmissa suljetuissa ratkaisuissa. Nykyisessä verkottuneessa automaatiomaailmassa edellä esitetyt ongelmat on tiedostettava ja ne otettava huomioon korkean käytettävyyden ja turvallisuuden varmistamiseksi. Tämä voi aiheuttaa ristiriitaa yritysten omiin tietoturvaperiaatteisiin ja käytäntöihin verrattuna, joten ongelmat on otettava huomioon jo toimintaperiaatteiden sopimisen yhteydessä.

5.3 Varmennukset ja toipuminen

Ennakoivan tietoturvan lisäksi on varauduttava suunnitelmallisesti myös tietoturvahäiriöihin ja niiden käsittelyyn, mukaan luettuna varmennukset

(Backup) ja toipuminen (Recovery). Toipumissuunnitelmassa tulee kuvata muun muassa sovitut toimenpiteet havaittaessa virustartunta.

Jotta toipuminen tietoturvahäiriöistä olisi mahdollisimman nopeaa, varmennusratkaisujen ja -käytäntöjen on oltava suunniteltuna ja niiden toiminnat testattuna. Automaatiojärjestelmät sisältävät monia ohjelmistoja, tietokantoja ja laitteita, jotka sisältävät käytettävyyden kannalta elintärkeää tietoa järjestelmän toimivuudesta. Toipumiseen on tarvittu järjestelmäkohtaisia konfigurointeja, koska osa tiedoista on tosiaikaista sisältäen esimerkiksi tuotantoprosessin tilatietoja.

Häiriöiden sattuessa ja laitteiden vikaantuessa on ensiarvoisen tärkeää saada automaatiojärjestelmä mahdollisimman nopea palautettua normaaliin tilaan järjestelmän käytettävyyden ja turvallisuuden varmistamiseksi. Ne osuudet, jotka voidaan varmistaa, on tyypillisesti hoidettu kahdennusratkaisuilla, esimerkiksi kahdennettujen kovalevyjen (esimerkiksi RAID-kovalevyt, Redundant Array of Independent Disk) ja palvelimien käytöllä. Tarvittaessa on huolehdittava tiedon varmistuksen lisäksi myös laitteiden varaosien saatavuudesta.

Kahdennetut RAID-kovalevyt

Viisi vuotta vanhan tietokantapalvelimen emolevyllä olevalla RAID-ohjaimella toteutettu tiedonvarmennus meni hukkaan, koska emolevyn hajottua ei löydetty toista samanlaista emolevyä eikä edes toista samanlaista RAID-ohjainta. Myös varaosat oli hankkimatta. Nauhavarmennus tietokannasta oli kuitenkin olemassa ja ajan tasalla, joten mitään kriittistä tietoa ei kadonnut. Toipumisaika kuitenkin moninkertaistui ja se vei lähes viikon, koska koko palvelin jouduttiin asentamaan alusta käsin.

Opetukset: Jatkossa varmennus hoidettiin paremmin käyttämällä erillistä tunnetun valmistajan ja pidemmällä elinkaarella tuettua RAID-ohjainta, ja ohjaimesta on nyt myös varaosat valmiiksi hankittuna.

Yllä mainittu kovalevyjen kahdennus ei kuitenkaan anna turvaa kaikissa tapauksissa. Tällaisia tapauksia ovat muun muassa vahingossa tapahtuvat tuhoamiset, tietomurtojen tai ohjelmistojen aiheuttamat tiedonmenetykset, tai muut onnettomuudet, esimerkiksi tulipalot. Kahdennusten lisäksi on hoidettava myös varmistukset erillisille tallennusvälineille. Kokemuksenkin perusteella on varmennusratkaisut syytä aina säännöllisesti testata myös palautusten toimivuuden osalta. Kahdennetut kovalevyt ja varmuuskopiot tuovat myös oman haasteensa tietoturvahäiriöiden käsittelyyn, esimerkiksi työasemassa oleva virus saattaa olla myös varmuuskopioissa.

Tietoturvaan liittyvien lokitiedostojen ja -tietojen varmistaminen on tehtävä siten, että tietomurron yhteydessä niihin ei ole suoraa pääsyä. Tämä voidaan hoitaa esimerkiksi ottamalla varmuuskopiot eri koneelle.

5.4 Automaation tietoliikenneverkot

Automaatiojärjestelmissä on alettu käyttää yhä enenevässä määrin yleisiä IP-pohjaisia verkkoteknologioita. Myös kenttälaitepuolella useat kenttäväylät, esimerkiksi PROFIBUS ja FF (Foundation Fieldbus), ovat alkaneet hyödyntää IP-pohjaisia verkkoteknologioita. Tämän vuoksi verkkoratkaisujen luotettavuus on elintärkeää automaatiojärjestelmien toimivuudelle. Automaatiossa perinteisesti käytetyt kenttäväylät ovat olleet suhteellisen tietoturvallisia, koska niiden liikenne ei reitity väylän ulkopuolelle. IP-protokollan käyttö kenttäväylissä tuo mukanaan paitsi sen edut myös sen haittapuolet, joista suurin on laitteen mahdollinen näkyvyys kenttäväylän ulkopuolelle.

Automaatioverkolta edellytetään riittävän nopeaa vasteaikaa, yleensä alle 1 sekunti, eikä uutta yhteyden muodostusta sallita esimerkiksi saman etenemissekvenssin aikana. Muun muassa tämän takia verkkoratkaisut poikkeavat normaaleista verkoista. Usein teollisuusautomaation verkot toteutetaankin redundanttisesti eli varmennettuina. Verkkolaitteissa ja työasemien verkkokorteissa on oltava redundattisuutta tukevat ratkaisut.

Erityisesti teollisuuteen tarkoitettuja verkkolaitteita käytetään nykyisin rajoitetusti ja ensisijaisesti vain sellaisissa tapauksissa, joissa vaaditaan nopeuden, vikasietoisuuden, ympäristöolosuhteiden tai muiden vaatimusten perusteella tarkemmin luokiteltuja ja hyväksyttyjä verkkolaitteita. Siksi useimmat ratkaisut perustuvat laitteisiin, joita käytetään muuallakin, esimerkiksi toimistoverkoissa.

Yleisiin verkkolaitteisiin ja -tekniikoihin perustuvat ratkaisut ovat asianmukaisesti toteutettuina suhteellisen luotettavia ja hinnaltaan kilpailukykyisiä. Automaatioverkkojen rakenne ja toiminta on kuitenkin suunniteltu käyttäen hyväksi tiettyjen laitevalmistajien merkkejä ja malleja, joiden käyttäytyminen ja suorituskyky on suunnitteluvaiheessa testauksilla varmistettu. Kaikkien laitetoimittajien kaikkia laitteistoja on mahdotonta testata ja varsinkaan ylläpitää, joten muiden kuin määriteltyjen ja testattujen laitteiden käyttö muodostaa aina riskin käytettävyydelle ja mahdollisesti myös turvallisuudelle.

Luvussa 5.1 esitettävät teollisuusautomaation tietoturvan hallinnan perusperiaatteet koskevat myös verkkoratkaisuja, ja niiden mukaan tuotteistetun verkkoratkaisun muuttaminen on aina riskialtista, vaikka riskiä voidaankin rajoittaa asianmukaisella testauksella. Pääsyynä näihin muutosvaatimuksiin on yleisesti se, että käytettäessä samoja laitteita kuin yleisesti käytetään toimistoverkon puolella, halutaan myös automaatioverkon kokoonpanoon tai vähintäänkin käytettäviin verkkolaitteisiin ja -malleihin tehdä vastaavia muutoksia ja valintoja kuin toimistoverkossa. Tällöin ei aina kuitenkaan osata ottaa huomioon automaation kokonaisuutta ja siltä vaadittavaa luotettavuutta.

Vaikka eri toimittajien automaatioverkot poikkeavatkin rakenteeltaan ja laitealustaltaan toisistaan, on niiden rakenteessa myös tiettyjä yhtäläisyyksiä.

Kaksi tärkeintä automaatioverkkojen suunnittelun ja toteutuksen perusperiaatetta ovat segmentointi (verkkojen erotus) ja liikenteen rajoitus.

5.4.1 Segmentointi

Automaatioverkko on erotettava omaksi verkkosegmentikseen muusta yrityksen verkosta, esimerkiksi toimistoverkosta, tehokkaasti ja turvallisesti. Palomuurit, kuten erilliset palomuurit ja reititinpalomuurit, ovat yleisesti käytettyjä hyviä ratkaisuja verkkojen erotukseen. Automaatioverkon suunnittelun pitäisi kuitenkin lähteä siitä perusolettamuksesta, että verkko suunnitellaan jo alun pitäen niin tietoturvalliseksi, että erillistä palomuuria ei tarvita.

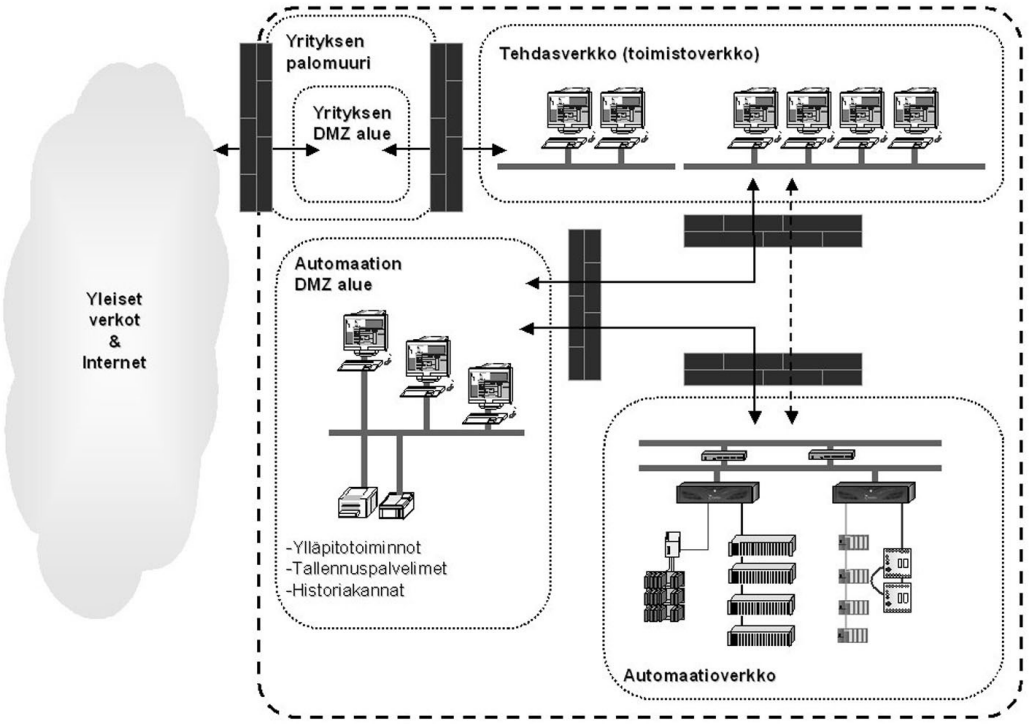
Segmentointi on tärkeää, koska se suojaa automaatiojärjestelmää muualla verkossa mahdollisesti tapahtuvilta häiriöiltä ja varmistaa osaltaan automaation häiriötöntä toimintaa. Oleellista on, että automaatio- ja tehdasverkon välinen liikenne pääsee kulkemaan vain yhtä reittiä pitkin. Tällöin myös liikenteen valvonta yksinkertaistuu. Koska asianmukaisesti toteutettu suoja on molemminpuolinen, se suojaa myös muuta verkkoa automaatiojärjestelmästä tulevilta häiriöiltä.

Myös automaatioverkkojen eri osajärjestelmien suhteen on noudatettava samaa periaatetta, eli osajärjestelmien tulee olla erotetut toisistaan. Yleensä tämä toteutetaan Virtual LAN (Virtual Local Area Network, VLAN) -tekniikan avulla, jolloin varsinaista lisäinvestointia laitteistojen osalta ei tarvita.

Verkkoratkaisua suunniteltaessa on tärkeää huomioida myös periaatteet väliaikaisten työasemien, esimerkiksi huoltopäätteiden, liittämiseksi automaatioverkkoon. Koska nämä periaatteet koskevat kaikkia osapuolia, joita automaatioverkon suunnittelussa, toteutuksessa ja käytössä tarvitaan, on myös ohjeistus ja tiedotus näiltä osin hoidettava asianmukaisesti.

Vaikka jatkuvasti edetään kohti yhä laajempaa verkkojen yhdistymistä, niin yleisenä suuntauksena näyttää olevan yhä tiukempi automaatioverkkojen erotus muusta tehdasverkosta. Yksi esitetty malli on toimisto- ja automaatioverkon väliin muodostettava välikerros eli eräänlainen suoja-alue, joka on suojattu sekä automaatioverkkoon että toimistoverkkoon päin palomuureilla, ja josta käsin tehdään muun muassa ylläpitoluonteiset toimenpiteet automaatioverkkoon. Suoraa yhteyttä toimistoverkosta automaatioverkkoon ei tässä mallissa sallita. Tämä ei-kenenkään-maa (Demilitarized Zone, DMZ) -malli on vastaava yritysten ulkopuolisissa liittymissä yleisesti käytetyn mallin kanssa (kuva 28).

Lisäturvaa tähän ajatteluun tuo malli, jossa koko liityntä toimistoverkkoon voidaan sulkea kokonaan silloin, kun toimistoverkon puolella havaitaan jokin uhka, esimerkiksi uhkaava virus. Tällöin liitynnän sulkemisen jälkeen automaatiojärjestelmä toimii ilman yhteyttä ulkopuolelle, kunnes toimistoverkon puolella havaittu uhka on tehty vaarattomaksi ja yhteys voidaan jälleen avata. Tämän lisäturvan toteuttaminen vaatii myös ratkaisuja, joilla viestin välitys verkkojen välillä hoidetaan siten, että katkon jälkeen kaikki



Kuva 28. Ei-kenenkään-maa-malli.

toiminnot ja sovellukset jatkavat toimintaansa normaalisti ilman tietojen katoamista ja muita ylimääräisiä häiriöitä.

5.4.2 Liikenteen rajoitus ja palomuurit

Liikenne automaatioverkon ja toimistoverkon välillä on rajoitettava mahdollisimman vähäiseksi. Tämä tarkoittaa sitä, että vain tarvittavat protokollat ja portit ovat käytössä, ja että yhteys mahdollistetaan vain tiettyjen nimettyjen koneiden välillä. Tässä yhteydessä myös mahdollisesti vaadittavat etäyhteydet on otettava huomioon.

Automaatioverkosta ei tule sallia koskaan suoraa Internet-yhteyttä. Myöskään muita tarpeettomia yhteyksiä ei tulisi sallia. Jos esimerkiksi valvomoon halutaan työntekijöiden käyttöön Internet-yhteys, se pitäisi hoitaa erikseen ilman yhteyttä automaatioverkkoon, esimerkiksi erillisellä selain-käyttöön tarkoitetulla työasemalla.

Kielletty Internet-käyttö valvomossa

Tehtaan valvomossa oli selain automaatiojärjestelmän sovelluksia varten, mutta selaimen suora Internetin käyttö oli estetty. Eräässä ohjelmiston

tarkastuksessa, joka ei varsinaisesti liittynyt ko. asiaan, havaittiin sattumalta, että koneella oli kuitenkin menty Internet-verkkoon ja että ylimääräisiä ohjelmistoja oli asennettu koneeseen. Lopulta selvisi, että eräs valvomotyöntekijä oli aika ajoin tuonut kotoaan oman näppäimistön, ja siinä olleilla ”ylimääräisillä” funktio-näppäimillä oli muodostettu yhteys Internet-verkkoon.

Yleinen tapa rajoittaa tietoliikennettä on käyttää palomuuriratkaisuja. Palomuureja on saatavissa sekä erillisinä laitteina että ohjelmistopalomuureina. Ohjelmistopalomuureja on sekä verkkosegmenttiä suojaavia että yhtä tietokonetta suojaavia. Hyviin verkon hallinnan periaatteisiin kuuluu suojata sekä verkko että yksittäiset koneet. Verkkolaitteissa olevia ominaisuuksia voidaan käyttää toteuttamaan osa palomuurien toiminnallisuudesta, kuten reitittimien pääsylistat (Access Control List, ACL). Pääsylistoilla rajoitetaan portti- tai IP-osoitekohtaista liikennettä. Varsinaiset palomuurit sisältävät ominaisuuksia, joilla voidaan rajoittaa tietoliikennettä vuo- ja sisältökohtaisesti. Vuokohtainen [28] liikenne tarkoittaa kahden pisteen välillä tapahtuvaa liikennettä ja sisältökohtainen sovellustason liikennettä.

Perusperiaate kaikessa tietoliikenteen rajoittamisessa on ”kiellä kaikki, salli vain tarvittava”, jolla tarkoitetaan, että vain järjestelmän käytön kannalta vaadittava liikenne sallitaan ja muuta liikennettä ei oletusarvoisesti sallita.

Yksittäisiä tietokoneita suojaavat palomuurit ovat käyttökelpoisia tehdasverkoissa, mutta niiden käyttö automaatioverkossa ei ole välttämättä mahdollista automaatio-ohjelmistoissa käytettävien verkkoteknologioiden vuoksi. Esimerkiksi OPC:n käyttö voi joissain tapauksissa olla yksi rajoittava tekijä (ks. luvut 5.4.3 ja 5.7.3).

Lisäturvaa voidaan toteuttaa uudemmilla ratkaisuilla, esimerkiksi hyökkäysten havaitsemisjärjestelmillä (IDS) sekä hyökkäysten estojärjestelmillä (IPS). Näiden todellinen hyöty lienee kuitenkin ylläpidon apuvälineenä automaatioverkon ja toimistoverkon sekä toimistoverkon ja yleisen verkon rajapinnoissa. Erityisesti niissä olevaan tietoliikennerajoituksia muuttavaan automatiikkaan on suhtauduttava varauksella.

5.4.3 OPC

OPC-tekniikan (OLE for Process Control) käyttö teollisuusautomaatiossa on kasvanut nopeasti, joten sitä kannattaa tarkastella myös tietoturvanäkökulmasta.

Tähän asti ei OPC-määrityksissä ole otettu juurikaan kantaa itse sovellusten tietoturvaan. Tietoturva on jätetty OPC:n toteutuksen pohjana olevan DCOM-tekniikan (Distributed Component Object Model) tietoturvan varaan [29]. COM-tekniikka puolestaan nojaa täysin MS Windows-käyttöjärjestelmän tietoturvaan, joskin DCOM tuo mukaan eräitä lisäkäsitteitä tietoturvaan liittyen. Tästä seuraa että OPC-sovellusten tietoturvan määrittelyyn

ja hallintaan käytetään MS Windows-käyttöjärjestelmän mukana tulevia työkaluja. Niiden käyttö tosin edellyttää, että käyttäjä ymmärtää toisaalta MS Windows -tietoturvan sekä DCOM -tietoturvan toimintaperiaatteita.

Koska samoilla hallintatyökaluilla määritetään kaikkien COM-pohjaisten palveluiden tietoturva, on näiden asetusten muuttamisessa noudatettava erityistä varovaisuutta. Erityisesti oletusasetusten muuttamista kannattaa välttää, koska näitä muuttamalla saa koko tietokoneen helposti täysin pysähdyksiin tai haavoittuvaksi. Mikäli COM-asetuksia on OPC-palvelimen osalta muutettava, on muutokset tehtävä vain niihin COM-komponentteihin, jotka liittyvät kyseiseen palvelimeen.

Oman lisänsä COM-komponenttien tietoturvaan tuo dllhost.exe -niminen ohjelma, joka nimensä mukaan ajaa dll-tiedostoihin (Dynamic Link Library, DLL) talletettuja ohjelmia. DLL on kokoelma pieniä ohjelmia, joita isompi ohjelma voi tarvitessaan kutsua. Osa OPC-palvelimista on juuri tällä tavalla pakattuja ohjelmia. Ongelmia aiheutuu dllhost.exe:n käyttämisestä sen vuoksi, että käyttöjärjestelmän prosessin nimestä ei voi päätellä, mikä ohjelmisto se itse asiassa on. Koska dllhost-ohjelmalle voi määritellä vain yhdet asetukset, vaikka se saattaa ajaa useita eri ohjelmia, aiheuttaa tämä muun muassa ongelman paikallisille palomuureille, joihin muuten voisi määritellä ohjelmakohtaisia (.exe) pakettisuodatuksia.

Yleisesti voi katsoa, että OPC-järjestelmän tietoturva saadaan riittäväksi asettamalla siihen liittyvät MS Windows -asetukset kuntoon ja käyttämällä sopivaa ja oikein konfiguroitua palomuuria [30]. Oletusasetuksia käytettäessä DCOM, johon OPC nojautuu, on erittäin haasteellinen sovellus palomuureille ja niiden konfiguroinnille [31]. Joissakin tapauksissa tietoturvan kannalta OPC ei sinänsä ole ongelma, vaan se, että sen vuoksi joudutaan sallimaan DCOM- ja RCP-liikennöinti, joiden protokollien toteutuksista on löytynyt haavoittuvuuksia.

Tietoturvan kanssa tulee helposti ongelmia, jos OPC-palvelimeen on saatava yhteys toisesta MS Windows -toimialueesta (domain) tai muusta huonommin yhteensopivasta ympäristöstä (esimerkiksi Java- tai Linux-ympäristöt). Näitä ongelmia varten on kuitenkin nykyään runsaasti erilaisia kaupallisia ratkaisuja, jotka on kuitenkin hankittava erikseen.

Yhteenvetona voidaan todeta, että OPC -järjestelmän tietoturva saadaan oikeilla toimenpiteillä riittäväksi. Mutta jos OPC-palvelin vain asennetaan, eikä tietoturvan tarkistamiseksi ja määrittämiseksi nähdä vaivaa, on järjestelmä todennäköisesti haavoittuva. Erityisesti tulee välttää COM-oletusasetusten muuttamista, mutta myöskään itse OPC-palvelimen tietoturva-asetuksia ei kannata turhaan lieventää.

5.4.4 Langattomat verkot

Langattomat verkot, kuten WLAN (Wireless Local Area Network), ovat tehnyt hitaasti tuloaan automaatioverkkojen puolelle. Suuntaus näyttää kuitenkin

olevan, että varsinainen automaatioverkko toteutetaan langallisesti ja langattomalla verkolla hoidetaan vain joitakin rajattuja toimintoja, esimerkiksi ylläpitoon liittyviä tehtäviä. Langattomat verkot perustuvat IEEE 802.11-standardeihin, ja niitä hyväksikäyttäen saadaan toimivat ratkaisut automaation tarpeisiin. Liityntä automaatioverkkoon voidaan toteuttaa käyttäen olemassa olevia ratkaisumalleja, esimerkiksi edellä mainittua palomuuria/reititinpalomuuria. Koska langaton verkko ei läpäise hyvin kaikkia kiinteitä esteitä, ja lisäksi ympäristössä voi olla erilaisia häiriötekijöitä, on langaton verkko suunniteltava asianmukaisesti, mukaan lukien vaadittava kattavuusalue. Verkko on myös testattava, ja mittausten avulla on varmistettava, että verkko toimii koko määritellyllä kattavuusalueella.

WEP (Wired Equivalent Privacy) on IEEE 802.11-suosituksen ensimmäinen työaseman ja tukiaseman välistä langatonta tietoliikennettä suojaamaan kehitetty WLAN-salausmenetelmä. WEP-salauksen on tarkoitus suojata langatonta verkkoa salakuuntelulta ja estää valtuuttamattomilta käyttäjiltä pääsy verkkoon. Tietoturvan osalta voidaan todeta, että vaikka laitteissa oletuksena oleva WEP-salaus ei olekaan riittävä, verkosta on silti mahdollisuus rakentaa tietoturvallisempi hyödyntäen esimerkiksi WPA (Wireless Fidelity Protected Access, Wi-Fi) -standardia tai uudempaa WPA2-standardia. WPA on välivaiheen tietoturvatekniikka, joka kehitettiin WEP-salauksen ongelmien paljastuttua. WPA sisältää tulevan IEEE 802.11i -tietoturvastandardin ominaisuuksia, ja se on yhteensopiva niin nykyisten kuin tulevienkin laitteiden kanssa.

Tietoturvallisin ratkaisu voidaan rakentaa käyttämällä tunnistuspalvelinta (esimerkiksi RADIUS), mutta sen käyttöä rajoittaa monesti korkea hinta, etenkin jos automaatiokäyttö on ainoa palvelimen käyttökohde. Tehokkaamman tunnistuspalvelimen käyttö onkin usein perusteltua vain tilanteissa, joissa ko. palvelin on jo olemassa. Edullisempana ja monesti riittävänä ratkaisuna voidaan käyttää valmistajakohtaisia ratkaisuja, esimerkiksi Ciscon LEAP (Light Extensible Authentication Protocol) -toteutusta, jota tukee osa muistakin valmistajista.

Langattomia yhteyksiä suunniteltaessa on otettava huomioon, että tukiasemien ja mediamuuntimien avulla tehtävä langattomuus sisältää yleensä tarpeelliset työkalut tietoturvallisen langattoman yhteyden muodostamiseksi. Ongelmallisia kohteita ovatkin lähinnä sulautetut tai vastaavat laitteet, joissa on suora langaton yhteys. Niissä ei yleensä ole resursseja vahvaan salaukseen tai VPN-yhteyksien muodostamiseen.

Langattoman verkon tietoturvaan vaikuttavia asioita ovat muun muassa kattavuusalue ja ympäristö sekä se, kuinka muutoinkin yleisestä tilaturvallisuudesta on huolehdittu. Erityisesti kuuluvuusalueen laajuus on syytä ottaa huomioon, koska se saattaa olla itse tehdasaluetta suurempi ja miettiä korjaavia toimenpiteitä, jos alue on liian laaja.Tietoja langattomista teknologioista ja niiden kehityksestä esitellään myös luvussa 5.7.1.

ANTURIVERKOT

Langattomille anturiverkoille löytyy tulevaisuudessa paljon sovelluskohteita. Näistä voidaan mainita esimerkiksi paperikoneprosessin erilaisten virtausten analysointi tai paikallisten sääennusteiden parantaminen. Anturiverkkojen leviäminen tulee lisäämään halua soveltaa niitä myös säätöön. Säätösovellukset ovat kuitenkin aikakriittisiä ja vaativat myös palvelunlaatuongelmien (Quality of Servive, QoS) ratkaisemisen langattomissa verkoissa. Tulevaisuudessa kehitetään varmasti uusia ratkaisuja palvelunlaadun takaamiseksi, mutta niissäkin tulisi erityisesti kiinnittää huomiota tietoturvan säilyttämiseen.

Älykkäät anturiverkot ovat olleet tutkimuksen kohteena useissa tutkimuslaitoksissa. Eräs tähän liittyvä tutkimushanke on Tampereen teknillisen yliopiston WIA-hanke (Wireless InterApplication Network) [32].

MOBIILIVERKOT

Pohjoismaissa voidaan suhteellisen luotettavasti käyttää paikallisten operaattoreiden mobiiliverkkoja. Silloin kun liikutaan maailmalla ja käytetään eri maiden ja eri operaattoreiden välisiä reitityksiä (Roaming), ei tietoturvan osalta voida antaa mitään takuita. Näissä tapauksissa olisi näin syntyneitä verkkoja pidettävä tietoturvamielessä epäluotettavina.

Teollisuusautomaatiossa mobiiliverkkoja käytetään rajoitetusti. Yleisimpiä käyttökohteita ovat hälytysten välittäminen puhelimiin sekä tuotanto- ja diagnostiikkatietojen siirtäminen.

Olemassa olevissa suomalaisissa verkoissa ja päätelaitteissa käytetään GSM (Global System for Mobile Communication)-, SMS (Short Message Service)-, GPRS (General Packet Radio Services)- ja Bluetooth-teknologioita (ja jopa UMTS-tekniikkaa, Universal Mobile Telecommunications Service). Näiden aiheuttamat uhkat ja ratkaisumallit ovat melko hyvin tunnettuja, mutta tätä uudemmat teknologiat voivat aiheuttaa arvaamattomampia uhkia. Tulevaisuudessa digitaalisen konvergenssin myötä mobiilipalvelujen piirissä ovat pitkälti vastaavat palvelut kuin IP-verkoissa yleensäkin.

Nykyaikaisia teknologioita ovat muun muassa UMTS-tekniikka, mobiiliverkkoihin yhdistetyt IP-pohjaiset yleiset- ja palveluverkot ja niissä tarjottavat palvelut kuten video, audio, digikuvat, Push-to-Talk, paikannuspalvelut, IP-puhelut, maksupalvelut sekä kontakti- ja tukipalvelut. Lisäksi uhkia tulee uudentyyppisistä verkkoyhteyksistä, kuten WLAN ja PAN (Personal Area Network). Asioita joihin tietoturvauhkat liittyvät ovat muun muassa

– toimijoiden ja käyttäjien tietoturvatoiminnan eritasoisuus
– toimijoiden (henkilöiden) osaamistasojen erot ja alan nopea muuttuminen
– palveluun tai laitteeseen kohdistuvat hyökkäykset ja virheet, palvelunesto, monimutkaisuus ja väärät asetukset
– käyttäjän ja palvelun tunnistus ja tietojen luottamuksellisuus
– palvelusisältöjen ja ohjelmien käyttöoikeudet ja laiton kopiointi

– uudenlaiset käyttötavat ja teknologia
– palvelujen luvaton käyttö
– haittaohjelmat, kuten virukset ja madot
– mobiili sähköinen maksaminen.

Lisätietoja mobiiliverkkojen ja -laitteiden sekä digitaalisen konvergenssin tuomista tietoturvauhkista ja -ratkaisuista esitetään muun muassa VTT:n selvityksessä [15].

RFID-TEKNOLOGIA

RFID-tekniikka (Radio Frequency Identifier) perustuu langattomaan tunnistamiseen, jossa lukulaitteella luetaan mikrosirujen sisältämät tiedot. RFID-teknologiaa käytetään muun muassa kulunvalvontajärjestelmissä, autojen lukitusjärjestelmissä ja tavaroiden merkitsemisessä. Edulliset mikrosirut voidaan sijoittaa esimerkiksi myytäviin tuotteisiin tuotetietojen esittämiseen ja logistiikan hallintaan.

RFID-teknologia mahdollistaa uusia sovellusalueita, mutta samalla se myös tuo uusia riskejä, kuten esimerkiksi yksilöllisen ja henkilökohtaisen RFID-tunnisteiden käytön mukanaan tuomat yksityisyyden suojaan liittyvät ongelmat. Toisin kuin viivakoodien sisältämät tiedot RFID-siru sisältää jokaiselle sirulle yksilöllisen tunnisteen, joten henkilöiden, yksittäisten tuotteiden sijainnin ja kulkureitin jäljittäminen on mahdollista. Riittävän voimakkaalla lukulaitteella voidaan lukea ja muuttaa sirujen tietoja, jolloin tiedon muuttamisesta voi aiheutua ongelmia. Esimerkiksi yrityksen logistiikan hallinta voidaan sekoittaa. Täten RFID-teknologian käyttöönottoon liittyvät tietoturva-asiat on syytä ottaa huomioon mahdollisimman varhaisessa vaiheessa.

5.4.5 Etäyhteydet ja tietoliikenteen salaus

Etäyhteydet ovat salaustekniikoiden käytöstä huolimatta vain yhtä turvallisia kuin niiden päätepisteet. Pahimmassa tapauksessa käyttäjä luo tietoturvallisen kanavan viruksille ja madoille yrityksen tehdasverkkoon.

Automaatiojärjestelmään vaaditaan nykyisin erilaisia etäyhteyksiä, joilla mahdollistetaan varsinkin erilaisia palvelutoimintoja. Nämä yhteydet on toteutettu usein Internetin yli, joten toteuttamisessa on erittäin tärkeää ottaa huomioon turvallisuusnäkökohdat. Yksi yleisimmistä ratkaisumalleista on käyttää suojattua liikennettä (VPN), jolloin itse liikenteeseen ei ulkopuolinen pääse käsiksi. Sen lisäksi käytetään jotain vahvaa tunnistusmenetelmää henkilön tunnistamiseen, kuten esimerkiksi RSA:n SecurID-kortteja.

Modeemien käyttö on edelleen yleistä esimerkiksi etähuollossa. Useimmiten modeemi ohittaa muut tietoliikenneratkaisut mukaan lukien tietoturvan. Lisäksi tietoturvanäkökulmasta modeemien hallinnointi on hankalaa.

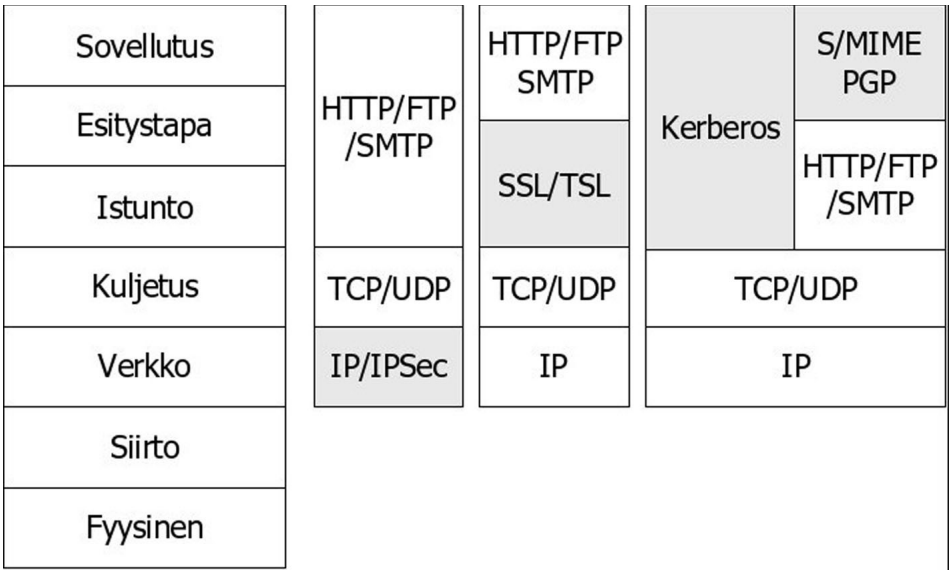
Suuntauksena onkin useita vuosia ollut siirtyminen pois modeemien käytöstä tietoturvallisempien ja paremmin hallittavien ratkaisujen käyttöön. Silloin kun modeemeja käytetään, on niiden käytön oltava valvottua ja vastuuhenkilöiden on oltava nimettyjä.

Useilla teollisuusyrityksillä on myös omia, konsernikohtaisia ratkaisumalleja, joilla etäyhteydet toteutetaan. Näillä ratkaisuilla hoidetaan etäyhteydet tavallisesti silloin, kun kyseessä on henkilön käyttämä yhteys (esimerkiksi huoltohenkilö). Nämä ratkaisut eivät normaalisti määrittele toteutustapaa silloin, kun kyseessä on sovellusten välinen liikenne (Machine-to-Machine, M2M), vaan tällöin sopiva ratkaisumalli on sovittava erikseen. Mitään yleistä ratkaisumallia ei tähän tilanteeseen näytä olevan lukuun ottamatta sitä, että yhteydet käyttävät pääsääntöisesti VPN-tekniikkaa liikenteen salaamiseen.

OSI-malli esitetään ISO:n kansainvälisessä standardissa ISO 7498-2:1989 [33]. Malli on tiedonsiirtoprotokollien yhdistelmä, jossa on määritelty seitsemän kerrosta. Kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäksi. Sen mukaisesti ei käytännön protokollapinoja juurikaan ole kehitetty. Päinvastainen tilanne vallitsee TCP/IP-viitemallin suhteen, jota ei paljoakaan käytetä, mutta siihen perustuvat protokollapinot ovat hyvin aktiivisessa käytössä.

Kuvassa 29 on esitetty yksinkertaistettu OSI-malli. Seuraavassa on esimerkkejä tietoturvan käytännön toteutuksista OSI-mallin eri kerroksilla:

- Verkkokerros: suojaamaton liikenne suojatussa kanavassa (VPN).
- Kuljetuskerros: selaimelta palvelimelle.
- Sovelluskerros: sähköpostiohjelmasta sähköpostiohjelmaan.



Kuva 29. OSI-malli sekä salauksen toteuttamismahdollisuuksia eri kerroksilla (harmaa). Kuvaa tulkittaessa on huomattavaa, että OSI-mallin eri kerrokset ja TCP/IP-protokollaperheen kerrokset eivät ole suoraan vertailtavissa.

5.5 Käytönhallinta

Tämän päivän automaatiojärjestelmässä on useita erilaisia ohjelmistoja, käyttäjiä ja laitteita. Ympäristön haasteellisuutta lisää se, että tehtaissa on yleensä kytketty yhteen useita eri toimittajien automaatiojärjestelmiä. Automaatiojärjestelmissä käytetään yhä enemmän yleisiä käyttöjärjestelmiä, kuten MS Windows ja GNU/Linux, ja lisäksi kokonaisuuteen kuuluu sekä automaatiotoimittajakohtaisia ohjelmistoja että erilaisia kolmansien osapuolien ohjelmistoja, kuten esimerkiksi tietokantaohjelmistoja. Laitepuolella käytetään myös monia erilaisia laitteita, kuten palvelimia, työasemia ja verkkolaitteita.

Tietoturvan keskeisenä tarkoituksena on varmistaa automaatiojärjestelmän oikea ja turvallinen toiminta sekä suojata järjestelmässä olevat tiedot. Tietoturvan toteutuksen eräs keskeinen tavoite on estää valtuuttamaton pääsy laitteisiin ja palveluihin sekä seurata kaikkea pääsyä eli sekä valtuutettuja että valtuuttamattomia pääsyjä ja pääsyn yrityksiä. Tämä vaatii asianmukaisen käyttäjien tunnistuksen ja toimivan käytönhallinnan.

Käyttäjien tietoturva käsittää tunnistuksen (Authentication), valtuutuksen (Authorisation) sekä seurannan (Accounting). Liikenteen tietoturva voidaan hoitaa palomuureilla, salauksilla sekä aktiivisella valvonnalla. Ongelmana on palvelujen (ohjelmistojen) ja laitteiden hallinta, esimerkkinä OPC-käyttö, joka on lisääntynyt räjähdysmäisesti automaatiojärjestelmissä ja joka voi vaatia tietoturvan hallitun poiskytkennän (ks. luku 5.7.3). Ihmisten osalta tietoturva tulisi hoitaa mahdollisimman kevyin ja luontevin menetelmin, jotta se myös käytännössä saataisiin toimimaan mahdollisimman hyvin (ks. luku 3.5.).

Käytönhallinnan (AAA) peruskäsitteet:

1. Tunnistus (Authentication, pääsynvalvonta) tarkoittaa sisään kirjautuvan henkilön tai järjestelmään kytkeytyvän laitteen luotettavaa tunnistusta. Normaalisti tämä tapahtuu esimerkiksi käyttäjätunnuksen ja salasanan avulla. Myös vahvempaa tunnistusta voidaan tarvittaessa käyttää, esimerkiksi SecurID-kortti henkilöillä ja varmenteisiin pohjautuvat menetelmät laitteilla.

   Tunnistuksen luotettavuutta parannetaan ja väärinkäyttö estetään kun
   – ohjelmistojen ja laitteiden oletussalasanoja ei käytetä
   – tyhjiä salasanoja ei käytetä
   – käyttäjien oikeudet pidetään mahdollisimman rajoitettuina (vaikka tämä ei suoranaisesti liity itse tunnistukseen, se parantaa oleellisesti väärinkäyttötapauksissa aiheutunutta haittaa).

2. Valtuutus (authorisation, pääsynrajoittaminen) tarkoittaa henkilön tai laitteen pääsyä tarpeen mukaan vain sallittuihin palveluihin ja osoitteisiin.

3. Seurannan (accounting, myös laskutus) tärkein funktio on jäljittävyyden varmistaminen. Ongelmatapauksissa voidaan selvittää, kuka tai mikä ja millä oikeuksilla on käyttänyt palvelua.

Käyttöoikeuksien päivitys

Kirjallisuudessa on kerrottu puunjalostusteollisuudesta tapaus, jossa automaatiojärjestelmässä alkoi ilmetä yhdellä ala-asemalla virhetoimintoja, joiden havaittiin johtuvan ylikuormituksesta ja tapahtuvan aina silloin, kun tietty tiedonkeruuohjelma säännöllisin väliajoin käynnistyi. Asiaa selvitettäessä ilmeni, että kyseisen tiedon keruuohjelman oli aikanaan asentanut ja laittanut käymään yhtiön keskustoimiston tutkija, joka oli saanut siihen asianmukaiset luvat ja käyttöoikeudet. Kyseinen tutkija oli yli puoli vuotta aikaisemmin vaihtanut työnantajaa, mutta ohjelma lähetti edelleen tuotantoprosessista datoja keskuskonttoriin, jossa niitä ei kukaan ollut käyttänyt. Tapaus siis paljasti käyttöoikeuksien hallinnassa olleita vakavia puutteita, jotka korjattiin.

5.6 Tietoturvapäivitysten hallinta

CERT/Coordination Center [34] arvioi, että 95 % kaikista verkkoon tunkeutumisista olisi voitu välttää pitämällä järjestelmät ajan tasalla sopivilla tietoturvapäivityksillä. Organisaatiot, jotka eivät sisällytä tietoturvaa yhtenä kriteerinään ohjelmistojen kehitykseen tai hankintaan, voivat havaita myöhemmin järjestelmän seisokkiajan kasvun, joka aiheutuu tietoturvan haavoittuvuuksista.

Yksi tämän päivän ongelmista on haavoittuvuuksien hyödyntäminen yhä nopeammin, mikä jättää vähemmän aikaa tietoturvapäivitysten testaamiseen ja asentamiseen [35]. Myös tästä syystä toimintaprosessien on oltava oikein suunniteltuja ja toimivia.

Tietoturvan haavoittuvuuksia on käyttöjärjestelmissä ja niissä käytettävissä eri tasoisissa ohjelmistoissa, kuten esimerkiksi tietokanta- ja web-palvelimien ohjelmistoissa, erilaisissa tietoturvaohjelmistoissa sekä yleisesti ottaen missä tahansa ohjelmistoissa. Näitä haavoittuvuuksia hyödyntämällä voivat erilaiset haittaohjelmat ja tunkeutujat aiheuttaa häiriöitä, jos haavoittuvuuksia ei korjata tai muulla tavoin vähennetä niihin liittyvää riskiä. Suuri osa julkistettavista haavoittuvuuksista ja korjaavista tietoturvapäivityksistä koskee sellaisia osuuksia, joita ei käytetä automaatioverkossa tai joiden tietoturvaa on esimerkiksi koventamisella aikaisemmin jo parannettu, joten ne eivät vaikuta suoraan automaatioverkkoon.

Tietoturvapäivityksiä tulee jatkuvasti ja automaatioverkon ylläpitoon liittyvät päivitykset pitäisi havaita, testata ja asentaa mahdollisimman nopeasti. Käyttöjärjestelmätason päivitysten asennus vaatii usein laitteen käyttöjärjestelmän alasajon ja uudelleen käynnistyksen. Tämä vaatii kaikilta tietoturvan

kanssa tekemisissä olevilta tahoilta, niin automaatiotoimittajilta kuin teollisuuslaitoksiltakin, aktiivista maailmanlaajuista tilanteiden seurantaa. Tämän vuoksi sisäverkoissa nuodatetaan yleistä ja suositeltavaa periaatetta, jonka mukaan kaikki päivitykset asennetaan automaattisella asennuksella. Tämä ei kuitenkaan ole mahdollista automaatioympäristössä, koska automaatioympäristössä ei ole mahdollista toteuttaa käytännössä tarvittavia testausjärjestelyjä riittävän kattavasti.

Automaatiojärjestelmien toimittajien on huolehdittava siitä, että haavoittuvuuksia ja uhkia seurataan aktiivisesti ja arvioidaan vaikuttavatko ne automaatiojärjestelmään. Kokonaisuhkan arviointi on mahdollista vain asennuskohtaisesti, joten automaatiotoimittaja joutuu arviointia tehdessään tekemään eräitä oletuksia. Esimerkiksi automaatiotoimittajan mahdollinen oletus voi olla, että automaatioverkko on erotettu toimistoverkosta automaatiotoimittajan määrittelemillä laitteistoilla ja asetuksilla. Jos näin ei ole toimittu, eivät toimittajan suositukset enää välttämättä pidä paikkaansa. Tämä on tietoturvamielessä yksi tärkeä peruste mahdollisimman vakioiduille ratkaisuille.

Jos haavoittuvuuksilla on vaikutusta järjestelmään, testataan korjaavat tietoturvapäivitykset mahdollisimman nopeasti ja kattavasti ja tiedotetaan tämän jälkeen mahdollisimman nopeasti myös asiakaskunnalle uhkista ja vaadittavista korjaavista toimenpiteistä. Eräänä haasteena on se, että vaikka päivitysten asennusautomatiikkaa ei käytännössä voida käyttää, niin päivitykset on asennettava kaikkiin tarvittaviin laitteisiin, koska pahimmassa tapauksessa yksi saastunut laite saattaa merkittävästi häiritä ympäristöään.

Koska uhkien vakavuuteen vaikuttavat myös itse teollisuuslaitosten omat tietoturvaratkaisut ja -toimenpiteet, on laitosten pidettävä huolta siitä, että haavoittuvuudet otetaan huomioon ja vaadittavat päätökset tehdään automaatiotoimittajien tiedotusten perusteella mahdollisimman nopeasti. Tietoturvapäivitysten osalta on tärkeää itse tietoturvaprosessin hyvä ja jatkuva toiminta.

Lisäksi on suositeltavaa, että myös sovelluksen käyttäjät suorittaisivat mahdollisuuksien mukaan testausta ennen päivitysten toteutusta. Esimerkkinä on RPC (Remote Procedure Call) -toiminto, jota käytetään ohjelmiston suorittamiseen kohdelaitteella etäkutsun suorittamiseen. Kun eräässä Windows-ohjelmiston korjauspäivityksessä tuli muutoksia kyseisen protokollan toimintaan, ei korjauspäivitystä voitu ottaa käyttöön ennen kuin ohjaavaan ohjelmistoon tehtiin protokollan mukaiset muutokset.

Automaatiojärjestelmien ohjelmistojen päivitykset ovat keskeinen tietoturvaongelma erityisesti laajalle alueelle hajautetuissa järjestelmissä, joissa sulautettujen laitteistojen elinkaari on varsin pitkä. Varsinkin suojausautomaation ohjelmistojen päivitys voi aiheuttaa vakavia riskejä, jos sitä ei toteuteta hallitusti. Tietoturvapäivitysten asennustarpeen määrää voidaan rajoittaa esimerkiksi tietoliikenteen rajoittamisella (haavoittuvan palveluohjelmiston porttiin kohdistuvat uhat) ja koventamisella, esimerkiksi ei pidetä käynnissä riskeiksi tunnistettuja tarpeettomia verkkopalveluja.

Muun muassa seuraavilla keinoilla voidaan ohjelmistojen päivitykset tehdä turvallisemmaksi:

- Valvotaan tarkasti tuotantoprosessin tilaa ja ohjausten järkevyyttä sekä sitä, miten paljon ohjelmat kuormittavat laskenta-, muisti- ja tietoliikenneresursseja, jotta mahdolliset ohjelman virhetoiminnot havaitaan nopeasti.
- Käytetään hyväksi redundanssia ja yksinkertaisia varajärjestelmiä.
- Käytetään hyväksi varmuuskopiointia, jotta voidaan tarvittaessa palata nopeasti päivitystä edeltäneeseen versioon.
- Arvioidaan onko olemassa käyttökelpoisia vaihtoehtoja tietoturvan parantamiseksi, jos päivitystä ei jostain syystä voida asentaa.

Päivitysten asennusten jälkeen on varmistettava normaalin toiminnan lisäksi myös se, että muu ympäristö on pysynyt muuttumattomana. Esimerkiksi MS Windows -tietoturvapäivitykset saattavat muuttaa joitain asetuksia, kuten esimerkiksi kovennukseen liittyviä asetuksia, joita kaikkia ei välttämättä pystytä testaamaan normaalissa testausympäristössä.

Päivitysten asennusten seuranta on myös suositeltavaa, jotta pystytään seuraamaan, onko kaikille laitteille asennettu kaikki vaadittavat päivitykset.

5.6.1 Eri ikäiset järjestelmät ja käyttöjärjestelmien elinkaari

Laitevalmistajat ja käyttöjärjestelmätoimittajat tukevat kaupallisia ja etupäässä toimistokäyttöön suunnattuja tuotteitaan vain tietyn ajan. Tyypillisesti tämä aika on muutamasta kuukaudesta (esimerkiksi toimistoverkon työasemat) muutamaan vuoteen (esimerkiksi MS Windows -käyttöjärjestelmä). Tämä tuo suuren haasteen teollisuusautomaatiosta vastuussa oleville tahoille, kuten automaatiotoimittajille ja tehtaiden automaatio-osastoille.

Uudet toimitukset ovat normaalisti tietoturvallisia, ja myös niiden elinkaaren hallintaan on olemassa ratkaisuja. Vanhempien olemassa olevien järjestelmien tietoturvan parantaminen on huomattavasti haastavampaa, ja se vaatii yleensä tapauskohtaisen arvioinnin tilanteesta ja korjaavista toimenpiteistä.

Automaatiotoimittajat pyrkivät toimittamaan tietoturvallisia tuotteita, mutta toimituksen jälkeinen hyvä tilanne voi huonontua nopeasti toimituksen jälkeen. Siten on syytä ottaa huomioon koko elinkaaren kattava näkökulma myös tietoturvaan ja selvittää aktiivisesti miten sitä voi parhaiten ylläpitää. Tässä korostuu myös eri osapuolten yhteistyön ja kommunikaation tarve.

5.7 Uudet ratkaisut ja teknologiat

5.7.1 Langattomat teknologiat

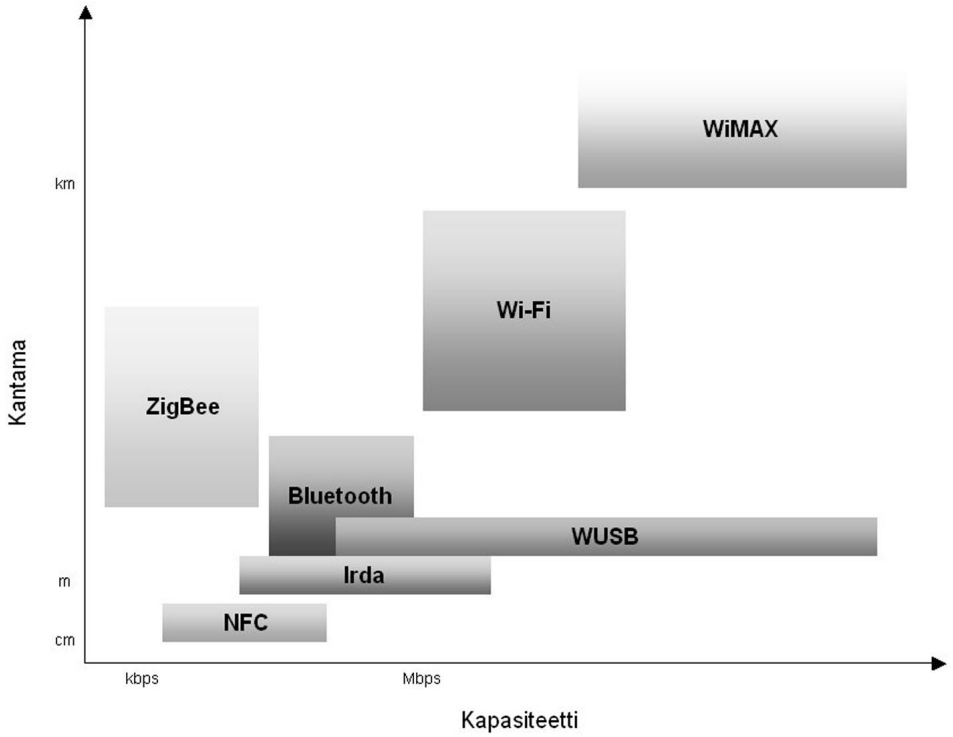
Langattomat tekniikat kehittyvät jatkuvasti, ja tulevaisuuden langattomien teknologioiden tietoturvaongelmat ovat osittain vielä tuntemattomia. Lyhyen

kantaman verkkoratkaisuja ovat muun muassa WUSB (Wireless Universal Serial Bus) ja ZigBee.

WUSB on langaton USB ja se perustuu USB:n arkkitehtuuriin. WUSB-verkossa on yksi keskitin, johon muut laitteet on liitetty. WUSB:a kehittää Wireless USB Promoter Group, ja ZigBEE on IEEE 802.15.4 -standardin mukainen lyhyen kantaman tietoliikenne-verkko.

Nämä ratkaisut ovat kuitenkin tietoturvamielessä helpompia hallita, koska niiden hyödyntäminen vaatii sijaintia hyvin lähellä verkkoa [36]. Vaikka tämä ei poista kokonaan uhkia, riskien arviointi on kuitenkin helpompaa. Suuremman ongelmakentän muodostavat WiMAX:in (Worldwide Interoperability for Microwave Access) tapaiset pitkän kantaman verkot, joita teollisuus mielellään soveltaisi, esimerkiksi SCADA-ympäristöissä, silloin kun yhteyden laatu sen sallii. WiMAX toimii langattomalla laajakaistatekniikalla. WiMAX perustuu IEEE 802-sarjan avoimeen 802.16 standardiin. Standardin kehitys on jatkunut koko ajan, ja sen kehittämisestä vastaa WiMAX Forum, johon kuuluu tällä hetkellä yli 200 yritystä ympäri maailmaa.

Pitkän kantaman kuluttajakäyttöönkin suoraan soveltuvat teknologiat tuovat valitettavasti myös hyökkääjiä (krakkereita) kiinnostavia haasteita. Jos tätä ei oteta huomioon, voidaan myös teollisuusautomaatioon luoda rajoittamaton ja ilman kulunvalvontaa oleva pääsy.



Kuva 30. Langattomat teknologiat, niiden tiedonsiirtonopeus (kapasiteetti) ja kantama.

5.7.2 IPv6 ja Internetin kehitys

Vaikka Internet-verkko on nykyisellään altis tietoturvahyökkäyksille, myös laite- ja ratkaisutoimittajien puolustautuminen kehittyy. Kehityksestä esimerkkeinä voidaan mainita AMD- ja Intel-prosessorivalmistajien ratkaisut, muun muassa puskuriylivuotojen ehkäisemiseksi sekä tietoliikenteen ennakoivan suodatuksen ja IPv6-protokollan kehittäminen ottamalla tietoturva huomioon. Myös lainsäädäntö ja kansainvälinen yhteistyö kehittyy vähitellen. Joka tapauksessa kriittisten järjestelmien kehittämisessä täytyy ottaa huomioon myös se mahdollisuus, että Internet ei aina ole käytettävissä.

Internet-protokolla IPv6 (Internet Protocol version 6) saattaa korvata tulevaisuudessa nykyisen Internet-protokollan (IPv4). IPv6 toimii jo nykyisin ja tuki protokollalle tulee muun muassa Windows XP-, Linux-, UNIX- ja MacOS-käyttöjärjestelmien mukana. IPv6 vaikuttaa jo nyt tietoturvaan, ja se on otettava huomioon verkkojen suunnittelussa sekä verkkolaitteita valittaessa ja konfiguroitaessa. Seuraavassa esitetään joitakin IPv6:n ominaisuuksia [37]:

- IPv6:ssa osoiteavaruus kasvaa 32 bitistä 128 bittiin, jolloin vaihtoehtoisia osoitteita on 2^{128} verrattuna aikaisempaan 2^{32}. Tällöin satunnainen verkko-osoitteiden etsiminen (skannaus) on käytännössä mahdotonta. Osoiteavaruuden kasvu ei estä tunnettuihin osoitteisiin perustuvaa etsintää.
- Koska IPv6 on jo käytössä, hyökkääjät saattavat käyttää protokollaa jo nyt. Ylläpitäjien taidot eivät ole vielä kehittyneet, eivätkä palomuurit ym. tietoturvaratkaisut vielä osaa välttämättä käsitellä IPv6-liikennettä.
- IPv6 sisältää IPSec-salauksen. IPSec protokollan laajennus määrittelee IP-protokollien tietoturvaominaisuuksia [38] ja [39].
- IPv6:ssa pyritään varmistamaan tietoliikennepaketin perillemeno muuntumattomana. IPv6:ssa lähettäjän väärentäminen on vaikeampaa, jolloin muun muassa haitallisen tietoliikenteen jäljittäminen helpottuu.

Salauksella voidaan muodostaa tiedonsiirtotunneleita, jotka ohittavat palomuurit. IPv6:een sisällytetty verkon automaattinen muokkaus (Autoconfiguration) vaikeuttaa hyökkääjää tutkimasta järjestelmän heikkouksia. Toisaalta hyökkääjä voi järjestelmään päästyään muuttaa verkon rakennetta.

Koska käytössä olevat laitteet ja ratkaisut ovat IPv4 toteutuksia, IPv6:n käyttöönotto ilman oikeaa konfigurointia esimerkiksi palomuureihin voi aiheuttaa tietoturvariskin. Tämä johtuu siitä, että IPv6 on oma protokollansa, jossa kaikki IPv4:lle suunnitellut tietoturvamekanismit eivät toimi. Pahimmassa tapauksessa voidaan luoda huomaamatta IPv6-tunneli yrityksen sisäverkkoon.

5.7.3 OPC jatkokehitys

Perus OPC-DA (Data Access) ei sovellu eri yritysten väliseen tai Internet-verkon yli hajautettuun integraatioon, jossa asiakas- ja palvelinkoneet ovat eri toimialueissa ja jopa eri ylläpitäjien valvonnassa. Toinen ongelma on

DCOM. Tällaiseen sovellukseen sopii periaatteessa OPC-DA:n pohjalta kehitetty OPC-XML-DA, joka pohjautuu nimensä mukaan XML-muotoiseen SOAP-protokollalla tapahtuvaan tiedonsiirtoon. Ongelmallista OPC-XML-DA:ssa on juuri tietoturva, jonka toteuttamiseen itse määrittely ei juurikaan ota kantaa.

OPC:sta on kehitteillä uusi versio nimeltään OPC-UA (Unified Architecture), joka aiemmista OPC määrityksistä poiketen määrittelee myös järjestelmän tietoturvalle minivaatimukset. Koska OPC-UA on vasta kehitysasteella sen tietoturvasta on toistaiseksi mahdotonta sanoa mitään varmaa. Tällä hetkellä näyttää siltä, että OPC-UA on kehitetty yhteensopivaksi Microsoftin kehitteillä olevan uuden web-sovelluspalvelu ympäristön (Web Service, WS) kanssa, koodinimeltään Indigo, joten OPC:n tietoturvan hallinta voidaan haluttaessa hoitaa MS Windows -käyttöjärjestelmän työkaluilla. OPC-UA ei kuitenkaan ole sidottu yhtä tiukasti MS Windows -käyttöjärjestelmään kuin perus-OPC.

Tietoturva on tullut mukaan myös OPC kehitykseen. Koska olemassa olevia ratkaisuja on kuitenkin runsaasti, vaatii OPC-järjestelmän toteutus edelleen suunnittelua ja oikeita toimenpiteitä tietoturvan varmistamiseen (ks. luku 5.4.3).

6

Teollisuusautomaation tietoturvan kehittäminen

Teollisuusautomaation verkottuminen yleisiin tietoverkkoihin etenee nopeasti. Tietoturvaongelmat lisääntyvät ja muuttavat muotoaan, toisaalta samalla esitellään uusia ja entistä tehokkaampia ratkaisuja tietoturvan parantamiseksi. Teollisuusautomaation parissa ammatikseen työskenteleville tarvitaan nykyistä vankempaa pohjaa tietoturvaa koskevan suunnittelun ja päätösten perustaksi.

Tämän kirjan tarkoituksena on käynnistää keskustelua ja toimintaa teollisuusautomaation tietoturvan edistämiseksi Suomessa sekä antaa perusteita jatkotoimenpiteille. Tietoturvan näkökulma olisi saatava mukaan teollisuusautomaation tutkimusohjelmiin. Tarvitaan sovellusohjeita, joiden avulla automaatiojärjestelmiä toimittava ja käyttävä yritys voi tunnistaa tietoturvauhkat, tehdä analyysejä sekä arvioida määrällisesti uhkien vakavuutta ja siten mitoittaa ja suunnitella niiden mukaisia suojausmenetelmiä.

Yhtenä tärkeänä tavoitteena olisi saada aikaan teollisuusautomaation tietoturvan käsikirja, jota voitaisiin hyödyntää sovellusten suunnittelussa, automaatiotuotteiden kehittämisessä sekä automaatioalan opetuksessa. Käsikirja kattaisi automaatiojärjestelmän koko elinkaaren suunnittelusta käyttöön ja ylläpitoon sekä vanhentuneen järjestelmän modernisointiin.

Seuraavassa esitetään eräitä kirjan valmistelun aikana tehtyjä ehdotuksia jatkotoimenpiteiksi:

1. Teollisuusautomaation tietoturvasta tarvittaisiin nykyistä tehokkaampi tietojenvaihtoympäristö. Käyttökokemuksia ja tietoturvaan liittyviä tapahtumia sekä esimerkkejä onnistumisista ja epäonnistumisista olisi kerättävä tehokkaammin yhteiseen tietopankkiin teollisuusaloittain. Eräs maailmanlaajuinen ja puolueeton taho, joka kerää tilastoja teollisuusautomaatiossa tapahtuneista tietoturvaan liittyneistä tapauksista, on British Columbia Institute of Technology:n ISIK-tietokanta [40].

2. Tulisi valmistella metodologiaa ja yleisiä kriteerejä teollisuuden tietoturvan suunnitteluun, käyttöönottoon ja ylläpitoon. Tätä tehdään jo useiden eri organisaatioiden toimesta (IEC, ISA, PCSRF, IAEA ja EWICS jne.). Keskeistä olisi tietoturvan organisointi ja hallinta yrityksissä sekä vastuukysymysten selventäminen nimenomaan automaation kannalta.

3. Tietoturvallisen tekniikan kehittäminen käsittäisi esimerkiksi palomuurien, tunkeutumisen havaitsemis- ja estämisjärjestelmien, salauksen ja muiden teknologioiden kehittämisen erityisesti teollisuuden ohjausjärjestelmiin. Tähän selvitykseen kuuluisi muun muassa liityntöjen valvontaan soveltuvien tietoturvajärjestelyiden ja proseduurien kehittäminen, järjestelmän toipuminen hyökkäyksen jälkeen, etäohjaus, segmentointi ym.

4. Olisi selvitettävä sovellusinfrastruktuurien muutoksia, esimerkiksi miten uusi IP-versio Ipv6 vaikuttaa luotettavuuteen ja tosiaikasovelluksiin. Tarvittaisiin myös nykyisten järjestelmien testausta, jotta voitaisiin paremmin ymmärtää tunkeutumisten seurauksia ja tunnistaa, mitä todella tarvitaan uusien järjestelmien ja teknologioiden kehittämisessä. Tätä voitaisiin tehdä laboratoriotutkimuksen ohella myös kenttätasolla.

5. Olisi selvitettävä komponenttityyppien ominaisuuksia ja esimerkiksi komponenttitietojen vertailuja, kaupallisten järjestelmien ominaisuuksia tietoturvan kannalta ja muun muassa sertifioitujen järjestelmien, ohjelmistojen ja komponenttien sertifikaattien pätevyyttä kartoittamalla testausmenetelmiä, niiden laajuutta ja testaajien vaatimuksia.

6. Tulisi valmistella tutkimusmalleja Internet-verkkoon perustuvista ohjausjärjestelmistä. Näissä otettaisiin huomioon myös ihminen–kone-vuorovaikutus (esimerkiksi ihmisen reaktiot ja toiminta järjestelmään tunkeutumisen yhteydessä).

7. Säädökset ja standardit sekä suunnittelu- ja soveltamisohjeet olisi saatava ajan tasalle muun muassa osallistumalla aktiivisesti standardisoimisyhteisöjen (ISO, IEC, ETSI, IAEA ja SESKO) toimintaan.

7
Viitteet

Liitteiden viittaukset ovat kyseisen liitteen lopussa.

[1] Suomen Automaatioseura ry.
http://www.automaatioseura.fi (Turvallisuusjaosto valikosta ”Toiminta”).

[2] ISO/IEC 17799:2005 ”Information technology – Security techniques – Code of practice for information security management”.
http://www.iso-17799.com (info-sivut).

[3] CERT-FI: Viestintäviraston (Ficora) CERT-FI-ryhmä.
http://www.ficora.fi/suomi/tietoturva/cert.htm

[4] Integrating Electronic Security into the manufacturing and Control Systems Environment. Technical Report, ISA – TR99.00.02 – 2004.

[5] Luottamukselliset tietoaineistot puntarissa. Jorma Kajava ja Juhani Anttila, Viestimies 2/2004.

[6] Tietoturvan tasapainoinen sulauttaminen liiketoimintaan. Juhani Anttila ja Jorma Kajava, Viestimies 1/2004.

[7] IEC 61508 1 – 7 ”Functional safety of electrical/electronic/programmable electronic safety-related systems”

[8] IEC 61511 1 – 3 ” Functional safety - Safety instrumented systems for the process industry sector”.

[9] EN ISO 14121 (entinen EN 1050) ”Safety of Machinery – Principles of Risk Assessment”.

[10] SFS 5438 ”Järjestelmän luotettavuuden analysointimenetelmät. Vika- ja vaikutusanalyysi (VVA)”.
VTT: http://riskianalyysit.vtt.fi/indexb078.html
FMEA Information Centre: http://www.fmeainfocentre.com/

[11] Software FMEA (SW-FMEA). Failure Mode and Effects Analysis of Software-Based Automation Systems. Pentti Haapanen ja Atte Helminen, STUK-YTO-TR 190 / August 2002.

[12] Vikapuuanalyysi, VTT: http://riskianalyysit.vtt.fi/index4bac.html

[13] Poikkeamatarkastelu Hazard and Operability Study (HAZOP), VTT.
http://riskianalyysit.vtt.fi/index3e68.html

[14] As Low As Reasonably Practicable (ALARP): Health and Safety Executive, UK.
http://www.hse.gov.uk/risk/theory/alarpglance.htm

[15] Ahonen, P. et al. (2005): Information Security Threats in the Mobile World – A Service Developer’s Perspective. VTT Publications, VTT Technical Research Centre of Finland, Espoo, Finland.

[16] Convention on Contracts for the International Sale of Goods. Tunnetaan myös nimillä CISG, Wienin konventio ja YK:n yleissopimus.

[17] Haapio et al.: Sovitaan näin – päätä omat pelisääntösi. Sampo Teollisuusvakuutuksen julkaisu 2001.

[18] ISO/IEC 21827 ”Information technology – Systems Security Engineering – Capability Maturity Model” (SSE-CMM).

[19] Information Technology Security Evaluation Criteria (ITSEC). Version 1.2, 1991, Commission for the European Communities.

[20] Trusted Computer System Evaluation Criteria (TCSEC) ”Orange Book”. 1985, U.S. Department of Defense Standard, DoD 5200.28-std.
[21] Common Criteria for Information Technology Security Evaluation (2004). Version 2.2, January 2004.
http://www.csrc.nist.gov/cc/
[22] Teollisuusautomaation vuosikymmeniltä, osat 1 ja 2. SAS julkaisusarja nrot 23 ja 25, Suomen Automaatioseura ry.
[23] Turvallisuuteen liittyvät ohjausjärjestelmät konesovelluksissa – esimerkkejä. Timo Malm ja Maarit Kivipuro, VTT Tiedotteita 2264, 2004.
[24] Tietoja direktiiveistä ja niihin liittyvistä standardeista.
http://www.teknologiateollisuus.fi/standard/direkt/
http://www.tukes.fi/
[25] IEC 62061 ”Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems”.
[26] 65/360/NP ”Security for Industrial Process Measurement and Control – Network and System Security”.
[27] 61784-4 ”Profiles for Secure Communications in Industrial Networks”.
[28] cflowd - Frequently Asked Questions – Q:What is a flow?
http://www.caida.org/tools/measurement/cflowd/newfaq.xml
[29] OPC Security Specification, OPC Foundation.
http://www.opcfoundation.org/Default.aspx/04_tech/04_spec_security.asp
[30] An Analysis of the Microsoft RPC/DCOM Vulnerability MS03-026, Wayne J.Freeman, Internet Security Information & Tools (ISIT).
http://www.inetsecurity.info/downloads/papers/MSRPCDCOM.pdf
[31] Using Distributed COM with Firewalls, Michael Nelson, The Microsoft Developer Network (MSDN).
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomfirewall.asp.
[32] WIA - Wireless InterApplication Network, Tampere University of Technology.
http://www.tkt.cs.tut.fi/research/daci/cp_wia_overview.html
[33] ISO 7498-2:1989 ”Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture”.
http://www.iso.org
OSI-malli, Tietotekniikan peruskurssi, Tampereen yliopisto.
http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html
[34] CERT/Coordination Center (ks. luku 9).
http://www.cert.org/
[35] Patching gap gets narrower, Madeline Bennett & Iain Thomson, IT Week.
http://www.itweek.co.uk/itweek/news/2085473/patching-gap-gets-narrower
[36] How To: Building a BlueSniper Rifle – Part 1, Humphrey Cheung, Tom’s Guides Publishing LLC.
http://www.tomsnetworking.com/Sections-article106.php
[37] IPv6 and IPv4 Threat Comparison and Best- Practice Evaluation, Sean Convery, Darrin Miller.
http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf
[38] A Cryptographic Evaluation of Ipsec, Niels Ferguson and Bruce Schneier, Counterpane Internet Security, Inc.
http://www.schneier.com/paper-ipsec.pdf
[39] Security Architecture for the Internet Protocol, R. Atkinson, RFC 1825, Network Working Group, Naval Research Laboratory.
http://www.rfc-archive.org/getrfc.php?rfc=1825
[40] The BCIT Industrial Security Incident Knowledgebase (ISIK).
http://www.bcit.ca/appliedresearch/security/projects/knowledge.shtml

8

Kirjallisuutta

Goble, William M. Control 1998. Systems Safety and Reliability. ISA, Second Edition.

Integrating Electronic Security into the Manufacturing and Control Systems Environment. ISA, Technical Report TR99.00.02, 2004.

Kyrölä, Tuija. 2001. Esimies ja tietoriskien hallinta. WSOY, Helsinki.

Laatu automaatiossa – parhaat käytännöt, Suomen Automaatioseura, 2001.

NISCC (National Infrastructure Security Co-ordination Centre) Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks by British Columbia Institute of Technology (BCIT). http://www.niscc.gov.uk/niscc/docs/re-20050223-00157.pdf

Northcutt, Zeltser, Winters, Frederick, Ritchey. 2003. Inside Network Perimeter Security. New Riders Publishing.

SCADA Security. Uutisia, parhaita käytäntöjä, tulevaisuuden trendejä, tietoturvastandardeja ja muita SCADA tietoturvaan liittyviä asioita. http://www.digitalbond.com/SCADA_Blog/SCADA_blog.htm

Security Technologies for Manufacturing and Control Systems. ISA, Technical report TR99.00.01, 2004.

Strandén, Lars & Hedberg, Johan & Sivencrona, Håkan. 2002. Machine Control via Internet – a Holistic Approach SP Report 2002:30, Borås.

Teumin, David J. 2004. Industrial Network Security, ISA.

Tiivis tietoturvasanasto. Sanastokeskus TSK, TSK 31, 2004. http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf

VAHTI 1/2003.Valtion tietohallinnon Internet-tietoturvaohje. Valtionvarainministeriön tietoturvallisuuden johtoryhmä, 2003.

VAHTI 4/2003. Valtionhallinnon tietoturvakäsitteistö. Valtiovarainministeriön tietoturvallisuuden johtoryhmä, 2003. http://www.vm.fi/tietoturvasanasto/su018.htm

9
Organisaatioita

AGA (American Gas Association) / GTI (Gas Technology Institute) SCADA Encryption Web Site http://www.gtiservices.org/security/

ARC Cyber Security Knowledge Center: tietotekniikan tietoturvaan liittyvää aineistoa. http://public.arcweb.com/cybersecurity/default.aspx

CERT (Computer Emergency Response Team): riipumaton tietoturvaa koordinoiva järjestö, jota kansallisella tasolla edustaa Suomessa viestintäviraston alaisuudessa toimiva CERT-FI. CERT pitää yllä luetteloa tietojärjestelmien tietoturvaan kohdistuvista uhkista, haavoittuvuuksista ja tietoturvaloukkauksista ja tiedottaa niistä edelleen yksityisten ja organisaatioiden tarpeisiin.

CERT-FI: Viestintäviraston ”Computer Emergency Response Team – FICORA” –ryhmä. http://www.ficora.fi/suomi/tietoturva/cert.htm

CEN (European Committee for Standardization) http://www.cenorm.be/cenorm/index.htm

CENELEC (European Committee for Electrotechnical Standardization) http://www.cenelec.org/Cenelec/Homepage.htm

CIDX (Cehmical Industry Data Exchange): Yhdysvaltalainen prosessiteollisuuden yhteenliittymä, joka valmistelee suosituksia muun muassa kemianteollisuuden tietoturvasta.
http://www.cidx.org/

ENISA (European Network and Information Security Agency): Euroopan tietoturvavirasto.
http://www.enisa.eu.int/
http://europa.eu.int/agencies/enisa/index_en.htm

EWICS (European Workshop on Industrial Computer Systems): 1970-luvulla perustettu ryhmä, joka saa avustusta Euroopan komissiolta. Se järjestää vuosittain Safe Comp-seminaarin ja julkaisee muun muassa alan standardointia koskevia julkaisuja.
http://www.ewics.org/

IAEA (International Atomic Energy Agency): kansainvälinen Yhdistyneiden Kansakuntien alainen atomienergiajärjestö, joka pyrkii edistämään rauhanomaista ydinenergian käyttöä. IAEA myös edistää säteilyturvallisuutta, ydinturvallisuutta ja ydinaseriisuntaa.
http://www.iaea.org/

IEC (International Electric Standardisation Committee): vuonna 1906 perustettu sähköalan kansainvälinen standardisoimisjärjestö.
http://www.iec.ch/

IEEE (the Institute of Electrical and Electronics Engineers): perustettiin 1884 ja se on maailman laajin ammatillinen insinööriyhteisö.
http://www.ieee.org/portal/site

ISA (The Instrumentation, Systems and Automation Society) on teollisuusautomaation tärkein järjestö. ISA on kansainvälisesti merkittävin automaatioalan julkaisujen kustantaja ja koulutusorganisaatio. ISA laatii raportteja ja suosituksia, joiden pohjalta standardisoimisjärjestöt (lähinnä IEC) valmistelevat normatiivisia standardeja.
http://www.isa.org

ISO (International Organisation for Standardisation): kansallisten standardisoimiselinten muodostama maailmanlaajuinen liitto (kansainvälinen standardisoimisjärjestö),

joka on perustettu vuonna 1947, ja jonka tehtävänä on edistää standardisoimista.
http://www.iso.org/

NERC (North American Electric Reliability Council) Cyber Security Standard CIP-002-1 - CIP-009-1.
http://www.digitalbond.com/SCADA_security/NERC.htm

NISCC (National Infrastructure Security Co-ordination Centre): NISCC:n rooli on minimoida elektronisten hyökkäysten riskit elintärkeitä palveluja ja järjestelmiä (Critical National Infrastructure, CNI) vastaan.
http://www.niscc.gov.uk/niscc/

NIST (National Institute of Standards and Technology): NIST:n tehtävänä on kehittää ja edistää mittauksia, standardeja ja teknologioita, joilla lisätään tuottavuutta, edistetään kaupankäyntiä ja parannetaan elämän tasoa. NIST:n Computer Security Division (CSD) sisältää aineistoa tietoturvasta.
http://www.nist.gov/

PCSRF (Process Control Security Requirements Forum): Yhdysvaltalaisen standardisoimisjärjestön NIST:in (National Institute of Standards and Technology) tukema prosessiteollisuuden yhteenliittymä, joka laatii suosituksia muun muassa prosessiteollisuuden tietoturvasta.
http://www.isd.mel.nist.gov/projects/processcontrol/

SESKO: sähkö- ja elektroniikka-alan kansallinen standardisoimisjärjestö. Sääntöjensä mukaan SESKO osallistuu alansa kansainväliseen (IEC) ja eurooppalaiseen (CENELEC) yhteistyöhön maamme edustajana sekä saattaa tämän työn tulokset kansallisiksi SFS-standardeiksi. Lisäksi SESKO osallistuu eräisiin sertifiointijärjestelmiin.
http://www.sesko.fi/

STUK: Säteilyturvakeskus on säteily- ja ydinturvallisuutta valvova viranomainen ja alan tutkimuslaitos.
www.stuk.fi

Tukes: Turvatekniikan keskus on viranomainen. joka toimii teknisen turvallisuuden ja luotettavuuden valvojana, kehittäjänä ja asiantuntijana.
www.tukes.fi

U.S.NRC: Yhdysvaltain ydinturvallisuusviranomainen (U.S. Nuclear Regulatory Commission
www.nrc.gov

LIITE 1

Tietojärjestelmän vaatimusten hallinta

Veli Taskinen, Ramse Consulting Oy

1. Vaatimusten hallinta järjestelmien elinkaaressa

Vaatimusten hallinta (Requirements Management) on systemaattinen lähestymistapa, jonka avulla on tarkoitus tunnistaa, määrittää, organisoida ja dokumentoida järjestelmälle (tuotteelle, palvelulle tai toiminnalle) asetetut vaatimukset ja ylläpitää niitä sekä hallita vaatimustietoja ja niiden muutoksia järjestelmän tai toiminnan koko elinkaaren ajan. Sen avulla pyritään varmistamaan, että hankittava tai tuotettava järjestelmätoiminta vastaa sidosryhmien tarpeita. Sidosryhmiä ovat kaikki yksilöt, ryhmät tai organisaatiot, joilla on jokin intressi järjestelmän tai kehitettävän toiminnan suhteen tai joihin järjestelmä tai kehitettävä toiminta jollakin tavalla vaikuttaa sen eri elinkaaren vaiheissa.

Vaatimusten hallinnan puutteet on todettu usein merkittävimmäksi hankkeiden ja projektien epäonnistumisten syyksi, seurauksena esimerkiksi aikataulujen venyminen, kustannusten ylittyminen ja tulosten laatupuutteet. Systemaattisella vaatimushallinnalla voidaan näitä puutteita ja niihin liittyviä riskejä vähentää ja poistaa. Se sopii erityisesti monimutkaisten järjestelmien hallintaan, missä vaatimuksiin perustuvan ohjauksen avulla saadaan kokonaisuus hyvin hallintaan.

Vaatimusten hallinta on osa projektinhallintaa, joka varmistaa, että projektissa saadaan aikaan halutunlainen järjestelmä. Projektinhallinta (Project Management) taas vastaa siitä, että tuote, järjestelmä tai palvelu saadaan aikaan halutussa aikataulussa, budjetissa ja laadussa.

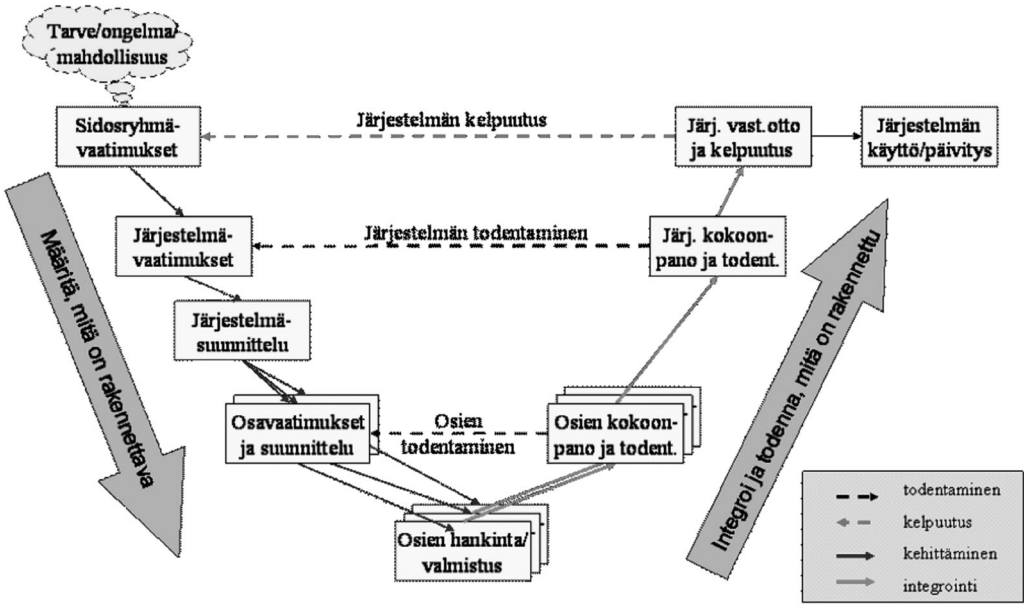
Vaatimusten hallintaa voidaan käyttää myös jatkuvaluonteisen toiminnan, kuten esimerkiksi koko yrityksen tai sen eri toimintojen ohjaukseen. Tällöin voidaan puhua vaatimusohjatusta toiminnasta.

Vaatimusten hallinta on tänä päivänä erittäin laaja osaamisalue, jolle on kehitetty lukuisa määrä erilaisia menettelytapoja, kuten esimerkiksi mallinnus- ja lähestymistapoja, prosesseja, kuvaustapoja yms. Vaatimusten hallinnan soveltajan onkin valittava omaan tarkoitukseensa parhaiten sopivat menettelyt.

2. Vaatimushallintaprosessi

Kuvassa 1-1 on esitetty järjestelmätekniikan (Systems Engineering) ns. V-malli, joka kuvaa järjestelmän elinkaarta. Järjestelmätekniikka on systemaat-

tinen järjestelmien suunnittelutapa, jossa vaatimusten hallinnalla on keskeinen rooli. Vaatimukset muodostavat siinä järjestelmän elinkaaren ”punaisen langan”, johon pohjautuen saadaan aikaan halutunlainen järjestelmä, joka tyydyttää järjestelmän hankinnan perimmäisen tarkoituksen.



Kuva 1-1. Järjestelmätekniikan V-malli.

Vaatimusten hallinnalla tarkoitetaan yleisimmin kaikkea sitä toimintaa, jolla määritetään, organisoidaan ja dokumentoidaan sidosryhmien vaatimukset järjestelmän (joka voi sisältää laitteita, ohjelmistoa ja ihmisiä) aikaansaamiseksi, todennetaan (Verification) järjestelmä näitä vaatimuksia vastaan sekä kelpuutetaan (Validation) valmis järjestelmä sidosryhmävaatimuksia mukaisesti sekä hallitaan kaikkea vaatimuksiin liittyvää tietoa ja niiden muutoksia. Vaatimushallinnan tärkeimmät osa-alueet ovat vaatimusmäärittely ja vaatimustietojen sekä vaatimusten muutosten hallinta.

3. Vaatimusten määrittely

Vaatimusten määrittely (Requirements Engineering) on osa vaatimushallintaa, mikä kattaa vaatimusten aikaansaamiseen liittyvän osuuden. Sillä haetaan vastauksia kysymykseen, mitä järjestelmältä tai kehitettävältä toiminnalta odotetaan.

Vaatimukset jaetaan sidosryhmä- ja järjestelmävaatimuksiksi. Sidosryhmävaatimukset kuvaavat järjestelmän sidosryhmien tarpeita, odotuksia ja toiveita.

Toiminnalliset sidosryhmävaatimukset vastaavat kysymykseen, mitä ko. sidosryhmä haluaa järjestelmällä tehdä tai saada aikaan ja kuinka hyvin se on tehtävä. Ei-toiminnalliset sidosryhmävaatimukset kuvaavat järjestelmälle asetettavia reunaehtoja (esimerkiksi sallitut mitat, väri, käyttöjärjestelmä, käytettävät standardit) sekä yleisiä laatuominaisuuksia (esimerkiksi luotettavuus, turvallisuus, kunnossapidettävyys).

Järjestelmävaatimukset johdetaan sidosryhmävaatimuksista. Ne ovat ohjeita järjestelmän suunnittelijalle ja kuvaavat pääasiassa, mitä järjestelmän on tehtävä (toiminnallinen järjestelmävaatimus) ja kuinka hyvin se on tehtävä (suoritusarvovaatimukset). Järjestelmävaatimukset voivat sisältää myös suunnittelun reunaehtoja.

Järjestelmätason vaatimukset kohdennetaan suunnitteluvaiheessa järjestelmän osille ja niistä johdetut vaatimukset edelleen alajärjestelmille, komponenteille jne. Vaatimuksia määritetään ja hallitaan siis monella eri tasolla järjestelmän elinkaaren eri vaiheissa.

Järjestelmähankkeiden tyypillisiä vaatimusmäärittelypuutteita ovat epämääräiset (ei-yksikäsitteiset) ja puutteelliset vaatimusilmaisut, mistä seuraa, että tarjoajalla on mahdollisuus tulkita niitä vapaasti. Sen seurauksena voi syntyä erimielisyyksiä toimittajan ja tilaajan kesken, mistä taas voi seurata projektin aikataulun pidentyminen ja kustannusten kasvu sekä järjestelmän toiminnallisia puutteita ja laatupuutteita. Myös järjestelmän todentaminen ja kelpuutus niiden perusteella on vaikeaa tai joskus jopa mahdotonta. Hyvin usein puutteita on myös järjestelmän ulkoisissa liitynnöissä, kun niitä ei ole esitetty kattavasti, jolloin järjestelmä ei sovi yhteen ulkomaailman kanssa, mistä voi seurata kalliita lisätöitä. Usein puuttuvat kokonaan myös järjestelmän ylläpitovaatimukset.

4. Vaatimustietojen hallinta

Vaatimuksiin liittyviä tietoja ovat muun muassa vaatimuskuvaukset (yleensä sanallisia, mutta ne voivat olla myös kuvia, kaavioita tms. sekä kuvauskielillä tehtyjä määrittelyitä). Vaatimuksiin liitetään myös ns. attribuutteja, joita voivat olla esimerkiksi vaatimuksen identifiointitunnus, vaatimuslähde, todentamistapa, prioriteetti, jäljitettävyystiedot, perustelu, päivämäärä ja vaatimuksen tila.

Jotta vaatimustietoja voitaisiin hyödyntää täysimittaisesti, on vaatimusten ja niihin liittyvien attribuuttitietojen hallinta tehtävä systemaattisesti ja tiedot on pidettävä ajan tasalla. Vaatimustietoja dokumentoidaan käyttäen toimisto-ohjelmistoja (esimerkiksi Word, Excel) tai erityisesti vaatimushallintaan tarkoitettuja työkaluja (esimerkiksi DOORS, Caliber). Suurten vaatimusmäärien hallitsemiseksi on syytä käyttää tarkoitukseen kehitettyjä vaatimushallintatyökaluja.

5. Vaatimusten muutosten hallinta

Vaatimusten muutosten hallinta (Requirements Change Management, RCM) käsittää vaatimusten muutoksiin liittyvät toiminnat mukaan luettuna vaatimusten jäljitettävyyden hallinta. Vaatimukset eivät ole pysyviä vaan ne voivat muuttua projektin aikana useastakin syystä. Muutosten tekemisen on oltava hallittua, jotta kuka tahansa ei voisi ilman perusteita tehdä muutoksia, jotka voivat vaikuttaa merkittävästi projektin onnistumiseen. Vaatimusten muutosten hallintaan kuuluu muutosten vaikutusten analysointi ja muutosten hyväksyminen. Ilman systemaattista muutosproseduuria ei vaatimuksia saa muuttaa kesken projektin.

Puuttuvan muutosten hallinnan riskinä on, että vaatimusten muutokset tapahtuvat hallitsemattomasti, ja että siitä seuraa haitallisia vaikutuksia projektin aikatauluun, työmääriin ja kustannuksiin sekä järjestelmän toiminnallisiin ja laatuominaisuuksiin.

Vaatimusten jäljitettävyydellä (Requirements Traceability) tarkoitetaan yleensä kykyä kuvata ja seurata vaatimuksen elinkaarta sekä eteen- että taaksepäin (esimerkiksi vaatimuksen lähteestä läpi järjestelmän kehitys-, suunnittelu-, toteutus- ja käyttövaiheiden sekä vaatimuksen jalostamis- ja iteraatiovaiheiden). Jäljitettävyyteen liittyvät liitynnät (linkit) luodaan jo vaatimusmäärittelyvaiheessa ja niitä ylläpidetään samalla kuin muitakin vaatimustietoja. Jäljitettävyyden hallinta edellyttää yleensä myös hyvän vaatimushallintatyökalun käyttöä.

Vaatimusten jäljitettävyyden hallinnan puuttuminen voi aiheuttaa monimutkaisten järjestelmien toteutuksessa järjestelmän toiminnallisia ja laatupuutteita sekä vaatimusten muutosten yhteydessä virhearvioita muutosten vaikutuksista projektin aikatauluun, työmääriin ja kustannuksiin. Jäljitettävyyden avulla pidetään myös kurissa tarpeettomien vaatimusten syntymistä projektin aikana.

6. Todentaminen ja kelpuutus

Järjestelmän (tai sen osien) todentamisella osoitetaan, että kunkin suunnittelu- ja toteutusvaiheen tulokset täyttävät vastaavat järjestelmävaatimukset. Tyypillinen järjestelmävaatimusten todentamistapa on testaus, esimerkiksi tehdastestit. Todentamistavat (ja -vaatimukset) on parasta määrittää samassa yhteydessä kun määritetään vastaavia järjestelmävaatimuksia. Tämä parantaa myös varsinaisten vaatimusten laatua, sillä kaikkien vaatimusten on oltava todennettavissa. Jos jokin vaatimus ei ole todennettavissa, ei sellaista saa myöskään esittää, eli siinä tapauksessa ko. vaatimusilmaisua on parannettava.

Kelpuutuksella osoitetaan, että valmis järjestelmä täyttää sidosryhmävaatimukset. Kelpuutus tehdään valmiilla järjestelmällä oikeassa käyttö-

ympäristössä ja -olosuhteissa. Kelpuutuksia ovat muun muassa käyttöönottotestit, koekäytöt, vastaanottotestit tms.

Todentamisella osoitetaan, että järjestelmä täyttää sille määritetyt järjestelmävaatimukset. Kelpuutuksella osoitetaan, onko rakennettu tai hankittu järjestelmä sidosryhmien tarpeita vastaava. Järjestelmävaatimusten täyttäminen ei välttämättä takaa sidosryhmätarpeiden täyttymistä.

Järjestelmähankkeissa puhutaan varsin yleisesti testauksista, jotka on käsitteellisesti eroteltu todentamis- ja kelpuutustestauksiin. Systemaattisessa vaatimustenhallinnassa näillä on selkeästi eri tehtävä.

Todentaminen ja kelpuutus on aina liitettävä vastaaviin vaatimuksiin. Perinteisesti näin ei ole toimittu kovinkaan usein, vaan esimerkiksi testausohjelmat on usein laadittu melkein irrallaan vaatimuksista jäljitettävyyden puuttuessa lähes kokonaan. Siten todentaminen ja kelpuutus jäävät heikolle pohjalle.

Jo hankintasopimuksissa tulisi olla määritettynä ainakin todentamis- ja kelpuutustavat sekä riittävän yksityiskohtaisella tasolla myös todentamis- ja kelpuutusvaatimukset ja niiden vastuut. Ongelmat jätetään aivan liian usein järjestelmän toimittajan vastuulle. Tällöin riskinä on, että syntyy erimielisyyttä todellisista vaatimuksista sekä testausten riittävyydestä ja tuloksista, mistä voi aiheutua muun muassa projektin aikataulun venymistä. Lisäksi järjestelmään voi jäädä sekä toiminnallisia että laatupuutteita.

LIITE 2

Teollisuusautomaatioon liittyvien riskien vakuuttaminen

Annika Havaste, If Vahinkovakuutusyhtiö Oy

1. Vakuutuksen merkitys riskienhallintakeinona

Vakuuttamisen päätehtävä on antaa yksityishenkilöille, yhteisöille ja yrityksille taloudellista varmuutta ja turvaa. Vakuutus on keino, jolla voidaan muuttaa sattumanvarainen vahinkokulu jatkuvaksi, tasaiseksi vuosikustannukseksi. Vakuuttaminen on riskin siirtämistä eli riski siirretään vakuutussopimuksella vakuutusyhtiön kannettavaksi.

Tietoturvan hallinnassa vakuuttaminen ei ole ensisijainen riskienhallintakeino, mutta osa riskeistä voidaan kattaa vakuutuksilla. Omaisuusvakuutukset kattavat tuhoutuneen tai vahingoittuneen omaisuuden uusimisesta tai korjaamisesta aiheutuvia kustannuksia. Omaisuusvahingon seurauksena syntyviä keskeytysvahinkoja, kuten katteen menetystä tai lisäkustannuksia, voidaan kattaa keskeytysvakuutuksilla. Vastuuvakuutustuotteilla katetaan vakuutuksenottajan vahingonkorvausvelvollisuutta kolmannelle osapuolelle aiheutetuista vahingoista.

Vakuuttamalla pystytään turvamaan taloudellisesti toiminnan jatkuvuus vahinkotilanteissa, mutta vakuutus korvaa harvoin kaikkia vahingosta aiheutuvia seurausvaikutuksia. Esimerkiksi useamman kuukauden poissaolo markkinoilta, virheet tai sopimusrikkomukset voivat aiheuttaa maineeseen tai asiakassuhteisiin pitkäaikaisen tai pysyvän kolauksen, jota vakuutukset eivät korvaa. Vakuuttaminen ei estä vahinkoja tapahtumasta ja näin ollen vakuuttaminen ei saa jäädä ainoaksi riskienhallintamenetelmäksi.

2. Omaisuus- ja keskeytysvakuutukset

Perusturvaa omaisuusvahinkojen varalta antavat omaisuusvakuutukset (esinevakuutukset). Omaisuusvakuutus (tai omaisuusvakuutuksen esinevakuutusosa) korvaa vahingoittuneen omaisuuden korjauskustannuksia tai tuhoutuneen omaisuuden uudelleen hankinnan. Omaisuuteen kohdistuvia vakuutettavia riskejä ovat muun muassa palo ja räjähdys, rikkoutuminen, salamaniskun, myrskyn tai sadeveden tulvimisen aiheuttamat vahingot, vuotovahingot

sekä rikosvahingot, kuten varkaus tai vahingonteko. Vakuutus kattaa vakuutuskirjassa mainittujen vahinkotapahtumien seurauksena syntyvät omaisuusvahingot. Turvalaajuuksista kattavin on ”all risks” -tyyppinen turva (esimerkiksi täysturva), jonka piiriin kuuluvat kaikki äkilliset ja ennalta arvaamattomat omaisuusvahinkotapahtumat, joita ei ole vakuutusehdoissa erikseen suljettu pois.

Omaisuusvahingon seurauksena syntyvä toiminnan keskeytyminen saattaa lamauttaa liiketoiminnan pitkäksi ajaksi. Keskeytysvakuuttamisen tavoitteena on turvata yrityksen toiminnan jatkuminen ja säilyttää yrityksen tulostaso samana kuin se oli ennen omaisuusvahinkoa. Keskeytysvakuutuksesta (tai omaisuusvakuutuksen keskeytysvakuutusosasta) korvataan vahingon seurauksena syntyvää katemenetystä ja ylimääräisiä kuluja. Keskeytysvahinko on yleensä seurausta omaisuusvahingosta, ja turvalaajuus määräytyy pääsääntöisesti omaisuusvakuutuksen turvalaajuuden mukaan.

Vakuuttamisen keskeisiä periaatteita ovat vahinkojen äkillisyys ja ennaltaarvaamattomuus. Kuluminen, syöpyminen ja muut hitaasti ja vähitellen tapahtuvat ilmiöt sekä niistä seuraavat rikkoutumiset eivät siten ole vakuutettavia riskejä. Kulumisesta aiheutuvat rikkoutumiset voidaan useimmiten sisällyttää laitteen huoltosopimukseen, joten vakuutus ja huoltosopimus ovat toisiaan täydentäviä riskienhallintakeinoja.

Tieto- ja automaatiojärjestelmiä tai tiedonsiirtoa palvelevien laitteiden lisäksi omaisuutena voidaan vakuuttaa tiedot ja ohjelmistot. Tiedot ja ohjelmat ovat vakuutettua omaisuutta vain, jos niistä on tehty erikseen merkintä vakuutuskirjaan. Tietojen ja ohjelmistojen osalta vakuutus- tai suojeluehdoissa edellytetään hyvää varmuuskopiointikäytäntöä, ja vahinkotilanteen jälkeen tiedot palautetaan ensisijaisesti varmuuskopioilta. Vakuutuksen tarkoituksena onkin korvata niitä kustannuksia, jotka syntyvät, kun tiedot ja ohjelmistot palautetaan korvattavan vahingon jälkeen varmuuskopioista käyttökuntoon ja päivitetään ajan tasalle. Osa vakuutusyhtiöistä on rajoittanut korvaukset pelkästään palautuskustannuksiin.

Tietojen tuhoutumisen tai vahingoittumisen ja siitä seuraavan toiminnan keskeytymisen korvauksiin on vakuutusehdoissa myös muita rajoituksia. Pääsääntöisesti korvataan vain vahinkoja, joiden syynä on fyysinen vahinko (laitteen tuhoutuminen tai rikkoutuminen). Pelkkä toimimattomuus ja siitä aiheutuva keskeytys ilman näkyvää fyysistä vahinkoa on rajattu vakuutuksen ulkopuolelle.

Omaisuus- ja keskeytysvakuutuksen ulkopuolelle on rajattu käyttö-, operointi- ja ohjelmistovirheistä, yhteensopimattomuudesta tai ylikuormittumisesta johtuvat vahingot sekä ohjelmisto- ja tiedostovahingot, joiden syynä on tietojärjestelmään oikeudettomasti tunkeutumalla tehty varkaus tai vahingonteko sekä tietokonevirus tai muu haittaohjelma. Jos sen sijaan virhe, virus tai oikeudeton tunkeutuminen johtaa korvattavaan esinevahinkoon, kuten esimerkiksi tulipaloon, on omaisuus- ja keskeytysvakuutuksesta mahdollista saada korvauksia. Laajempaa turvaa virusten ja oikeudettoman

tunkeutumisen (hakkeroinnin) varalta on tällä hetkellä vaikea saada kotimaisilta markkinoilta. Kansainvälisillä markkinoilla niitä on tarjolla, mutta ei kovin edullisesti.

Korvausta ei makseta omaisuus- ja keskeytysvakuutuksista myöskään silloin, kun vahingon on aiheuttanut petos, kavallus tai muu vilpillinen menettely. Tietoon kohdistuvaa rikollista toimintaa kattavien vakuutusten käyttö on harvinaista, vaikkakin niitä on rajallisesti olemassa (esimerkiksi kavallusturva ja omaisuusrikosturva).

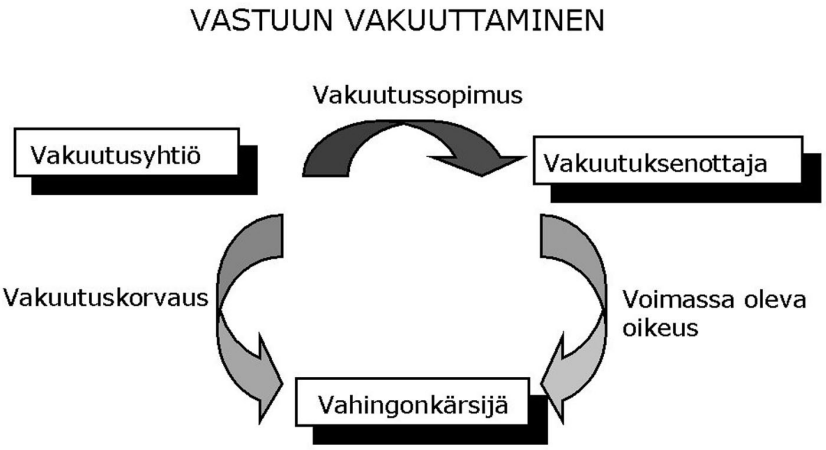
Eri vakuutusyhtiöiden ehdot sekä pk-yritysten vakuutusratkaisut ja suuryritysten räätälöidymmät ratkaisut poikkeavat jonkin verran toisistaan. Oman vakuutusturvan kattavuus ja ehdoissa mainitut rajoituksen on aina syytä tarkastaa omasta vakuutussopimuksesta.

3. Vastuuvakuuttaminen

Vastuujuridiikan peruskäsitteiden ymmärtäminen on välttämätöntä niin yrityksen vastuiden kuin vastuuvakuutuksenkin kannalta. Lähtökohtaisesti vahingon aiheuttajan on korvattava vahingon kärsineelle aiheuttamansa vahinko, joka voi olla henkilö- tai esinevahinko. Puhdas taloudellinen vahinko tulee korvattavaksi yleensä vain sopimussuhteessa. Vahingonkorvausvastuu voi syntyä monen eri lain perusteella, joista esimerkkeinä voidaan mainita vahingonkorvauslaki, tuotevastuulaki ja kauppalaki. Yritysten välisessä irtaimen kaupassa sovelletaan kauppalakia, joka sopimusmääräysten puuttuessa antaa oikeusohjeet vahingonkorvausvelvollisuudesta esimerkiksi kaupan kohteen ollessa virheellinen ja aiheuttaessa vahinkoa. Palvelun kaupassa oikeusohjeina sopimusmääräysten puuttuessa ovat yleiset sopimusoikeudelliset periaatteet, joiden mukaan sopimuskumppanilla on kärsimästään vahingosta oikeus täyteen korvaukseen vahingonaiheuttajalta. Osa vahingonkorvausvastuista on mahdollista kattaa erilaisilla vastuuvakuutuksilla, mutta koko liikeriskiä ei kuitenkaan voi eikä kannattaisikaan vakuuttaa.

Vastuuvakuutus eroaa muusta vahinkovakuutuksesta siten, että korvauksen saaja on joku muu kuin vakuutuksenottaja. Välittömän vahingon kärsineelle maksetaan vakuutuksenottajan vastuuvakuutuksesta korvaus, mikäli tämä on lain mukaan vahingonkorvausvelvollinen vahingosta. Vastuuvakuutus on kuitenkin vakuutuksenottajan hyväksi voimassa jo silloin, kun häneltä vasta vaaditaan korvausta, vaikka lopulta todettaisiin, että hän ei ole vastuussa vahingosta.

Korvausasiassa ratkaistaan ensin kysymys vahingonkorvausvelvollisuudesta voimassa olevan oikeuden mukaan. Sen jälkeen arvioidaan vahingon korvaaminen vastuuvakuutuksesta. Vakuutuksenottajan ja vakuutusyhtiön välillä on olemassa sopimussuhde, jonka sisältönä on vastuuvakuutus vakuutusehtoineen. Näiden ehtojen mukaan ratkaistaan, onko aiheutettu vahinko



Kuva 2-1. Vastuuvakuuttamiseen liittyvät kolme osapuolta.

sellainen, että se kuuluu vakuutuksen korvauspiiriin eli korvataan vastuuvakuutuksesta. Myönteisessä tapauksessa vakuutusyhtiö maksaa vakuutukseen kuuluvana korvauspalveluna korvauksen suoraan vahingonkärsineelle. Tähän korvauspalveluun kuuluu myös korvausasian selvittäminen, esimerkiksi neuvottelut korvauksen vaatijan kanssa, sekä oikeudenkäynnin hoitaminen, jos vahingonkorvausvelvollisuus perusteiltaan tai määrältään on epäselvä vahingonkärsineen ja vakuutuksenottajan välillä.

Vastuuvakuutuksen tarkoitus on siten suojata vakuutuksenottajaa tilanteessa, jossa häneltä vaaditaan vahingonkorvausta tai vahingonkorvausvelvollisuuden todetaan syntyneen. Tämän lisäksi vakuutuksella on merkitystä vahingonkärsijän kannalta, koska yleensä hänellä on vahingonaiheuttajan vastuuvakuutuksen johdosta paremmat mahdollisuudet saada täysi korvaus aiheutuneesta vahingosta.

Vakuutus on voimassa myös vakuutuksenottajan työntekijän hyväksi, koska työnantaja on korvausvelvollinen isännänvastuun perusteella työntekijän aiheuttamasta vahingosta.

4. Korvattava vahinko

Vastuuvakuutuksesta korvataan vakuutuskirjassa mainitussa toiminnassa toiselle aiheutettu vahinko. Jos siis yhtiön toiminta jollain tavalla muuttuu, on tämä ilmoitettava vakuutusyhtiölle, koska eri toimialoihin liittyy erisuuruinen riski ja tämä otetaan huomioon vakuutusta hinnoiteltaessa. Yleensä yrityksen koko toiminta on vakuutuksen piirissä.

Vastuuvakuutus korvaa vahingon, joka on aiheutettu vakuutuksen maantieteellisellä voimassaoloalueella. Tämä on otettava huomioon vakuutussopi-

musta tehdessä ja aina, kun yrityksen toiminta-alue muuttuu. Eri maantieteellisillä alueilla riski voi olla erilainen, ja esimerkiksi USA:ssa riski ja näin ollen myös vakuutuksen hinta, on suurempi kuin Euroopassa.

Vastuuvakuutus on yleensä voimassa kalenterivuoden ja uudistuu automaattisesti seuraavalle vuodelle, jos sitä ei irtisanota. Ajallinen ulottuvuus voidaan määritellä eri tavoin. Vakuutus voi kattaa vahingon, joka aiheutettiin sen voimassaoloaikana, tai joka todettiin sen voimassaoloaikana tai jota koskeva vaatimus esitetään vakuutuksenottajalle vakuutuksen voimassaoloaikana.

Vastuuvakuutuksesta korvataan kaikki vahingot, joita ei ole poissuljettu vakuutusehdoissa. Eri vakuutusyhtiöiden ehtojen sanamuodoissa on jonkin verran eroja, mutta kuitenkin tietyt rajoitukset ehdoista löytyvät. Vakuutuksenottajan kannalta olennaisia rajoituksia käsitellään seuraavissa kohdissa. Vakuutusturvassa on muitakin kuin seuraavassa esitettyjä rajoituksia.

5. Toiminnanvastuuvakuutus

Toiminnanvastuuvakuutus korvaa vakuutetun toiminnasta johtuvat vahingot. Vakuutuksen piiriin kuuluvat yhtiön eli vakuutetun työntekijät. Toiminnanvastuuvakuutuksesta korvataan esimerkiksi ulkopuoliselle yhtiön toimitiloissa tai kiinteistöllä aiheutunut henkilövahinko, tai työntekijän asiakaskäynnillään aiheuttama henkilö- tai esinevahinko. Vahinkoa voi aiheutua esimerkiksi huoltotyön yhteydessä asiakkaan korjattavana olevalle omaisuudelle.

Ns. ”haltuun uskotulle” omaisuudelle aiheutunutta vahinkoa ei korvata, jos siitä ei ole erikseen sovittu vakuutusyhtiön kanssa. Tällaista omaisuutta on esimerkiksi alihankkijan omaisuus vakuutuksenottajan tiloissa tai lainassa oleva omaisuus. Rajoituksen motiivina on, että tällaista omaisuutta on hoidettava kuten omaa omaisuutta, ja jos vastuuvakuutus kattaisi sen, motivaatio huolellisuuteen voisi vähetä. Vieraan omaisuuden voi lisäksi vakuuttaa omaisuusvakuutuksella, jolloin myös vakuutuksen hinnoittelu saadaan paremmin riskiä vastaavaksi.

Vakuutuksenottajan lukuun valmistettavana, asennettavana, korjattavana, säilytettävänä tai muulla tavoin käsiteltävänä tai huolehdittavana oleva omaisuus ei ole vakuutuksen korvauspiirissä, ellei siitä sovita erikseen vakuutusyhtiön kanssa. Rajoitus koskee pääasiassa yrityksiä, jotka saamansa toimeksiannon perusteella käsittelevät vierasta, asiakkaansa omaisuutta.

Toiminnanvastuuvakuutuksen ulkopuolelle jäävät myös vastuut, jotka perustuvat yksinomaan sopimukseen, sitoumukseen, lupaukseen tai takuuseen. Tällä tarkoitetaan mahdollista ylimääräistä vastuuta, jota ei syntyisi, jos asiaa arvioitaisiin pelkästään lain mukaan. Sopimussakko on esimerkki vastuusta, johon yritys voi sitoutua, mutta mistä ei ole laissa säädetty. Laajem-

piakin tulkintoja rajoitusehdoista on joskus tehty ja asia kannattaa ottaa esille vakuutusyhtiön kanssa vastuuvakuutussopimusta solmittaessa.

Vastuu tavaran virheettömyydestä ei ole toiminnanvastuuvakuutuksesta korvattava vahinko. Mikäli tuotteen virheellisyys aiheuttaa vahinkoa muulle omaisuudelle tai henkilölle, se korvataan tuotevastuuvakuutuksesta.

6. Tuotevastuuvakuutus

Tuotteen valmistajan ja myyjän vastuu tuotteen virheettömyydestä perustuu tuotevastuu-, vahingonkorvaus- ja kuluttajansuojalakeihin sekä kun on kysymyksessä elinkeinonharjoittajien välinen kauppa, kauppalakiin. Virheellisyys voi syntyä tuotteen suunnitteluprosessissa, valmistusprosessissa, varastoinnin aikana tai siten, että tuotteen käyttöohje on virheellinen.

Tuotevastuuvakuutus korvaa vakuutuksenottajan elinkeinotoiminnassaan liikkeelle laskeman tuotteen virheellisyydestä tai puutteellisesta turvallisuudesta toiselle aiheutuneen henkilö- tai esinevahingon, josta vakuutuksenottaja on em. lakien mukaan vastuussa. On tärkeää huomata, että itse tuotteen virhettä tai tuotteelle aiheutunutta vahinkoa ei korvata, vaan tuotteen aiheuttama vahinko muulle omaisuudelle tai henkilölle korvataan.

Tuotevastuuvakuutus ei korvaa vahinkoa myöskään silloin, kun virhe voidaan poistaa korjaamalla luovutetun tuotteen virheellisyys. Tällöin vahinkoa muulle omaisuudelle ei ole aiheutunut, vaan ainoastaan itse tuote on viallinen.

Myöskään puhdasta varallisuusvahinkoa ei korvata tuotevastuuvakuutuksesta. Esimerkkinä voi mainita tilanteen, jossa aiheutetaan asiakasyritykselle pelkkä toiminnan keskeytyminen ilman, että olisi aiheutettu esimerkiksi koneen rikkoutumista eli esinevahinkoa. Sen sijaan esinevahinkoon liittyvä taloudellinen vahinko, kuten toiminnan keskeytymisestä johtuva tappio, korvataan vastuuvakuutuksesta.

7. Konsultin vastuuvakuutus

Konsultin vastuuvakuutuksessa konsultilla tarkoitetaan tahoa, joka tekee toisen toimeksiannosta suunnitelmia, piirustuksia, laskelmia, työselostuksia sekä antaa neuvoja ja ohjeita niihin liittyen. Konsultin vastuu perustuu sopimukseen, kun vahinko aiheutuu sopimuskumppanille tai vahingonkorvauslakiin, jos vahinko aiheutuu ulkopuoliselle. Toimeksiantajalle aiheutettu vahinko korvataan palkkion määrään saakka. Myös konsultti yleisesti rajoittaa vastuunsa palkkion määrään.

Konsultin vastuuvakuutus myönnetään työhön, jota tehdään konsultin ominaisuudessa ja siitä korvataan henkilö- ja esinevahingon lisäksi puhdas taloudellinen vahinko. Konsultin vastuuvakuutuksen rajoitusehdoista on

huomattava ainakin rajoitus, jonka mukaan virheellisen tai puutteellisen työsuorituksen uudelleen suorittamisesta tai työn viivästymisestä aiheutuneet vahingot ovat vakuutuksen ulkopuolella.

8. Varallisuusvastuuvakuutus

Toiminnanvastuu- ja tuotevastuuvakuutuksissa korvauspiirin ulkopuolelle jää puhdas varallisuusvahinko ilman henkilö- tai esinevahinkoa. Vastuu perustuu tällöin pääsääntöisesti osapuolten sopimukseen, jossa muuten täysimääräistä vastuuta usein rajoitetaan. Riski varallisuusvahingon aiheuttamisesta liittyy moniin aloihin (kuten asianajajat, tilintarkastajat ym.) ja informaatioteknologian alalla se on myös suuri riski. Toimitetun tuotteen toimimattomuudesta tai siitä, että se toimii vajaasti tai väärin, voi aiheutua asiakasyritykselle mittavia toiminnankeskeytysvahinkoja sekä esimerkiksi tiedostojen katoamiseen ja uudelleen luomiseen liittyviä vahinkoja. Myös palvelutoimintaan, kuten ylläpitopalveluihin, liittyy varallisuusvahingon riski. IT-alalla taloudellisen vastuun kattavia vakuutuksia on voimassa jonkin verran. Vakuutusyhtiön kannalta riski on usein vaikea arvioida ja yksittäisestä riskistä riippuu, voidaanko se kattaa varallisuusvastuuvakuutuksella. Osa riskeistä jää aina liikeriskiksi, jota voidaan parhaiten rajoittaa tehokkaalla sopimustoiminnalla.

LIITE 3

Aktiivihakemistot automaatiossa

Terho Riipinen, Outokumpu Stainless Oy

Tässä liitteessä käytetään seuraavia käsitteitä ja lyhenteitä:

Järjestelmänvalvoja (Administrator) = Aktiivihakemiston kaikkien objektien ja palveluiden hallinnasta vastaava henkilö.
Pääkäyttäjä (Local Administrator) = Aktiivihakemiston OU-rakenteen tai muun erikseen rajatun osa-alueen hallinnasta vastaava henkilö.
DC (Domain Controller) = Toimialueen ohjauspalvelin, jossa sijaitsevat hakemistorakenne ja erilaiset toimialueen palvelut.
DDNS (Dynamic DNS) = Toimialueen nimipalvelu, johon laitteet rekisteröityvät automaattisesti.
DNS (Domain Name System) = Toimialueen nimipalvelu, johon hallinnointia helpottava laitenimi ja sitä vastaava tietoliikenteen tarvitsema IP-osoite rekisteröidään.
Domain = Toimialue, joka muodostuu ohjauspalvelimien, muiden palvelimien, työasemien sekä käyttäjä- ja konetilien muodostamasta laitteiden ja objektien yhdistelmästä.
OU (Organizational Unit) = Organisaatioyksikkö.
WINS (Windows Internet Name Service) = Nimipalvelu, joka on käytössä NT4- tai varhaisemmissa käyttöjärjestelmäympäristöissä

1. Johdanto

Outokumpu-konserni on tällä hetkellä maailman toiseksi suurin ruostumattoman teräksen tuottaja. Tämän liitteen kirjoittaja on ollut mukana Outokumpu-konsernin projektissa, jossa Outokummun 40 maassa ja 200 paikkakunnalla olevat Windows NT4 työasema- ja palvelinympäristöt on päivitetty pääosin yhdeksi koko konsernin käsittäväksi aktiivihakemistoksi. Työasemien määrä on koko yrityksessä 14000 ja palvelimien määrä 1000. Konsernin suunnitteluryhmän jäsenyyden lisäksi kirjoittaja on ollut projektipäällikkönä toteuttamassa aktiivihakemistoon siirtymistä Tornion Terästehtaalla ja Kemin Kaivoksella, joissa 1200 työasemaa ja 100 palvelinta on liitetty konsernin yhteiseen hakemistoon sekä lisäksi 100 työasemaa ja 30 palvelinta automaatio-osaston omaan aktiivihakemistoon.

Aktiivihakemisto on tietoverkossa olevan tiedon ja laitteiden hallinnointiin käytetty hakemistopalvelu. Tässä liitteessä kuvataan aktiivihakemiston erilaisia toteutustapoja Outokumpu-konsernissa käyttöönotetun mallin pohjalta. Microsoftin ilmoitettua, ettei se enää toimita tietoturvapäivityksiä NT4 -käyttöjärjestelmälleen, ovat monet yritykset ryhtyneet päivittämään entisiä NT4 -toimialueisiin perustuvia järjestelmiään aktiivihakemistoksi. Aktiivi-

hakemiston ja siihen liittyvien uudempien käyttöjärjestelmäversioiden avulla saadaan aikaan parempi suoja tietoturvan uhkia vastaan. Näitä uhkia ovat muun muassa haittaohjelmat.

Useat automaatiojärjestelmät ovat olleet suljettuja siten, että kenttälaitteiden koko tietoliikenne on ollut erillään yritysverkon tietoliikenteestä. Näissä järjestelmissä käyttäjien oikeudet, hallintamenettelyt ja järjestelmän sisäiset palvelut ovat olleet omintakeisia, kunkin järjestelmän sisälle rakennettuja ratkaisuja. Joissakin automaatiojärjestelmissä myös käyttöjärjestelmä on jokin muu kuin Windows, jolloin niiden liittäminen aktiivihakemistoon tai muuhun Windows -järjestelmään ei ole mahdollista.

Uusimmissa automaatiojärjestelmissä järjestelmän objektien hallinta ja osa järjestelmän sisäisten prosessien toiminnasta perustuu aktiivihakemistoon. Toinen vähitellen tapahtunut muutos on ollut se, että automaatioon liittyvät työasemat ja palvelimet käyttävät usein samaa verkkoteknologiaa kuin toimistoverkot. Näiden muutosten vuoksi joutuu pohtimaan järjestelmähallinnan vaihtoehtoja: sijoitetaanko automaatiojärjestelmät yrityksen toimistotyöasemille rakennettuun aktiivihakemistoon vai rakennetaanko automaatiojärjestelmille oma aktiivihakemisto.

2. Siirtyminen aktiivihakemistoon

Markkinoilla ei toistaiseksi ole ollut kilpailukykyisiä järjestelmiä varsinkaan suurten työasemaympäristöjen hallintaan, joten käytännössä ainoaksi vaihtoehdoksi on jäänyt Microsoftin aktiivihakemisto. Yleistavoitteena on ollut kaikkien Windows-työasemien ja -palvelimien hallinnoinnin saaminen yhteen yhteiseen aktiivihakemistoon. Toimistojärjestelmien yhtenäistäminen onnistuu yleensä hyvin ja infrastruktuurin yhtenäistämisellä saadaan muun muassa selkeän rakenteen mukanaan tuomia etuja.

Automaation sijoittaminen keskitettyyn aktiivihakemistoon ei ole kaikissa tapauksissa ongelmatonta. Tämän vuoksi Outokumpu-konsernissa on laadittu automaation erityisvaatimukset huomioon ottava aktiivihakemistomalli. Automaatiolaitteiden liittyessä yhteiseen hakemistoon, tarvitaan tiettyjä turvajärjestelyjä (ks. kohta 2.3). Kaikissa tapauksissa ne eivät kuitenkaan riitä, joten vaihtoehtona on rakentaa automaatiolle oma aktiivihakemisto.

Seuraavassa on vertailtu muutamia yleisesti esille tulevia syitä, miksi automaation liittäminen toimiston aktiivihakemistoon ei teollisuusympäristöissä aina onnistu, vaikka käyttöjärjestelmänä molemmissa tapauksissa onkin Windows:

- Vastuualueet: Yleensä automaatio-organisaatio vastaa itsenäisesti kaikista automaation tietojärjestelmistä.
- Häiriöttömyys: Automaation eräänä perusasiana on häiriöiden rajaaminen järjestelmän ulkopuolelle. Perinteisesti automaatiojärjestelmään kuulu-

vaksi osaksi ei ole totuttu liitämään tuhansia toimistotyöasemia, tulostimia ja palvelimia. Niiden mukana järjestelmään tulee turhia uhkia.

- Ylläpito-oikeudet: Aktiivihakemiston ylimmistä hallintaoikeuksista vastaa järjestelmänvalvoja (Administrator). Näiden oikeuksien antaminen suurelle määrälle henkilöitä muodostaa riskin koko aktiivihakemiston turvallisuudelle. Oikeuksia on yleensä annettu vain muutamalle siihen organisaatioon kuuluvalle henkilölle, jonka hallinnassa kyseinen aktiivihakemisto on. Useassa tapauksessa se on toimistojärjestelmän IT-organisaatio. Tästä seuraa ongelmia automaatio-organisaatioille. Riittävän suurten ylläpito-oikeuksien puuttuminen saattaa vaikeuttaa automaation hallinnointia. Toisaalta ylimmät hallintaoikeudet automaatiojärjestelmään ovat organisaatiolla, jolla niitä ei perinteisesti ole ollut.
- Takuukysymykset: Monissa tapauksissa automaatiojärjestelmän toimittajan luottamus yrityksen yhteiseen aktiivihakemistoon on heikko. Vastuualueeseen halutaan ymmärrettävästi vain omaa järjestelmää koskevat komponentit.
- Toimintarutiinit: Koko aktiivihakemistojärjestelmä saatetaan joutua käynnistämään uudelleen varsinkin automaatiojärjestelmän rakennusvaiheessa ja ohjelmapäivityksiä suoritettaessa. Se ei sovi välttämättä yhteen yrityksen muun aktiivihakemiston käytön kanssa.
- Kaavamuutokset: Kaavassa eli schemassa määritetään, aktiivihakemiston objektit ja niiden attribuutit. Kullakin aktiivihakemistolla on oma kaavansa. Muutokset kaavassa eivät yleensä ole toivottuja. Jos niitä on tarve toteuttaa esimerkiksi jonkin sovellusohjelman tarpeiden vuoksi, automaation vaatimat muutokset eivät välttämättä sovi toimistoympäristön puolelle ja päinvastoin.
- Tietoturvavyöhyke: Koska jokaisessa hakemistossa on omat järjestelmänvalvojansa, ovat kaikki pääsyoikeudet hakemistokohtaisia. Jokaisessa erillisesti toteutetussa aktiivihakemistossa voidaan siten toteuttaa omaa erillistä tietoturvatasoa ja hallinnoida kaikkia hakemistopalveluja.

2.1 Aktiivihakemiston käsitteitä

Aktiivihakemisto on tietokanta, johon on tallennettu tietoa tietoverkon objekteista. Hakemistopalvelut (Directory Services) ovat automaattisia (aktiivisia) toimintoja, joiden avulla tiedot saadaan hyödynnettäväksi. Näitä palveluita ovat muun muassa: verkkoon kirjautuminen, käyttäjän tunnistustavat palvelut, käyttöoikeuksien hallinta, taustatulostus, nimenselvityspalvelut (DNS ja WINS) sekä DHCP-palvelu (Dynamic Host Configuration Protocol), jonka avulla tietokoneet voivat saada tarvitsemansa IP-osoitteen automaattisesti.

Aktiivihakemisto voi sisältää yhden tai useampia toimialueita (Domain). Aktiivihakemistoa kutsutaan myös ”metsäksi” (Forest), koska se voi sisältää useista eri toimialueista koostuvia puumaisia rakenteita. Hierarkiassa toimi-

alueesta seuraavana ovat organisaatioyksiköt (Organizational Unit OU). Hallittavia tietoverkon resursseja voidaan jakaa OU:ksi esimerkiksi paikkakunnan, organisaation, rakennuksen, ohjauspaikan tai järjestelmän mukaan. Jaottelu voi perustua myös siihen, kuka tai ketkä hallinnoivat kyseisiä resursseja. Outokummun tapauksessa ylimpänä OU:na ovat kaikki 200 paikkakuntaa. Joissakin tapauksissa myös saman paikkakunnan eri IT- ja automaatio-osastoilla on käytössään oma OU. Kunkin paikkakunnan alla hierarkiassa ovat seuraavat OU:t, joilla jaetaan omiksi ryhmikseen

– käyttäjätilit (User Accounts)
– konetilit (Machine Accounts)
– käyttäjä- tai koneryhmät (Groups)
– tulostimet (Printers)
– levyjaot (Shares)
– palvelut (Services).

Näillä tietoverkon resursseja edustavilla objekteilla puolestaan on omat attribuuttinsa erilaisten tietojen tallennusta varten. Käyttäjätilin objektille on mahdollista tallentaa käyttäjänimen ja -tunnuksen lisäksi muun muassa osoitetiedot, milloin tunnuksella on viimeksi kirjauduttu järjestelmään, milloin määräaikaisen työntekijän tunnus lukkiutuu automaattisesti ja mille palvelimelle henkilöllä on oikeuksia.

Konetilin objektilla ovat attribuutteina muun muassa työasemanimi ja kenelle se kuuluu. Osa tiedoista tallentuu automaattisesti, kuten tiedot työaseman käyttöjärjestelmästä. Samaa konetiliobjektia käytetään työasemille ja palvelimille.

Käyttöliittymänä voi käyttää Microsoftin hallintakonsolia (Active Directory Users and Computers, ADUC). Sen avulla voidaan käytännössä muodostaa ja hallita OU-rakenteita.

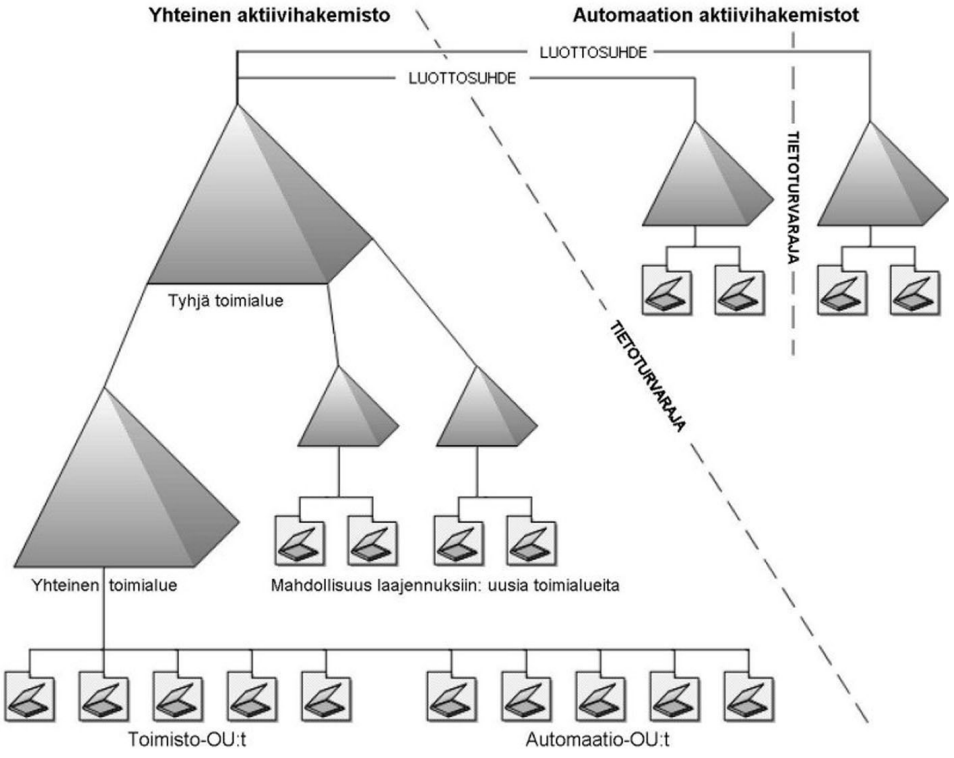
Pääsääntöisesti sama OU-hierarkiamalli on käytössä myös automaation aktiivihakemistossa. Paikkakuntajaon korvaa automaatiojärjestelmä- ja osastokohtainen ryhmittely.

Hierarkian tarkoituksena on hallinnoinnin helpottaminen jakamalla objektit sopiviin ryhmiin. OU:n avulla ryhmiteltyihin objekteihin voidaan soveltaa ryhmäkäytäntöjä (Group Policy). Ryhmäkäytännöillä rajataan oikeuksia kuten: pääseekö Internet-verkkoon, minkä ohjelman voi käynnistää, mitä ikoneja näkyy työpöydällä ja saako koneen CD-asemaa käyttää. Ryhmäkäytännöillä voidaan luoda myös automaattisesti tapahtuvia toimintoja kuten automaattinen ohjelmien ja tietoturvapäivitysten asennus.

Ryhmäkäytäntöjä voidaan soveltaa myös aktiivihakemisto- tai toimialuekohtaisesti, jolloin näin tehdyt asetukset tulevat voimaan koko yrityksessä. Tällaisia asetuksia voisivat olla esimerkiksi salasanan pituus ja vaihtoväli.

Aktiivihakemiston puumaisen hierarkian rakenneosina ovat toimialueet ja organisaatioyksiköt (ks. kuva 3-1):

- Juuritoimialue (Root Domain) on ”metsän” ensimmäinen, joissakin tapauksissa ainoa toimialue. Kuvan tapauksessa toimialue on jätetty tyhjäksi eli ilman OU:ita, jolloin se sisältää vain aktiivihakemiston rakenteeseen keskeisesti liittyvät palvelut. Tällä varmistetaan hakemistorakenteen eheys ja luodaan joustava hallinnointimalli.
- Alitoimialue (Child Domain) on DNS-nimialueen haarautuma, jolla on oma hallinnointi. Kuvan ratkaisussa kaikki metsän OU:t on keskitetty yhden toimialueen alaisuuteen. Mahdollisuus muihin toimialueisiin on olemassa. Näitä voisivat olla esimerkiksi tytäryhtiöt, joilla halutaan säilyttää itsenäisempi hallinnointi. Myös tuotantoyksiköt voisivat olla tällaisia toimialueita. Tähän liittyy kuitenkin pieni tietoturvariski, koska alitoimialueen järjestelmänvalvojat (Administrators) voivat saada ylemmän toimialueen hallinnointioikeudet itselleen. Vaikka riski on pieni, sitä ei välttämättä haluta ottaa.
- Kullekin automaatiossa käytetylle aktiivihakemistolle riittää yleensä pelkkä juuritoimialue, koska hakemiston koko on pieni. Siihen on sisällytetty kaikki hakemiston vaatimat toiminnot.
- Organisaatioyksiköillä rakennetaan hierarkia, joka yleensä vastaa olemassa olevan organisaation rakennetta. Organisaatiorakenteen muuttuessa OU:iden järjestely uutta organisaatiota vastaavaksi on helposti toteutettavissa.



Kuva 3-1. Aktiivihakemiston rakenne.

Erilliset automaation aktiivihakemistot voivat tarvittaessa liittyä yhteiseen hakemistoon yksi- tai kaksisuuntaisella luottosuhteella. DNS-nimipalvelut toimivat molempiin suuntiin käyttäen Windows Server 2003:n Conditional Forwarding -ominaisuutta.

Hallinnoinnista voidaan antaa pieniä osia kenen tahansa hallittavaksi vaarantamatta silti tietoturvaa muilta osin. Tätä asiaa kuvataan aktiivihakemistossa käsitteellä delegointi. Tähän perustuen voidaan luoda eritasoisia hallinnointia suorittavia käyttäjäryhmiä, joita kutsutaan pääkäyttäjiksi. Myös yksittäinen tehtävä, kuten salasanan vaihto-oikeus voidaan delegoida joillekin henkilöille. Tämäkin tehdään yleensä ryhmäoikeuksien avulla.

2.2 Yrityksen yhteinen aktiivihakemisto

Lähes kaikki toimistopuolen tietotekniikka on Outokummun tapauksessa yhteisessä aktiivihakemistossa. Se tarkoittaa myös toimialueen ohjauspalvelinten (Domain Controller, DC) sijoittamista useille paikkakunnille. Tällä hetkellä käytössä olevaan toimialueeseen kuuluu maailmanlaajuisesti lähes 100 DC:tä. Jollakin paikkakunnalla tehdyt muutokset kopioituvat (replikoituvat) paikalliselta palvelimelta tietyn aikavälin mukaisesti kaikkiin muihin palvelimiin ja hakemisto on ajan tasalla noin tunnin kuluttua muutoksesta. Suuremman määrän käyttäjiä ja laitteita käsittävillä paikkakunnilla DC:itä saattaa olla useita, kun taas pienempien, esimerkiksi myyntikonttoreiden laitteet ottavat yhteyden lähimpään, nopeimmin saatavissa olevaan DC:hen yhtymäverkon välityksellä.

Käytännön kokemukset osoittavat, että aktiivihakemisto toimii Windows Server 2003 -käyttöjärjestelmäpohjaisena luotettavasti laajassakin ympäristössä. Laitteet rekisteröityvät automaattisesti hakemiston DNS:ään. Käytössä on dynaaminen nimenselvityspalvelu (Dynamic Domain Name Service, DDNS). Suuri muutos NT4 -järjestelmään verrattuna on se, että paikallista DNS:n hallinnointia ei enää tarvita.

Muutamien aktiivihakemiston ulkopuolelle jäävien vanhojen järjestelmien kiinteät osoitteet on ilmoitettava erikseen toimialueen pääkäyttäjälle. Sama koskee myös muita kuin Windows -käyttöjärjestelmään perustuvia laitteita. Tällaiset muutokset tuovat hieman kankeutta ylläpitoon, jolloin ennalta sovitut toimintatavat ovat tärkeitä virhetilanteiden välttämiseksi. Sama osoitetietojen ylläpitomenettely koskee WINS-palvelua, joka tosin on poistumassa NT4:n mukana. DNS:n suhteen voi siirtymävaiheessa tai muuten paikallisen tarpeen mukaan rakentaa erillisiä DNS-vyöhykkeitä (Zones), joiden hallinnoinnin voi delegoida paikallisille OU-pääkäyttäjille. Vyöhykkeiden rakentaminen voi tehdä järjestelmästä monimutkaisen, joten niiden tarpeellisuutta on syytä harkita tarkasti.

Aiemmin lähes 200 erillistä NT4 -toimialueita käsittävässä ympäristössä oli myös 200 nimenselvityspalvelinta, joiden yhteistoiminta oli monesti sekavaa. Tämä DNS/WINS -nimien selvityksen yhtenäistyminen ja yksinkertaisuus on myös selkeä aktiivihakemiston mukanaan tuoma parannus.

2.3 Automaatio yhteisessä aktiivihakemistossa

Myös osa tuotantojärjestelmistä on liitetty yhteiseen aktiivihakemistoon. Automaation kannalta merkityksellistä on se riski, joka aiheutuu yhteyden katketessa hakemistoon. Riskin torjumiseksi tehdaspaikkakunnille on sijoitettu oma DC. Se voidaan suuremmilla paikkakunnilla sijoittaa lisäksi kullekin tuotanto-osastolle, jolloin ne toimivat toistensa varapalvelimina, vaikka yhteys ko. paikkakunnalta olisi poikki muille DC:ille. Tilanteessa, jossa paikkakunnan ainoa DC vioittuu, palvelut ovat koko ajan saatavilla muilta paikkakunnilta. Tällöin ainoastaan hakemistopalveluiden nopeus riippuu käytössä olevan tietoverkon nopeudesta.

Paikallinen DC voidaan suojata omaan verkkoonsa palomuurilla, mutta tarpeellisia tietoliikenneportteja on kuitenkin jätettävä avoimeksi. Liikenteen Aktiivihakemiston sisäisen päivitysrutiinin takia on tietoliikenteen toimittava, jonka lisäksi muunkin tarvittavan liikenteen on päästävä palomuurin läpi.

Automaation kannalta tärkeää on myös tyhjä juuritoimialue. Tyhjän toimialueen ja yhteisen toimialueen hallinnointi on järjestetty siten, että vahinkoja ei pääsisi tapahtumaan. Tällöin erilaisten hallintotehtävien määrittely ja roolien jako on tärkeää. Vaikka enemmän oikeuksia omaava henkilö voisi oikeuksiensa puolesta tehdä kaikkia hallinnointitehtäviä alempana aktiivihakemiston puurakenteessa, niin ei kuitenkaan menetellä roolijakoon perustuen. Tällä varmistetaan paikallisten hallinnointiorganisaatioiden vapaa ja ehdoton itsemääräämisoikeus omiin objekteihinsa.

2.4 Automaation aktiivihakemistot

Mikäli yhteinen aktiivihakemisto ei täytä automaation vaatimuksia, voidaan rakentaa osasto- tai tehdaskohtaisia aktiivihakemistoja pelkästään automaatiolle. Yksittäiset järjestelmätoimittajat luottavat usein vain omiin järjestelmiinsä, ja nämä ovat rakentaneet järjestelmänsä toimimaan vain omassa ympäristössään. Siksi on vaarassa syntyä useita aktiivihakemistoja Windows NT4 -toimialueiden tapaan. Eräänä ratkaisuna on rakentaa sopivan kokoisen tehdasyksikön aktiivihakemisto pelkästään automaatiolle, johon kunkin sen alueen järjestelmätoimittajan ympäristöt sijoitetaan. Tähän kannattaa varautua ennen kuin yhtään aktiivihakemistoa käyttävää automaatiojärjestelmää on hankittu, jotta ei jouduttaisi mukautumaan yhden järjestelmätoimittajan standardiin. Selkeän toimintamallin vuoksi järjestelmätoimittajien takuukysymyksiin liittyvät ongelmat ovat samalla kertaa ratkenneet ainakin toistaiseksi.

Jos yrityksessä on usean automaatiojärjestelmätoimittajan järjestelmiä, lisäsuojausta voidaan tarvittaessa toteuttaa järjestelmäkohtaisella DC:illä, joista jokainen sijoitetaan omaan verkkoonsa palomuurin taakse. Tässäkin tapauksessa on joitakin tarpeellisia tietoliikenneportteja jätettävä avoimeksi.

Toistaiseksi vain muutamat suurimmat tuotantoyksiköt ovat rakentaneet oman aktiivihakemistonsa. Näitä tilanteita pyritään välttämään, koska yhteisen hakemiston edut on koettu merkittäviksi. Erillisen aktiivihakemiston

rakentaminen ja ylläpito vaatii paljon paikallista osaamista. Tämän vuoksi automaation aktiivihakemiston tapauksessa kannattaa noudattaa samoja suunnitteluperiaatteita ja muun muassa nimistandardeja, joita yhteisessä aktiivihakemistossa on käytetty. Koska erilliset aktiivihakemistot ovat täysin ulkopuolisilta suljettuja järjestelmiä, mainittuja periaatteita noudattaen tiedetään myös yrityksen IT-johdon ja tietoturvaorganisaation tasolla, että rakennetut järjestelmät täyttävät tarvittavat tietoturvakriteerit.

Tuotantoyksiköiden aktiivihakemisto palvelee paikallisesti toimivia tuotantoprosesseja. Siihen liittyvän aktiivihakemiston DC:tä ei ole yleensä tarpeellista sijoittaa maantieteellisesti muualle toisin kuin koko yrityksen yhteisessä hakemistossa.

Hallinnoinnin helpottamiseksi aktiivihakemistojen välille on mahdollista luoda ns. luottosuhteita (Trust). Luottosuhteiden avulla toisen aktiivihakemiston objekteille, kuten käyttäjät (User) ja käyttäjäryhmät (Group), voidaan antaa käyttöoikeuksia.Ilman luottosuhteita olisi eri hakemistoissa oltava kullakin käyttäjällä oma käyttäjätili (User Account). Sekin on mahdollista, mutta hallinnoinnin kannalta työlästä ja sekavaa. Luottosuhteet voivat olla tarvittaessa yksisuuntaisiakin, jolloin yhteisestä hakemistosta voidaan poimia ne käyttäjäryhmät, joille annetaan oikeuksia automaation aktiivihakemiston resursseihin.

Yhteisessä hakemistossa joidenkin tärkeiden palvelujen hallintaa ei ole järkevää delegoida paikallisille pääkäyttäjille eli OU:n pääkäyttäjille. Oikeudet ovat vain toimialueen pääkäyttäjällä. Näitä palveluja (Services) ovat muun muassa DNS- ja WINS-palvelut. Automaation omassa hakemistossa on luonnollisesti täydet hallintaoikeudet koko hakemistoon.

On erityisesti huomattava, että usealla paikkakunnalla toimiva ja koko yrityksen mittakaavaan rakennettu kaikkien automaatio-osastojen yhteinen automaation aktiivihakemisto ei palvele paikallista suojautumistarkoitusta.

3. Windows -ympäristö – erilaisia vaihtoehtoja

Prosessinohjauksen toiminnan turvaamiseksi pyritään yleensä eliminoimaan kaikenlaiset ulkoiset häiriöt. Muun muassa sen vuoksi on syntynyt organisaation mukaisia tai järjestelmäkohtaisia hallinnointivyöhykkeitä. Samalla tällaisissa vyöhykkeissä voi soveltaa kunkin organisaation haluamaa tietoturvatasoa. Windows -ympäristöissä työryhmä (Workgroup) ja NT4 -toimialue (NT4 Domain) ovat olleet tähänastisista keinoista käytetyimmät. Automaatiojärjestelmien pitkän elinkaaren vuoksi kaikki sovellukset eivät välttämättä toimi uusimmilla käyttöjärjestelmäversioilla, joten voi olla vaikea perustella hyvin toimivan järjestelmän uusimista pelkästään ulkoisen tietoturvauhkan vuoksi. Eräs mahdollisuus jatkaa NT4-ympäristön käyttöä on järjestelmän eristäminen omaan tietoverkkoonsa, jos ulkopuolisia yhteyksiä ei tarvita.

3.1 Työryhmä

Työryhmässä (Workgroup) työasemat ja palvelimet ovat kukin itsenäisiä tietokoneita, ja niitä hallinnoidaan erikseen vailla keskitettyjä hallinnointiohjelmia, vaikka etähallinta on mahdollista siten, että kullekin koneelle luodaan etäyhteys, silti käyttäjätiedot, pääsyoikeudet, tietoturva- ja kaikki muutkin asetukset tehdään yksitellen työasema- ja palvelinkohtaisesti. Ylläpidon ajantasaisuus saattaa kärsiä ja muodostua työlääksi. Työryhmämalli on sopiva vain pienissä järjestelmissä. Tämä soveltuu kaikille Windows-versioille. Työasemissa ja palvelimissa on suositeltavinta käyttää vähintään Windows 2000 -versioita, koska Microsoft toimittaa sille ja sitä uudemmille käyttöjärjestelmäversioille tietoturvapäivityksiä. Virustorjuntaohjelmiston päivitys ei ole välttämättä ongelma, koska osalla näistä ohjelmista on myös oma etäjakelumenetelmänsä.

3.2 NT4-toimialue

Windows NT4 -toimialueen hallintaan on käytettävissä useita hallintatyökaluja, joilla voidaan hallita käyttäjätilejä ja salasanoja sekä pääsyoikeuksia ryhmätilien avulla. Käyttäjätileille voidaan kohdistaa järjestelmäkäytäntöjä (System Policy). Siinä suhteessa järjestelmä on täysin toimiva. Jos kaikki NT4-järjestelmän työasemat ja palvelimet olisivat vähintään Windows 2000-tasoisia, tietoturvan uhkatekijät olisivat pienet. Ongelman muodostavat eritysroolissa olevat toimialueen ohjauspalvelimet, joita ei voida päivittää uudempaan versioon. Tietoturvan osalta heikoin kohta on juuri pahin mahdollinen. Kaikki keskitetty hallinta ja toiminnallisuus on juuri näiden palvelinten varassa ja niiden toimimattomuus heijastuu koko järjestelmään.

4. Yrityksen sisäinen tietoturva

Tänä päivänä automaatio- ja toimistojärjestelmien raja on epäselvä. Osa automaatiosta on siirtynyt jo kauan aikaa sitten toimistoverkon puolelle. Sellaisia osia ovat muun muassa tuotannonsuunnittelu- ja tehdasjärjestelmät. Jos ylemmältä ohjaustasolta tulevat tuotteen valmistustiedot puuttuvat, olisi tuotteiden valmistus useassa tapauksessa mahdotonta, vaikka automaation perustaso toimisikin normaalisti.

Kun automaatio- ja toimistojärjestelmät ovat samassa verkossa, asettaa se kaikille osapuolille erityisen suuren haasteen. Suojaustasojen on oltava yhteisesti sovittujen mallien mukaan laadittuja. Esimerkiksi virusten aiheuttamien haittojen kannalta on yhdentekevää, tulevatko ne yrityksen sisäverkkoon valvomon työasemasta tai vaikkapa toisella paikkakunnalla sijaitsevan toimiston kahvihuoneen työasemasta, jossa käytetään Internet-verkkoa. Teollisuudessa valvomoiden työasemat ja automaation palvelimet on tavallisesti muistettu suojata, mutta yrityksen muiden työasemien suojausta ei välttämättä ole koettu yhtä tärkeäksi.

Automaatio-organisaatioilla on vastuu automaatiolaitteista ja sitä kautta tuotantoprosessien toiminnasta. Vikatilanteet eivät saa aiheuttaa vaaraa ihmisille ja ympäristölle. Sen vuoksi automaatiojärjestelmän osajärjestelminä ei voi olla laitteita tai organisaatiossa sellaisia osapuolia, joiden toimintaa ei voida ennakoida.

Kun yrityksen sisällä melkein koko tietoliikenne on samassa verkossa, on automaatioon liittyvä suojausajattelu ulotettava koko yritykseen. Seuraavissa kohdissa esitetään eräitä ongelma-alueita, jotka arkipäivän tilanteissa uhkaavat merkittävästi yrityksen tietoturvaa.

4.1 Yhteiskäyttöisyyden ongelmat

Tapaukset, joissa yhtä työasemaa käyttää useampi käyttäjä, muodostavat selkeän turvallisuusriskin verrattuna ns. henkilökohtaiseen tietokoneeseen. Yhteisen työaseman luonne mielletään sellaiseksi, että kaikki mitä sillä voidaan tehdä, on luvallista. Kun käyttäjätunnus on eräänlainen anonyymi ryhmätunnus, ei mahdollisissa väärinkäytöksissä voida näin ollen osoittaa vastuutahoa.

Tällaisia yhteisiä työasemia ovat muun muassa valvomoiden, työryhmien, kahvihuoneiden ja infopäätteinä olevat työasemat ja käyttäjätunnukset. Käyttäjätunnukset (käyttäjätilit) on otettava huomioon, koska Windows -järjestelmässä ilman erityisiä rajoituksia voi mihin tahansa työasemaan kirjautua millä tahansa käyttäjätunnuksella. Neuvotteluhuoneiden työasemat muodostavat tässä oman erityisongelmansa.

Edellisestä seuraa, että työaseman ja käyttäjätunnuksen oikeuksia on rajoitettava. Yleensä rajoitukset johtavat siihen, että kaikki työtehtäviin kuulumattomat ohjelmat sekä toiminnot karsitaan pois käytöstä. Tällä tavoin voidaan estää tahalliset vahingoittamisyritykset sekä tahattomat vahingot.

Näiden sääntöjen tulisi koskea kaikkia yrityksessä käytettäviä yhteiskäyttöisiä työasemia ja yhteisesti käytettyjä käyttäjätunnuksia. Yhteisiin työasemiin ei sovellu myöskään menettely, jossa työasemaan kirjaudutaan ajoittain jollakin toisella käyttäjätunnuksella. Käytännössä työasema usein unohtuu auki käyttäen sellaista tunnusta, jolla on suurimmat oikeudet. Tästä johtuen yhteiskäyttöisissä työasemissa kirjautuminen sallitaan vain yhdellä tunnuksella. Poikkeuksen muodostavat neuvotteluhuoneet, joihin nimenomaisesti kirjautuu kukin vain henkilökohtaisella tunnuksellaan, eikä yhteistunnuksilla, saaden siten vain omat henkilökohtaiset oikeudet.

Yrityksen kaikki henkilökohtaisetkin työasemat on suojattava siten, että niihin pääsee kirjautumaan vain kunkin työaseman paikalliseen käyttäjäryhmään kuuluvat henkilöt. Kyseistä ryhmää on helppo hallita etätyökaluilla. Ryhmään liitetään vain pääkäyttäjäryhmä ja työaseman käyttäjän käyttäjätunnus.

Windows-käyttöjärjestelmän perusasetuksissa käyttäjällä on näkyvissä monia työaseman hallinnointiin liittyviä työkaluohjelmia. Suuressa ympäristössä verkosta saattaa löytyä kohtia, joiden tietoturva ei välttämättä ole

kunnossa. Tietoverkon selaaminen (Browse) ei useinkaan ole tarpeellista. Myös annettaessa tietoja liian laajalle ryhmälle tiedon jakaja ei välttämättä huomaa ketkä kaikki todellisuudessa saavat tietoja. Kun kaikki verkosta löytyvät levyjaot avataan erikseen kullekin käyttäjälle tai oikeastaan käyttäjäryhmäkohtaisesti, mahdollisimman vähän tietoa joutuu vääriin käsiin.

Jos kaikkea ei saada toimimaan työasemassa pelkillä käyttäjän oikeuksilla, saatetaan henkilölle antaa täysi hallintaoikeus omaan työasemaan. Kaikki tällaiset seikat ovat riskitekijöitä yhteisessä tietoverkossa, jos niitä ei ennakolta ehkäistä.

Eräiksi suurimmista tietoturvaa uhkaavista asioista ovat osoittautuneet Internet-verkko ja sähköposti. Niiden kautta työasemaan ja siten koko järjestelmään tulee tietoturvaa uhkaavaa materiaalia. Näitä ovat muun muassa virukset, madot, pelit, ohjelmat ja levytilaa vievät tarpeettomat tiedostot. Muina kanavina ovat CD- ja levykeasemat sekä USB-väylään liitettävät muistitikut. Windowsin ja aktiivihakemiston ryhmäkäytäntöjen avulla tietoturvan hallinta on kuitenkin helposti toteutettavissa.

4.2 Internet-verkon riskit

Internet-verkossa on suodatusmenetelmistä huolimatta runsaasti sivustoja, joiden sisältö altistaa tietojärjestelmät vaaroille. Oikeuden Internet-verkon käyttöön tulee perustua vain henkilökohtaisiin oikeuksiin. Tällöin aktiivihakemiston Internet-käyttäjäryhmässä (Group) saa olla vain luonnollisten henkilöiden käyttäjätunnuksia. Asetukset työasemassa perustuvat aktiivihakemiston ryhmäkäytäntöihin, jotka astuvat voimaan aina käyttäjän kirjautuessa työasemalle. Kun käyttäjä kuuluu mainittuun Internet-käyttäjäryhmään, hänen työasemansa Internet-selainohjelma saa automaattisesti proxy- (välityspalvelin) ym. Internet-asetukset. Vastaavasti ryhmään kuulumattomuus jättää selainohjelman proxy-asetukset pois ja pääsy Internet-verkkoon ei ole mahdollista. Kummassakaan tapauksessa käyttäjällä ei ole mahdollisuutta muuttaa asetuksia.

Käytössä on edelleen Windows NT4 -työasemia, eivätkä niiden järjestelmäkäytännöt ole riittävän tehokkaita estämään Internet-liikennettä. Eräs ratkaisu on määrittää proxy-palvelimiin IP-osoitteet tai -osoitealueet, joita vastaavista työasemista ei ole lupa päästä Internet-verkkoon. Varmuuden vuoksi tätä menetelmää ja ryhmäkäytäntöjä on hyvä käyttää samanaikaisesti myös aktiivihakemiston yhteydessä.

4.3 Yhteiskäyttöisen sähköpostin riskit

Jos jollakin ryhmällä, esimerkiksi valvomon henkilöillä, on yhteinen sähköposti, on sen oltava vain talon sisäinen. Tämä on eräs mahdollinen suojautumistapa, koska maailmanlaajuisen Internet-käyttäjäkunnan kanssa ei voida sopia sääntöä: ”Älkää lähettäkö meille tarpeetonta ja palvelinten levytilat

täyttävää materiaalia, joka saattaa uhata myös tietoturvaa". Ohjeistus yrityksen sisällä on tarpeen. Tarvittaessa liitetiedostot voidaan suodattaa pois. Yhteinen sähköposti voidaan luokitella myös ilmoitustauluksi, jonka hoitajana on esimerkiksi työnjohtaja, jolloin sähköpostiliikenne on valvottavissa.

Myös tiedon lähettämiseen liittyy omat ongelmansa, joten sitäkin on syytä rajoittaa ennen kuin ongelmia esiintyy. Yhteiskäyttöisen sähköpostin luonnehan on anonyymi, jolloin yrityksen nimissä voidaan lähettää mitä tahansa tietoa ilman kiinnijäämisen vaaraa. Siksi myös tiedon lähettäminen yrityksen ulkopuolelle on estetty.

Mikäli sähköpostia käytetään valvomoista, sitä ei pitäisi tehdä niistä työasemista, jotka ohjaavat perusautomaatiota. Työaseman vikaantumisesta johtuva yhteyden katkeaminen automaatiojärjestelmään voi olla kohtalokasta. Joissakin tapauksissa tässä kuvatut menetelmät on todettu työläiksi eikä sähköposteja käytetä yhteiskäyttöisissä työasemissa.

4.4 Valvomotyöasemat

Työasema on voitava suojata väärinkäytöksiltä, mutta samanaikaisesti on luotava ympäristö, jossa työntekoa ei ole vaikeutettu turhilla suojauksilla. Järkevimmäksi vaihtoehdoksi jää tämän toteuttaminen siten, että työasemille asennetaan vain automaatiojärjestelmän ohjaukseen tarvittavat sovellusohjelmat ja kaikki muu on estetty. Monitorille tarkoitettu kuvaruudunsäästäjä sekä salasanan kirjoittaminen ovat eräitä työtä häiritseviä asioita. Toiminnot, joita työasemalla voidaan suorittaa, ovat verrattavissa valvomossa oleviin ohjauskytkimiin ja muihin hallintalaitteisiin. Nekin ovat kaikkien valvomossa asioivien saatavilla eivätkä vaadi salasanoja.

Kun valvomo on sellainen, että siellä on aina miehitys, salasanan kyselyä ei erityisesti tarvita. Todellisuudessa tunnuksella on salasana, jota käyttäjät eivät tiedä, koska kirjautuminen järjestelmään suoritetaan automaattisesti työaseman käynnistyksen yhteydessä. Salasana tarvitaan sen vuoksi, että kyseisellä tunnuksella ei pääsisi kirjautumaan järjestelmään mistään muualta.

Seuraavat asiat on otettava huomioon valvomotyöasemien yhteydessä (järjestelmän koventaminen, Hardening):

- Tietokoneen käynnistys levykkeeltä tai CD:ltä estetään BIOS:in määrityksillä ja määritysten muuttaminen suojataan salasanalla, kuten kaikissa työasemissa.
- Työasemaan pääsee kirjautumaan vain tietyllä tunnuksella, kuten muissakin työasemissa.
- Fyysinen suojaus, jossa työasemat ovat lukitussa tilassa ja ulkoisten medialaitteiden käyttö on mahdotonta.
- Poistetaan kaikki Windowsin oletuksena tulevat turhat ohjelmat.
- Poistetaan kaikki turhat palvelut (Services) ja verkkoliikenneprotokollat
- Poistetaan oikeudet tietoverkon selaamiseen.
- Otetaan käyttöön sallittujen ohjelmien lista ryhmäkäytännöillä.

- Kiintolevylle tallennus estetään.
- Pyritään välttämään tiedostojen tallennuksia ja se voidaan tehdä tarvittaessa ainoastaan palvelimen levylle.
- Ruudunsäästäjä kytketään pois käytöstä.
- Ulkoisen median käyttö estetään: CD- ja levykeasemat sekä USB-portit ryhmäkäytännöillä tai erillisellä ohjelmalla ja lisäksi, jos mahdollista, laitetila lukitaan.
- Internet ei ole sallittu.
- Sähköposti on talon sisäinen tai sitä ei ole ollenkaan.

5. Pääsyoikeuksien hallinta

Ulkopuolisten ja talon omankin väen tietoverkkoon pääsyn hallintaan tarvitaan rajauksia käyttöjärjestelmän pääsyoikeuksiin. Aktiivihakemistossa yksittäisille käyttäjätileille ei määritetä suoraan palvelimen käyttöoikeuksia, vaan pääsy sallitaan ainoastaan ryhmäoikeuksien kautta. Palvelimelta poistetaan Windowsin oletuksena oleva pääsy kaikille.

Windows palvelimen päällekkäisiä määrityksiä on kolmella tasolla, jotka ovat

– pääsy palvelimelle
– pääsy levyjakoon
– pääsy kansiorakenteeseen.

Palvelimelle pääsevät kaikki sen palvelimen käyttäjäryhmät. Samalla palvelimella voi olla useita levyjakoja, jolloin kuhunkin jaettuun resurssiin pääsevät vain ne ryhmät, joilla on oikeuksia kyseisen jaon sisältämiin kansioihin. Pääsy eri kansioihin voi olla erikseen rajattu useammalle ryhmälle.

Kutakin käyttäjäryhmää hallinnoidaan aktiivihakemistosta käsin, jolloin palvelimen käyttöoikeuksiin ei tarvitse alkumääritysten jälkeen puuttua millään tavoin. Aktiivihakemiston hallinnointityökalulla voidaan käyttäjätili linkittää tarvittaviin käyttäjäryhmiin. Tähän voidaan liittää myös ryhmäkäytäntöjen avulla tapahtuva verkkolevyn automaattinen avaaminen.

Oman ryhmänsä pääsyoikeuksien hallinnassa muodostaa ulkopuolisten työntekijöiden pääsy verkkoon omalla tietokoneellaan. Automaatiojärjestelmien huollossa sellainen tarve esiintyy varsinkin uusien järjestelmien käyttöönoton yhteydessä. Työasemat sekä niiden tietoturvataso tarkastetaan aina ennen luvan antamista. Lisäksi annetaan toimintaohjeet ja vaaditaan, että saadut tiedot on pidettävä salassa. Tämä varmennetaan sopimuksen allekirjoituksella. Eräänä menetelmänä on virtuaalisen LAN-verkon rakentaminen näille huoltohenkilöille. Verkosta annetaan yhteydet vain tietyille palvelimille tai käytetään pääsyoikeuslistoja (ACL). Työntekijöiden omien koneiden lähtötarkastus on käytännössä hankalaa ja sen vuoksi on pyrittävä

ensisijaisesti järjestämään yrityksen oma kone talon ulkopuolisille henkilöille.

Mikäli käytetään huoltomodeemiyhteyksiä automaatiojärjestelmiin, tulee niiden olla päällä vain huoltojen suorituksen ajan. Sama sääntö koskee VPN-yhteyksiä. Huoltomiesten toiminta perustuu tietyssä mielessä luottamukseen, koska etäyhteydessä käytetyn koneen tarkastus on käytännössä vaikeaa pitkän maantieteellisen etäisyyden vuoksi ja tarkastuspäivän jälkeistä tilannetta on mahdotonta valvoa. Nykytekniikalla tietoa voidaan salakuljettaa liiankin helposti, joten viimekädessä ulkopuolisen kuten omankin henkilöstön pääsy tietoverkkoon perustuu luottamukseen.

6. Tietoturvapäivitykset

Outokummun tietoturvaorganisaatio lähettää 40 maan yhteensä 200 paikkakunnan tietoturvayhteyshenkilöille tiedon siitä, että Intranet-sivustoille on ilmestynyt uusin tietoturvapäivitys. Päivityksiä ei siis haeta jokaiselle koneelle Internetistä. Jokainen päivitys saa näin konsernin hyväksynnän siitä, että se voidaan ottaa käyttöön. Ne asennetaan paikallisesti niihin koneisiin, joihin se on mahdollista tehdä ilmoitettuun ajankohtaan mennessä. Poikkeuksen muodostavat automaatio- tai muut järjestelmät, joihin on järjestelmäkohtaiset erityisohjeet. Yleensä uusimmat päivitykset saadaan näissä tapauksissa asennettua viiveellä, koska ensin tutkitaan mahdolliset vaikutukset sovellusohjelmistoille. Parhaiten tämä onnistuu järjestelmätoimittajalta, joka on takuukysymyksien vuoksi ainoa oikea taho.

Suurimman ongelman muodostavat NT4 -palvelimet. Ongelmana ovat järjestelmätoimittajat, joiden resurssit eivät riitä tietoturvapäivitysten testaukseen tai sovellusten uusimiseen. Silti myös näiden järjestelmien kanssa on tultava toimeen ja testattava ne itse. Tämä voidaan toteuttaa asentamalla päivitykset esimerkiksi ensin järjestelmäkopioon ja tarkastamalla mitä käytännössä tapahtuu.

Virustorjuntaohjelmistojen päivitykset tulevat yhden yhteyden kautta yrityksen sisäverkkoon. Työaseman virustorjuntaohjelmisto hakee uusimman virustietokannan automaattisesti sille määritetyltä palvelimelta.

LIITE 4

Energian jakeluautomaation tietoturva

Pekka Koponen/VTT Prosessit

1. Johdanto

1.1 Lähtökohdat

Puutteellinen tietoturva energiajärjestelmien hallinnassa saattaa aiheuttaa vakavia vahinkoja, kuten esimerkiksi

– sähkön ja lämmön tulo käyttökohteeseen lakkaa (seurausten merkitys riippuu kohteesta)
– huomattavia laitevaurioita ja henkilöturvallisuusriskejä, jos suojausjärjestelmät eivät toimi oikein
– järjestelmä voi tarjota reitin siihen liitettyihin järjestelmiin tunkeutumiseen
– luottamuksellisten kulutustietojen joutuminen kilpailijalle tai rikolliselle
– tarjousten, laskutuksen yms. kaupallisten tietojen muuttumista
– viranomaisvalvontaan liittyvien tietojen muuttumista
– energiankulutuksen ja päästöjen lisääntymistä.

Tässä liitteessä tarkastellaan energianjakelun järjestelmien automaation tietoturvaan kohdistuvia vaatimuksia ja haasteita. Näkökulma painottuu sähkönjakeluun, mutta laajalla maantieteellisellä alueella toimivaa automaatiota tarvitaan ainakin myös

– kaukolämmön, maakaasun ja veden jakelussa
– energian siirrossa, kuten sähkön, lämmön ja maakaasun siirrossa
– sähkökaupassa
– monien sähkön- ja lämmön tuotannon muotojen hallinnassa
– hajallaan sijaitsevien energiankäyttökohteiden hallinnassa, kuten kiinteistöjen etähallinnassa.

Esitetyt näkökohdat pätevät siis monissa muissakin hyvin laajalle alueelle hajautetuissa automaatiojärjestelmissä. Sähkönjakelun automaation lisäksi tässä liitteessä tarkastellaan erikseen vain hajautetun energiantuotannon tietoturvan hallintaa.

Edellä esitettyjen automaation sovellusalueiden erityispiirteinä ovat alueellinen laajuus, suuret etäisyydet ja järjestelmien hajautetun osan pitkä käyttöikä sekä suuri määrä kytkentöjä muihin osapuoliin ja järjestelmiin. Siitä huolimatta monilta automaatiotoiminnoilta edellytetään nopeaa vaste-aikaa

ja luotettavuutta. Hyvän tietoturvan tason toteuttaminen tässä ympäristössä ei onnistu, jos vastuualueita ei rajata hallittavan kokoisiksi ja jos kulloinkin kyseessä olevan automaatiojärjestelmän erityispiirteitä ei oteta huomioon. Kuhunkin tapaukseen on valittava siihen parhaiten sopivat keinot varsin laajasta menetelmävalikoimasta.

1.2 Sähkövoima-alan omia tietoturvaohjeita ja -standardeja

Sähkövoima-alan kansainväliset järjestöt ja standardointiorganisaatiot työskentelevät alan tietoturvan ohjeistuksen kehittämiseksi [1, 2, 3, 4, 5]. Viitteissä 1, 2 ja 3 kuvataan sähkön tuotannon, siirron ja jakelun tietojärjestelmien erityispiirteitä tietoturvan osalta.

Viite [1] esittää taustatietoja seuraavista asioista:
- Miksi tietoturva on tärkeää sähköenergiateollisuudelle?
- Missä ovat uhkat ja järjestelmien heikkoudet?
- Miksi tietojärjestelmäarkkitehtuurien kehitys on lisännyt uusien järjestelmien alttiutta tietoturvaongelmille?
- Mitä tietoturvaa tarkastelleita työryhmiä on ollut tai on ja mitä ne ovat tehneet?

Viite [2] käsittelee seuraavia asioita:
- Miksi sähköenergiateollisuuteen on kehittynyt monia toisiinsa kytkettyjä tietojärjestelmien verkkoja?
- Mitkä erityispiirteet tekevät automaatio- ja hallintajärjestelmät alttiiksi tietoturvan uhkille?
- Yhteenveto niistä harvoista tunnetuista tapauksista, jossa on ilmennyt vakavia tietoturvaongelmia.
- Ehdotus joistakin välittömistä toimenpiteistä keskeisten tietojärjestelmien turvaamiseksi.

Viitteessä [3] korostetaan ISO/IEC 17799 -standardin suositusten soveltamista ja siinä on myös runsaasti hyviä kirjallisuusviittauksia.

Viitteessä [6] tarkastellaan olemassa olevien sähköverkon tiedonsiirto- ja tietojärjestelmien heikkouksia ja ehdotetaan järjestelmäarkkitehtuuria näiden puutteiden korjaamiseksi.

1.3 Vaatimuksista

Tässä yhteydessä ei ole mielekästä rajata tietoturvan tarkastelua käsittämään pelkästään tietoliikenteen ja tietokoneiden ohjelmia. Turvallisuusriskien tarkastelun on katettava koko sovellus myös fyysisten laitteiden toiminnat ja signaalit sekä koko asiaan vaikuttava järjestelmäkokonaisuus. Oleellista on

energian toimituksen luotettavuus, ihmisten ja laitteiden vahingoittumisen estäminen, tietojen luottamuksellisuuden säilyttäminen, kustannustehokas energiaa ja ympäristöä säästävä toiminta sekä energiakauppaan ja valvontaan tarvittavien tietojen virheettömyys. Yksittäisen tietoliikenneyhteyden tietoturvan parantamisesta ei ole merkittävää hyötyä, jos huomattavasti heikompi lenkki on muualla. Riskejä voivat aiheuttaa tahallinen tai tahaton tunkeutuminen, asennusvirheet, operaattorin tai ohjelmistojen virhetoiminnat, laitteiden rikkoutumiset ja energianjakeluverkon tai tietoliikenneverkon toiminnan keskeytykset.

Automaatio- tai muun järjestelmän toimintavarmuus riippuu myös sähkönsyötön ja varavoiman luotettavuudesta. Automaatio ja etävalvonta voivat olla varavoimalan ja akkujen luotettavan toiminnan edellytys, mutta ne saattavat samalla lisätä varavoiman haavoittuvuutta hyökkäyksille. Jos varavoimaratkaisuihin sekä niiden automaation ja etähallinnan tietoturvaan ei kiinnitetä riittävästi huomiota, ne saattavat olla järjestelmän heikko kohta.

2. Sähkönjakelun automaation erityispiirteitä

2.1 Toimijoiden ja järjestelmien laaja verkosto

Sähkönjakelujärjestelmien toiminta riippuu nykyisin pitkälti tietokoneista ja -järjestelmistä. Sähköenergiajärjestelmien automaatiojärjestelmissä on paljon laajalle maantieteelliselle alueelle sijoitettuja päätelaitteita ja alajärjestelmiä, joiden pikainen vaihtaminen uusiin tulisi suurten etäisyyksien takia liian kalliiksi. Järjestelmien laitteisto- ja ohjelmistokokoonpano sekä ulkoiset liitännät kuitenkin muuttuvat ja lisääntyvät ajoittain jossakin kohdassa järjestelmää. Myös tietoliikenneverkoston konfiguraatio ja toteutusratkaisut muuttuvat nopeasti.

Sähkömarkkinoiden avaaminen kilpailulle ja vertikaalisesti integroitujen sähköyritysten purkaminen on pirstonut alan eriytettyihin liiketoimintoihin, joita ovat tuotanto, siirto, jakelu ja vähittäismyynti. Yritysten rakenne on siis huomattavasti muuttunut ja tietojärjestelmien on pitänyt muuttua tämän mukaisesti. Näin ollen erilaisia ja erillisiä tietojärjestelmiä on paljon ja näiden tietojärjestelmien on kyettävä yhteistoimintaan vaikka ne nyt kuuluvat eri osapuolille. Automaatiojärjestelmien on tällöinkin kyettävä hallittuun keskinäiseen tietojenvaihtoon.

Eriyttämisen ohella myös toimintojen ja asiantuntemuksen ulkoistaminen on lisännyt osapuolten määrää. Vastuut ja omistussuhteet muodostavat tapauskohtaisesti vaihtelevia verkostoja. Osapuolten ja roolien suuri määrä vaikeuttaa tietoturvavastuiden ja riskien hallintaa. Monissa sähkönjakeluyhtiöissä ulkopuoliset osapuolet hoitavat varsin keskeisiä toimintoja.

On erikokoisia sähkönjakeluyhtiöitä. Pienet joutuvat verkottumaan muiden yritysten kanssa sekä ulkoistamaan hyvin suuren osan toiminnoistaan. Isot toimivat useissa maissa ja monilla enemmän tai vähemmän erillisillä sähkönjakelualueilla. Ne myös ostavat ja myyvät sähkönjakelualueita muiden yhtiöiden kanssa. Eri jakelualueilla automaatiojärjestelmät ovat historiallisista syistä hyvin erilaisia. Näin ollen monet sähkönjakeluyritykset ovat automaation optimoinnin osalta riippuvaisia sekä julkisista että muiden osapuolten hallitsemista tietoverkoista ja Internet-protokollien käytöstä.

Sähköverkon ylläpito, vahvistaminen, laajentaminen ja vikojen korjaus perustuvat entistä enemmän ulkoisten osapuolten käyttöön. Kaikilla osapuolilla on syytä olla tarvittavassa laajuudessa tietoa jakeluverkon ja sen automaation tilasta, jotta omaisuus- ja henkilövahinkojen riskiä voidaan pienentää, ja jotta eri ryhmien toiminta voidaan koordinoida tehokkaaksi sekä ajankäytön että kustannusten osalta.

Ei voida luottaa siihen, että ne muut osapuolet, joiden kanssa tietoja joudutaan vaihtamaan, olisivat hoitaneet tietoturvansa hyvin. Voi myös esiintyä houkutuksia esimerkiksi vuotaa tietoja saman omistajan muille liiketoiminnoille tai asiakkaiden kilpailijoille. Ei voida lähteä siitä, että saman yrityksen sisällä olevat eri järjestelmät olisivat samalla turvallisuustasolla tai olisivat muutenkaan oikeutettuja samoihin tietoihin. Tietoturvan merkitys ja tietoisuus siitä vaihtelee eri sovellusten välillä.

Tiedonsiirrossa muiden osapuolten kanssa käytetään usein yleisiä tietoverkkoja kuten Internet-verkkoa. Eri osapuolten välillä tarvitaan turvallista, luotettavaa ja luottamuksellista tiedonsiirtoa. Laitteistokeskeinen näkökulma tietoturvaan ei toimi, koska eri järjestelmät ovat entistä enemmän toisiinsa kytkeytyneitä ja keskenään muutenkin integroituneita.

Sähkön siirto- ja jakeluyhtiöillä on käytössään ainakin seuraavia tietojärjestelmiä:

- Energianhallintajärjestelmä, joka koostuu teknisten sähköenergiataseiden hallinnasta ja kaupallisten energiataseiden laskennasta.
- SCADA-järjestelmä (Supervisory Control and Data Acquisition System), (aikaisemman kaukokäyttöjärjestelmän vastine).
- Sähköverkossa ja sähköasemilla sijaitsevat etäohjausasemat (Remote Terminal Unit RTU) (päätelaitteet) ja paikalliset automaatiojärjestelmät
- Suojausjärjestelmät (suojareleet).
- Asiakastietojärjestelmä (Customer Information System, CIS).
- Verkkotietojärjestelmä (Geographical Information System, GIS).
- Kulutusmittauksen lukujärjestelmät.
- Laskutusjärjestelmä.
- Kirjanpitojärjestelmä.
- Verkoston suunnittelujärjestelmä.
- Verkosto-omaisuuden hallintajärjestelmä (Asset Management System).
- Sähkön laadun valvontajärjestelmä.

Myös sähkön tuotannon ja kaupan yhtiöillä on useita järjestelmiä. Nämä ovat energiakauppaa, energianhallintaa, optimointia, ennustusta, asiakastietojen hallintaa ynnä muuta varten.

Monet edellä mainitusta järjestelmistä, esimerkiksi SCADA-järjestelmät, kattavat maantieteellisesti erityisen laajoja alueita. Jotkut alajärjestelmät taas voivat rajoittua vain hyvin pienelle alueelle, esimerkiksi monet suojausjärjestelmät ja sähköasemien automaatiojärjestelmät ovat varsin paikallisia.

Monien, mutta ei kaikkien, edellä mainituista järjestelmistä on toimittava ajan tasalla. Ajantasaista toimintaa ei saisi pysäyttää tai liiaksi hidastaa tietoturvatoimintojen, -päivitysten tai -ongelmien takia.

Järjestelmissä käsitellään muita osapuolia koskevia luottamuksellisia tietoja. Esimerkiksi asiakastietoja ja asiakkaiden kulutustietoja ei saa levittää eteenpäin tai myydä ilman asiakkaan erikseen antamaa lupaa. Tällaisten tietojen kysyntä on lisääntymässä.

Sähkönjakeluautomaatio ei toistaiseksi ole juurikaan kattanut pienjänniteverkkoa eikä edes keskijänniteverkon ääriä, vaikka automaatiosta olisikin siinä merkittäviä hyötyjä. Automaation avulla sähkön jakeluverkon kapasiteetti voidaan käyttää tarkemmin, ongelmia voidaan ennakoida ja jakeluverkkoon tarvittavia investointeja suunnata ja hyödyntää tarkemmin. Syynä jakeluverkon ääripäiden automaation puutteeseen ovat olleet hajautetun automaation toteutuksen ja mittarihankintojen suuret kustannukset. Eräs mahdollisuus saada jakeluverkon ääripäät kohtuullisin kustannuksin automaation piiriin on se, että hyödynnetään muiden osapuolten muita automaatiojärjestelmiä ja tiedonsiirtoverkkoja.

Sähkön jakeluverkon äärialueiden automaatiota joudutaan myös parantamaan, jotta voitaisiin välttää verkostoinvestointeja ja jotta hajautettua tuotantoa voitaisiin lisätä viranomaisten ja poliittisten tahojen suunnitelmien edellyttämällä tavalla. Hajautetun tuotannon lisäämisen taustalla on toisaalta tarve lisätä uusiutuvien energiavarojen hyödyntämistä ja toisaalta parantaa sähköenergiajärjestelmien käyttövarmuutta. Samalla lisääntyy myös tarve ohjata asiakkaiden automaatiojärjestelmien välityksellä sekä sähkön kulutusta että hajautettua tuotantoa. Muutoin hajautetun tuotannon lisääminen aiheuttaa sähköenergiainfrastruktuurin vahvistamisinvestointeja, energiahäviöitä ja kasvaneita päästöjä. Toisaalta sähköenergian tuotannossa tapahtuu samaan aikaan myös tuotannon keskittämistä entistä suurempiin tuotantoyksiköihin. Myös tämä lisää ohjattavien energiaresurssien tarvetta.

Eri järjestelmät on alun pitäen suunniteltu toisistaan erillään laitteisto- ja ohjelmistoratkaisujen sekä tiedonsiirtoprotokollien suhteen. Ne ovat myös eri-ikäisiä. Myöhemmin näiden järjestelmien välille on kuitenkin rakennettu yhä lisää yhteyksiä, koska tarve eri järjestelmien väliseen tietojen vaihtoon ja koordinointiin lisääntyy koko ajan. Näitä yhteyksiä toteutettaessa ei tietoturvaa ja tietoturvaratkaisujen yhteensopivuutta ole aina riittävästi ajateltu. Jos tietoturvasta ei riittävästi huolehdita, on vaarana se, että yhteen järjestelmään päässyt tietoturvaongelma leviää muihinkin järjestelmiin.

Sähköenergiainfrastruktuurin automaatiossa tietoturva on pitkälti perustunut siihen, että kyseisillä järjestelmillä on mahdollisimman vähän yhteyksiä muihin järjestelmiin. Sähkömarkkinoiden toimintojen eriyttäminen, jakeluverkkojen hyväksikäytön tehostaminen, hajautetun tuotannon sekä ohjattavien hajautettujen energiaresurssien lisääminen aiheuttavat kuitenkin sen, että eristäminen muista automaatiojärjestelmistä ja muista osapuolista ei ole enää käytännössä yleensä mahdollista. Erityisesti tämä koskee jakeluverkkoautomaatiota, energian vähittäiskauppaa, kulutusmittausten automaatiota ja verraten pienten kohteiden kulutuksen ja tuotannon hallintaa. Tietoturvan merkitys tulee korostumaan muun muassa siksi, että sen hoitaminen tällaisessa monen osapuolen useiden automaatiojärjestelmien vuorovaikutusympäristössä on varsin haasteellista.

2.2 Sähkönjakeluautomaation protokollista

Sähkönjakeluautomaation järjestelmien protokollissa on hiljalleen tapahtumassa muutos. Perinteisesti tiedonsiirron protokollissa ensisijaisena tavoitteena oli tiedonsiirtokaistan minimoiminen ja muut tavoitteet olivat siihen nähden selvästi taka-alalla. Maailmanlaajuista protokollastandardia ei ollut, vaan eri puolilla maailmaa oli omat protokollansa. Valmistajakohtaisia protokollia ja erityispiirteitä esiintyi myös runsaasti. Vuonna 1990 julkaistiin IEC60870-5-standardi, jota yhä päivitetään säännöllisesti. Sitä käytetään melko yleisesti eri puolilla maailmaa ja erityisesti Euroopassa. Avoimuuden takia sillä korvataan vieläkin valmistajakohtaisia protokollia. Myös IEC 60870-5-standardi on suunniteltu tiedonsiirtokaistan minimoimiseen ja pisteestä pisteeseen liikennöintiin. Se ei myöskään poistanut sitä ongelmaa, että sähkön jakeluautomaation eri osajärjestelmillä ja tasoilla on omat keskenään yhteen sopimattomat standardiprotokollansa.

Monia järjestelmiä tullaan vielä käyttämään pitkään, vaikka protokollien standardoinnin tilanne onkin nyt selvästi muuttumassa. Uudet olio-pohjaiset tietoliikenneverkoissa käytettäväksi suunnitellut IEC 61850 -standardit ja niihin pohjautuvat standardit on nyt varsin yleisesti hyväksytty lähes koko maailmassa tulevaisuuden sähkönjakeluautomaation käyttämiksi standardiprotokolliksi. IEC 61850 -standardit perustuvat uuteen Manufacturing Message Specification (MMS) -versioon ISO 9506:2003, eli myös yhteensopivuus muiden alojen automaation kanssa paranee sitä kautta. Niissä ensisijaisena tavoitteena on tietojen hallittavuus, joka saadaan oliopohjaisten tietomallien avulla. IEC 61850 -standardit pystyvät myös korvaamaan useita sähkönjakeluautomaatiojärjestelmän eri osissa käytettyjä protokollastandardeja.

IEC 61850 -protokollissa alemmilla protokollatasoilla käytetään yleisesti käytettyjä vakiintuneita standardeja, kuten TCP/IP-protokollaa. Aikakriittiseen tiedonsiirtoon on kuitenkin ollut tarpeen kehittää oma protokolla, GOOSE, joka lähettää IP-verkossa tapahtumatietoja ilman kättelyjä ja kuittauksia samanaikaisesti useaan ennalta määrättyyn pisteeseen. Tiedonsiirto-

kaistan minimoimista ei enää ole pidetty tärkeänä, koska se on nykyisin varsin halpaa. Sähköenergiajärjestelmien valvomojen välisessä tiedonsiirrossa käytettävät oliomallit määrittelee standardi IEC 61970. Tärkeimmillä järjestelmävalmistajilla on jo tarjolla IEC 61850 -protokollaa käyttäviä järjestelmiä ja laitteita. Sitä on alettu käyttää jonkin verran etenkin sellaisissa toteutuksissa, joissa käytännössä koko järjestelmä uusitaan.

IEC 61850 -protokollat ovat selvästi tiedonsiirron avointa kerrosmallia (ISO-standardin OSI 7-kerrosmallin periaatteita) toteuttavia ja verkkoorientoituneita. Vallitseviin järjestelmiin verrattuna tämä luultavasti tulee helpottamaan tietoturvan analysointia, arviointia ja toteuttamista sekä muuttuneiden tietojen havaitsemista. Itse protokollastandardi IEC 61850 ei huolehdi tietoturvasta, vaan tietoturva voidaan toteuttaa itse sovelluksesta riippumatta kulloinkin parhaaksi katsotuilla tavoilla. Voidaan myös suoraan käyttää valmiita TCP/IP-verkoissa yleisesti käytettyjä ja koettuja tietoturvaratkaisuja. Toisaalta oliomallien mukaan jäsennellyn tiedon perusteella jokaisen sovellusaluetta tuntevan, joka näkee tiedot selväkielisenä, on helppo saada käsitys tietojen merkityksestä ja löytää haluamansa tieto. Tietoturvasta huolehtiminen helpottuu, mutta toisaalta tietoturvan hoitamisen tärkeys myös korostuu. Eri sukupolvia olevia tietoliikenneprotokollia tullaan käyttämään vielä pitkään rinnakkain ja olisi ymmärrettävä kaikkien käytössä olevien protokollien erityispiirteet tietoturvan kannalta.

Käytössä on kerrottu (J. Weiss) olevan sellaisia SCADA-protokollia, jotka hylkäävät järjestelmän tunnetun tilan kanssa ristiriidassa olevia sanomia virheellisinä tekemättä siitä edes virheilmoitusta saati tarkistuskyselyä. Näin tunkeutuja ja virhetoiminto on voinut muuttaa ala-aseman ohjaussignaalin tilaa ilman, että siitä on tullut mitään ilmoitusta valvomoon tai tapahtumaraporttiin. Näin ongelman selvittely on kestänyt kauan ja vahinkojen määrä on ehtinyt kasvaa.

Sähköenergiajärjestelmien tietoturvasta on alan protokollista vastaavalla IEC-komitealla TC57 tekeillä standardijoukko IEC 62351 (ks. viite [4]). Se tulee käsittelemään sitä, miten tietoturvaa toteutetaan käytettäessä saman työryhmän alaisia tietoliikenneprotokollia, joihin myös edellä mainitut IEC60870-5-, IEC 61850- ja IEC 61970 -standardisarjat kuuluvat. Taustalla on TC57-komitean havainto, että pelkästään salaus ja VPN-verkot eivät tuo riittävää tietoturvaa, koska tietoturvan vaatimus koskee tiedon tuottajan ja sen käyttäjän välistä (tiedonsiirtoverkon kautta kulkevaa) yhteyttä päästä päähän.

3. Tietoturva sähkönjakeluautomaatiossa

3.1 Automaatiojärjestelmien mahdollisesti heikkoja kohtia

Viitteessä [2] pohditaan kohtia, joista tosiaikajärjestelmiin voidaan tunkeutua. Seuraava luettelo näistä kohdista perustuu osittain viitteeseen [2].

- Järjestelmän osien tai tietoliikenteen ylläpitoliitännät, muun muassa modeemiyhteyksien tai kannettavien tietokoneiden kautta, voivat mahdollistaa tunkeutujan muuttamaan järjestelmän konfigurointeja ja sanomia sekä pääsyn SCADA-järjestelmän ja ala-asemien välisen tietoliikenteen kautta muuallekin kuin ylläpidon kohteena olevaan osajärjestelmään.
- Erityisesti on syytä tarkastella suojausten ohjelmiston ja parametrien ylläpitoliitännät, koska suojausten muuttamisella voi olla vakavat seuraukset. Suojausten toiminnasta vastaavalla henkilöllä on tarvetta muuttaa suojausten parametreja ja jopa ladata suojareleiden ohjelmistopäivityksiä.
- SCADA-järjestelmään kiinteästi tai tilapäisesti liitetyt PC:t ja sulautetut PC:t.
- Automaatiojärjestelmän sekä siihen liitettyjen PC-laitteiden käyttöjärjestelmien ja ohjelmistojen päivitykset.
- Voi olla mahdollista, että esimerkiksi viruksesta saastunut ala-asema tai alajärjestelmä ylikuormittaa tietoliikenneyhteyksiä.
- Tietoliikenne erityisesti yleisiä tietoverkkoja, Internet-verkkoa tai langattomia yhteyksiä käytettäessä.
- Huonosti automaatiojärjestelmän kanssa yhteensopivat tietoturvamekanismit voivat ylikuormittaa ja haitata automaatiojärjestelmän toimintaa ja käyttöä kriittisillä hetkillä. Tämän seurauksena tahallisen tai tahattoman tietoturvahyökkäyksen aiheuttamat vahingot voivat kasvaa.
- Tiettyjä tieto- ja automaatiojärjestelmiä operoidaan valvomoiden sijasta entistä enemmän Internetin yli verkkoselaimilla näytettävien valvomonäyttöjen kautta, esimerkiksi päivystäjän kotoa tai liikkuvan ryhmän autosta. Samoin matkapuhelimilla saatetaan ohjata joitakin automaatiojärjestelmiä. Tietoturvan laiminlyönneistä voi näissä tapauksissa aiheutua suuria riskejä.
- Henkilöstö.

3.2 Raportoituja tapauksia

Kirjallisuudessa on mainittu seuraavia sähköenergiajärjestelmien automaatioon liittyviä tapauksia:

- Säätöjärjestelmään tunkeutunut virus aiheutti usean 100 MW sähköntuotantolaitoksen tuotannon alasajon muutamassa sekunnissa. Virus tuli yrityksen yleisen tietoverkon kautta. Sen jälkeen automaatioverkko erotettiin täysin toimistoverkosta [2].
- Sähkön jakelun SCADA-järjestelmä meni osittain toimintakyvyttömäksi usean päivän ajaksi, kun viruksen saastuttama kannettava PC oli kytketty tietoliikennereitittimen ylläpitoa varten. SCADA-järjestelmän kaikki tietoliikennesolmut saastuivat viruksesta. Myöhemmin muun muassa kannettavien tietokoneiden virustorjunnan hallintaa parannettiin [2].
- Järjestelmätoimittaja oli tehnyt energianhallintajärjestelmään sovellusten päivityksiä ilman lupaa. Varsinaista vahinkoa ei tapahtunut, mutta tapaus

paljasti sen, että tietoliikenneportti Internetiin oli jäänyt auki. Hallitsemattomien päivitysten mahdollisten tahattomien riskien lisäksi järjestelmä oli siis ollut alttiina myös ulkopuoliselle hyökkäykselle [2].

- SCADA-järjestelmän käyttämiä tietoliikenneyhteyksiä oli ylikuormittunut, kun tunkeutujat olivat alkaneet hyödyntää kyseisiä yrityksen sisäisiä etätiedonsiirtoyhteyksiä omiin tarkoituksiinsa. Ylikuormitus ehti aiheuttaa joitakin järjestelmän virhetoimintoja, mutta vakavilta seurauksilta vältyttiin.
- Esiintyy mainintoja siitä, että ylläpitoa suorittava henkilöstö on tietoturvan aukkojen ja puutteellisen käyttöoikeuksien hallinnan kautta tahattomasti aiheuttanut tai ollut lähellä aiheuttaa virhetoimintoja tai automaatiojärjestelmän ylikuormitusta. Ilman asianmukaisia lupia ja dokumentointia tehtyjä ohjelmistomuutoksia on myös mainittu.
- USA:n ja Kanadan itärannikon elokuun 2003 suuren sähkökeskeytyksen syitä tutkittaessa ilmeni myös tietoturvaongelmia, joilla ei kuitenkaan tässä tapauksessa liene ollut ainakaan oleellista merkitystä tapahtumien kehittymiseen. Tärkeimmät syyt olivat kuitenkin ihan muita eli sähkönsiirron ja tuotannon varakapasiteetin lähes täydellinen puuttuminen sekä se, että toimintaa, menettelytapoja ja valtuuksia nopeasti etenevän suurhäiriön rajoittamisesta ei oltu kunnolla sovittu ja suunniteltu etukäteen. Laukaisevina syinä oli muun muassa laiminlyöntejä siirtoyhteyksien kunnossapidossa sekä kilpailutilanteen aiheuttanut ohjelmointivirhe laajassa energianhallintajärjestelmän ohjelmistossa. Tapauksella on tässä yhteydessä merkitystä seuraavista syistä:
  - Kriittisissä järjestelmissä tietoturvaongelma voisi myös aiheuttaa tai pahentaa laajoja sähkön syötön keskeytyksiä.
  - Tapaus osoitti selvästi varavoimajärjestelmien ja niiden toimintakunnon tärkeyden.
  - Laajasta sähkön syötön keskeytyksestä aiheutuu hyvin suuret taloudelliset menetykset yhteiskunnalle. Hyvin karkeana arviona on esitetty noin 50 000 000 000 USD. Koko Etelä-Ruotsin pimentäneen sähkön syötön keskeytyksen on arvioitu aiheuttaneen noin 250 000 000 € menetykset.
  - Koska käytetään hyvin laajoja ohjelmistoja, ei niitä ole mahdollista täydellisesti testata ja olisikin kiinnitettävä enemmän huomiota siihen, että järjestelmät rakennetaan havaitsemaan virhetoiminnat ja toipumaan niistä hallitusti.

Joe Weiss (KEMA) on maininnut (26.4.2004), että hänen tiedossaan on yli 40 onnistunutta ja vahinkoa aiheuttanutta hyökkäystä, jotka on vahvistettu tapahtuneeksi. Nämä koskevat sähkö-, vesi- ja jätevesi-infrastruktuurin automaatiojärjestelmiä. Eriasteisia tahallisia tai tahattomia automaatioverkkoon tunkeutumisyrityksiä on tietoliikennettä valvottaessa havaittu paljon enemmän eli jopa 100–150 päivässä. Sähköenergiajärjestelmien automaatiojärjes-

telmään toteutuneita tunkeutumisia oli hänen tiedossaan 17 kappaletta ja lisäksi kaksi toteutunutta palvelunestotapausta. Kolme tapauksista oli johtanut automaatiotoimintojen menetyksiin, jotka olivat kohdistuneet kytkinlaitteiden tai höyrykattilalaitoksen toimintaan.

Lisäksi hän mainitsi kirjallisuudessa usein mainitun jätteenpuhdistuslaitosta koskevan tapauksen, jossa entinen SCADA-toimittajan työntekijä oli hyvin yksinkertaisen omatekoisen radiolähettimen avulla onnistunut 46 eri kertaa tyhjentämään hyvin suuria määriä käsittelemätöntä jätevettä ympäristöön (puistoon, jokeen ja jopa hotellin pihalle) ennen kuin hän jäi kiinni ja tuomittiin vankeuteen. SCADA-järjestelmän tiedonsiirtoliikenneprotokolla oli sellainen, että se hylkäsi virheellisenä kentältä tulevan tilatiedon, jos se oli ristiriidassa valvomosta ohjatun tilan kanssa. Näin valvomo ei saanut tietoa siitä, että tunkeutuja oli avannut venttiilin, jolloin tiedonsiirtoprotokollan puutteet lisäsivät vahinkojen laajuutta ja hidastivat syyn löytämistä. Weissin mukaan vastaavanlaisia protokollapuutteita on havaittu joissakin muissakin SCADA-järjestelmissä ja myös sähköenergiajärjestelmien automaatiossa.

3.3 Välittömiä toimenpiteitä

Viite [2] ehdottaa seuraavia toimenpiteitä tehtäväksi välittömästi:

Riskien tunnistus ja hallinta:

- Määritetään selkeät vastuut ja oikeudet. Pidetään henkilöstö tietoisena tietoturvariskeistä ja kunkin omasta vastuusta niiden minimoimisessa.
- Dokumentoidaan automaatiojärjestelmien ja tietoverkkojen arkkitehtuuri ja tunnistetaan siitä kaikki ne järjestelmät, joiden on toimittava ajantasalla.
- Identifioidaan kaikki liitännät automaatiojärjestelmiin.
- Tehdään säännöllisin väliajoin tietoturvakatselmukset kaikille automaatiojärjestelmille sekä niihin liittyville järjestelmille ja tietoverkoille.
- Arvioidaan automaatiojärjestelmän fyysinen turvallisuus.
- Tiedostetaan riskit, mikä vaatii jatkuvaa riskien kartoitusta ja sitä, että yhtiön johto tietää ja hyväksyy jäljelle jäävän riskin .
- Luodaan organisaatioon selkeä tietoturvafilosofia.
- Laaditaan varajärjestelmien toteutussuunnitelma ja menettelytavat siitä miten toivutaan tietoturvakatastrofista. Varajärjestelmillä ja varmuuskopioilla on keskeinen rooli sekä katastrofin vahinkojen minimoimisessa että toipumisen nopeuttamisessa.

Teknisiä suojautumistoimenpiteitä:

- Poistetaan tarpeettomat liitännät, sovellukset ja palvelut automaatiojärjestelmästä. Kaikki muut paitsi välttämättömät Internet-yhteydet on poistettava. Kielletään laite- ja järjestelmävalmistajien omat takaovet.

- Tiukennetaan jäljellä olevien yhteyksien käyttöoikeuksien hallintaa ja käyttäjän tunnistusta.
- Asennetaan ja otetaan käyttöön järjestelmävalmistajien tarjoamat tarkoituksenmukaiset tietoturvaratkaisut. Valmistajakohtaisten protokollien käyttö ei sinällään paranna tietoturvaa.
- Tiukennetaan tilapäisten käyttöoikeuksien valvontaa ja hallintaa, vahvennetaan käyttäjän tunnistusta, estetään langattomia yhteyksiä ja suljetaan tilapäiset liitännät heti kun käyttöoikeus loppuu.
- Toteutetaan/asennetaan tunkeutumisen havaitsemisjärjestelmä.

Tähän listaan voisi lisätä vielä ainakin seuraavat toimenpiteet:
- Jatkuva kaiken kriittisen datan varmuuskopiointi.
- Estetään suorat ulkopuoliset yhteydet automaatiojärjestelmän tietokantaan ja käytetään kyseisiä yhteyksiä varten erillistä kopiota tietokannan tarvittavasta osasta.
- Jaetaan automaatiojärjestelmä tietoturvarajapinnoilla pienempiin osiin, jotta tietoturvavastuut ovat hallittavissa ja jotta mahdollisen saastumisen laajuus tai inhimillisen virheen mahdollinen vaikutusalue saadaan rajattua. Esimerkiksi laaja VPN-verkko voi olla merkittävä tietoturvariski varsinkin jos se ohittaa palomuurin.
- Suojataan kriittisimmät asiat useammalla tietoturvavyöhykkeellä. Tunkeutumista kriittisiin osajärjestelmiin voidaan tarvittaessa hankaloittaa lisää toteuttamalla eri tasoilla rajapinnat erilaisin käyttöjärjestelmin ja ohjelmistoin.

3.4 Menetelmiä

Keinoja energiajärjestelmien hajautettujen automaatiojärjestelmien tietoturvan mainittuja keinoja luetellaan seuraavassa:
- Ulkopuolisia ei lasketa suoraan käyttämään automaatiojärjestelmän tietokantoja, vaan tiedot kopioidaan ensin toiseen tietokantaan.
- Poistetaan jatkuvasti päällä olevista käyttöjärjestelmistä ne toiminnot ja ohjelmat, jotka eivät ole kyseisessä tehtävässä ja näin tunkeutumismahdollisuudet vähenevät. Kannattaa valita käyttöjärjestelmä, josta liiat ominaisuudet ovat riisuttavissa.
- Toteutetaan turvallisuuskriittisten osajärjestelmien yhteydet ulkomaailmaan siten, että ne kulkevat kahden käyttöjärjestelmää myöten erilaisen tietoturvarajapinnan (palomuurin) kautta.
- Suljetaan tietoliikenneportit heti käytön jälkeen. Huomaa, että OPC:n käyttämä DCOM jättää tietoliikenneportteja perässään auki.
- Estetään tavanomainen Internetin käyttö automaatiojärjestelmien tietoverkoista.
- Täytetään tietoliikenteessä tietoturvaa varten suunniteltuja protokollia [alkuperän varmistus, salaus, käyttöoikeuksien hallinta, tunnelointi, Web Services Security (WSS)].

- Ei hyväksytä turvattomaksi tunnettuja tietoliikenneprotokollia, kuten langattomassa lähiverkossa pelkkää 802.11b-protokollaa.
- Käytetään palomuureja havaitsemaan ja estämään epäilyttävä liikenne.
- Luodaan TCP/IP-paketit uudestaan proxy-palvelimilla ennen niiden lähettämistä eteenpäin.
- Jaetaan verkko tietoturvan suhteen osiin, jotta tietoturvavastuut ovat hallittavissa ja jotta käyttöoikeudet ja tunkeutumiset saadaan rajattua mahdollisimman pienelle alueelle.
- Tarkkaillaan tietoverkkoliikennettä.
- Tarkastetaan, että kannettavissa tietokoneissa ei ole viruksia aina ennen niiden kytkemistä automaatiojärjestelmän tietoverkkoon. Kielletään kannettavan tietokoneen yhteydet ulkopuolisiin verkkoihin silloin, kun kannettava tietokone on kytkettynä automaatioverkkoon.
- Toteutetaan ratkaisuja, joilla palvelunestohyökkäyksiä harhautetaan ja niiden onnistumismahdollisuuksia huononnetaan.
- Käytetään omia tietoliikenneverkkoja silloin, kun toiminnon kriittisyys sitä edellyttää ja kun sen kustannukset kestetään.
- Käytetään sovelluksen malleja, tietomalleja ja redundanssia siten, että datojen muuttuminen ja virhetoiminnot voidaan heti havaita.
- Toteutetaan automaatiojärjestelmän arkkitehtuuri siten, että järjestelmä kykenee mahdollisimman hyvin toimimaan myös silloin, kun tietoliikenneyhteys tai joku muu järjestelmän osa ei toimi. Tässä auttavat tietojen käsittelyn ja varastoinnin hajauttaminen sekä paikalliset järjestelmien väliset liitännät.
- Käytetään itsenäisiä paikallisia yksinkertaisia varajärjestelmiä, jotka ottavat komennon ja ylläpitävät kriittiset perustoiminnot silloin, kun muu järjestelmä ei toimi oikein.
- Määritetään kaikkien osapuolten vastuut ja käyttöoikeudet selkeästi.
- Määritetään selkeästi, kuka vastaa tietoturvasta järjestelmän missäkin osassa.
- Koulutetaan kaikki osapuolet.

Suunnittelussa tulee varautua siihen, että tunkeutumista ei aina kyetä estämään. Internetin ja langattomien yhteyksien, kuten WLAN, käyttö lisää automaatiojärjestelmään tunkeutumisen mahdollisuuksia. Kustannussyistä näiden tekniikoiden käyttöä ei usein voida kuitenkaan välttää hajautetussa automaatiossa. Tunkeutumista voidaan huomattavasti vaikeuttaa tarkoitukseen sopivin tekniikoin. Järjestelmistä olisi tehtävä sellaisia, että ne itse tunnistavat virheelliset toiminnot ja rajoittavat mahdollisten vahinkojen laajuuden siedettäväksi.

On tärkeää, että yritys määrittää tietoturvan osalta tavoitetilan. Tämä on kaiken lähtökohtana tietoturvaan liittyvässä toiminnassa. Käytännössä se tarkoittaa, että laaditaan tietoturvahallinnolle dokumentti tietoturvahallin-

nosta, jossa määritetään vastuut, tavoitteet, kehittäminen, seuranta ja sen avulla otetaan kantaa riskeihin ja niiden hallintaan. Tämän jälkeen laaditaan sopimukset ja ohjeet siitä miten toimitaan. Nämä dokumentit koskevat niin omaa henkilöstöä kuin toimittajiakin. Tähän kuuluvat monet muutkin tietoturvaan liittyvät asiat, esimerkiksi kulunvalvonta, millaisella laitteella kytkeydytään ylläpidettävään ympäristöön, mitä koneessa on otettava huomioon (esimerkiksi virustorjunta), tietoturvan tarkistamiseen ja testaukseen liittyvät kohdat. Pelkät tekniset ratkaisut eivät riitä, vaan tärkeimpänä tekijänä on otettava huomioon ihmisen toiminta tietoturvan toteuttamisessa.

4. Tietoturva hajautetun energiantuotannon näkökulmasta

Hajautetuilla energiaresursseilla tarkoitetaan sekä hajautettua energian (sähkön ja lämmön) tuotantoa että ohjattavaa energian kulutusta ja varastointia. Hajautetulla energian tuotannolla tarkoitetaan sähkön ja lämmön tuotantoa, joka on liitetty sähkön jakeluverkkoon sekä mahdollisesti kaasun ja lämmön jakeluverkkoihin.

Hajautettujen energiaresurssien hallinta ja automaatio on tietoturvan kannalta sähkönjakeluautomaatiotakin haasteellisempaa seuraavien seikkojen osalta:

- Kannattavuus on herkkää järjestelmäkustannuksille.
- Langatonta tiedonsiirtoa käytetään paljon.
- Avoimien kaupallisten tietoverkkojen käyttö on usein välttämätöntä kustannusten säästämiseksi.
- Samoja järjestelmäinvestointeja hyödynnetään moniin eri etäpalveluihin kustannussyistä.
- Tarvitaan eri automaatiojärjestelmien välisiä yhteyksiä suoraan kenttätasolla, sillä tiedonsiirto keskitetyn järjestelmän kautta on liian hidasta, epäluotettavaa ja kallista.
- Vasteaikavaatimukset ja käytettävyysvaatimukset on täytettävä.
- Monia eri osapuolia käyttää ja ylläpitää samaa järjestelmää (eri järjestelmätoimittajat, eri valvomo-operaattorit, huolto- ja korjaushenkilöt, etäpalvelujen tarjoajat, konsultit, tutkijat jne.). Hajautettujen energianresurssien hallintajärjestelmän on perustuttava monia eri osapuolia palvelevaan automaatioinfrastruktuuriin ollakseen kannattavaa.
- Järjestelmän hajautetun osan elinikä on pitkä, koska asennus- ja ylläpitokäynnit hajallaan oleviin kohteisiin ovat hyvin kalliita.
- Hajautetun osan tulee olla verraten halpa.
- Pääsyä automaatiojärjestelmän hajautettujen laitteiden luo ei useinkaan voida estää.
- Etäkäyttö, -valvonta ja -ylläpito ovat välttämättömiä kustannusten pitämiseksi kohtuullisina. Näihin tarkoituksiin käytetään usein yleisiä tieto-

verkkoja, kuten Internetiä ja matkapuhelinverkkoa. Käyttöliittymät toteutetaan usein siten, että ne perustuvat verkkoselaimiin.
- Automaattisia ohjelmistopäivityksiä ei voida sallia, koska niitä ei ole testattu kyseisessä ympäristössä ja ne muodostavat muun muassa siksi huomattavan turvallisuusriskin.
- Pahimmissa tapauksissa ihmishenkiä voi vaarantua ja huomattava määrä omaisuutta voi vahingoittua.
- Selväkielisten sanomien käyttö on yleistä.
- Tietoturvaratkaisut eivät saisi liikaa huonontaa järjestelmän käytettävyyttä.
- Runsas hajautettu energiantuotanto edellyttää sähkönjakeluverkon ääripäiden automaation parantamista. Siinä on ratkaistava samoja haasteita.

Hajautettujen energiaresurssien tietoliikenteen protokollastandardit [5] tulevat näillä näkymin pohjautumaan jakeluautomaation IEC 61850 -standardeihin. Hajautettujen energiaresurssien etäautomaation tietoliikenteessä tulee Web Services Security (WSS) -mekanismeilla olemaan luultavasti keskeinen merkitys tietoturvan toteuttamisessa (ks. esimerkiksi [5]). Syynä tähän on se, että kustannussyistä johtuen etähallinnan tietoa joudutaan siirtämään muiden osapuolien järjestelmien ja tietoliikenneverkkojen kautta.

5. Yhteenveto

Energian jakelussa joudutaan kiinnittämään entistä enemmän huomiota tietoturvaan muun muassa seuraavista syistä:
- Yhteyksiä eri järjestelmien ja toimijoiden välillä tarvitaan entistä enemmän
- Vaaditaan entistä parempaa sähkön syötön luotettavuutta ja jännitteen laatua
- Automaation parantaminen on usein kustannustehokas vaihtoehto ylimitoitukselle
- Hajautetun sähkön tuotannon määrää suunnitellaan lisättäväksi
- Etähallintaa ja automaatiota joudutaan ulottamaan entistä pienempiin kohteisiin
- Kustannusten suhteen herkissä kohteissa joudutaan käyttämään yleisiä tietoliikenneverkkoja ja langattomia tietoliikenneyhteyksiä sekä yhdistämään monia sovelluksia samaan järjestelmään
- Käytössä on eri-ikäisiä ja ominaisuuksiltaan hyvin erilaisia tietoliikenneprotokollia ja kenttälaitteita.

Tietoturvaratkaisut joudutaan usein valitsemaan tapauskohtaisesti kuhunkin tilanteeseen sopiviksi varsin laajasta menetelmäjoukosta. Selkeiden ja tarkoituksenmukaisten vastuiden määrittelyn ja rajauksen merkitys korostuu.

6. Kirjallisuusviitteet

[1] CIGRE Working Group D2-B3-C2.01. ”Managing Information Security in an Electric Utility”, Electra, October 2004.
[2] CIGRE Working Group D2-B3-C2.01. ”Cyber Security Considerations in Power System Operations”, Electra February 2005. pp. 15 – 23.
[3] Ericsson, G.N.; Torkilseng, A.; Management of Information Security for an Electric Power Utility – On Security Domains and Use of ISO/IEC17799 Standard, IEEE Transactions on Power Delivery. Volume 20, Issue 2, April 2005 Page(s):683 – 690.
[4] IEC 62351-1 CD, Data and Communications Security – Introduction and Overview, IEC, April 2005, 23 p.
[5] IEEE P1547.3 Draft 0.1, Draft guide for Monitoring, Information Exchange and Control of Distributed Resources Interconnected with Electric Power Systems, July 28 2004, 102 p. (Luonnos IEEE P.1547.3 ei ole julkinen, mutta sen tietoturvaa koskevan luvun luonnos on IEEE P1547.3 -standardia laativan työryhmän julkisen kokousmuistion liitteenä).
[6] Zhaoxia Xie; Manimaran, G.; Vittal, V.; Phadke, A.G.; Centeno, V.;An information architecture for future power systems and its reliability analysis, IEEE Transactions on Power Systems. Volume 17, Issue 3, Aug. 2002 Page(s):857 – 863.

7. Kirjallisuutta

Abshier J., Weiss J., ”Securing Control Systems: What you need to know”. Control, February 2004, pp. 43 – 48. (www.controlmag.com)
Pollet J., ”Developing a solid SCADA security strategy”, Sensors for Industry Conference, Houston Texas, USA, 19 – 21 November 2002, pages 148 – 156.

LIITE 5

Automaatiojärjestelmän antiviruskuvaustiedostojen ja Microsoft tietoturvapäivitysten hallinta

Esa Tuovinen, Honeywell Oy

1. Johdanto

Nykyaikaiset automaatiojärjestelmät perustuvat yhä enemmän niin sanottuihin kaupallisiin ratkaisuihin pohjautuviin Microsoft Windows ja Linux-käyttöjärjestelmiin. Kummassakin käyttöjärjestelmässä on tietoturvahaavoittuvuuksia ja järjestelmät voivat saastua tietokoneviruksen takia. Järjestelmien operointiin ja ohjaukseen liittyvät ohjelmistot käyttävät tunnettuja käyttöjärjestelmän palveluja kuten tietokantapalvelut (SQL-Server, Structured Query Language Server), kirjautumispalvelut (Windows Logon, LSASS), tiedoston käsittelypalvelut jne. Laitteet kommunikoivat toistensa välillä tunnetuilla tietoliikenneprotokollilla kuten http-, ftp-, RPC- (Remote Procedure Calling Protocol), OPC-, DCOM- ja NetBIOS-protokollilla. Myös alemmalla tasolla olevat laitteet käyttävät järjestelmän valmistajien TCP/IP- tai UDP-tason (User Datagram Protocol) protokollatoteutuksia. Usein alemman laitetason protokollat perustuvat johonkin tunnettuun Free BSD tai Open BSD IPV4 -version mukaiseen protokollapinoon. Niinpä näissä vapaasti ”portatuissa” kuin kaupallisissakin pinototeutuksissa on samantyyppiset virheet, joissa tunkeutuja tai viruksen tekijä voi käyttää hyväksi protokollapinon tai sanoman kehysrakenteen haavoittuvuuksia.

Haavoittuvuudesta ja tietoturvaan liittyvistä ohjelmistovirheistä on saatavana tietoja useilta verkkosivuilta [5-1] sekä valmistajien omilta sivuilta. Kun esimerkiksi käyttöjärjestelmän valmistaja Microsoft ilmoittaa omien tuotteidensa haavoittuvuuksista ja niiden korjauksista kerran kuukaudessa omalla ”security bulletin” sivuillaan, tulee haavoittuvuus laajempaan tietoisuuteen. Viruksen tekijä käyttää tunnettuja tietoliikenteeseen ja käyttöjärjestelmiin liittyviä haavoittuvuuksia hyväksi virusten levityksessä kuten esimerkiksi Blaster- ja Sasser-virusten tapauksissa.

Automaatiojärjestelmän toimittaja seuraa jatkuvasti tietoturvaan liittyvää kehitystä ja saa tietoa mahdollisista haavoittuvuuksista käyttöjärjestelmien valmistajilta ja laitteistotoimittajilta. Automaatiotoimittaja testaa haavoittu-

vuuksiin liittyviä tietoturvapäivityksiä ja korjaustiedostoja (Hotfix) omissa tuotteissaan ja välittää ennakkotiedon omaan tuotteeseen mahdollisesti liittyvistä haavoittuvuuksista ja niiden vaikutuksista asiakkailleen joko julkisten verkkosivujen kautta tai erikseen kohdennettuna jakeluna.

Regressiotestauksessa korjauspäivitysten vaikutukset testataan yleensä tietyissä automaatiojärjestelmän tuoteversioissa (pääversiot). Testauksessa selvitetään mahdolliset vaikutukset järjestelmän toimintaan. Tämän jälkeen toimittaja välittää tiedon asiakkailleen, jonka jälkeen päivitykset ovat asennettavissa automaatiojärjestelmään. Päivitysten jakaminen laajoissa järjestelmissä on hankalaa ja vaatii monesti tehtaan toiminnan kannalta sopivan hetken tai seisokin, koska usein käyttöjärjestelmän valmistajan toimittama korjauspäivitys vaatii automaatiojärjestelmän työaseman tai palvelimen uudelleen käynnistyksen. Päivitysten hallintaan ja antiviruskuvaustiedostojen päivittämiseen voidaan käyttää keskitettyä hallintapalvelinta.

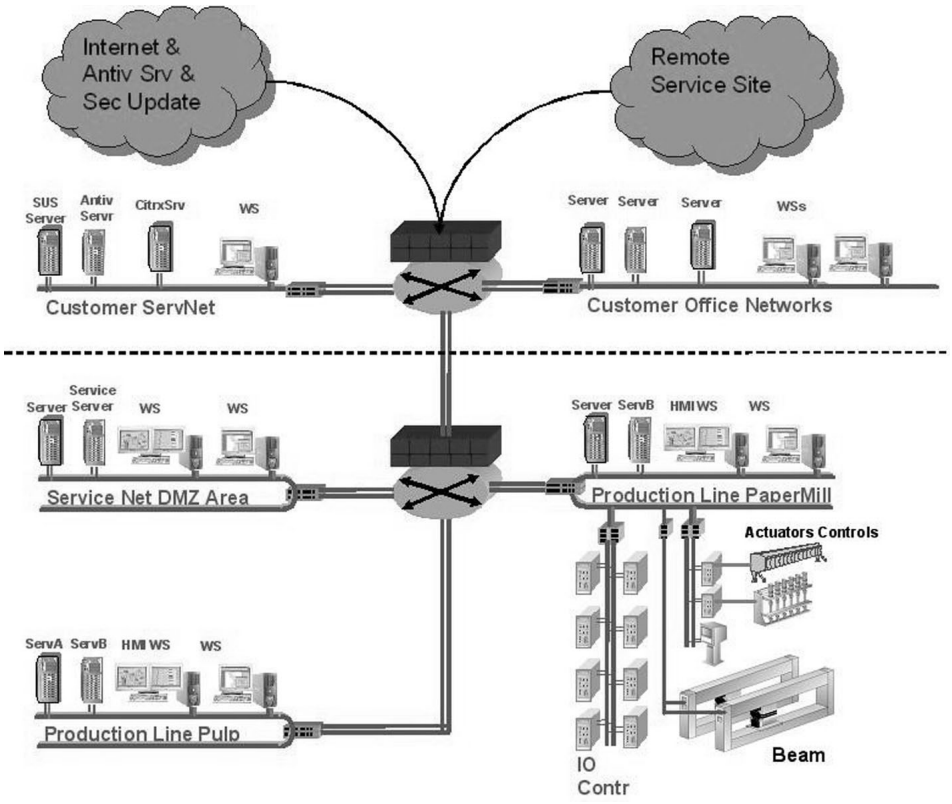
2. Tietoturva- ja antiviruspäivitysten hallintapalvelimen toiminta

Tietoturvapäivitysten ja antiviruskuvaustiedostojen päivitysten hallintaan on useita valmistajakohtaisia toteutustapoja. Microsoft suosittaa käyttämään päivitysten jakeluissa joko Software Management Server (SMS) ja Security Update Server (SUS) -hallintapalvelimia [5-2].

Ensiksi mainittua on kuitenkin automaatiojärjestelmän kannalta melko hankalaa ylläpitää ja se vaatii runsaasti erikoisosaamista, joten jälkimmäinen vaihtoehto on varteenotettavampi ohjelmistopäivitysten hallintaan. Uudempi versio Windows Server Update Services (WSUS) soveltuu useamman automaatiojärjestelmän tai osakokonaisuuden päivitysten hallintaan.

Antivirusohjelmistojen valmistajia on useita ja niillä on kullakin omat toteutustavat kuvaustiedostojen ja niin sanotun antivirusmoottorin (Engine) päivittämiseen. Suomalainen F-Secure käyttää Policy Manager -ohjelmistoa omien tuotteidensa jakelussa. McAfee suosittelee käyttämään ePolicy Orchestration -ratkaisua tai vähemmän resursseja vaativaa Autoupdate Architect -toteutusta. Norton/Symantec suosittelee puolestaan LiveUpdate-ratkaisua.

Usein edellä mainitut ratkaisut eivät kuitenkaan sovellu sellaisenaan automaatiojärjestelmän antiviruspäivitysten hallitsemiseen, koska valmistajan tarjoama uudempi ohjelmistoversio tai antivirusmoottori ei välttämättä sovellu ohjausjärjestelmään. Uudessa ohjelmistoversiossa voi olla toimintoja, jotka voivat estää jonkin protokollan tai tiedonsiirtoportin tai ohjauksen kannalta tärkeän toiminnon. Itse kuvaustiedostojen päivityksessä ei normaalisti ole estettä automaattiselle päivittämiselle. Automaatiojärjestelmän valmistaja testaa ja suosittelee asiakkaalle sopivimmat vaihtoehdot.



Kuva 5-1. Eräs ratkaisu päivitysten hallinnalle.

Kuvassa 5-1 nähdään eräs toteutustapa päivitysten hallitsemiseksi useamman automaatiojärjestelmän tai osaston ylläpitämiseksi. Automaatiojärjestelmät eristetään asiakkaan toimistojärjestelmistä palomuuri- ja reititinratkaisuilla. Palveluvyöhykkeeseen (DMZ) sijoitetulla palvelimella voidaan hallita tietoturvapäivitykset ja virustietokantojen päivitykset.

Ensimmäisessä vaiheessa konsernitasolla oleva palvelin käy hakemassa uusimmat korjaus- ja kuvaustiedostot Master SUS -palvelimelle käyttöjärjestelmän valmistajan hallinnassa olevilta verkkosivuilta tai antivirusohjelmiston valmistajan sivuilta. Tässä vaiheessa tarvitaan Internet- yhteyttä. Konsernitasolla voidaan päättää päivitysten jakeluajankohdasta ja merkitä päivitykset hyväksyttyyn tilaan, jolloin päivitysten jakelu saadaan tehtyä toimistotasolla sopivana ajankohtana.

Automaatiojärjestelmätason palveluvyöhykkeessä oleva palvelin käy hakemassa päivitykset omalle SUS -palvelimelle, jossa voidaan paikallisesti vielä joko sallia tai kieltää päivitys. Yleensä kun automaatiojärjestelmän toimittajalta on saatu lupa korjaustiedostojen levitykseen, voidaan päivitys merkitä ”hyväksytty” -tilaan. Tällä tasolla voidaan helposti määrittää vain Master SUS -palvelimen ja SUS -palvelimen välille sallittu tapa kommunikoida käyttäen

joko palomuuria tai pääsylistoja. Työasemat ja palvelimet käyvät hakemassa päivitykset sopivaksi katsottuna ajankohtana. Jos päivitys edellyttää työaseman tai palvelimen uudelleen käynnistystä, se tehdään ohjaavan prosessin tilanteen mukaan. Työasemilla ja palvelimilla on otettava käyttöön Windows Update -palvelu, joka on konfiguroitava järjestelmään sopivaksi. SUS-palvelimen hallinta voidaan antaa myös hallitun ja valvotun VPN-etäyhteyden tehtäväksi automaatiojärjestelmän toimittajan ja asiakkaan välisellä sopimuksella.

Päivityksistä jää kirjanpito ja niistä on saatavana raportit, joita automaatiojärjestelmän ylläpitohenkilöstö voi käyttää apuna määräaikaishuoltokäynneillä. Lisäksi järjestelmän ylläpidon helpottamiseen on saatavilla aputyökaluja kuten Microsoft Baseline Security Analyzer Tools. Koska automatisoitujen tietoturvapäivitysten hallinta onnistuu Windows-2000- tai sitä uudemmissa käyttöjärjestelmissä, voidaan erillisenä työkaluna käyttää NT4-ympäristön päivityksiin soveltuvaa päivitysohjelmistoa.

Antivirusohjelmistojen päivittämiseen voidaan käyttää samaa SUS-palvelinta, jolla tehdään tietoturvapäivitysten jakelu ja hallinta. Konsernitasolla voi olla käytössä oma ylläpitopalvelin antiviruspäivitysten jakeluun, josta automaatiojärjestelmätasolla oleva palvelin käy tarkastamassa ja tarvittaessa hakemassa päivitykset säännöllisin välein ja jakelee ne edelleen järjestelmään.

Viitteet

[5-1] Secunia on tietoturvaan kohdistuvien haavoittuvuuksien tilastointia ylläpitävä organisaatio, jonka pääpaikka on Tanskassa. Organisaatiolta on saatavana yksityiskohtaista tilastoa eri käyttöjärjestelmien tietoturvauhkista jaettuna eri vakavuusasteisiin. Sama organisaatio ylläpitää tilastoa myös eri Antivirusohjelmistotoimittajille raportoiduista viruksista ja niiden ilmentymistä.
www.secunia.com
www.cert.org

[5-2] Windows Server Update Services. Microsoft pitää yllä keskitettyä käyttöjärjestelmiin kohdistuvaa ”Security bulletin” tietokantaa ja kuinka Microsoft-järjestelmien päivitysten ylläpitäminen voidaan toteuttaa heidän työkaluohjelmistoilla.
http://www.microsoft.com/windowsserversystem/updateservices/default.mspx

LIITE 6

Ydinvoimalaitosautomaatio

Harri Heimbürger, Säteilyturvakeskus STUK

Slammer-Mato tunkeutui ydinvoimalaitokseen

Mitä käytännössä tapahtui: Ydinvoimalaitoksessa (Davis-Besse, Ohio, USA, 2003) MS-SQL Server -mato esti ohjaajien tukijärjestelmän (SPDS, Safety Parameter Display System) toiminnan noin neljäksi tunniksi ja prosessitietokoneen (PTK) toiminnan noin seitsemäksi tunniksi aiheuttaen tietoverkkojen ja myös ohjaajien ylikuormittumisen.

Tapahtuman syy: Tammikuussa 2003 Slammer-mato poisti käytöstä kaksi tärkeää (SPDS ja PTK) valvontajärjestelmää. Mato levisi järjestelmään yhteistyökumppanin tietoverkosta ensin Davis-Bessen kaupalliseen tietoverkkoon. Tämän jälkeen mato tunkeutui luvatonta tietoliikenneyhteyttä pitkin kriittiseen tietoverkkoon. Yhteys ohitti laitoksen palomuurin, joka oli kaupallisen tietoverkon ja kriittisen tietoverkon välissä.

Opetuksia:
- Epävirallliset ja tilapäiset tietoyhteydet vaarallisia.
- Järjestelmien yhdistämisestä aiheutuvat riskit on tiedostettava.
- Yhteistyökumppanien tietoturvan taso on aina tarkastettava.
- Tietoverkkojen jakaminen lohkoihin tai vyöhykkeisiin on suositeltavaa.
- Järjestelmien eriyttäminen ja varajärjestelmät lisäävät turvallisuutta.
- Toipumissuunnitelman (Recovery Plan) teko ja toipumisen harjoittelu on tärkeää kaiken varalta.

Ydinvoimalaitosten (YVL) automaatio- ja tietokonejärjestelmiä koskevia tietoturvavaatimuksia ja -suosituksia esitetään IAEA:n automaatioalan suunnitteluohjeistuksessa. IAEA:n (ks. luku 9) turvallisuusjulkaisusarjoja on useita, mutta keskeiset YVL-automaatiota koskevat tietoturvan suunnitteluvaatimukset on esitetty ”IAEA Safety Standards” -sarjan Safety Guide-julkaisuissa [6-1] ja [6-2] ja myös Tecdoc-sarjan julkaisuissa, esimerkiksi ”IAEA – Tecdoc - 1252” [6-3]. Tecdoc-sarjan julkaisuilla luodaan teknistä pohjaa tuleville ohjeille ja käytännöille. Viitteissä [6-1] ja [6-2] on esitetty yksityiskohtaisempia vaatimuksia ohjelmoitavan automaation ja tietojärjestelmien tietoturvalle. Työn alla oleva Tecdoc [6-4] tuo esille muun muassa käsitteen ”Design Basis Threat (DBT)”, jota on käsiteltävä tietoturvasuunnitelmassa. Suunnitelmassa on kiinnitettävä huomiota myös mahdollisen hyökkäyksen eri vaiheisiin kuten esimerkiksi sen estämiseen, havaitsemiseen, viivästämiseen, lieventä-

miseen ja siitä toipumiseen. DBT-riskianalyysissä on myös käsiteltävä sisäpiirin ja ulkoisten toimijoiden mahdollista toimintaa yhdessä ja erikseen.

Suomessa Säteilyturvakeskus STUK antaa ydinenergian käytön turvallisuutta, turva- ja valmiusjärjestelyjä koskevat yksityiskohtaiset määräykset YVL-ohjeissa ydinenergialain (990/1987) ja valtioneuvoston päätösten (395, 396 ja 397/1991) nojalla.

YVL-ohjeen julkaiseminen ei sinänsä muuta STUKin ennen ohjeen julkaisemista tekemiä päätöksiä. Vasta kuultuaan asianosaisia STUK antaa erillisen päätöksen siitä, miten uutta tai uusittua YVL-ohjetta sovelletaan käytössä tai rakenteilla oleviin ydinlaitoksiin ja luvanhaltijoiden toimintoihin. Uusiin ydinlaitoksiin uusittuja ohjeita sovelletaan sellaisenaan.

Kun STUK harkitsee YVL-ohjeissa esitettyjen, uusien turvallisuusvaatimuksien soveltamista käytössä tai rakenteilla oleviin ydinlaitoksiin, se ottaa huomioon valtioneuvoston päätöksen (395/1991) 27 §:ssä säädetyn periaatteen. Sen mukaan turvallisuuden edelleen parantamiseksi on toteutettava sellaiset toimenpiteet, joita käyttökokemukset ja turvallisuustutkimukset sekä tieteen ja tekniikan kehitys huomioon ottaen voidaan pitää perusteltuina. Jos halutaan poiketa YVL-ohjeessa esitetyistä vaatimuksista, on STUKille esitettävä muu hyväksyttävä menettelytapa tai ratkaisu, jolla saavutetaan YVL-ohjeessa esitetty turvallisuustaso.

Ydinvoimalaitosautiomaatiota koskevia tietoturvavaatimuksia esitetään STUKin ohjeessa YVL 5.5, ”Ydinlaitosten automaatiojärjestelmät ja -laitteet” [6-5]. Em. ohjeen luvussa 3.4 esitetään seuraava tietoturvaa koskeva keskeinen perusvaatimus:

> *”Automaatiojärjestelmän suunnittelussa, käytössä ja ylläpidossa tulee huolehtia tietoturvallisuustekijöiden huomioon ottamisesta. Luvaton pääsy laitoksen häiriöttömän toiminnan kannalta tärkeisiin laitteisiin, ohjelmistoihin tai tietojärjestelmiin tulee estää. Luvaton pääsy turvallisuudelle tärkeiden järjestelmien laitteisiin tulee estää käyttäen fyysisiä, teknisiä ja hallinnollisia turvajärjestelyjä. Asiattomien ohjelmanosien asentaminen tulee estää luotettavasti suunnittelun, valmistuksen, käyttöönoton, määräaikaiskokeiden ja ylläpidon aikana. Luvalliset käynnit järjestelmään ja niiden aikana tehdyt muutokset tulee voida jäljittää.”*

Ohjeen YVL 5.5 STUKin valvontaa käsittelevässä luvussa 6.3 esitetään vaatimuksia koskien viranomaiselle toimitettavaa ennakkotarkastusaineistoa ohjeen YVL 2.1 [6-6] mukaisesti:

> *”…turvallisuusluokkien 2 ja 3 automaatiojärjestelmän ennakkotarkastusaineiston sekä soveltuvin osin turvallisuusluokan 4 automaatiojärjestelmän ennakkotarkastusaineiston tulee pääsääntöisesti vastata lopullista turvallisuusselosteen sisältöä ja sen tulee mm. tietoturvallisuussuunnitelma. ”Tietoturvallisuussuunnitelmaan liittyvät toiminta- ja menettelyohjeet toimitetaan tiedoksi STUKiin”.*

Eurooppalaisten voimayhtiöiden ns. EUR-vaatimuksissa esitetään muun muassa seuraavia automaation tietoturvaa koskevia vaatimuksia [6-7]:

- Tietoturvamielessä virheellisten tulosignaalien pääsy ohjelmoitavaan YVL-automaatiojärjestelmään ja -laitteeseen on estettävä.
- Asiaton pääsy ohjelmoitaviin YVL-automaatiojärjestelmiin ja -laitteisiin on estettävä.
- Tietoturvanäkökohdat on suunniteltava ja toteutettava riittävässä määrin ohjelmoitavien automaatiojärjestelmien ja -laitteiden käyttö- ja kunnossapitotehtävissä informaatioergonomian periaatteita ja vaatimuksia unohtamatta.
- Ohjelmoitavan automaation suunnittelussa käytössä olevassa laatusuunnitelmassa on käsiteltävä seuraavia tietoturvaan vaikuttavia näkökohtia
  - tietoturvan merkityksen ymmärryksen varmistaminen ja vastuut
  - turvallisuuden (turvaluokitus) vastuurajojen sopimusperusteinen tunnistus
  - tietoturvan hallinnointi
  - ohjelmoitavien automaatiojärjestelmien ja -laitteiden kanssa työskentelevien oikeuksien ja velvollisuuksien määrittely
  - ohjelmoitavien automaatiojärjestelmien ja -laitteiden fyysisen pääsyn valvonta
  - ohjelmistoihin pääsyn ja käyttöoikeuksien valvonta
  - erilaisten ohjelmointilaitteiden ja työasemien käytön ja käyttöoikeuksien valvonta
  - tehtyjen toimenpiteiden jäljitettävyys
  - tiedostojen tietoturvallinen siirto verkkojen yli
  - ajantasaisen dokumentaation hallinta
  - varmuuskopioinnin hallinta
  - automaation itsensä tekemien toimenpiteiden ja toimintojen valvonta.

Esimerkkinä Yhdysvaltain ydinturvallisuusviranomaisen (U.S. Nuclear Regulatory Commission, U.S.NRC) toiminnasta tietoturvasäännöstön kehittämiseksi on ohjeluonnos [6-8], jossa käsitellään muun muassa

- luonnoksessa on vaatimuksia hallinnollisiksi menettelytavoiksi tietoturvan varmistamiseksi automaatiojärjestelmän erityisesti suojausautomaation elinkaaren aikana.
- vaatimuksia automaation suunnitteluprosessille.
- viittauksia standardiin IEEE 7-4.3.2-2003 [6-9] ja sen informatiivisiin liitteisiin koskien tietoturvavaatimuksia.

Yhteenvetona voidaan todeta, että myös ydinvoimalaitosautomaation alalla kansainvälinen tutkimus- ja säännöstön kehitysyhteistyö muun muassa IAEAn ja IEC:n työryhmissä on käynnissä tietoturvavaatimusten täsmentämiseksi.

Ydinvoimalaitosautomaation turvallisuusvaatimuksia ja suunnittelusuosituksia on esitetty myös seuraavissa IEC:n standardeissa:

– IEC 61513 [6-10] (järjestelmätason kattostandardi)
– IEC 60880 [6-11] ja sen täydennysosa [6-12] (ohjelmistostandardi, kategoria A)
– IEC 60987 [6-13] (laitteistostandardi)
– IEC 62138 [6-14] (ohjelmistostandardi, kategoria B ja C).

Viitteitä

[6-1] IAEA Safety Standards Series ”Software for Computer Based Systems Important to Safety in Nuclear Power Plants”, Safety Guide No. NS-G-1.1, September 2000.

[6-2] IAEA Safety Standards Series ”Instrumentation and Control Systems Important to Safety in Nuclear Power Plants”, Safety Guide No. NS-G-1.3, March 2002.

[6-3] IAEA – TECDOC – 1252 ”Information integration in control rooms and technical offices in nuclear power plants”, 2001.

[6-4] IAEA – TECDOC – xxxx ”Guidance on the Security of Computer Systems at Nuclear Facilities”, (unpublished draft 2004).

[6-5] Ohje YVL 5.5 ”Ydinlaitosten automaatiojärjestelmät ja -laitteet”, 2002.

[6-6] Ohje YVL 2.1 ”Ydinvoimalaitosten järjestelmien, rakenteiden ja laitteiden turvallisuusluokitus”, 2000.

[6-7] EUR-dokumentti. http://www.europeanutilityrequirements.org/

[6-8] U.S.NRC, Draft regulatory guide DG-1130: Criteria for use of computers in safety systems of nuclear power plants.

[6-9] IEEE Std 7-4.3.2-2003, ”Standard Criteria for Digital Computers in Safety Systems of Nuclear Generating Stations”.

[6-10] IEC 61513 ”Nuclear power plants-Instrumentation and control for systems important to safety – General requirements for systems”, 2001-03.

[6-11] IEC 60880 ”Software for computers in the safety systems of nuclear power stations”, First edition 1986.

[6-12] IEC 60880-2 ”Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failure, use of software tools and of pre-developed software”, First edition 2000-12.

[6-13] IEC 60987 ”Programmed digital computers important to safety for nuclear power stations”, First edition 1989-11.

[6-14] IEC 62138 ”Nuclear Power Plants Instrumentation and Control-Computers-based systems important for safety-Software aspects for I&C systems of class 2 and 3”, First edition 2004-01.

LIITE 7

Tietoturvan toteuttaminen pk-yrityksen kannalta

Antti Ala-Tala, Remion Oy

Pk-yrityksen on mahdollista tarjota omia verkkopalveluitaan pienilläkin resursseilla. Seuraavassa esitetään käytännön toiminta-malleja tietoturvanäkökulman huomioon ottamiseksi.

1. Tietoturva ja toimintamallit

Tietoturva-asioissa ei tekniikka ole etusijalla. Tietokoneita ja -verkkoja käyttävien työntekijöiden on oltava tehtävänsä tasalla ja sopivasti koulutettuja. Yhdeksän kymmenestä tietoturvaongelmasta on oman henkilökunnan aiheuttamia.

Pk-yrityksen tietoturvan tarkastuslista sisältää vähintään seuraavat asiat:

1. Käyttöjärjestelmän ja Internet-selaimen päivitykset kannattaa pitää ajan tasalla. Käyttöjärjestelmiin kuuluu nykyisin automaattisia päivitystyökaluja, jotka eivät vaadi käyttäjältä toimenpiteitä. Nimetty vastuuhenkilö kytkee asetukset päälle ja seuraa mahdollisesti tietoturvatiedotteita (CERT-FI-tietoturvatiedotteita ja -ohjeita: ks. kirjan viite [3]).
2. Windows XP sisältää palomuurin, joka kannattaa aktivoida. Palomuurin alkuasettelu saattaa tuntua hankalalta. Yksi henkilö selvittää sopivat asetukset ja monistaa ne sitten muille koneille.
3. MS Windows -konetta ei saa kytkeä suojaamattomaan verkkoon heti asennuksen jälkeen, vaan palomuurien yms. on oltava ensin päällä.
4. Sähköpostiohjelmista kannattaa viestien automaattinen esikatselu kytkeä pois päältä. Automaattinen esikatselu saattaa käynnistää sähköpostista tulevan haittaohjelman. Työntekijöitä kannattaa opastaa tuhoamaan epäilyttävät viestit jo otsikkotasolla avaamatta niitä.
5. Sähköpostipalveluun kannattaa tilata operaattorilta automaattinen roskapostin suodatus.

6. Jos työntekijöille sallitaan etäyhteyksiä kotikoneilta yrityksen verkkoon esimerkiksi VPN-tunnelin avulla, yrityksen kannattaa tarjota työntekijöille virussuojaohjelmisto ja velvoittaa käyttämään sitä. Kustannus on luokkaa 30 € vuodessa per työntekijä. VPN-yhteydessä käyttäjän kotikone on yrityksen sisäverkossa. Jos kotikoneella on haittaohjelmia, ne saattavat tulla yrityksen sisäverkkoon VPN-yhteyden avulla. Tällä tavalla on onnistuttu kaappaamaan muun muassa Microsoftin lähdekoodeja.
7. Yrityksen www-sivut ja sähköposti kannattaa sijoittaa palveluntarjoajan palvelimelle. Niihin kohdistuvat hyökkäykset eivät aiheuta ongelmia omaan verkkoon.

Jos yrityksessä ei ole sopivaa henkilöä suorittamaan edellä lueteltuja toimenpiteitä, voi palvelun tilata ulkopuolisesta tietotekniikkayrityksestä. Tosin kaikki alan yrityksetkään eivät ole asiaan perehtyneet.

Mikäli yrityksessä käytetään langatonta WLAN-verkkoa, se asettaa omat haasteensa tietoturvalle. Oleellisimmat toiminnot ovat laitteissa sisäänrakennettuna, mutta ne on myös otettava käyttöön.

2. Oman verkkopalvelun tarjoaminen

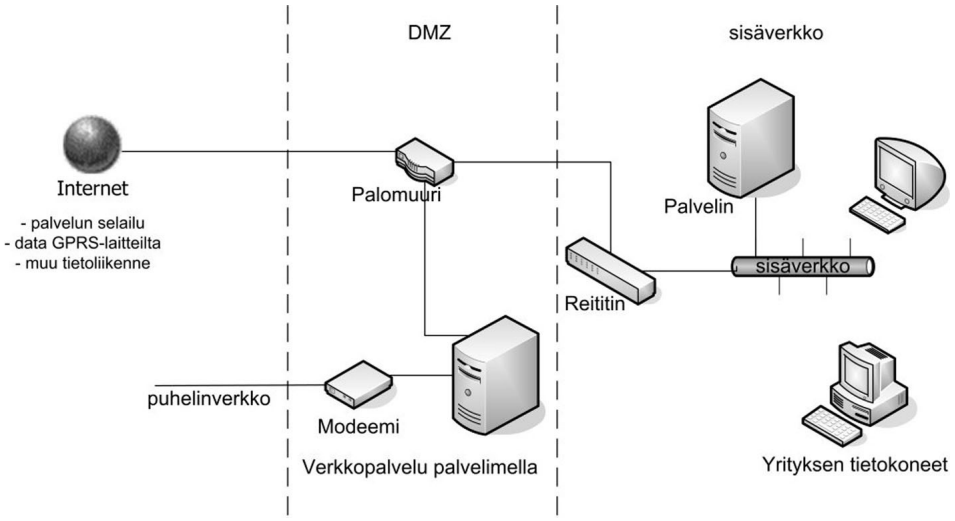
Yrityksen Internet-liittymä perustuu useimmiten ADSL-liittymään (Asymmetrical Digital Subscriber Line). ADSL-modeemin jälkeen seuraava verkkoelementti on palomuuri. Palomuuri on yleensä erillinen laite tai ADSL-modeemiin sisältyvä toiminto. Palomuurissa on hyvä olla TCP-porttien suodatus ja DoS-hyökkäyksien esto. Oletusarvoisesti kaikki TCP-portit ja ylimääräiset palvelut on suljettu. Erillisen peruspalomuurin hinta on 100–300 €.

Mikäli halutaan tarjota verkkopalveluita julkiseen Internet-verkkoon, kannattaa verkkoon muodostaa välivyöhyke (Demilitarized Zone, DMZ). DMZ saadaan aikaiseksi asettelemalla palomuuri tai reititin ohjaamaan verkkopalvelun liikenne ko. palvelua toteuttavalle tietokoneelle erillään yrityksen sisäverkosta.

Mikäli tarjottava palvelu on kohdennettu tietylle asiakaskunnalle eikä julkiseen selailuun, kannattaa noudattaa periaatetta, ettei palveluja näytetä suoraan ulkoa tuleville selailupyynnöille. Tämä saadaan aikaiseksi TCP-portin uudelleenreitityksellä ja käyttäjien autentikoinnilla. Palomuuri voi suodattaa liikennettä myös asiakaskunnan IP-osoitteiden perusteella.

3. Esimerkki nestevarastojen etävalvonnasta

Esimerkki tuotantokäytössä olevasta verkkopalvelusta, jossa sovelletaan edellä esitettyjä periaatteita (kuva 7-1).



Kuva 7-1. Nestevarastojen etävalvonta.

Kentällä oleva laitteisto sisältää kahden eri sukupolven mittalaitteita, joista toiseen soitetaan modeemilinjalla ja toinen lähettää tietoja automaattisesti GPRS-yhteyden avulla (General Packet Radio Service). GPRS-yhteyksiä käytettäessä on erikseen huolehdittava tiedon salauksesta. Tässä järjestelmässä käytetään verkkopankeistakin tuttua TLS-salausta (Transmission Layer Security).

Asiakkaat pääsevät selaamaan tietoja ottamalla yhteyden erikseen sovittuun TCP-porttiin, jonka palomuuri reitittää palvelimelle. Palvelimelle on kirjauduttava sisään käyttäjätunnuksella ja salasanalla. Verkkopalvelun toiminnasta on kerättävä monipuolisia lokitietoja mahdollisten ongelmien selvittämiseksi.

Kaikki verkkopalveluun ja sen hallintaan liittymättömät toiminnot on karsittava pois palvelinkoneelta.

LIITE 8

Ulkoisten uhkien torjuminen tietoturvapalveluilla

Markku Henttu, Metso Automation Oy

Tietokonevirusten ja -matojen määrän lisääntyminen uhkaa yritysten liiketoimintaa kaikkialla maailmassa. Ongelma ei koske ainoastaan toimistoja, vaan myös tuotantolaitokset ovat vaarassa. Energiayhtiö E.ON tiedosti asian ja investoi Suomenojalla sijaitsevan voimalaitoksensa tietoturvakartoitukseen ja tietoturvaa parantaviin toimenpiteisiin.

Suomenojan voimalaitos tuottaa sähköä (125 MW) ja kaukolämpöä (373 MW) Espoon kaupungille. Automaatio-osaston tiimipäällikkö Harri Ropposen mukaan laitoksen tehokkuus ja kannattavuus ovat parantuneet huomattavasti nykyisen etäoperointi mahdollisuuden myötä. ”Valitettavasti avoimuus toi kerran myös odottamattoman vieraan”, Ropponen lisää.

Helppo pääsy – myös tietokonemadoille?

E.ON:in tietoverkkoon tunkeutui tietokonemato, joka tunnetaan nimellä Blaster. Mato hidasti liikennettä metsoDNA-automaatiojärjestelmän valvomoväylässä, jonne se pääsi tunkeutumalla E.ON:in toimistoverkosta MS Windows -pohjaiseen operointiasemaan. E.ON:in onneksi automaatioasiantuntijat paikallistivat madon nopeasti ja poistivat sen välittömästi. Asiantuntijoiden nopea toiminta esti ongelmien synnyn käytönvalvonnassa.

Ropponen piti suurimpana uhkana madon aiheuttamia häiriöitä yksittäisten laitteiden käytössä. Hän ei ollut huolissaan valvomotason ongelmista, sillä hän luotti hyvin ylläpidetyn automaatioratkaisun suojaavan valvomon toimintaa.

Investointi tietoturvaan kannattaa

Välttääkseen vastaavan vaaratilanteen E.ON tilasi Metso Automation Oy:ltä perusteellisen tietoturvakartoituksen, joka sisälsi analyysin kaikista voimalaitoksen PC-työasemista, palvelimista sekä automaatioverkosta, sisältäen

reitittimet ja muut aktiiviset automaatioverkon komponentit. Selvitys oli Suomenojan laitoksella toteutetuista tietoturvaselvityksistä laajin. Ropponen on vakuuttunut, että tietoturvaan panostus maksaa itsensä takaisin estämällä eitoivottuja ja turhia häiriötekijöitä voimalaitoksen toiminnassa.

”On tärkeää toteuttaa tietoturvaselvitys automaatioasiantuntijoiden kanssa, sillä IT-asiantuntijat eivät välttämättä ymmärrä sitä, mitä reitittimien toisella puolella automaatiomaailmassa on,” kertoo Joni Vainio, E.ON:in systeemiasiantuntija. Vainio painottaa selvityksen vaatimaa automaatioteknologian syvällistä ymmärrystä.

Tietoturvakartoituksen tuloksena syntyi muun muassa ehdotus PC-työasemien ja käyttäjärajapinnan koventamisprosessista, joka auttoi poistamaan tarpeettomia ohjelmia ja vähentämään näin tietoverkon kuormitusta. ”Kaiken kaikkiaan E.ON oli tyytyväinen tietoturvaselvitykseen ja toteutti siinä esitetyt parannusehdotukset”, kertoo J-P Vihmo, Metso Automation Oy:n järjestelmäinsinööri ja alueensa tietoturvavastaava.

Palomuuri, virustorjunta ja PC-asemien koventaminen

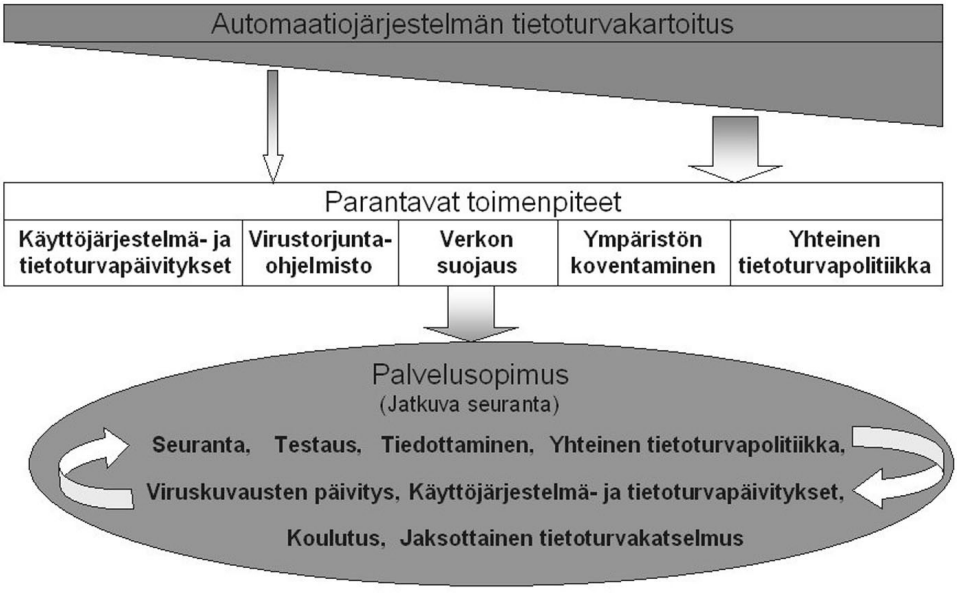
E.ON paransi automaatioverkkojensa turvallisuutta tiukentamalla automaatioverkkojen ja toimistoverkkojen välistä yhteyttä reititinpalomuuurien avulla. Palomuurit eivät yksinään ratkaise tietoturvan ongelmia, mutta yhdessä IP-rajoitusten ja porttikohtaisten konfiguraatioiden kanssa ne muodostavat yhden olennaisen osan tietoturvan kokonaisratkaisusta.

Metso Automation Oy:n tietoturvapalveluihin kuuluva virustorjuntaohjelmisto ja sen ylläpitopalvelu otettiin käyttöön. Palvelu sisältää virustorjuntaohjelmiston tietoturvallisen ylläpidon, johon kuuluu muun muassa jatkuva viruskuvaustiedostojen päivitysten testaus ennen käyttöönottoa sekä päivitysten jakelu tietoturvallisia etäyhteyksiä käyttäen.

Lisäksi automaatioverkon tietoturvaa parannettiin koventamalla metsoDNA:n PC-työasemat ja palvelimet, sekä toteuttamalla muut tietoturvakartoituksessa suositellut parannustoimenpiteet.

Tietoturvaa ylläpitävät ja parantavat toimenpiteet

Tietoturvaa parantavat toimenpiteet ovat toisiaan tukevia eikä yksi toimenpide sulje toista pois. Tilanteessa, jossa jotakin toimenpidettä ei voida toteuttaa, on hyvä olla muita sellaisia toimenpiteitä, jotka voidaan toteuttaa. Termi Layered Security (tai Defense-in-Depth) eli moneen eri kerrokseen toteutettu tietoturva kuvaa hyvin näitä toisiaan tukevia toimenpiteitä.



Kuva 8-1. Metso Automation Oy:n tietoturvapalvelut.

Tietoturvaa parantavat toimintatavat kehittyvät jatkuvasti. Näin pitääkin olla, koska haittaohjelmat ja niiden ympäristökin muuttuu koko ajan.

Metso Automation Oy:n laitosratkaisut kattavat asiakkaan laitoksen koko elinkaaren, aina luotettavasta käyttöönotosta ja tuotantoprosessin käytettävyyden turvaamisesta jatkuvaan tuotantoprosessin suorituskyvyn parantamiseen (kuva 8-1). Tietoturvapalvelut auttavat havaitsemaan ja estämään laitoksen automaatioverkkoon kohdistuvia ulkoisia uhkia ja samalla ne parantavat laitoksen käytettävyyttä.

LIITE 9

Asiakkaan ja automaatiotoimittajan välillä käsiteltäviä asioita

Ari Meldo, Metsäliitto Oy
Markku Tyynelä, Metso Automation Oy

Kuten tässä kirjassa on esitetty, teollisuusautomaation tietoturvaan liittyvien asioiden huomioon ottaminen on erittäin vaativaa. Käytännössä näitä asioita ei ole aina edes käsitelty, ja jos asioista on jotain sovittu, ei sovittuja asioita ole kirjattu ja dokumentoitu. Asiat on kuitenkin selvitettävä, jotta automaatiojärjestelmien tietoturva voidaan varmistaa koko tehtaan elinkaaren ajan. Asioita selvitettäessä on otettava huomioon vaatimukset luotettavuuden, vasteaikojen ja käytettävyyden suhteen.

Seuraavassa on koottu tiivistetysti listaa tärkeimmistä käytännön toiminnassa esille tulleista asioista, jotka on käytävä läpi ja tarpeen mukaan tapauskohtaisesti sovittava kulloinkin vaadittavista toimenpiteistä. Jokaisessa kohdassa on esitetty lyhyt yhteenveto asiasta ja siinä yhteydessä esitetään listamuodossa esimerkkejä oleellisimmista ko. kohtaan liittyvistä yksityiskohdista.

1. Toimintaprosessit, tiedotus ja tiedonvaihto

Tietoturva aiheuttaa lisätarpeita yrityksen ja automaatio-osaston toimintaprosesseille ja näistä on asianmukaisesti huolehdittava. Oleellista on saada aikaan toimiva tiedonvaihto eri osapuolten välille ja nimetä yhteyshenkilöt sekä toimintatavat siitä, miten tiedotusta hoidetaan. Myös se, miten tiedotusten ja viestien mahdollisesti vaatimat toimenpiteet viedään eteenpäin yrityksessä, on tärkeää. Jatkuvat muutokset edellyttävät asianmukaista muutosten hallintaa.

- Miten tiedottaminen ja tiedonvaihto hoidetaan (toimittaja → asiakas ja asiakas → toimittaja).
- Dokumenttien ylläpito.
- Muutosten hallinta.
- Yhteyshenkilöt.
- Koulutus (mitä koulutusta ja kenelle).
- Tiedottaminen (mitä omalle henkilökunnalle, mitä kaikille osapuolille, kuinka tiedotetaan tehokkaasti).

2. Verkkotopologia ja liityntä tehdas(toimisto)verkkoon

Automaatioverkon toimivuus on yksi oleellisimmista asioista automaatiojärjestelmän käytettävyyden varmistamisessa. Siten verkkoratkaisuja ja -laitteita valittaessa ja suunniteltaessa on tiedostettava, että tuntemattomien (testaamattomien) laitteiden ja ratkaisujen käyttö voi vaarantaa koko järjestelmän toimivuuden. Liitäntä automaatioverkosta tehdasverkkoon muodostaa rajapinnan, joka suojaa verkkoja toisella puolella tapahtuvista häiriöistä, ja se on suojattava sekä sovittava kuka on vastuussa tämän rajapinnan ylläpidosta. Suoraa Internet-yhteyttä rajapinnan läpi ei ole syytä sallia ilman painavia perusteita. Myös muita automaatioverkkoon liittyviä asioita, kuten käytettävä osoiteavaruus, laitteiden nimeäminen (IP-osoite, koneiden nimet) ja huoltotyöasemien liityntätavat on syytä käydä läpi.

- Topologia (VLAN).
- Osoitteet.
- Nimeäminen (nimeämiskäytännöt).
- Laitteet (merkit, mallit, jne.).
- Liityntä tehdasverkkoon: reititin, palomuuri, kahdennus.
- Rajapinnan ylläpito (toimittaja/asiakas).
- Kuinka huolto- yms. väliaikaiset työasemat liitetään automaatioverkkoon.
- Hajautus (missä tiedot tallennetaan ja missä varmennetaan).
- Internet-yhteys (suoraa yhteyttä ei tule sallia).

3. Virustorjuntaohjelmisto

Virustorjuntaohjelmistoa valittaessa on syytä käyttää vain automaatiojärjestelmässä testattua ohjelmistoa, jota on suositeltavaa käyttää niin kattavasti kuin se automaatiojärjestelmässä on mahdollista (rajoituksia voivat asettaa esimerkiksi vaatimukset nopeille vasteille). Virustorjuntaohjelmiston käytössä myös lisenssiasiat on sovittava. Tärkeää on varmistaa virustorjuntaohjelmiston ajan tasalla pitäminen, eli kuinka viruskuvaustiedostojen päivitys voidaan suorittaa nopeasti ja turvallisesti ilman häiriöitä. Tämä vaatii että myös päivitykset on testattu ennen käyttöönottoa.

- Mitä ohjelmistoa käytetään (miten vastuut jos valittua ohjelmistoa ei tueta tai sitä ei ole testattu automaatiojärjestelmässä).
- Kuinka ohjelmistoa ylläpidetään.
- Lisenssikysymykset.

4. Tietoturvapäivitykset

Käyttöjärjestelmiin ja ohjelmistoihin tulee jatkuvasti tietoturvaan liittyviä korjauksia ja päivityksiä, jotka on testattava ennen käyttöönottoa. Yleisesti

ottaen automaatiojärjestelmätoimittajat huolehtivat näiden päivitysten seurannasta arvioinnista, testauksesta sekä tiedottamisesta. Päivitys on aina myös käytettävyysriski, joten on sovittava kuka sen toteuttaa. Koska tietoturvapäivitykset vaativat usein tietokoneen uudelleenkäynnistyksen, on myös mahdollisuus muihin korjaaviin toimenpiteisiin syytä olla selvitettynä silloin, kun itse päivitystä ei voida jostain syystä suorittaa (esimerkiksi jos uudelleenkäynnistys aiheuttaa katkon tuotannossa).

- Tiedotus → sopiminen → asennus (kuka asentaa).
- Miten toimitaan, jos päivitystä ei voida asentaa.

5. Koventaminen (Hardening)

Uusissa toimituksissa on syytä sopia että toimitettavat laitteet ovat valmiiksi kovennettuja. Olemassa oleviin toimituksiin on syytä sopia erikseen miten tämä hoidetaan. Varsinkin sellaisiin käyttöjärjestelmäversioihin, joista valmistajan tuki on jo loppunut, koventaminen on eräs tehokas keino parantaa tietoturvaa.

- Uusien toimitusten koventamisesta on sovittava.
- Vanhojen toimitusten osalta kovennus on sovittava tarvittaessa erikseen.

6. Liikenteen dokumentointi

Tällä tarkoitetaan automaatiojärjestelmän mukana toimitettavaa dokumentointia, jossa selvitetään yksityiskohtaisesti automaatio- ja tehdasverkon välillä tarvittava tietoliikenne (protokollat, portit) muun muassa yrityksen IT-osastoa varten. Erityisesti on tiedostettava tämän tiedon tärkeys sekä huolehdittava, että tieto ei kulkeudu vääriin käsiin. Tärkein osuus on automaatioverkon ja tehdasverkon välinen tietoliikenne.

- Kuinka tarkasti ja miltä laajuudelta tietoliikenne dokumentoidaan (rajapinta vs. koko automaatioverkko).
- Kenelle tieto annetaan (mahdollinen tietoturvariski).

7. Käyttäjätunnukset ja salasanapolitiikka

Nämä ovat yhteisesti sovittavia käytäntöjä, joissa tärkeintä on varmistaa turvalliset periaatteet aiheuttamatta vaaraa automaation käytettävyydelle ja turvallisuudelle. Tärkeää on nimetä yhteyshenkilöt häiriöiden varalta ja myös huolehtia yhteyshenkilöiden nimien tiedottamisesta eri osapuolille.

- Käytetäänkö toimittajan vai asiakkaan politiikkaa.
- Yhteyshenkilöt.

8. Asiakkaan ja toimittajan väliset tietoliikenneyhteydet

Huolto- ja etäyhteyksien toteutusratkaisuista ja ylläpidosta on syytä sopia. Tavallisesti henkilöiden yhteyksiin on käytettävissä menetelmiä, mutta sovellusten välinen liikenne saattaa vaatia eritysjärjestelyjä, jotka voivat vaatia oman tietoturvaratkaisun. Tarvittaessa myös asiakkaan mahdollisesti tarvitsemat yhteydet automaatiotoimittajaan, esimerkiksi pääsy dokumentaatioon, on sovittava. Modeemeja käytettäessä on niiden käytöstä syytä sopia erikseen.

- Toimittajan tarvitsemat tuki-, huolto- ja päivitysyhteydet.
- Asiakkaan tarvitsemat yhteydet toimittajaan, esimerkiksi dokumentaatioon.
- Tarvittavien sovellusten välinen liikenne (M2M, Machine to Machine).
- Sallitaanko modeemien käyttö.

9. Varmistus ja palautus (Backup and Recovery)

Jotta vian tai häiriön tapahtuessa siitä toipuminen olisi mahdollisimman nopeaa, on sovittava varmistus ja palautuskäytännöistä ja -ratkaisuista. Tämä koskee niin tiedon (tallennusvälineet) kuin laitteidenkin (varaosat) varmennusta. Säännöllisellä testauksella on pidettävä huoli siitä että käytössä olevat ratkaisut toimivat ja esimerkiksi tallennus tallennusvälineelle toimii, esimerkiksi nauhalle.

- Kuinka hoidetaan laitteiden varmennus.
- Palautuskäytännöt ja ratkaisut.

10. Asiakkaan muiden IT-ratkaisujen käyttö

Yrityksellä saattaa olla käytössä erilaisia järjestelmiä ja ratkaisuja, joita halutaan käyttää myös automaatiojärjestelmässä. Näitä voivat olla esimerkiksi yleinen varmennusratkaisu (ks. edellinen kohta), verkkojen monitorointiratkaisu tai MS Windows -verkoissa esimerkiksi aktiivihakemiston käyttö. Näiden käytöstä automaatioverkossa on aina sovittava erikseen ja ennen niiden käyttöönottoa on varmistettava riittävällä testauksella, että ne eivät aiheuta häiriöitä automaatioverkkoon.

- Asiakkaan varmistusratkaisun käyttö (testaus).
- Automaatioverkon monitorointi (ei kuitenkaan automaatioverkon automaattinen päivitys).
- Domain- ja Active Directory -käyttö.

11. Langaton liikenne (esimerkiksi WLAN)

Langattomien ratkaisujen käyttö on yleistymässä, ja oleellisinta niiden käytössä on varmentaa, että ratkaisujen tietoturvasta huolehditaan asianmukaisesti ja riittävällä tasolla.

- Miten tietoturva hoidetaan.

12. Vastuut

Kun sovitaan edellä esitettyjen asioiden toteutuksesta, otetaan samalla kantaa myös siihen, kuka vastaa asioiden toimivuudesta ja ylläpidosta. Sovitut ratkaisut ja menetelmät vaikuttavat täten suoraan vastuujakoon. Koska osa valituista ratkaisuista ja menetelmistä ei kuitenkaan suoraan määrittele vastuuta, on suositeltavaa sopia vastuullinen osapuoli myös kirjallisesti. Tässä on otettava huomioon myös sovittujen ratkaisujen ja menetelmien mahdolliset vaikutukset laajemminkin koko toimituksen vastuu- ja takuuasioihin.

- Organisaatiosta, tehtävistä ja vastuista sopiminen (kuka hoitaa ja mitä, tietoturvarajapinnat ja vastuurajapinnat eri osapuolien välillä).
- Sovittujen ratkaisujen ja menetelmien mahdolliset vaikutukset laajemmin koko toimituksen vastuu- ja takuuasioihin.

Tavoitetila: edellä olevan listan käsittelyn lopputuloksena syntyy yhteinen dokumentointi, esimerkiksi automaatiojärjestelmän tietoturvaohjeisto, jossa on dokumentoitu miten yllä mainitut asiat hoidetaan.