VTT TIEDOTTEITA 2545

Pasi Ahonen

TITAN-käsikirja

VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa

VTT TIEDOTTEITA – RESEARCH NOTES 2545

TITAN-käsikirja

VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa

Pasi Ahonen

ISBN 978-951-38-7642-5 (nid.)
ISSN 1235-0605 (nid.)

ISBN 978-951-38-7643-2 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 5, PL 1000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 5, PB 1000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 5, P.O. Box 1000, FI-02044 VTT, Finland
phone internat. +358 20 722 111, fax +358 20 722 4374

Edita Prima Oy, Helsinki 2010

Pasi Ahonen. TITAN-käsikirja. VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa. Espoo 2010. VTT Tiedotteita – Research Notes 2545. 152 s.

Avainsanat Industrial systems, information security, security practices, security evaluation, security testing, standards

Tiivistelmä

Teknologian ja innovaatioiden kehittämiskeskus Tekesin Turvallisuusohjelmaan kuuluvan ”Tietoturvaa teollisuusautomaatioon” (TITAN) hankkeen VTT:n osuuden päätulokset on koottu tähän käsikirjaan. Tarkoituksena on esittää tärkeimpiä teollisuusautomaation tietoturvaa sivuavia trendejä, standardeja, vaatimuksia, referenssimalleja, ohjeita, testausmenetelmiä ja -kokemuksia tiiviin käsikirjan muodossa.

Projektissa on päädytty muun muassa seuraaviin johtopäätöksiin:

- Standardien mukaisen, turvallisen automaatiojärjestelmän hankinta on vaikeaa, joten yrityksen hankintaprosessin kehittämiseen kannattaa varata aikaa ja resursseja. Yhtenäisiä hankintakäytäntöjä täytyy edelleen kehittää.
- Tietoturvan parantaminen vaatii selkeitä, helppokäyttöisiä ja tehokkaita työkaluja ja käytäntöjä, jotka voidaan ottaa käyttöön kaikilla tarvittavilla osa-alueilla kriittisten järjestelmien toiminnan jatkuvuuden varmistamiseksi.
- Tietoturvavaatimukset täytyy työstää kehittäjien ja käyttäjien ymmärtämään muotoon.
- Kansallisella tasolla tarvitaan lisää yhteistyöfoorumeita ja verkostoja tietoturvatilanteen kartoittamiseksi ja tulevaisuuden riskiskenaarioiden tunnistamiseksi.

Mikään yksittäinen toimenpide ei turvaa Suomen automaatioteollisuuden tietoturvatilannetta kokonaisuutena, sillä kilpailu- ja toimintakyvyn varmistaminen tulevaisuudessa edellyttää avoimuuden ja monenkeskisen kommunikaation lisäämistä muun muassa operaattoreiden, laite- ja ohjelmistovalmistajien, automaatiojärjestelmätoimittajien, asiakkaiden, sääntelijöiden, sekä jopa kuluttajien välisissä ja keskinäisissä verkostoissa.

Sisällysluettelo

Kuvat

Taulukot

Kiitokset

Suuret kiitokset kaikille ystävällisille ja hankkeeseemme myötämielisesti suhtautuneille asiantuntijoille, jotka ovat tehneet tämän käsikirjan kirjoittamisen mahdolliseksi. Lukujen 4 ja 7 kirjoittamisprosessiin ovat osallistuneet VTT:stä tiimini tutkijat Sami Noponen, Anni Karinsalo, Matti Mantere ja Mirko Sailio. Ilman teitä tämä käsikirja olisi paljon vajavaisempi. Kiitokset kuuluvat myös Jarkko Holapalle ja Timo Wianderille, jotka VTT:ssä toimiessaan ansiokkaasti valmistelivat TITAN-hanketta, ennen valmisteluvastuun siirtymistä minulle.

Haluan lisäksi kiittää erityisesti seuraavia henkilöitä, jotka ovat edesauttaneet aiheen työstämisprosessia kukin omalla tavallaan:

Codenomicon: Ari Takanen, Lari Huttunen, Heikki Kortti, Ari Knuuti, Rauli Kaksonen

Deloitte & Touche: Jukka Eklund, Mikko Salonen

Elisa: Kari Keskitalo

EXFO NetHawk: Jouko Sankala, Pasi Heikkinen

FiCom ry.: Kari Wirman

Fortum: Juha Härkönen, Jarmo Huhta, Mikapetteri Heino, Henri Pirinen

F-Secure: Mika Ståhlberg, Janne Järvinen

Huoltovarmuuskeskus: Tuija Kyrölä, Hannu Sivonen, Atte Kokkinen

Inspecta Tarkastus: Antti Ylinen

Landis+Gyr Enermet: Jari Savolainen, Anssi Savelius, Ilkka Hokkanen, Seppo Räihä, Seppo Salmela, Markku Pihlajamaa

Liikenne- ja viestintäministeriö: Mari Herranen

Metso: Markku Tyynelä, Teemu Kiviniemi, Mika Vanne, Marko Stenvik, Pekka Niiranen, Petri Ehonsalo, Jaakko Oksanen, Mika Karaila, Ari Koikkalainen

Microsoft: Kimmo Bergius

Neste Oil: Pauli Kaunisto

Nokia: Tapio Ypyä, Mika Lauhde

Nokia Siemens Networks: Gabriel Waller

Nordea: Mikael Salonaho

OP-Pohjola: Heikki Kääriäinen

Oulun Seudun Ammattikorkeakoulu: Tero Hietanen, Timo Heikkinen

Pöyry: Juha Sipilä, Pekka Nykänen

Saint-Gobain: Tommi Nieminen

Sitra: Ossi Kuittinen

Sundcon: Matti Sundquist

Symantec: Marko Haarala

Säteilyturvakeskus: Harri Heimbürger, Mika Koskela, Mika Kaijanen

Tampereen teknillinen yliopisto: Jari Seppälä, Olli Post, Mikko Salmenperä, Hannu Koivisto

Tekes: Janne Peräjoki

TeliaSonera: Olli Haukkovaara

Teollisuuden Voima: Pekka Peltonen, Raimo Kivimäki, Esko Rauta, Janne Rintamaa

Tieto: Erkki Heliö

Tietotekniikan tutkimuslaitos HIIT: Risto Sarvas, Olli Pitkänen

Työ- ja elinkeinoministeriö: Antti Eskola

Uudenmaan työsuojelupiiri: Tapio Siirilä

Viestintävirasto: Jarkko Saarimäki, Kauto Huopio, Timo Lehtimäki

VTT: Mikko Metso, Hannu Honkanen (VTT:ssä työskennellessään), Reijo Savola, Pekka Koponen, Kaarina Karppinen, Arto Juhola, Pekka Ruuska, Teemu Väisänen, Matias Vierimaa, Mika Rautila, Jussi Paakkari

Yara Suomi: Hannu Lehtonen

ÅF: Tuomas Viskari.

Pasi Ahonen
Erikoistutkija, tiimipäällikkö, VTT
pasi.ahonen@vtt.fi

Lyhenteitä

ACL	Access Contol List
AGA	American Gas Association
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
AP	Access Point
API	American Petroleum Institute
ARP	Address Resolution Protocol
BIOS	Basic Input/Output System
BOOTP	Bootstrap Protocol
BSD	Berkeley Software Distribution
CC	Common Criteria
CD	Compact Disc
CDP	Cisco Discovery Protocol
CERT	Computer Emergency Readiness Team
CGI	Common Gateway Interface
CIP	Critical Infrastructure Protection, Common Industrial Protocol
CMD	Command Line
CPU	Central Processing Unit
CSSC	US-CERT Control Systems Security Center
CSSP	Control System Security Program
CSV	Comma Separated Values
DCOM	Distributed Component Object Model
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol

DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol
DTP	Dynamic Trunking Protocol
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
ERP	Enterprise Resource Planning
ESISAC	Information Sharing and Analysis Center for the Electricity Sector
FAT	Factory Acceptance Test
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FW	Firewall
GPL	GNU General Public License
GUI	Graphic User Interface
HIDS	Host-Based IDS
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAONA	Industrial Automation Open Networking Alliance
ICCP	Inter-Control Center Communications Protocol
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
ICT	Information and Communication Technologies
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission

IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
INL	Idaho National Laboratory
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security Architecture
ISA	Instrumentation, Systems and Automation Society
ISL	Inter-Switch Link
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
LLDP-MED	Link Layer Discovery Protocol for Media Endpoint Discovery
LTE	Long Term Evolution
MAC	Media Access Control
MMS	Manufacturing Message Specification
MS	Microsoft
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASL	Nessus Attack Scripting Language
NERC	North American Electric Reliability Corporation
NIDS	Network IDS
NIST	National Institute of Standards and Technology
NMAP	Network MAPper
NTP	Network Time Protocol

OPC	Object Linking and Embedding (OLE) for Process Control
OS	Operating System
OWASP	Open Web Application Security Project
PCAP	Packet Capture
PHP	Hypertext Preprocessor
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
QoS	Quality of Service
RBAC	Role-Based Access Contol
RPC	Remote Procedure Call
RTU	Remote Terminal Unit
SANS	SysAdmin, Audit, Network, Security Institute
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access-Control System
TC	Technical Committee
TCP	Transmission Control Protocol
Telnet	TELE NETwork (virtual terminal connection)

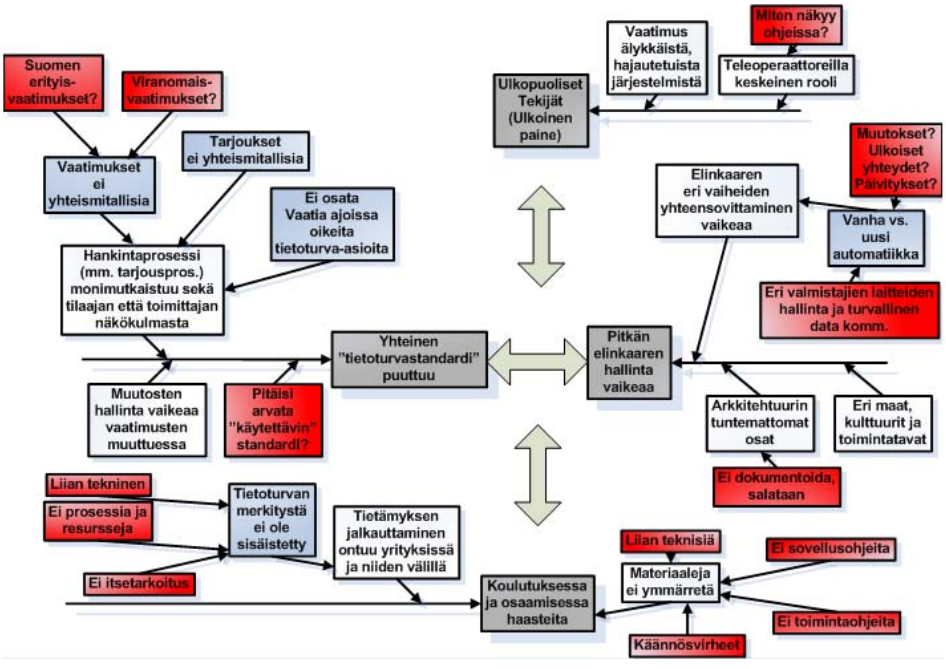
TLS	Transport Layer Security
TR	Technical Report
UA	Unified Architecture
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTP	VLAN Trunk Protocol
WG	Working Group
WLAN	Wireless Local Area Network
XML	eXtensible Markup Language

1. Johdanto teollisuusautomaation tietoturvaan

1.1 Motivaatio tietoturvan hallintaan

Hankkeen päätavoitteena oli selvittää teollisuusautomaatioympäristöön soveltuvat parhaat tietoturvamenettelytavat ja -ratkaisut sekä kehittää niitä erityisesti suomalaisten alan yritysten tarpeet huomioiden. Tietoturvanhallinnan työpakettia aloiteltaessa päätettiin järjestää työpaja, jossa mietittäisiin tietoturva-asioita yhdessä alan suomalaisten toimijoiden kesken. Työpajan alkuperäisenä tavoitteena oli pohtia tulevaisuuden automaatiojärjestelmän järjestelmäkehitykselle, järjestelmien käyttöönotolle sekä käytön hallinnalle asetettavia luotettavuus- ja laatuvaatimuksia erityisesti tietoturvallisuuden näkökulmasta. Lisäksi esillä oli kysymys siitä, miten automaatioteollisuuden pitäisi asettaa tietoturvavaatimuksia automaatiojärjestelmä-, laite- ja ohjelmistotoimittajille käytännössä.

Työpajan lopputuloksena syntyi jäsennelty kuva suomalaisen teollisuusautomaation kipupisteistä; siitä, millaiset tekijät vaikuttavat negatiivisesti tietoturvatilanteen hallinnassa pitämiseen. Seuraavassa on esitetty tiivistetty kuva lopputuloksesta, tietoturvan kipupisteistä suomalaisessa teollisuusautomaatiossa.



Kuva 1. Tietoturvan kipupisteet suomalaisessa teollisuusautomaatiossa.

Tärkeimpiä negatiivisia tietoturva-asioita suomalaisessa teollisuusautomaatiossa olivat

- yhteisen ”tietoturvastandardin” puuttuminen
- ulkopuoliset tekijät ja ulkoinen paine
- pitkän elinkaaren hallitsemisen vaikeus
- koulutuksen ja osaamisen haasteet.

Koska yhteinen tietoturvastandardi puuttuu, projektissa päätettiin, että suomalaisille automaatioteollisuuden toimijoille koostetaan käytännön lähtökohdista suomenkielinen, suoraviivaisesti sovellettavissa oleva ohjeistus tietoturvan hallitsemiseen. Tätä ohjeistusta onkin nyt sisällytetty tähän käsikirjaan. Mukana on lisäksi lyhyitä esittelyjä tärkeimmistä tietoturvan hallinnan standardeista ja käytännöistä, joita ohjeistusta laadittaessa käytettiin. Eri toimijoiden on kuitenkin hyvä tutustua itse heille keskeisimpiin standardimäärittelyihin käytännön soveltamista varten. Tarkoituksena oli lisäksi syventää saavutettua näkemystä erityisissä yritysevaluaatioissa, jotta saataisiin tarkempaa tietoa muun muassa ohjeistojen laadusta ja soveltuvuudesta erityisesti Suomen automaatioteollisuuden käyttöön.

1.2 Lyhyt johdatus teollisuusautomaation tietoturvan erityispiirteisiin

Teollisuusautomaatiojärjestelmät ovat osa yhteiskunnan kriittistä infrastruktuuria, ja siksi mahdollisilla tietoturvan ongelmatilanteilla voi olla laaja-alaisia vaikutuksia. Teollisuusautomaatiolla on muista tietojärjestelmistä poikkeavia erityispiirteitä, joista tärkeimpiä ovat seuraavat [Teollisuusautomaation tietoturva – Verkottumisen riskit ja niiden hallinta; Suomen Automaatioseura ry, Turvallisuusjaosto 2005]:

- **Häiriöiden vakavat seuraukset** – Tuotantojärjestelmissä ei-toivotut seuraukset voivat olla tuhoisia. Tuotantojärjestelmät voivat olla hyvin monimutkaisia, ja kaikki tietoturvatoiminnot, joita yhdistetään tuotantoprosessiin, on huolellisesti testattava ennen niiden käyttöönottoa. Automaation virhetoiminnat voivat aiheuttaa suuria henkilö-, ympäristö-, talous- ja esinevahinkoja sekä laajakantoisia yhteiskunnallisia seurauksia. Valtaosa käytössä olevista *state-of-art*-tietoturvaratkaisuista on kehitetty toimistojärjestelmien ja kuluttajien tietoliikenteen käyttötilanteisiin, joissa tietoturvaloukkaukset eivät aiheuta näin vakavia seurauksia. Myöskään avoimiin tietoliikenneratkaisuihin suunnitellut tietoturvaratkaisut eivät täytä suoraan kriittisten järjestelmien vaatimuksia.
- **Automaatiojärjestelmien pitkä elinkaari** – Elinkaaren pituus rajoittaa sovellettavien tietoturvateknologioiden käyttöönottoa ja edellyttää omia erityisratkaisuja. Monia erilaisia järjestelmäsukupolvia on yhtä aikaa käytössä, ja ratkaisut on osattava sovittaa niihin. Useimmat tuotantojärjestelmät ovat jatkuvatoimisia, jolloin odottamattomat seisokit eivät ole hyväksyttävissä. Järjestelmiä ei voida useinkaan pysäyttää (esim. päivityksiä varten) ilman merkittävää haittaa tuotantomääriin tai laatuun. Järjestelmien vikasietoisuuden ja selviytymiskyvyn täytyy olla korkealla tasolla.
- **Erityisohjelmistot** – Tuotantojärjestelmien ohjelmistojen hallinta on vaativampaa kuin tavallisissa tietoteknisissä järjestelmissä, ja niiden ylläpito vaatii erityisasiantuntemusta. Tosiaikajärjestelmät ovat usein resursseiltaan rajoittuneita, hajautettuja ja vasteajaltaan kriittisiä, eikä niissä yleensä ole voitu käyttää tyypillisiä toimistojen tietojärjestelmissä käytettyjä tietoturvaratkaisuja, kuten salausta, käyttäjäntunnistusta tai järjestelmälokeja.

- **Erilaiset käyttäjäryhmät** – Tuotantolaitoksessa toimii useita erilaisia käyttäjäryhmiä (esim. laitoksen omat henkilöstöryhmät, alihankkijat, palveluntarjoajat), mikä aiheuttaa tietoturvanhallinnalle omat erityisvaatimuksensa.

Automaatiojärjestelmän osien suunnittelun ja toteutuksen jokaiseen vaiheeseen liittyy tietoturvauhkia. Tietoturvatietoisuuden puute yrityksessä voi aiheuttaa sen, että uskotaan sokeasti tiettyyn teknologiaan ja valitaan valmiita kaupallisia ratkaisuja, jotka eivät loppujen lopuksi olekaan tietoturvan näkökulmasta sopivia. Käyttöympäristöstä ja ihmisten käyttäytymisestä saatetaan tehdä vääränlaisia oletuksia. Automaatiojärjestelmässä käytettävyys ja saatavuus ovat paljon tärkeämpiä ominaisuuksia kuin tavallisessa toimistojärjestelmässä. Harkitsemattomasti käyttöönotetut tietoturvaratkaisut ovat ainakin aiemmin olleet merkittävä yksittäinen syy käytettävyyden ongelmille. Automaatiosovellukset onkin jo alun alkaen suunniteltava erityisen vikasietoisiksi.

Toteutusvaiheessa tietoturvauhkia luovat muun muassa inhimilliset virheet ja vääräntyyppiset tietoliikenneratkaisut. Lisäksi tukijärjestelmien (esim. käyttöjärjestelmät) puutteet luovat uhkia. Yleisiä ongelmia toteutuksessa ovat henkilöresurssien puute ja liian kireät aikataulut. On pidettävä mielessä, että usein tietoturvan taso muuttuu ohjelmistopäivitysten ja konfiguraation muutosten yhteydessä. Automaatiosovellusten laadulla on yleensäkin suuri vaikutus tietoturvariskeihin.

Varsinkin IP-protokollaperheen ratkaisuja sekä standardeja käyttöjärjestelmiä käytetään teollisuusautomaatiossa yhä enemmän. Vanhojen erikoistarpeisiin räätälöityjen ratkaisujen täytyy kuitenkin toimia uuden tekniikan kanssa – ja vieläpä niin, että riittävä tietoturvan taso toteutuu. Myös langattoman etäohjauksen ja -diagnostiikan käyttö lisääntyy koko ajan. Alihankkijoiden tarpeet ohjaavat kehitystä kohti monikäyttöisiä, liikkuvia ja langattomia ratkaisuja. Langattomien lähiverkkojen (WLAN) käyttö voi aiheuttaa vakavia tietoturvauhkia, jos ratkaisuja ei ole kunnolla suunniteltu tietoturvan näkökulmasta.

Kriittisten järjestelmien ja inhimillisen toiminnan keskinäisriippuvuuksia ei ole tutkittu riittävän kokonaisvaltaisesti tieteellisillä menetelmillä, ja siksi niiden yhteisvaikutuksia ei tunneta. Kuten työpajamme tulokset osoittavat, teollisuusautomaation organisaatioilta puuttuu sekä menetelmiä että konkreettisia työkaluja toimintansa turvaamiseksi. Yhteiskunnan näkökulmasta tietoturvan toimivuus on tärkeää jatkuvuuden turvaamiseksi sekä normaali- että poikkeusolosuhteissa.

1.3 Tunnistettuja tietoturvatrendejä

Keväällä 2010 osallistuimme kansallisen tietoturvastrategian toimeenpanon yhteydessä Hankkeen 8 – Tulevaisuuden tietoturvatrendit -työpajaan, jossa pohdittiin suomalaisten asiantuntijoiden kesken tietoturvaan liittyviä trendejä. Työpajassa käsittely jaettiin kolmeen teemaan:

- ihmiset, yhteiskunta ja yhteisöt
- teollisuus/liiketoiminta/palvelunäkökulmat
- tekniikan trendit.

Työpajassa työskenneltiin siten, että kustakin teemasta pidettiin muutamia alustuksia, ja lisäksi teemoista keskusteltiin paikan päällä sekä reaaliaikaisesti verkossa ryhmätyökalua käyttäen. Seuraavassa esitetään otteita kunkin teeman tuloksista.

1.3.1 Ihmiset, yhteiskunta ja yhteisöt

Tunnistettuja trendejä

Sosiaalinen vuorovaikutus muuttuu tietoverkkovälitteiseksi. *Always-on*-yhteiskunta laajenee, ja *online presence* - ja yhteisöpalveluja käytetään entistä enemmän. Yksilöillä on enemmän kuin yksi identiteetti. Palvelun käyttäjän tunnistautuminen ja tunteminen korostuvat: ei riitä, että käyttäjä tunnistetaan, vaan tunteminen on tärkeämpää liiketoiminnan tai regulaation takia. Tulevaisuuden yhteiskunnassa voi olla vaikea elää ilman virtuaali-identiteettiä. Voiko loppukäyttäjälle jättää tulevaisuudessa vastuuta teknisestä tietoturvasta jonkin tietyn sovelluksen käytössä?

Yksityisyydensuojan käsite muuttuu. Ihmiset julkistavat aikaisemmin luottamuksellisina pidettyjä tietoja itsestään verkkoyhteisöissä. Arjessakin pitää koko ajan tietää, miten toimia, jos haluaa säilyttää yksityisyyden tai ylläpitää vahvaa tietoturvaa. Euroopassa on varsin kattava tietosuojalainsäädäntö. Miten lainsäädäntö pysyy teknologisen kehityksen perässä? Lainsäädännön mahdollisuudet rajoittaa globaaleja palveluita ovat heikot. Mikä tulee olemaan tietoturvalain soveltamisala?

Maineen merkitys korostuu myös yksityishenkilöillä. Yksilöt voidaan tunnistaa yhdistämällä eri tietoja, joita verkosta voidaan löytää. Yksityisyys rapautuu. Voidaan myös kysyä, mikä suojaisi henkilöä hänen omilta virhearvioiltaan sosi-

aalisissa medioissa. Mitä ihmeellisemmät tallenteet ja tietokannat muodostavat henkilörekisterin, mutta ymmärtävätkö palveluntarjoajat tämän?

Pilvipalveluiden haasteet. Minkä maan lainsäädännön mukaan pilvioperaattori toimii? Mahdollisuus kontrolloida omaa tietoa poistuu – kuka valvoo pilvipalveluita ja miten? Mistä ihmiset tietävät, missä heihin liittyvä informaatio säilytetään? Internet ei tunne lakeja – paitsi Kiinassa.

Virtuaalirahan käyttö. Virtuaaliraha yleistyy virtuaaliyhteisöissä ja voi aiheuttaa talouskriisin. Sen käyttöä tai arvon vakautta eivät viranomaiset valvo. Raha siirtyy verkkoon, jossa liiketoimintaa tapahtuu entistä enemmän.

Rahan tekeminen verkossa rikollisin keinoin. Rikollisesti verkosta hankittua tietoa myydään. Verkkorikollisuus on usein ”*multi-jurisdiction*”-asia. Sen tutkiminen ja rikollisten tuomitseminen on hankalaa, joskus jopa mahdotonta. Virtuaalirahan kautta rahanpesumahdollisuudet helpottuvat. Palveluketjut ja ulkoistaminen ovat tulleet osaksi rikollisorganisaatioiden toimintaa. Nettirikollisuus näyttää normaalille ulkoistukselle mallia – ulkoistuksen myötä nettirikollisuus kasvaa yli 200 prosenttia vuosittain. Yhteistyötä rikollisten kiinnisaamiseksi on tiivistettävä – ei vain kotimaassa vaan myös kansainvälisesti.

Miten estetään **haittaohjelmien leviäminen**? Löytyykö siihen uusia lääkkeitä? Suomessa yhteistyö **verkon turvallisuuden** ylläpitämiseksi toimii edelleen melko hyvin. Kotimainen yhteistyö ei kuitenkaan riitä, vaan vaaditaan kansainvälistä yhteistyötä. Miten sitä voitaisiin parantaa? Tietoturva perustuu viranomaisten ja teollisuuden, esimerkiksi operaattoreiden, yhteistyöhön. Tieto pitää saada liikkumaan nopeammin (automaattisesti) ja standardeja käyttäen. Tarvitaan lyhyen aikavälin reaaliaikaista tilannekuvatietoa sekä pidemmän aikavälin tilannekatsauksia.

Tietoturvarikollisuus ja ”uudet mahdollisuudet” uusissa sosiaalisissa prosesseissa (identiteetit, suhteet, konventiot ja normit; vrt. nuorten netti-sosiaaliset prosessit), joihin lainsäädäntö, valvonta ja viranomaiset eivät ole ehtineet vielä reagoida. Vaikka yhteisöissä voi valita valtuutetut käyttäjät, pitää tietoturvan kannalta muistaa kaksi eri asiaa: a) käytettyjen tekniikoiden ongelmat, jotka mahdollistavat esimerkiksi tietomurrot ja b) valtuutettujen käyttäjien aiheuttamat vuodot ja tiedon siirtäminen vääriin paikkoihin. Tiedon siirtoa pitäisi siis pystyä estämään, valvomaan ja seuraamaan.

Turvallinen ohjelmakehitys on kaikkien kehittäjien selkärangassa, vai onko? Jos ei, miten asia voidaan korjata? Uusi teknologia siirtyy nopeasti rikollistenkin käsiin.

Käytettävyys tietoturvatekijänä: kuka vastaa helppokäyttöisyydestä?

1.3.2 Teollisuus/liiketoiminta/palvelunäkökulmat

Tunnistettuja trendejä

Liiketoiminnan strategiasuunnittelu on liitettävä toiminnan jatkuvuuden varmistamiseen. Miten ekstrapoloidaan liiketoiminnan (yritysten) jatkuvuusteoriat yhteiskunnan jatkuvuusstrategiaksi? Entä suunta yhteiskunnasta yrityksiin? ”Tietoturva” on menetetty, täydellistä tietoturvaa ei ole – **jatkuvuus** voidaan vielä laittaa kuntoon. **Käytettävyyden ja saatavuuden varmistamisessa** ollaan vielä alkuvaiheessa. Miten todella varmistutaan että järjestelmät tulevat toimimaan kaikissa tilanteissa? Hätätilannesuunnittelua ei todellisuudessa tehdä paljon; ohjelmistomäärä on erittäin suuri jo perushallinnan kannalta. Nykyinen tietoturvakäsite on liian suppea, ja tietoturvauhkien jäsennystavan tuleekin muuttua, koska myös uhkat ovat muuttuneet.

Verkostojohtamisen myötä jatkuvuuden hallinnan kompleksisuus on lisääntynyt. Verkostojohtamista tarvitaan, mutta osataanko sitä riittävän hyvin? Alihankinta on yksinkertaista, kumppanuus ei. Teknologioihin liittyvät riskit on saatava hallintaan **henkilöverkostojen** tiedon avulla. Myös **teknologiariippuvuus** kasvaa – etenkin Suomessa. Sallivatko **operaattorit** täysin vapaan sovelluskehityksen? Toteutuuko mobiiliverkkojen *network neutrality* enää jatkossa?

Tärkein tuotannon tekijä on tieto – ei teknologia. Suojattavia tietoja ovat esimerkiksi asiakastietojärjestelmät ja tiedonsiirron kannalta telerunkoverkkojen reititystiedot. **Ennakointi** on saatava johdon agendalle, sillä muutoin häiriöt eivät ole hallinnassa. Tiedonkulun varmistamiseksi täytyy yhteiskunnassa tehdä rakenteellisia uudistuksia. Kuka omistaa tiedot nykyisissä verkkopalveluissa? Loppukäyttäjäsopimukset kannattaa tutkia.

Rikolliset miettivät jatkuvasti, mitä voidaan muuttaa rahaksi. Teollisuusautomaatiota hyödyntää enimmäkseen ns. perinteinen teollisuus, joka on selkeästi altavastaajana tietoturvarikollisiin nähden. Tiedon omistaja ei välttämättä osaa arvioida kaiken tietonsa arvoa, ja verkkoon laitetut palvelut saattavat kiinnostaa toimijoita, joita ei ole ajateltu ennalta. Omistajia kiristetään palvelunestohyökkäyksillä (palvelut pakotetaan alas, tiedot hävitetään tms.). On olemassa erikoistuneita ryhmiä, jotka tekevät verkon kautta löydettävälle tiedolle jonkin operaation, minkä jälkeen tieto myydään. Näin ”rikosketju” on valmis. Motiivina voi olla kateus, pettymys tai mielenterveyden ongelmat.

Yritysten **tietoturvaohjeita** pitää päivittää säännöllisesti. **Yksinkertainen ja ymmärrettävä tietoturva** on myyntivaltti potentiaalisille asiakkaille. Teolli-

suusautomaation **tietoturvastandardit** ovat vasta kehittymässä. Teknologioita nopeasti sovellettaessa yrityksen riskienhallinta kriisiytyy. Missä sisäverkon ulkoraja todellisuudessa kulkee? Ovatko yritykset heitteillä, onko riskienhallinta ajan tasalla ja onko erinäisiin ongelmiin varauduttu? Perinteinen riskien tarkastelu ei riitä, koska todellisia tietoturvariskejä on vaikea tunnistaa ja ne muuttuvat jatkuvasti.

Automaatioon tulee uusia haasteita siirryttäessä uuteen **teknologiaan**. Siirtyminen suljetuista järjestelmistä ja verkoista avoimiin järjestelmiin on haasteellista. Verkostotapauksessa on mahdollista, että monen eri organisaation automaatiojärjestelmät kommunikoivat keskenään. **Automaatioverkon yhteydet ERP-järjestelmiin** aiheuttavat ongelmia. Onko automaatioverkko aidosti erotettavissa ulkomaailmasta?

Toimitusajat ovat lyhentyneet, mikä tekee järjestelmien testaamisesta haasteellista. Palvelun testaaminen tietoturvamielessä voi olla haaste paitsi teknologisesti myös aikataulullisesti. Miten osataan **arvioida tietoturvariskit** palvelun kehittämisen aikana, jos hyökkäystapoja ei tunnisteta ennalta? **Ohjelmistokehityksen ja testauksen laatu** ratkaisee, miten pärjätään. Kehitystyössä käytetään valmiita komponentteja – miten niiden laatu testataan? **Luottamus** on kaiken perusta.

Vaikea ja huonosti toimiva **käyttäjän yksityisyyden hallinta** on kriittinen tietoturvahaaste erityisesti sosiaalisen median palveluissa, jotka ovat nyt tunkeutumassa myös teollisuusautomaation toimistoverkkoihin (esim. Facebook ja sen jatkuvasti muuttuva yksityisyydenhallinta). Sosiaalisen median palveluissa sekä muissa palveluissa, joissa käyttäjien itse tuottama **sisältö** on keskeistä, tietoturvan hallinta ja **vastuu siirtyy olennaisilta osin käyttäjille**. Yrityksen tai henkilöstön positiivinen tunnettuus tuo lisäarvoa yrityksen palveluille. Tietoturva ei ole toimihenkilölle enää pelkästään taustalla toimiva teknologia vaan osa vuorovaikutusta ja palveluiden käyttöä. Voisiko esimerkiksi yritysten tietojen varmuuskopioinnista löytyä liiketoimintaa Suomeen (tavoitteena turvallinen ja vakaa toimintaympäristö)?

Vastuut yrityksissä ovat epäselviä: kuka vastaa ja mistä jne. Miten teollisuuden **pk-sektorin toimijat saadaan tietoisiksi** ja mukaan tietoturvatalkoisiin – selkeän tiedon lisäksi tarvitaan helposti käytettäviä ja kustannustehokkaita ratkaisuja. Suomi ei ole turvassa, vaikka saatamme niin kuvitella. Vanhat ratkaisut tietoturvaan eivät enää päde.

Tietoturva-asiantuntijuuden käyttöä pitäisi hyödyntää laajemmin järjestelmien laadun ja luotettavuuden kehittämisessä. **Järjestelmäosaaminen sekä konfi-**

guraatioiden ja päivitysten hallinta on yhä tärkeämpää. Miten ohjelma **korjataan** tehtaan järjestelmissä, joiden tulee ohjata prosessia ympäri vuorokauden?

1.3.3 Tekniikan trendejä

Tunnistettuja trendejä

Nettiyhteydet ovat saatavilla aina ja kaikkialla. Lisälaitteetkin ovat jo verkossa. **Tietoliikenneverkkojen konvergenssi** lisääntyy, vaikka markkinajohtajat saattavatkin tahallaan hidastaa konvergenssikehitystä. Broadcastingin (mm. TV-lähetykset) yhdistäminen tietoliikenneteknologioihin lisääntyy, samoin kuin monikanavajakelu broadcasting-alueella ja interaktiivisten palveluiden kehittyminen. Eri teknologioiden väliset yhteensopivuusstandardit saattavat epäonnistua kaupallisesti. Kuinka hyvin Suomi on mukana **standardien kehityksessä**? Entä mikä on Suomen rooli **tietoturva-arkkitehtuurin** kehittämisessä?

Itseorganisoituvat verkot kehittyvät jatkuvasti. Miten käyttäjä on perillä automaattisesti luotavista yhteyksistä eri laitteisiin? Kännykässä voi jo nykyään olla neljä eri radioteknologiaa, ja laite on yhteydessä useampaan radioverkkoon yhtä aikaa. Tunteeko käyttäjä riskit ja osaako hän konfiguroida laitteet oikein? Laite valitsee verkot käyttäjän puolesta – onko käyttäjä tietoinen kustannuksista? Myös laitteiden määrä kasvaa valtavasti, samoin autonomiset laiteverkot lisääntyvät. Ubiikkikäyttöliittymä – web-selain?

Kognitiiviradio (ja ohjelmoitavat radiomoduulit) tekevät joustavat ratkaisut mahdolliseksi. Matkaviestinpuolella sekä operaattorisegmentti (joissakin maissa) että jotkin päätelaitevalmistajat haluavat kontrolloida konvergenssikehitystä. Kaikki tuskin tulevat käyttämään samaa 4G-teknologiaa (LTE), eli ongelmat jatkuvat. Radioteknologian tarvitsemat chipsetit halpenevat standardisoinnin ja massatuotannon myötä.

Pilviteknologiat ovat keskeisiä. Näissä yksityisyyden ja tietoturvan haasteita ovat lainsäädäntö, omistajuus ja vastuut. Yhdysvallat on edellä pilviteknologioiden kehittämisessä ja kaupallistamisessa EU:hun verrattuna. Pilviteknologioihin tarvitaan satsauksia, mutta miten liiketoiminta saadaan mukaan? Käyttäjäkokemuksen toteutus pilvipalveluissa on oleellista, samoin tietoturvan joustava soveltaminen ja näkyvyys käyttäjälle. Miten käyttäjät saadaan luottamaan palveluun? Pilvipalveluilla on oltava vähintään samat tietoturvavaatimukset kuin perinteisesti tuotetuilla palveluilla. Pilvipalveluihin liittyvä hype ajaa organisaatioita teknologian käyttöönottoon ilman, että riskejä on arvioitu. Pilvipalveluiden

asettamat vaatimukset ohjelmistokehitykselle on selvitettävä. Voidaanko tietovarastot todella virtualisoida pilveen turvallisesti?

Smart gridien tietoturvariskit korostuvat, ja hyökkäykset sähköverkon osia vastaan lisääntyvät.

Millä nettiliikenteestä **profiloidaan** merkittävät uhat ja seurattavat asiat? Miten tunnistetaan todelliset hyökkäykset kohinan joukosta? Tietoturvan mittaaminen on aina ollut hankalaa, mutta jatkossa perinteinen tapa ei enää toimi.

Social engineeringin käyttö on lisääntynyt teknisissä, haittaohjelmiin perustuvissa hyökkäyksissä. Käyttäjiä on suhteellisen helppo harhauttaa. **Viihteen käyttö** on lisääntynyt käyttäjien pettämisessä ja itsetuhoisten toimenpiteiden tekemisessä.

1.3.4 Yhteenveto teollisuusautomaation trendeistä

Hankkeen kuluessa syntyneiden keskusteluiden, työpajojen ja lähdeaineistonkin perusteella voidaan nimetä seuraavanlaisia päätrendejä, jotka vaikuttavat välittömästi joillain tavoin teollisuusautomaation tietoturvaan. Kustakin teemasta on otettu listalle vain kolme tärkeintä trendiä.

Taulukko 1. Teollisuusautomaation tietoturvaan vaikuttavien trendien yhteenveto.

Teema	**Trendin kuvaus**	**Seurauksia**
Ihmisten käyttäytyminen	Sosiaalinen vuorovaikutus kehittyy verkkovälitteiseksi. Työntekijät asentavat omia (mm. sosiaalinen media) ohjelmiaan työpaikan tietokoneisiin.	Luottamus ja konfiguraation hallinta heikkenee, välittömät tietoturvariskit kasvavat.
	Yksityisyydensuoja muuttuu ja heikkenee. Työntekijöiden seurattavuus lisääntyy ja maineen jatkuvan ylläpidon merkitys korostuu.	Työntekijöihin liittyvät riskit kasvavat.
	Rikollisuus siirtyy tietoverkkoon. Rikollisuuden osa-alueet verkossa kehittyvät ja rikollisten yhteistoiminta helpottuu. Laillinen ja rikollinen liiketoiminta sekoittuvat.	Yritysten tietojärjestelmiin tunkeutuminen helpottuu. Tietoja voidaan ostaa.
Liiketoiminta/palvelut	Teollisuusautomaatioyritysten IT-osastoja ulkoistetaan. Erikoistumiskehitys jatkuu. Liiketoiminnalle kriittistä osaamista ja työtä hankitaan halpamaista.	Ulkoiset riskit kasvavat. Ydinosaamisen hallinta heikkenee.
	Kaikki liiketoiminta verkostoituu yhä laajemmiksi kokonaisuuksiksi. Henkilöverkostojen tieto on avainasemassa.	Liiketoiminnan, strategisen tiedon ja jatkuvuuden hallinta monimutkaistuu.
	Liiketoiminta muuttuu entistä dynaamisemmaksi ja arvonmuodostukseltaan muuttuvammaksi. Toimitusajat lyhentyvät.	Kriittistä tietoa saattaa löytyä yllättävistä pisteistä. Laadunhallinta heikkenee.
Tekniikka	Lähes kaikki laitteet liitetään osaksi tietoverkkoja, itseorganisoituvat verkot kehittyvät. Pilvipalveluiden ja -teknologioiden käyttö yleistyy.	Tietoverkkojen saatavuuden ja luotettavuuden merkitys korostuu. Strategisen tiedon hallintaa ulkoistetaan.
	Kommunikaatioteknologiat kypsyvät helppokäyttöisiksi ja toimivat yhdessä. Kehitystyö kiihtyy sovellusalueella.	Sovellustason (tietoturva) ratkaisujen ja monitoroinnin merkitys kasvaa.
	Tietojärjestelmät kehittyvät nopeasti, ja tiedon integroitavuuden tarve kasvaa.	Tiedonhallinta heikkenee, jäljitettävyyden tarve kasvaa.

2. Soveltuvat tietoturvastandardit ja -käytännöt automaatiojärjestelmien tietoturvassa

2.1 Taustaa

Teollisuusautomaation alueella **ei ole** Suomessa, eikä globaalistikaan ajatellen, yritysten tietoturvan hallinnan tarpeisiin soveltuvaa **yhteistä standardia tai oletusarvoisesti sovellettavaa referenssiä**. On toki olemassa erilaisten standardointiorganisaatioiden ja käyttäjäyhteisöjen erillisiä standardeja ja parhaita käytäntöjä määrittäviä dokumentteja, mutta niiden soveltaminen ja käyttö toimialalla on kirjavaa ja hajanaista. Tämä johtaa selkeästi ongelmatilanteisiin yhteisten tietoturvavaatimusten määrittelyssä sekä käytännön toiminnan arvioinnissa ja kehittämisessä, kuten esimerkiksi riittävien tietoturvasuojauksien määrittelyssä ja tulkinnassa. Aikaa ja työpanosta kuluu hukkaan ns. yhteisen kielen tai sapluunan puuttuessa tietoturva-asioista keskusteltaessa ja sovittaessa.

Niinpä onkin tarpeen määritellä yhtenäinen joukko parhaita käytäntöjä, joita Suomessa tulisi soveltaa eri toimijoiden toiminnassa sekä toimijoiden välisessä yhteistyössä. Toiminnalla tarkoitetaan yrityksen tai organisaation normaaleja perustoimintoja, kuten prosessin ohjausta, tuotantoa, säätöä, ylläpitotoimintoja, etävalvontaa jne. Yhteistyöllä tarkoitetaan tyypillisimmillään laitoksen tai teollisuustuotannon operatiivisen toiminnan yhteistyötä esimerkiksi alihankkijoiden kuten laite- ja ohjelmistovalmistajien kanssa mutta myös yhteistyötä perustoimijoiden kuten kehitystoimintojen, ylläpidon ja viranomaisvalvonnan välillä.

Kaikki parhaiden käytäntöjen kuvaukset eivät välttämättä tarvitse suoraa referenssiä, vaikka siitä monesti apua varmasti olisikin. Riittää, kun yhteisössä on yhteisymmärrys siitä, että kuvattavat tietoturvakäytännöt ovat tehokkaita sekä tarpeeksi selkeitä ja yksikäsitteisiä mahdollistaakseen yhtenevien suojausten

rakentamisen sekä toiminnan määrittelyn ongelmatilanteissa. Tärkeää on ohjeistuksen laatu ja käytännöllisyys, eivät niinkään muotoseikat.

Seuraavassa pyrimme esittelemään soveltuvimpia tietoturvastandardeja ja -ohjeistuksia, joihin lähes jokaisessa teollisuusautomaatioalueella toimivassa yrityksessä tulisi olla soveltavan tason ymmärrystä ja substanssia. On huomattava, että yritys voi hankkia osan tietoturvaan liittyvästä erityisosaamisesta, kuten esimerkiksi testaustoiminnasta, ulkopuolisilta toimijoilta. Tämä edellyttää kuitenkin, että kriteeristö, kuten vaatimukset ja etenkin kokonaisuuden (prosessien, ylläpidon, jne.) turvallisuuden tärkeysjärjestys ja siihen vaadittava ymmärrys, on varmasti yrityksen hallinnassa.

2.1.1 Yleistä valituista standardeista

Jotta standardi tai paras käytäntö olisi relevantti, sillä täytyy olla tiettyjä ominaisuuksia tai erityisten määräysvaltaisten tahojen tulee edellyttää sen toteutumista. Jälkimmäisellä tarkoitamme sitä, että alalta löytyy jo toimijoita, jotka ovat pystyneet asettamaan tietoturvaan liittyviä reunaehtoja tai minimivaatimuksia rajatulla maantieteellisellä alueella tapahtuvalle tietyntyyppiselle teollisuustoiminnalle. Hyvä esimerkki tästä on NERC (*North American Electric Reliability Corporation*), joka on määritellyt Pohjois-Amerikan sähköteollisuudelle minimivaatimuksia (mm. sähkölaitosten SCADA-verkkojen tietoturva), joiden täyttämättä jättämiselle on asetettu organisoitu seuranta sekä ankarat rangaistusvaatimukset.

2.1.2 Valittujen standardien käyttötarkoitus ja valintakriteeristö

Prosessikuvaus (TITAN-hankkeessa)

Ensin **tunnistetaan** sellaiset tietoturvan hallintaan liittyvät käytännön standardit, ohjeet ja suositukset, joita hyödyntämällä teollisuusautomaatioalan toimijat voivat muun muassa kommunikoida tehokkaasti omat spesifit tietoturvan hallinnan vaatimuksensa sekä organisaation sisällä että eri organisaatioiden välillä. Seuraavaksi hyviksi tunnistetut ohjeistukset **kuvataan** yleisellä tasolla. Sitten valittujen osuuksien käyttökelpoisuutta **arvioidaan** alan toimijoiden keskuudessa (mm. yritysevaluaatioiden ja ryhmätyön keinoin). Lopuksi **koostetaan** ohjeistus suomalaisten alan toimijoiden käyttöön sekä **informoidaan** toimialaa muun muassa seminaarien ja kirjallisen materiaalin avulla.

Valintakriteeristö

Miten olemassa olevia tietoturvanhallinnan määrittelyjä pitäisi arvioida, ts. miten valita parhaat käytännöt? Seuraavassa esitetään valintakriteeristö, jota on käytetty parhaiden käytäntöjen tunnistamisessa, kuvauksessa ja arvioinnissa.

Taulukko 2. Valintakriteeristö relevanttien standardien (ohjeiden) tunnistamiseksi, kuvaamiseksi ja arvioimiseksi.

Valintakriteeri	Selitys	Perustelut lyhyesti
Laatu	Ohjeen tai sen osan koettu subjektiivinen laatutaso.	Laatu ja substanssi ovat edellytyksiä.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Miten yleiskäyttöisenä ohje koetaan? Onko ohje kattava vai liian suppea?	Käytännöllisyys- ja käytettävyystekijät
Meriitit	Referenssit. Kuinka yleisesti ohje on käytössä relevanteissa organisaatioissa?	Aiemmat soveltajat lisäävät luottamusta.
Sääntely	Käytön pakollisuus. Asettaako viranomainen tai muu tärkeä toimija vaatimuksia käyttöönotolle?	Sääntely ohjaa toimintaa.
Ylläpito ja saatavuus	Miten hyvin ohjetta päivitetään ja onko se yleisesti saatavilla? (Avoin/maksullinen/suljettu)	Avoimuus parantaa laatua ja saatavuutta.
Erityispiirteet	Kuinka hyvin teollisuusautomaation erityispiirteet on otettu huomioon?	Toimialan vaatimukset, kuten vaatimukset käyttövarmuudelle.

2.2 Soveltuvat yleiskäyttöiset standardit

2.2.1 ISO/IEC 15408: *Common Criteria – Evaluation criteria for IT security*

ISO/IEC:n hallinnoima *Common Criteria* (CC) on ehkäpä laajimmin käytetty standardi, jonka mukaisesti sertifioituja IT-tuotteita pidetään tietoturvallisina sekä toimittajan että tilaajan mielestä. Tuotteet evaluoidaan valitun CC-kriteeristön mukaisesti riippumattomissa, lisensioiduissa laboratorioissa (tilaajan) osoittaman tietoturvatason vaatimusten mukaisesti. Kullekin teknologialle on määritelty oma kriteeristö, ns. suojausprofiili.

CC-standardi määrittelee peruskäsitteet ja mallit IT-järjestelmien tietoturvan arvioimiseksi. Se sisältää määrittelyt muun muassa evaluaatiokohteen (*Target of Evaluation*, ToE) ja suojausprofiilien (*Protection Profile*, PP) käsitteille.

Standardi ei sisällä ICS-spesifisiä määrittelyjä tai ohjeita. Silti ICS-alueen toimijalla on hyvä olla saatavilla tämä standardi, sillä siihen voidaan viitata useissa yhteyksissä muun muassa tietoturvan tason määrittämisen yhteydessä.

IEC 15408 -standardi sisältää seuraavat osat:

- Osa 1: Esittely ja yleinen malli
- Osa 2: Tietoturvan toiminnalliset vaatimukset
- Osa 3: Tietoturvan varmistamisen vaatimukset.

Osa 2 jaottelee tietoturvan toiminnalliset vaatimukset seuraaviin luokkiin:

- FAU: *Security audit*
- FCO: *Communication*
- FCS: *Cryptographic support*
- FDP: *User data protection*
- FIA: *Identification and authentication*
- FMT: *Security management*
- FPR: *Privacy*
- FPT: *Protection of target's security functions*
- FRU: *Resource utilisation*
- FTA: *Target of evaluation access*
- FTP: *Trusted path/channels*.

Osa 3 puolestaan jaottelee tietoturvan varmistamisen vaatimukset seuraaviin luokkiin:

- ACM: *Configuration management*
- ADO: *Delivery and operation*
- ADV: *Development*
- AGD: *Guidance documents*
- ALC: *Life cycle support*
- APE: *Protection profile evaluation*
- ASE: *Security target evaluation*
- ATE: *Tests*
- AVA: *Vulnerability assessment*.

Osa 3 myös määrittelee nousevat EAL (*Evaluation Assurance Level*) -vaatimustasot yhdestä seitsemään, tavoitellen kustannustehokkainta ja soveltuvinta varmistamisen tasoa kuhunkin tarpeeseen. Korkein luokka (EAL-7) asettaa laajimmat ja syvimmät vaatimukset kohteen tietoturvan varmistamiselle. Vaatimukset ovat melko yksityiskohtaisia mutta samalla periaatteellisia ja hyviä.

Lisäksi standardin yhteyteen on tuotettu evaluaatiometodologiasta hyödyllinen dokumentti (CCMB-2007-09-004), joka tarkentaa ja selkeyttää muun muassa evaluaatioaktiviteetteja ja terminologiaa sekä auttaa valitsemaan ja fokusoimaan suunniteltuja evaluaatioita tehokkaalla tavalla. (Osat 1–3 saattavat olla joiltain osin hieman vaikeaselkoisia.)

Referenssi: esimerkiksi http://www.commoncriteriaportal.org/.

Taulukko 3. ISO/IEC 15408 CC – yhteenveto.

Valintakriteeri	**Arvio**	**Selitys**
Laatu	Erittäin paljon työstetty, laadukas ja paljon käytetty yhteinen standardi.	CC on usein lähtökohta yleiselle tietoturvaevaluaatiolle.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Ohjeet ovat yleiskäyttöisiä, käyttökelpoisia ja kattavat laajan alueen tietoturvasta. Haittapuolena ohjeiston suuri sivumäärä ja lievä vaikeaselkoisuus.	CC-evaluaatiokriteeristö. Evaluointi usein hidasta ja kallista.
Meriitit	Laajasti käytössä tietoturvakriittisissä organisaatioissa, mm. kriittisen infrastruktuurin yritykset, laite- ja ohjelmistovalmistajat jne.	
Sääntely	Ei aseta varsinaista sääntelyä. Määrittelee standardin tavan esittää tietoturvavaatimuksia. Osa muista standardeista ja ohjeista referoi tätä.	Tilaajatahot voivat vaatia tuotteilta tietyn EAL-tason evaluointia.
Ylläpito ja saatavuus	Hyvin ylläpidetty ja saatavissa julkisesti (Avoin).	
Erityispiirteet	Teollisuusautomaation erityispiirteitä ei ole nostettu esiin, mutta ohjeisto kyllä tukee hyvin teollisuusautomaation tietoturvaa.	Perustavanlaatuinen, tietoturvan varmistamista määrittelevä standardi.

2.2.2 DHS – *Department of Homeland Security* (CSSP-käytännöt)

2.2.2.1 DHS CSSP *Recommended Practices*

Yhdysvaltain *Homeland Security* -hallinto on tukenut *Control System Security Program* (CSSP) -ohjelmaa, joka koordinoi tietoturvahaavoittuvuuksia ja -riske- ja vähentäviä toimenpiteitä Yhdysvaltojen kaikkien ohjausjärjestelmien (*control systems*) toiminnoissa. Mukana toiminnassa on muun muassa liittovaltion, osavaltioiden, omistajien, operaattoreiden ja laitevalmistajien edustajia. Toiminta tuntuu olevan hyödyllistä toimijoille myös Euroopassa, sillä informaatio on yleiskäyttöistä ja riittävän yksityiskohtaista.

Referenssi: http://www.us-cert.gov/control_systems/

CSSP on määritellyt ohjausjärjestelmille kattavat suositeltavat käytännöt (*recommended practices*). Käytännöt on yleisesti ottaen määritelty asiallisesti, mutta joissain niistä ollaan ehkä hieman liian monisanaisia tai käsittely keskittyy liialti käytännön organisatoriseen toimeenpanoon (byrokratian määrittelyyn). Käytäntöjen laadinnassa on onneksi yleensä keskitytty

- uhkien käytännönläheiseen ymmärtämiseen
- ohjausjärjestelmien haavoittuvuuksiin sekä hyökkäystapojen ja -polkujen kuvaamiseen
- käytännön toimenpiteisiin uhkien torjumiseksi.

Käytännöt kuvaavat seuraavia alueita (referenssi: http://www.us-cert.gov/control_systems/practices/)

- *defense-in-depth*-strategiat
- forensiikan suunnittelu
- palomuurien käyttöönotto
- OPC-asemien kovennus
- verkkojen haavoittuvuuksien eliminointi
- ohjelmistokorjausten hallinnan käytännöt
- modeemien turvaaminen
- WLANin turvaaminen
- ZigBee:n turvaaminen
- operatiivinen turvallisuus.

Taulukko 4. CSSP *Recommended Practices* – yhteenveto (yhteisesti kaikista).

Valintakriteeri	**Arvio**	**Selitys**
Laatu	Yleisesti ottaen hyvä laatu. Osa käytännöistä voisi olla tiiviimmin kuvattu.	Tekninen laatu yleisesti hyvä.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Käytännöt on kuvattu tarpeeksi yleisellä tasolla, jotta niitä voidaan soveltaa eri tilanteisiin. Riittävän yksityiskohtaisia kuvauksia. Kattaa sekä teknisiä aspekteja sekä operatiivisia toimenpiteitä.	Sekä käytännöllisyys että käytettävyys on otettu hyvin huomioon.
Meriitit	Ohjeet ovat hyvin todennäköisesti laajassa käytössä relevanteissa organisaatioissa Yhdysvalloissa, tosin osa ohjeista on melko tuoreita.	Ohjeiden soveltaminen aiheuttanee vain vähän virheitä tai väärinkäsityksiä.
Sääntely	Osa käytännöistä voi olla sidottu NERC-vaatimuksiin, joten ne voivat auttaa regulatiivisten vaatimusten täytäntöönpanossa.	Avustaa vaatimusten täyttämisessä.
Ylläpito ja saatavuus	Ohjeet ovat julkisesti saatavilla internetissä ja ne ovat kohtuullisen hyvin ajan tasalla.	Riittävä ylläpito.
Erityispiirteet	Teollisuusautomaation erityispiirteet on otettu käytäntöjen laadinnassa erityisesti huomioon.	Toimialan vaatimukset huomioitu erinomaisesti.

2.2.2.2 US-CERT *Control Systems Security Center* (CSSC)

US-CERT *Control Systems Security Center* (CSSC) puolestaan koordinoi (ICS-alueen)

- tietoturvatapahtumien hallintaa
- viimeisintä tietoturvan tilannetietoa
- hallinnoi haavoittuvuuksien ja riskien vähentämisaktiviteetteja.

Referenssi: http://www.uscert.gov/control_systems/.

CSSC on samalla Yhdysvaltain tietoturva-analyysin ja tietoturvatestauksen keskus, jota hallinnoi Idaho National Laboratory (INL). Toiminta perustuu

- hyvään yhteistoimintaan teollisuuden ja laitetoimittajien kanssa
- tietoturva-analyysiin ja sen tulosten hyödyntämiseen
- työkalujen kehittämiseen tietoturvan varmistamiseen
- tietoturvatietoisuuden ja ongelmiin reagoimisen vahvistamiseen.

CSSC:llä on palvelu, jossa yritys voi sopia järjestelmänsä tietoturvatestaamisesta INL:ssä, joten kaikkea yksityiskohtaista osaamista ja testilaitteistoa ei tarvitse hankkia oman yrityksen yhteyteen.

2.2.3 ISA99 *Industrial Automation and Control Systems Security Standards*

Instrumentation, Systems and Automation Society (ISA) on yhdysvaltalainen globaali automaatioteollisuuden asiantuntijoiden organisaatio, joka

- kehittää standardeja teollisuusautomaatioon
- sertifioi teollisuuden osaajia
- järjestää koulutusta ja konferensseja automaation eri osa-alueilla
- julkaisee kirjoja ja teknisiä artikkeleita.

Referenssi: http://www.isa.org/.

Samalla ISA pyrkii määrittelemään proseduureja ja kriteerejä tietoturvallisten ICS-järjestelmien kehittämiseksi ja hankkimiseksi sekä järjestelmien tietoturvan arvioimiseksi. Ohjeistaminen on yleensä suunnattu järjestelmien suunnittelijoille, toteuttajille, hallinnoijille, käyttäjille, integraattoreille sekä laitevalmistajille.

Tietoturvan standardointityö ISA:ssa sisältää perustavanlaatuisia asioita, vaikkakin osa työstä on vielä kesken:

- ISA 99.00.01 Konseptit, mallit ja terminologia (v. 2007 standardi)
- ISA 99.00.02 Tietoturvaohjelman alkuun saaminen organisaatiossa
- ISA 99.00.03 Tietoturvaohjelman operointi organisaatiossa (kesken)
- ISA 99.00.04 Tietoturvavaatimusten asettaminen järjestelmille (kesken).

Lisäksi muutama tekninen raportti (TR) on jo valmistunut:

- ANSI/ISA-TR99.00.01 (v. 2007) – *Security technologies for industrial automation and control systems*, joka määrittelee *state-of-the-art*-teknologiat, niiden heikkoudet, vastatoimet ja työkalut, jotka soveltuvat teollisuusautomaatiojärjestelmien tietoturvaamiseen. Tämä dokumentti on hyödyllinen lukea ennen suojausjärjestelmien valintaa ja asennusta. Raportti sisältää
  - käyttäjätunnistuksen ja valtuutuksen
  - pääsynvalvonnan ja suodattamisen
  - salausteknologiat ja datan autenttisuuden tarkistamisen

  - laitehallinnan, auditoinnin, mittaamisen ja monitoroinnin
  - ohjelmistot
  - fyysisen turvallisuuden kontrollit.

- ANSI/ISA-TR99.00.02 (v. 2004) – *Integrating electronic security into the manufacturing and control systems environment* antaa suosituksia seuraavista asioista:
  - sähköisten tietoturvateknologioiden käyttäminen tehokkaasti
  - tietoturvaohjelman alkuun saaminen organisaatiossa.

Taulukko 5. ISA99 – yhteenveto.

Valintakriteeri	Arvio	Selitys
Laatu	Hyvä.	Vuoden 2007 versiot TR:stä.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Käytännönläheinen ja tavoitteet oikeansuuntaiset, mutta joissain kohdin epäselvyyttä tietoturvan toteutuksen kannalta.	Hyvää taustamateriaalia asioihin perehtymiseksi.
Meriitit	ISA-lähtöisyys on meriitti automaatioteollisuudessa. ISA99:ään referoidaan yleisesti.	
Sääntely	Ei sääntele mutta tarjoaa ohjeistusta ja suunnan näyttöä.	Perustuu määritelmiin ISA-95:ssä ja IEC 15408:ssa
Ylläpito ja saatavuus	Standardit useimmiten maksullisia. Useiden dokumenttien valmistuminen on viivästynyt.	Dokumentteja päivitetään muutaman vuoden välein.
Erityispiirteet	Automaatioteollisuuslähtöinen näkökulma tietoturvaan. Järjestelmien perustoimintakyvyn vahvistaminen ensisijainen tavoite.	

2.2.4 ISO/IEC 27000 -sarja

Tämä sarja standardeja tunnetaan yleisesti nimillä (ISO:n) ISMS-standardit (*Information Security Management System*), Tietoturvanhallinnan standardit tai lyhyesti ISO27k.

27000-sarja sisältää suosituksia parhaiksi käytännöiksi yrityksen riskiarviointiin pohjautuvaan tietoturvan hallintaan ja kontrollien määrittelyyn. Standardisarjan aihepiiri on laaja, ja se tuntuu laajentuvan edelleen.

27000-sarja ehdottaa kaikkia organisaatioita identifioimaan suojattavat tietoomaisuutensa ja arvioimaan niihin liittyvät riskitekijät, minkä jälkeen organisaatio voi määritellä tarpeidensa mukaiset tietoturvan hallintajärjestelmät. Tämän tekemiseen annetaan käytännöllisiä ohjeita ja ehdotuksia. Lisäksi kehotetaan pitämään järjestelmä jatkuvasti ajanmukaisena (*Plan-Do-Check-Act*) arvioimalla muun muassa uusia riskitekijöitä, haavoittuvuuksia ja maailmalla tapahtuneita tietoturvaloukkauksia.

Julkaistuja standardeja (http://en.wikipedia.org/wiki/ISO/IEC_27000-series):

- ISO/IEC 27000 – Information security management systems — Overview and vocabulary (tästä on olemassa myös SFS:n toimittama suomenkielinen käännös)
- ISO/IEC 27001 – Information security management systems — Requirements
- ISO/IEC 27002 – Code of practice for information security management
- ISO/IEC 27003 – Information security management system implementation guidance
- ISO/IEC 27004 – Information security management — Measurement
- ISO/IEC 27005 – Information security risk management
- ISO/IEC 27006 – Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27011 – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Tulossaolevia dokumentteja (http://en.wikipedia.org/wiki/ISO/IEC_27000-series):

- ISO/IEC 27007 – Guidelines for information security management systems auditing
- ISO/IEC 27008 – Guidance for auditors on ISMS controls
- ISO/IEC 27013 – Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001

- ISO/IEC 27014 – Information security governance framework
- ISO/IEC 27015 – Information security management guidelines for the finance and insurance sectors
- ISO/IEC 27031 – Guideline for ICT readiness for business continuity
- ISO/IEC 27032 – Guideline for cybersecurity
- ISO/IEC 27033 – IT network security
- ISO/IEC 27034 – Guideline for application security
- ISO/IEC 27035 – Security incident management
- ISO/IEC 27036 – Guidelines for security of outsourcing
- ISO/IEC 27037 – Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Taulukko 6. ISO/IEC 27001-27006 – yhteenveto.

Valintakriteeri	**Arvio**	**Selitys**
Laatu	Korkealaatuisia dokumentteja.	Osa drafteista voi olla epätasaisia laadultaan.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Erittäin yleiskäyttöisiä standardeja, silti usein riittävän yksityiskohtaisia. Laaja kattavuus eri alueille. Ongelmana laaja sivumäärä.	Olemassa myös yksinkertaistettuja sovelluksia standardista.
Meriitit	Erittäin paljon käytössä eri alojen organisaatioissa, myös ICS-alueella.	Eri organisaatioista löytyy lukuisia sovelluksia tästä standardista.
Sääntely	Ei aseta varsinaista sääntelyä. Määrittelee kuitenkin sertifiointitoimintaa. Toimijat voivat toki asettaa vaatimuksia tämän standardin käyttämisestä ja sertifioinnista.	
Ylläpito ja saatavuus	Ohjeet hyvin päivitettyjä mutta usein maksullisia.	
Erityispiirteet	Kattavuus laaja, joten monia automaation erityispiirteitä mukana.	Kannattaa vielä räätälöidä automaatiospesifiksi.

Referenssi: esimerkiksi http://www.27000.org/.

2.2.4.1 ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*

ISO 27001 on hyvä referenssi sellaisen järjestelmän rakentamiseen, joka suojaa organisaatiota tietoriskeiltä. Tavallaan se on myös geneerinen spesifikaatio oman tietoturvan hallintajärjestelmän (ISMS) rakentamiseen. ISO 27001 on samalla hyvä perusta kolmansien osapuolten tekemille auditoinneille ja sertifioinneille antaessaan mahdollisuuden ulkoistaa tarkastustoimintaa. ISO 27001 -standardia voidaan periaatteessa soveltaa mille tahansa organisaatiolle, mutta se on tarpeen ennen kaikkea elintärkeää tietoa generoiville ja käsitteleville toimialoille (kuten automaatioteollisuus). Standardia käytetään yhdessä ISO 27002:n kanssa.

Määrätyt akkreditoidut sertifiointiorganisaatiot voivat sertifioida organisaatioita ISO/IEC 27001 -yhteensopiviksi. Sertifioitiin vaadittavat auditoinnit tekee (tavallisesti) ISO/IEC 27001 *Lead Auditor*.

2.2.4.2 ISO/IEC 27002: *Security Techniques – Code of Practice for Information Security Management*

ISO 27002 määrittää ohjeita ja suosituksia tietoturvan hallitsemiseksi. Esimerkiksi yksittäiset kontrollit voidaan vaatia mukaan organisaatiokohtaisesti. Spesifikaatiossa asioita käsitellään määriteltyinä käytäntöinä (*policy*) ja hyvinä toimintatapoina (*good practices*). Tämä spesifikaatio antaakin hyviä malleja organisaatiospesifisten tietoturvaohjeistusten rakentamiseksi.

Dokumentti käsittelee seuraavia asioita:

- riskien arviointi (kukin organisaatio tekee ensin arvion, johon sitten muut valinnat pohjautuvat)
- organisaation tietoturvapolitiikka
- organisaation tietoturvainfrastruktuuri
- suojattavien omaisuuksien luokittelu ja hallinta
- henkilöstöturvallisuus
- fyysinen turvallisuus ja ympäristön turvallisuus
- kommunikaation ja toimintojen hallinta
- pääsynvalvonta
- järjestelmien hankinta, kehittäminen ja ylläpito

- tietoturvatapahtumien hallinta
- liiketoiminnan jatkuvuuden hallinta
- tietoturvavaatimusten toteutuminen.

2.2.4.3 ISO/IEC 27033: *Guidelines for network security*

ISO/IEC 27033 on tulossa oleva IEC-standardi. Tällä hetkellä standardiluonnos kattaa paljon tärkeitä asioita mutta on hieman sekava ja keskeneräisen tuntuinen. Tästä standardista voi poimia joitain asioita ICS-yhteydessä käytettävien verkkojen ja niiden tietoturvan suunnitteluun. Lopussa on hyvä listaus eri verkkoteknologioiden tietoturvariskeistä ja keinosta niiden hallitsemiseksi.

2.2.4.4 ISO/IEC 27035: *Information security incident management*

Myös ISO/IEC 27035 on tulossa oleva standardi. Nykyinen versio on keskeneräisen tuntuinen ja toistaa itseään. Silti dokumentissa on hyviä ajatuksia siitä, mitä asioita tietoturvatapahtumien yhteydessä tulisi seurata. Lopussa on laaja mallipohja tietoturvatapahtumien raportointiin, joka mahdollistaa muun muassa selkeän tietoturvatapahtumien luokittelun ja yksityiskohtien ylläpidon.

2.2.5 NIST 800 *Series Security Guidelines*

Yhdysvaltain *National Institute of Standards and Technology (NIST)* -organisaatiossa on *Computer Security* -osasto, joka on pitkään työstänyt laadukkaita standardeja ja ohjeistoja erilaisiin tietoturvateknologioihin. Osaston työ keskittyy muun muassa seuraaviin asioihin:

- kryptografian soveltaminen
- tunnistusmenetelmät, julkisen avaimen infrastruktuuri (PKI)
- verkkoyhteyksien tietoturva
- tietoturvakriiteeristöt ja tietoturvan varmistaminen
- tietoturvan hallinta ja tuki.

Tärkein standardiluonnos, joka liittyy suoraan teollisuusautomaation tietototurvaan, on NIST SP 800-82 *Guide to Industrial Control Systems (ICS) Security*, jossa käydään läpi muun muassa ICS-järjestelmien haavoittuvuudet, tietoturvan hallinnan organisointi, verkkoarkkitehtuuri, sekä spesifit tietoturvakontrollit.

Seuraavassa on listattu muita NIST SP 800 -sarjan dokumentteja, joilla on yhteys teollisuusautomaation tietoturvaan:

Referenssi: http://csrc.nist.gov/publications/nistpubs/index.html.

- NIST SP 800-40 *Creating a Patch and Vulnerability Management Program*
- NIST SP 800-41 *Guidelines on Firewalls and Firewall Policy*
- NIST SP 800-42 *Guideline on Network Security Testing*
- NIST SP 800-48 *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*
- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*
- NIST SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems*
- NIST SP 800-61 *Computer Security Incident Handling Guide*
- NIST SP 800-63 *Electronic Authentication Guideline*
- NIST SP 800-64 *Security Considerations in the Information System Development Life Cycle*
- NIST SP 800-70 *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*
- NIST SP 800-77 *Guide to IPSec VPNs*
- NIST SP 800-83 *Guide to Malware Incident Prevention and Handling*
- NIST SP 800-86 *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-88 *Guidelines for Media Sanitization*
- NIST SP 800-92 *Guide to Computer Security Log Management*
- NIST SP 800-94 *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST SP 880-97 *Guide to IEEE 802.11i: Robust Security Networks.*

Lisäksi NISTissä on käynnissä ICS-spesifinen tietoturvaprojekti, jossa otetaan huomioon, että SP 800-53 -tietoturvakontrolleja voi olla vaikea soveltaa sellaisenaan ympäristöön, jossa on modernien laitteiden seassa esimerkiksi 25 vuotta vanhaa laitteistoa ja ohjelmistoa. Projektissa tuotetaan yhdessä julkisen ja yksityisen sektorin kanssa erityinen ohjeistus tärkeimpien NIST-standardien kuvaamien tietoturvakontrollien soveltamisesta ICS-ympäristöön.

Taulukko 7. NIST SP 800 -sarja – yhteenveto.

Valintakriteeri	**Arvio**	**Selitys**
Laatu	Erittäin korkea laatu sekä teknisissä että hallinnollisissa kysymyksissä.	Laajat katselmoinnit ja yhteisön hyväksikäyttö.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Ohjeet ovat varsin yleiskäyttöisiä. Osa ohjeista on hyvin spesifisiä kuten kryptografisten funktioiden toteutus, osa taas yleisempiä teknologioiden turvalliseen käyttöön ja soveltamiseen liittyviä. Yhdessä ohjeet kattavat laajoja kokonaisuuksia.	Ohjeistojen käytännöllisyys- ja käytettävyystekijät ovat kunnossa.
Meriitit	Dokumentaatio on erittäin laajasti käytössä ympäri maailman, ja niihin referoidaan usein.	
Sääntely	Yhdysvaltain liittovaltion toimistojen on noudatettava FIPS-standardeja. Myös SP-luokan standardeja on noudatettava useimmissa liittovaltion toimistoissa.	Laajasti käytössä kansallisten velvoitteiden ansiosta.
Ylläpito ja saatavuus	Ohjeita päivitetään hyvin viimeistelyvaiheessa, ja lopputulos on tarkka. Jotkut dokumentit voivat olla vanhoja. Dokumentit ovat julkisesti saatavilla internetissä.	
Erityispiirteet	Soveltuvat jo yleisestikin erittäin hyvin automaatioteollisuuden käyttöön teknisestä ja käytännöllisestä lähestymistavasta johtuen. Lisäksi ollaan työstämässä ICS-spesifisiä ohjeita.	Laatu ja käyttövarmuusominaisuudet käsi kädessä.

Referenssi: http://csrc.nist.gov/groups/SMA/fisma/ics/.

2.2.6 MSISAC/SANS*: SCADA and Control Systems Procurement Language*

Yhdysvaltain *Homeland Security* -hallinto on sponsoroinut ns. *SCADA Procurement* -projektia, jossa on ollut mukana *Idaho National Laboratory* (INL), New Yorkin osavaltion *Multi-State Information Sharing Analysis* -keskus (MSISAC) sekä *System Audit Network Security* (SANS) -instituutti. Lisäksi mukana auttamassa on ollut muun muassa automaatioalan yrityksiä, teknologiatoimittajia sekä viranomaisia.

Projektin tuloksena oli yhteinen *Procurement Language* -dokumentti, jota mikä tahansa ohjausjärjestelmien alueella toimiva organisaatio voisi käyttää. Lopputuloksen avulla voidaan yhtenäisellä tavalla määritellä tietoturvavaatimuksia ICS-järjestelmien hankintatoimeen liittyen. Tiettyyn käyttötarkoitukseen tulevan järjestelmän tilaajan täytyy tietenkin itse tarkasti tietää, mitkä osuudet tästä ”vaatimuskannasta” ovat heidän toiminnassaan tärkeitä ja kuinka tarkkaa vaatimusten toteuttamista automaatiojärjestelmätoimittajalta todellisuudessa vaaditaan.

Referenssi: http://www.msisac.org/scada/.

Dokumentti sisältää vaatimusmäärittelyt seuraavista asiakokonaisuuksista:

- järjestelmän kovennus
- ympäristön (mm. verkkojen) suojaus
- käyttäjätilien hallinta
- koodauskäytännöt
- vikojen käsittely
- haittaohjelmilta suojaaminen
- verkko-osoitteiden ja nimien toiminnallisuus
- päätelaitteet
- etäyhteydet
- fyysinen turvallisuus
- verkon segmentointi.

Kunkin asiakokonaisuuden tietty alakokonaisuus (esim. ”tarpeettomien palvelujen ja ohjelmistojen poistaminen”) sisältää muun muassa seuraavat määrittelyt:

- vaatimuksen tarpeen perustelu, esimerkiksi relevanttien haavoittuvuuksien kuvaus
- esimerkkivaatimukset tietoturvasta
- FAT-testauksen toimenpiteet tai vaatimukset

- SAT-testauksen toimenpiteet tai vaatimukset
- ylläpito-ohjeistus.

Taulukko 8. MSISAC/SANS: *SCADA and Control Systems Procurement Language* – yhteenveto.

Valintakriteeri	Arvio	Selitys
Laatu	Korkea laatu.	
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Erittäin käyttökelpoinen ja yleiskäyttöinen dokumentti. Ohjeet tuntuvat riittävän kattavilta.	Helppo käyttää.
Meriitit	Dokumentti on tuoreudestaan huolimatta jo mainittu useissa yhteyksissä.	Soveltajina Yhdysvaltain ICS-alueen toimijat.
Sääntely	Ohjeistus sovellettavaksi; ei aseta itsessään eksakteja vaatimuksia toimijoille.	Toimijat voivat dokumenttia soveltamalla asettaa vaatimuksia toisilleen.
Ylläpito ja saatavuus	Vaikuttaa olevan hyvin ylläpidetty dokumentti, ja on hyvin saatavilla internetissä.	
Erityispiirteet	Dokumentti on räätälöity ohjausjärjestelmäsektorin toimijoiden käytettäväksi.	Toimialan vaatimukset huomioitu hyvin, mm. käyttövarmuus.

2.3 Öljy- ja kaasualojen standardit

2.3.1 American Gas Association (AGA) Standard 12, Cryptographic Protection of SCADA Communications

AGA eli *American Gas Association* on yhdistys, joka edustaa yli kahtasataa paikallista energiayhtiötä, jotka toimittavat maakaasua Yhdysvalloissa. AGA palvelee jäsenyrityksiä erilaisilla teknisillä komiteoilla sekä muilla ohjelmilla ja palveluilla, mutta toimintaan liittyy avoimuutta ja yleisesti saatavilla olevaa informaatiota, esimerkiksi *American Gas Magazine*, ks. http://www.aga.org/. AGA ei ole viranomainen, joten sille ei kuulu sääntely eikä se järjestä valvontaa esimerkiksi toimintaohjeiden noudattamisesta.

Tekninen komitea *Natural Gas Security* pitää sisällään mielenkiintoisia alueita kuten *Cyber Security*, *Consolidated Edison's Security Operations Center* (SOC), *AGA Membership Security Skills Database* ja *Gas Measurement Fraud*.

Muutamia vuosia sitten perustettiin *AGA 12 Task Group*, jossa AGA ja GTI (*Gas Technology Institute*) kehittivät yhdessä viranomaisten, laitevalmistajien ja SCADA-asiantuntijoiden kanssa dokumentteja aihealueesta *Cryptographic Protection of SCADA Communications.* Näihin dokumentteihin monien yhteneväisyyksien takia myös vesi- ja sähköaloihin liittyvät SCADA-järjestelmät, ja näiden alojen yhtiöt otettiin mukaan määrittelytyöhön. N*orth American Electric Reliability Corporation* (NERC) seurasi aktiivisesti dokumentin edistymistä. Raportit nimettiin seuraavasti:

- AGA 12, *Part 1: Cryptographic Protection of SCADA Communications: Background, Policies & Test Plan*
- AGA 12, *Part 2: Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications*
- AGA 12, *Part 3: Cryptographic Protection of SCADA Communications: Protection of Networked Systems*
- AGA 12, *Part 4: Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components.*

Nämä dokumentit pyrkivät muun muassa säästämään SCADA-operaattoreiden aikaa ja työmäärää tarjoamalla kattavan mallin tai järjestelmäkuvauksen SCADA-tietoliikenteen suojaamiseksi.

Ainoastaan ensimmäistä (*Part 1*) dokumenttia on tässä arvioitu tarkemmin; muiden osien saatavuus ja status olivat kirjoittajalle vielä epäselviä.

AGA 12 (*Part 1*) -dokumentti

- edellyttää, että operaattori tekee aluksi tietojärjestelmänsä riskianalyysin, arvion vahinkojen seurauksista ja niiden kustannuksista jne.
- kuvaa yrityksen tietoturvakäytäntöjen perusteet (tietoturvapolitiikka, arviointi, auditointi)
- kokoaa hyödyllistä taustatietoa muun muassa yrityksen tietoturvaarviointia varten
- antaa tietoa yrityksen tietoturvatavoitteiden määrittelemiseksi sekä esittää suojausjärjestelmän kryptovaatimukset
- esittää kryptojärjestelmän testisuunnitelman.

Taulukko 9. AGA 12 – yhteenveto.

Valintakriteeri	Arvio	Selitys
Laatu	Hyvä laatu. Informaatio on tarkkaa ja tuntuu tukevan tietoturvan yksityiskohtaista toteuttamista.	Tietoturva- ja tietoliikenneasiantuntijoiden katselmoima.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Dokumentti on erittäin käyttökelpoinen ja yleiskäyttöinen kuvatuilla toimialoilla. Laaja kattavuus. Voidaan käyttää mm. järjestelmätilaajan vaatimusten laadinnassa.	Sisältää asiaa taustoittavia, selittäviä osuuksia, jotka auttavat mm. ratkaisun räätälöinnissä.
Meriitit	Tunnustettu hyväksi perustyöksi. Laadittu laajassa yhteistyössä eri alojen asiantuntijoiden kesken.	*Part 1*:tä referoitu monissa yhteyksissä.
Sääntely	Käytetään ohjeen (*guideline*) tavoin. Ei sääntele mutta sisältää mm. vaatimuksia, joita voidaan soveltaa eri käyttötarkoituksiin.	Mm. FIPS PUB 140-2 -kelpoisuus vaadittu, ym. NIST-vaatimuksia.
Ylläpito ja saatavuus	*Part 1* (14.3.2006) saatavilla vapaasti internetistä. Nyt muutama yksityiskohta saattaa olla jo hieman vanhentunutta.	Muiden osien saatavuus ja tila epävarma.
Erityispiirteet	Määrittelee melko tarkasti esimerkkitoteutuksen mm. toimintatavoista, vaatimuksista ja suojausjärjestelmistä kaasu- vesi- ja sähköaloille.	

2.3.2 American Petroleum Institute (API) Standard 1164, Pipeline SCADA Security

API eli *American Petroleum Institute* (http://www.api.org/) on Yhdysvaltojen kansallinen kauppaliitto, joka yhdessä edustaa lähes kaikkia maan öljy- ja maakaasuteollisuuden näkökantoja. Yli neljäsataa jäsenorganisaatiota saa sen kautta käyttöönsä API Std 1164 -standardin, jonka ensimmäinen painos ilmestyi syyskuussa 2004 sekä toinen painos kesäkuussa 2009. Uutta painosta varten tehtiin katselmointi, jossa selvitettiin asiantuntijoiden avulla muun muassa teknologian kehittymisestä johtuvat muutokset, uusimpien standardien vaatimukset ja NIS-Tin määrittelemä *Catalog of Control System Security Requirements.*

API 1164 perustaa ohjeensa sille, että (*pipeline*-) operaattori ymmärtää SCADA-järjestelmänsä haavoittuvuudet ja riskit hyvin kokonaisvaltaisesti, ei pelkästään erillisinä teknisinä yksityiskohtina. Ensimmäinen versio standardista

pyrki ohjeistamaan eritoten pieniä ja keskisuuria *pipeline*-operaattoreita tietoturvakäytännöissään; toisessa versiossa ohjeisiin tuli pieniä laajennuksia. Ohjeiston käyttötarkoitus ei ole sertifiointi tai edes vaatimuksien määrittely omaehtoista sertifiointia varten, sillä API 1164 ei ole millekään organisaatiolle suoraan sopiva kuvaus vaadittavista tietoturvamekanismeista tai käytännöistä. Pikemminkin se on vakioitu ja yksinkertaistettu lista tietoturvaan liittyvistä teollisuudenalan parhaista käytännöistä, joka voidaan ottaa lähtökohdaksi yrityskohtaisen ohjeistuksen laatimisessa.

Standardin toinen painos sisältää seuraavien asioiden lyhyen käsittelyn (melko yleisellä tasolla):

- tietoturvan hallintajärjestelmä (ISMS)
- fyysinen turvallisuus
- järjestelmän pääsynvalvonta
- jaettavan informaation luokittelu
- verkon suunnittelu ja datansiirto (mm. suositeltu yksinkertainen DMZ implementaatio)
- kenttälaitteiden turvallisuus.

Lisäksi standardi kuvaa erillisillä liitteillä yksityiskohtaisesti seuraavat asiat:

A. tarkistuslistat SCADA-järjestelmän tietoturvan katselmointiin tai evaluointiin
B. esimerkin SCADA- tai kontrollijärjestelmän tietoturvasuunnitelmasta.

Erityisesti nämä liitteiden tarkistuslistat on kirjoitettu melko selkeästi ja riittävällä tarkkuudella, joten niistä on todellista hyötyä SCADA-järjestelmän tietoturvaa arvioitaessa ja kehitettäessä.

Taulukko 10. API – yhteenveto.

Valintakriteeri	Arvio	Selitys
Laatu	Hyvä laatu. Runkotekstissä yleisellä tasolla tärkeimpien tietoturvatoimintojen kuvaus, liitteissä tarkemmat esimerkit.	Toisen painoksen kehitys tehty laajassa asiantuntijaryhmässä.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Käyttökelpoisuus erittäin hyvä. Dokumentti on helpompi lukea ja soveltaa kuin monet muut referenssit. Toisaalta puutteena suppeampi kattavuus, sillä dokumentti on melko lyhyt ja tiivis.	Keskittyy tietoturva-asioiden saamiseen hallintaan nopeasti mutta perustellusti.
Meriitit	Yhdysvaltain öljy- ja maakaasuteollisuus voimavaroineen taustalla. Sovellettu monissa organisaatioissa.	Viitataan useissa yhteyksissä kansainvälisestikin.
Sääntely	API-organisaatio ei aseta sääntelyä eikä sertifiointia.	Toimialakohtainen itsesääntely voisi hyödyntää tätä.
Ylläpito ja saatavuus	Hyvä ylläpito. API-standardit katselmoidaan ja päivitetään pääsääntöisesti vähintään kerran viidessä vuodessa. Maksullinen.	Kuka tahansa voi hankkia standardin käyttöönsä. Hinta noin $ 150.
Erityispiirteet	Valitut palat sovellettavaksi *pipeline*-operaattoreille. Sisältää tärkeimpiä hallinnollisia ja teknisiä aspekteja tietoturvan kehittämiseen.	Tiivis ja yksinkertaistettu esitys.

2.4 Sähköenergia-alan standardit

2.4.1 North American Electric Reliability Corporation (NERC) – CIP Standards

Vuodesta 1968 lähtien *North American Electric Reliability Corporation* (NERC) on toiminut aktiivisesti Pohjois-Amerikan sähkönsiirtoon liittyvien järjestelmien **luotettavuuden ja käyttövarmuuden** varmistamiseksi. NERC on itsesääntelevä (*self-regulatory*) organisaatio, joka ei ole osa Yhdysvaltain hallitusta vaan toimeenpaneva yksikkö. Käytännössä tämä tarkoittaa, että NERCillä on lakisääteinen vastuu säännellä sähkönsiirtoon liittyvien järjestelmien käyttäjien, omistajien ja operaattoreiden toimia. Tämä toteutetaan maanlaajuisesti muun muassa standardien määrittelyn sekä valvonnan keinoin, käyttäen hyväksi paikallisia käyttövarmuutta varmistavia organisaatioita ja -koordinaattoreita. (http://www.nerc.com/.)

Nämä NERCin laajoilla valtuuksillaan määrittelemät käyttövarmuusstandardit ovat käytännössä **suunnittelusääntöjä ja toimintaohjeita**, joita alan toimijoiden on noudatettava ja joiden avulla käyttövarmuutta ja luotettavuutta yritetään parantaa merkittävästi sekä paikallisesti että laajempien sähkönsiirtojärjestelmien tasolla. Itse standardeja kehitetään NERCin standardisointikomiteassa teollisuusvetoisesti ANSI-akkreditoidulla prosessilla, joka on avoin kaikille, jotka ovat relevanteissa organisaatioissa tekemisissä ko. järjestelmien kanssa. Lopputuloksena syntyneet hyväksytyt standardit ovat vapaasti saatavilla internetissä.

Ensimmäiset määrättyjä toimijoita sääntelevät käyttövarmuusstandardit tulivat voimaan kesäkuussa 2007, ja päivitys näihin dokumentteihin on tehty toukokuussa 2009. Mukana on joukko tietoturvalle oleellisia CIP (*Critical Infrastructure Protection*) -standardeja.

NERC CIP -standardit määrittelevät toiminnalliset vaatimukset seuraaville asioille:

CIP-001: sabotaasien raportointi (tätä ei normaalisti sisällytetä automaatiostandardeihin)

CIP-002: kriittisen tietopääoman tunnistaminen

CIP-003: turvallisuuden hallinnan kontrollit (minimikontrollit kriittisten tietopääomien suojaamiseksi)

CIP-004: henkilöstö ja tietoturvakoulutus (henkilöstön koulutus, tietoturvatietoisuus ja mm. henkilöiden taustan tarkistaminen)

CIP-005: suojattavien kohteiden vyöhykkeen (*electronic perimeter*) tunnistaminen ja suojaus (sis. liityntäpisteet)

CIP-006: kriittisen tietopääoman fyysinen turvallisuus

CIP-007: järjestelmien turvallisuuden hallinta (metodit, prosessit ja proseduurit järjestelmien kriittisten tietopääomien suojaamiseksi)

CIP-008: tietoturvaloukkausten ja -tapahtumien raportointi ja reagointisuunnitelmat (sis. tapahtumien tunnistamisen ja luokittelun)

CIP-009: toipumissuunnittelu (kriittisten tietopääomien palautussuunnitelmat, ottaen huomioon liiketoiminnan jatkuvuuden ja onnettomuuksista toipumisen tekniikat ja -käytännöt).

Taulukko 11. NERC CIP – yhteenveto.

Valintakriteeri	Arvio	Selitys
Laatu	Hyvä laatu. Standardoinnin kohteeksi valitut alueet on kuvattu selkeällä ja koherentilla tavalla. Sääntelee mitkä prosessit ja dokumentit on oltava määriteltynä ja käytössä eri toimijoilla.	Mm. NERCin *Board of Trustees* -katselmointistandardit.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Erittäin käyttökelpoinen operaattoreille perusohjeiston ja tietoturvan hallinnan prosessien laatimiseksi. Hyödyllinen perusvaatimusluettelo laitevalmistajille referenssiksi vaatimuksista.	Ei kuitenkaan yleensä määrää (teknisen) toteutuksen tapaa.
Meriitit	Erittäin laajasti käytetty ja referoitu, myös Pohjois-Amerikan ulkopuolella. Vahva sääntely, joka vaikuttaa alkuperäisen alueen ulkopuolellakin laajasti.	NERC sertifioi organisaatioita. Tästäkin on standardeja tulossa.
Sääntely	NERCillä lakisääteinen vastuu säännellä ja valvoa sähkönsiirron toimijoita luotettavassa toiminnassa. Sisältää mm. raportointivelvoitteen, auditit sekä tarvittaessa tutkinnan. NERC vastaanottaa dataa mm. kahdeksalta paikalliselta koordinaattorilta.	Yhdysvaltain liittovaltion energiakomissio (+ Kanada) hyväksyy standardit laillisesti sitoviksi.
Ylläpito ja saatavuus	Hyvä saatavuus ja ylläpito. Lisäksi NERCillä on reaaliaikainen tilannetietoisuusjärjestelmä.	+ESISAC uhkien ja tapahtumien seuranta.
Erityispiirteet	Pyrkii saamaan sähkölaitosten ja sähkönsiirtojärjestelmien kokonaisuuden käyttövarmuuden hallintaan Pohjois-Amerikassa.	Häiriöiden (Events) analyysi keskitetysti NERC:issä.

2.4.2 IEEE 1686 – *Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*

IEEE *Power Engineering Societyn* standardi (Std) 1686 (hyväksytty 5. joulukuuta 2007) ei pyri olemaan paras tai suositeltu tietoturvakäytäntö, vaan sen tarkoituksena on esittää joukko tietoturvaan liittyviä vähimmäisvaatimuksia (*baseline*) SCADA-järjestelmissä käytetyille älykkäille kenttälaitteille. Taustalla on NERC CIP-standardien operaattoreille asettamat vaatimukset, joiden täyttämiseksi tarvitaan sekä laitteiden tilaajia että toimittajia koskevat konkreettiset vaatimukset laitteiden tarjoamille tietoturvaominaisuuksille. Standardin erityispiirre on, että laitetoimittajan on esitettävä tarkkaan määritelty ns. *Table of Compliance*, jossa

tuki kullekin standardin vaatimukselle täytyy esittää erillisellä rivillä tietyssä formaatissa (*Acknowledge, Exception, Comply, Exceed*). Esimerkkitaulukko tästä on esitetty standardin Annex A:ssa. Kentällä laitteen on toki oltava muun muassa turvallisesti konfiguroitu, testattu ja ylläpidetty, joten laitteen IEEE 1686 -tuki ei vielä yksin takaa SCADA-operaattorin tietoturvatavoitteiden toteutumista.

Referenssi: http://www.ieee.org/web/standards/home/index.html.

Standardissa määriteltäviä kenttälaitteen turvallisuusominaisuuksia ovat muun muassa seuraavat:

Pääsynvalvontaan liittyvät ominaisuudet:

- kunnollinen salasanasuojaus, suojauksen kiertämisen valvonta, tunnusten minimimäärä
- erilaiset valtuutustasot eri tunnuksille (kuten datan tai konfiguraation lukuoikeus, muutostenteko-oikeudet eri toiminnoille, pakotetut asetukset, lokin seuranta)
- istunnon kesto.

Lokiseurannan (tapahtumat *first-in-first-out*-menetelmällä ASCII-tiedostoon) ominaisuudet:

- tapahtumien (Events) tallennuskapasiteetin minimimäärä
- lokirekisterin sisällön kuvaus
- tallennettavien tapahtumien tyyppien määrittely.

Tietoturvaan liittyvä kenttälaitteen reaaliaikainen monitorointitoiminnallisuus (keskitetty seuranta tapahtuu valvontakeskuksessa):

- tapahtumien (*events*) ja hälytysten (*alarms*) määrittely ja ryhmittelymahdollisuus
- valvontakeskuksen operaattorin pakottama kenttälaitteen kontrollien sääntely.

Lopussa määritellään lyhyesti vielä konfiguraatio-ohjelmiston tietoturvaaminen (mm. autenttisuus ja pääsynvalvonta), tietoliikenneporttien aktivointi tai passivointi sekä nimetään Firmwaren laadunvalvontastandardi.

Taulukko 12. IEEE 1686 – yhteenveto.

Valintakriteeri	Arvio	Selitys
Laatu	Hyvä. IEEE:ssä katselmoitu standardi.	Viitteitä ja tarkennuksia voisi olla enemmän.
Käyttökelpoisuus, yleiskäyttöisyys ja kattavuus	Erittäin käyttökelpoinen kenttälaitteiden vaatimusmäärittelyssä. Kattaa NERC CIP -standardien vaatimuksia. Voidaan käyttää evaluoinnissa.	Taustalla käytännön tarve olla yhteensopiva NERC CIP -vaatimuksiin.
Meriitit	NERC-vaatimusten käytännön toteutus sähköenergia-alan yrityksissä. Laitevalmistajat.	Paljon soveltajia.
Sääntely	Ei sääntele suoraan. Ei pakota toteuttamaan toiminnallisuutta tietyllä tekniikalla.	*Table of Compliances-sa* oltava tarkka kuvaus toteutetuista ominaisuuksista.
Ylläpito ja saatavuus	Maksullinen, saatavissa PDF:nä heti. IEEE-standardit ylläpidetään järjestelmällisesti, mutta esim. päivitys tai korjaus voi yllättää.	Standardi saatavilla hintaan noin $ 80.
Erityispiirteet	Yksinkertainen ja selkeä standardi tietoturvaominaisuuksien konformanssia varten.	Standardi on vain 15 sivua liitteineen.

2.5 Vaatimusten oletettuja vaikutuksia automaatiojärjestelmien tietoturvaan

2.5.1 Yleistä

Käytäntö monessa yrityksessä on osoittanut, että tietoturvavaatimusten johdonmukainen kirjaaminen sekä implementointi käytäntöön ovat molemmat varsin ongelmallisia tehtäviä. Monissa tapauksissa tietoturvavaatimusten kirjaaminen on saatettu kyllä aloittaa, mutta vaatimuslistan ylläpito esimerkiksi yrityskohtaisen tietoturvavyöhykkeiden systemaattiseksi hallitsemiseksi on ollut harvinaista. Laitteita ja ohjelmistoja on luultavimmin tilattu eri laitevalmistajilta jopa ilman tarkkaa tietoa niiden tietoturvaominaisuuksista. Niinpä onkin selvää, että vaatimuksilla ei ole juurikaan positiivisia vaikutuksia, ellei niitä panna laaja-alaisesti käytäntöön.

Aiemmissa luvuissa kuvatut standardit ja parhaat käytännöt sisältävät monissa tapauksissa jokseenkin samansuuntaisia ohjeita tai vaatimuksia tietoturvanhallinnan eri osa-alueille. Eräissä tapauksissa samankaltaisten ohjeiden oletettu

soveltamiskohde on kuitenkin erityyppinen: kohteena voi olla esimerkiksi sähköenergia-alan toimijaan erityisesti kohdistuva vaatimus yleisemmän vaatimuksen sijasta. Tämä ei kuitenkaan tarkoita sitä, ettei energia-alalla päteviä vaatimuksia voisi soveltaa prosessiteollisuudessa tai muussa tuotannollisessa teollisuustoiminnassa. Jos tietyn teollisuuden toimialan vaatimuksia on taiten ja menestyksellisesti sovellettu muualle, siirtyvät standardin positiiviset tietoturvavaikutukset laajemmalle kuin alun perin oli ehkä määritelty. On myös muistettava, että tietylle toimialalle määriteltyjen standardien lähtökohtina ovat usein olleet tietoturvan yleisemmät hallinnan standardit, joten synergioita ja riippuvuuksia eri standardien välillä on paljon. Kukin tapaus vaatii joka tapauksessa aina omat soveltamispohdintansa ja yksityiskohtansa.

Muun muassa näistä seikoista johtuen seuraavassa pyritään listamaan edellä esitellyissä standardeissa ja parhaissa käytännöissä kuvattujen vaatimusten yleisiä vaikutuksia niitä soveltavien yksikköjen, kuten teollisuuslaitosten ja siellä käytettävien kohdejärjestelmien, tietoturvaan. Toisin sanoen tässä ei pyritä esittämään esimerkiksi kokeellisiin tutkimuksiin perustuvia johtopäätöksiä vaan pikemminkin motivoimaan potentiaalisia soveltajia ottamaan tietoturvan hallinnan standardeja systemaattisesti käyttöön.

2.5.2 Yleisiä vaikutuksia tietoturvaan

Tietoturvan asiaankuuluva hallinta vaikuttaa luonnollisesti siihen, että alttius teollisen normaalitoiminnan jatkumista uhkaaville erilaisille tekijöille pienenee. Se, mitä nämä erilaiset operatiivisen toiminnan uhkatekijät yksityiskohdissaan ovat, riippuu luonnollisesti hyvin paljon tarkasteltavan teollisuuslaitoksen ominaisuuksista ja tavoitteista. Esimerkiksi laitoksen sijainti sekä sen tietojärjestelmien ja tietoliikenteen toteutus ja ylläpito vaikuttavat erilaisten tietoturvariskien realisoitumisen todennäköisyyteen erittäin paljon.

Tietoturvastandardien ja -käytäntöjen menestyksellisellä soveltamisella on muun muassa seuraavia **positiivisia vaikutuksia**:

- Altistus **operatiivisen toiminnan jatkumista** uhkaaville tekijöille pienenee, jolloin myös toimintahäiriöiden ja -katkosten negatiiviset vaikutukset yrityksen liiketoiminnalle ja maineelle pienenevät.
- Laitoksen toiminnan **riskejä voidaan tunnistaa entistä paremmin** ja laatia suuremmilta vahingoilta suojaavia varautumissuunnitelmia jo ennakkoon.

- **Väestön yleinen turvallisuus paranee** laitosten toimintahäiriöiden vähentyessä.
- Toiminnan turvallisuutta ja henkilötietojen käsittelyä säänteleviä **lakeja ja asetuksia** voidaan noudattaa paremmin.
- Suojaavat toimenpiteet osataan kohdistaa **kustannustehokkaimmalla tavalla** kriittisiin kohteisiin.
- **Automaatiojärjestelmät toimivat häiriöittä** tietoturvahyökkäysten uhatessa.
- Tietoturvatapahtumien sattuessa **negatiiviset vaikutukset voidaan minimoida** ja siirtyä reagointisuunnitelman mukaisesta toiminnasta nopeasti takaisin normaalimuotoiseen operatiiviseen toimintaan.
- Haittaohjelmat ja niiden torjuntajärjestelmät **eivät aiheuta häiriöitä tietojärjestelmiin** tai tietoliikenteen sujuvuuteen, jolloin sekä teollisuus- että toimistoverkot säilyttävät kykynsä normaaliin liiketoimintaan.
- Laitteisiin ja ohjelmistoihin soveltuvat tietoturvaominaisuudet **estävät laitteiden asiattoman käytön ja konfiguroinnin** muun muassa rikollisiin tai muuten haittaa tuottaviin tarkoituksiin.
- Laitteiden ja ohjelmistojen **tilaaminen ja ylläpito yksinkertaistuvat**, sillä tietoturvavaatimuksia osataan esittää yhtenevästi, ja odotukset tietoturvan ylläpitämiseksi vaadittavista tilauksista, kustannuksista ja ylläpidosta ovat realistisia.

Toisaalta tietoturvastandardien ja -käytäntöjen soveltamisella voi olla myös **negatiivisia vaikutuksia** yrityksissä:

- Järjestelmien ja toiminnan määrittely vaatii **alkuvaiheessa enemmän työtä**.
- Tietoturva-asioihin perehtyminen **vie työaikaa muulta toiminnalta**.
- Henkilön **osaaminen saattaa olla riittämätöntä** tietoturva-asioiden käsittelyyn (mikä saattaa johtaa henkilöstön vaihtuvuuden lisääntymiseen).
- Mikäli laitoksen tai yksikön varsinaista ydintoimintaa ei ymmärretä tarpeeksi syvällisesti, saatetaan lisäämällä tietoturvamekanismeja ilman asiantuntemusta heikentää operatiivisen toiminnan käyttövarmuutta ja lopulta vaarantaa jopa yleistä turvallisuutta.

2.5.3 Lyhyt yhteenveto eri standardien yleisistä vaikutuksista

Seuraavassa taulukossa esitetään laatimamme yhteenvedon tärkeimpien standardien ja parhaiden käytäntöjen yleisistä vaikutuksia automaatiojärjestelmien tietoturvaan.

Taulukko 13. Standardien yleisiä vaikutuksia automaatiojärjestelmien tietoturvaan.

Standardi	**Yhteenveto vaikutuksista**	**Päävaikutustapa**
ISO/IEC 15408 (*Common Criteria*)	Yhteinen perusta IT-tuotteiden tietoturvan yhteismitalliseen ja riippumattomaan evaluoimiseen ja varmistamiseen. Voidaan soveltaa esim. vaatimalla tietyn EAL-tason tuotteita suojavyöhykkeittäin → systemaattinen vaatimustasomäärittely.	Arvioinnit/ kriteerit
DHS CSSP	Ymmärretään uhkia ja haavoittuvuuksia käytännössä. Haavoittuvuuksien vaikutus voidaan minimoida. Yksityiskohtainen suojausten käyttöönoton suunnittelu paranee.	Käytännöt
ISA99	Antaa perustiedot tietoturvamekanismien soveltamisesta teollisuusautomaatioon. Soveltuvat käytännöt ja ratkaisut voidaan yrityksen tarkemmassa analyysissä räätälöidä, jolloin relevantit suojaukset saadaan helpommin käyttöön.	Mallit/ esimerkit
ISO/IEC 27000 -sarja	Yrityksen merkittävimmät riskit saadaan arvioitua ja kontrolloitua tietoturvanhallintajärjestelmässä. Laajan alueen kattavia tietoturvavaatimuksia ja käytäntöjä voidaan valita suojaamaan toimintaa soveltuvin osin. Normikäytännöt parantavat operatiivista tietoturvaa.	Käytännöt
NIST 800 -sarja	Ymmärretään erityyppisten järjestelmien (myös ICS) haavoittuvuudet, soveltuvat verkkoarkkitehtuurit, sekä spesifit tekniset tietoturvakontrollit, jolloin tietoturvan hallinta saadaan organisoitua tehokkaasti.	Teknologian käyttö
MSISAC/SANS Procurement	Hankintatoimi tehostuu yhtenevien tietoturvavaatimusten ansiosta. Ymmärretään pääasiat relevanteista uhkista ja ratkaisuista.	Mallit/ esimerkit
AGA Std 12	Auttaa yritystä kuvaamaan tietoturvakäytäntöjen perusteet.	Käytännöt

	Tietoturvatavoitteet ja käytäntöjen määrittely auttavat arvioimaan riskitoteumaa ja kehittämään tietoturvatoimintaa.	
API Std 1164	Auttaa yritystä kuvaamaan tietoturvakäytäntöjen perusteet. Operaattorin ymmärtäessä toimintojen sekä järjestelmien haavoittuvuudet ja riskit, voidaan suojaavat toimenpiteet kohdistaa oikein.	Käytännöt
NERC CIP	Yhteneväiset vaatimukset operatiivisten tietoturvatoimintojen määrittelyyn tuovat synergiaetuja, mm. laitevalmistajille esitetään yhteneviä tietoturvavaatimuksia. Tämä antaa mahdollisuuden investoida laadukkaisiin toteutuksiin.	Arvioinnit/ kriteerit
IEEE 1686	Kenttälaitteille saadaan määriteltyä yhteneväiset tietoturvaominaisuudet. Antaa mallin NERCin vaatimusten mukaisesta laitesuojasta.	Mallit/ esimerkit

2.6 Johtopäätöksiä standardeista

Teollisuusautomaation tarpeisiin löytyy lukuisia erilaisia (mainiosti tai heikommin soveltuvia) tietoturvastandardeja ja parhaita käytäntöjä. Käytännössä ongelmana onkin tunnistaa, valita ja räätälöidä näistä soveltuvimmat osat kunkin suomalaisen alan yrityksen erityistarpeisiin. Yritysten tietoturvavaatimukset ja -käytännöt eivät koskaan voine olla täysin yhteneviä johtuen ajan kuluessa toimijoille asetetuista erilaisista vaatimuksista tai mahdollisista eroista toimintaympäristöjen yleisessä kehityksessä.

Tässä luvussa on esitelty joukko erittäin potentiaalisia ohjeistoja sekä muun muassa vaatimus- ja tarkastuslistoja, joita voitaisiin käyttää hyväksi parhaiden käytäntöjen suomenkielisten kuvausten laadinnassa. On kuitenkin syytä korostaa, että soveltuvimman ”tietoturvareferenssin” kiinnittäminen menestyksellisesti kullekin tietoturvan hallinnan osa-alueelle edellyttää relevanttien yritysten ja laitosten aktiivista osallistumista määrittelytyöhön. Yritysevaluaatiot ja laajat asiantuntijakatselmoinnit Suomessa ovatkin tärkeitä keinoja asian edistämiseen käytännössä. Pelkkä teoreettinen tarkastelu ei vielä riitä erilaisten näkemysten huomioonottamiseksi laadittaessa kuvauksia eri tarkoituksiin.

3. Automaatiojärjestelmän tietoturvan arviointi

Tässä luvussa on kuvattu yleisiä, parhaiten soveltuvia ratkaisumalleja automaatiojärjestelmän tietoturvan arviointiin. Tavoitteen saavuttamiseksi on vertailtu useiden erilaisten arviointimallien ja -ratkaisujen käyttökelpoisuutta. Erityisesti tässä luvussa kuvataan erityyppisiä tietoturvatavoitteita ja -vaatimuksia, joita voidaan (soveltuvin osin) käyttää järjestelmän tietoturvan evaluoimiseen yleisluontoisissa, teollisuusautomaatioon liittyvissä tapauksissa.

3.1 Yleistä

Erilaiset automaatiojärjestelmät ja niiden yksittäiset komponentit vaativat erityiskäsittelyä, kun ajatellaan operatiiviseen toimintaan otettavan tieto-, kommunikointi- tai ohjausjärjestelmien tietoturvan arvioimista. ICS (*Industrial Control Systems*) -alueen järjestelmien tietoturva-arvioinnissa on otettava huomioon useita erityispiirteitä, jotka voivat olla jopa ristiriidassa toistensa kanssa. Tällöin niiden välille on pyrittävä löytämään tasapaino.

Ensimmäinen ulottuvuus on, että tuotantoa ohjaavien ja seuraavien järjestelmien käyttövarmuus ja oikea toiminta on varmistettava ensisijaisesti. Sopivan tasoisten tietoturvaominaisuuksien tulee olla käytössä, mutta ne eivät saa aiheuttaa häiriöitä, jotka voisivat heikentää käyttövarmuutta.

Toinen ulottuvuus on erilaiset arviointimenetelmät ja niiden käyttö. Suomalaistenkin toimijoiden käyttöön on yleisesti saatavilla erilaisia avoimia ja kaupallisia ohjelmistotyökaluja, jotka määrittävät tietoturvahaavoittuvuuksien sekä käyttöjärjestelmien ja erilaisten sovellusten konfiguraatioiden turvallisuutta. Niiden soveltuvuutta ICS-alueella toimivaan organisaatioon tai yritykseen voi kuitenkin olla vaikea arvioida. Tietty menetelmä tai työkalu voi esimerkiksi listata käyttäjälle kuusisataa erilaista järjestelmän tietoturvaan liittyvää varoitus-

ta, mutta käyttäjän voi olla hankala soveltaa tulosta järjestelmän kehittämiseksi tai sen arvioimiseksi, onko järjestelmän turvallisuus riittävän hyvä. Tällöin eri yhteisöissä tarvitaan melko tarkkaa yhteistä määrittelyä siitä, miten tiettyä tietoturvan varmistamisen menetelmää tai työkalua sovelletaan jollakin käyttöalueella. Työkalulle on määriteltävä esimerkiksi erityisiä profiileja, joissa valmiit testitapaukset testaavat vaikkapa automaatiosovelluksen käyttämien käyttöjärjestelmä- ja sovellusominaisuuksien sallitut versiot ja asetukset.

3.2 Evaluaation tavoitteet ja vaiheet

Tietoturvaevaluaatioon tarvitaan taustatiedoiksi käyttöönotettavan järjestelmän tai tuotteen tietoturvatavoitteet, vaatimukset, asennuspisteessä vallitseva tietoturvapolitiikka ym. Näiden määrittelemisessä operoiva yritys on voinut käyttää apuna valmiita skelettejä (esim. maksullista standardia API Std 1164 [API-1164], sen Annex B: SCADA-järjestelmän tietoturvasuunnitelma). On välttämätöntä tuoda esiin olemassa olevat tietoturvan taustavaatimukset. Jos määrittely on kesken, viimeistään nyt tulee määritellä ne tarkemmin. Alue on laaja ja monimutkainen: kunkin operatiivisen toiminnan tietoturvatavoitteisiin ja -vaatimuksiin vaikuttavat muun muassa ko. teolliselle toiminnalle asetettu lainsäädäntö, sääntely, asiakassopimukset, yleisen turvallisuuden ylläpitäminen, jne.

Periaate 1. Evaluaation perusidea – vertailu.

> Evaluaatio perustuu ennen kaikkea vertailuun: mahdollisimman varman tiedon keräämiseen siitä, ovatko evaluaatiokohteen ominaisuudet tavoitteiden mukaiset. Jos kohde ei täytä ennakkovaatimuksia, on yleensä järkevää selvittää ja kirjata, millaisia löydetyt poikkeamat ovat, miten paljon niitä on jne.

Tässä käsikirjassa ei määritellä, millä menetelmällä tavoitteet ja vaatimukset tulisi yksityiskohtaisesti määrittää tai mistä kaikkialta vaatimuksia voi tulla. Sitä vastoin esitetään erityyppisiä yleisiä tavoitteita ja vaatimuksia sekä joitain yksityiskohtia näiden evaluoimiseksi.

Periaate 2. Tietoturvaevaluaatioon liittyviä kysymyksiä.

Tietoturvaevaluaation yhteydessä voidaan tarkastella esimerkiksi seuraavia kysymyksiä:

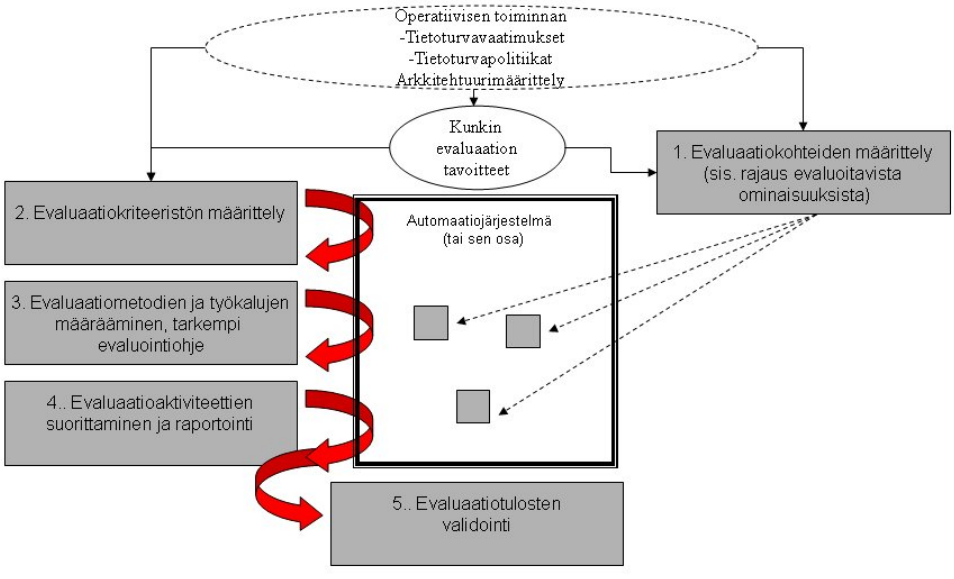
1. Vastaako järjestelmän (käyttöjärjestelmä, sovellukset, tietoliikenne, jne.) asetukset ennalta määriteltyä mallia tai sallittua konfiguraatiota?
2. Kestääkö järjestelmä toiminnassa, vaikka sitä vastaan suunnataan tietyntyyppisiä tietoturvahyökkäyksiä (esim. palvelunestohyökkäykset, *fuzz*-testaus)?
3. Onko järjestelmän toteutukseen jäänyt tietoturvahaavoittuvuuksia (esim. puskuriylivuodot, puutteellinen *input/output*-käsittely)?
4. Onko järjestelmästä poistettu kaikki sellainen toiminnallisuus, joka ei ole käytössä (esim. web-palvelinohjelmistot, toimisto-ohjelmistot)?
5. Onko ohjelmistojen päivitysominaisuuksien turvallisuudesta huolehdittu? Entä vikojen korjaamisesta?
6. Onko järjestelmässä huomioitu haittaohjelmien torjunta? Voivatko torjuntamekanismit itsessään aiheuttaa haittaa?

Näihin kysymyksiin vastaaminen riippuu vahvasti siitä, mihin kohtaan järjestelmän elinkaarta kyseessä oleva tietoturvaevaluaatio kohdistuu. Mikäli evaluaatio suoritetaan **tuotekehityksen aikana**, korostuvat yleispätevät asiat, kuten hyvien suunnittelusääntöjen käyttö ja lähdekoodin virheettömyyden varmistaminen. Toisaalta jos evaluaatio kohdistuu **käytössä olevan** (tai käyttöönotettavan) järjestelmän evaluoimiseen, siirtyy painopiste helposti järjestelmäasetusten oikeellisuuteen, kovennukseen, päivitysprosesseihin tms. ominaisuuksiin, jotka voivat riippua voimakkaastikin esimerkiksi tietyn asiakkaan tai projektin vaatimuksista.

Huolimatta edellä mainitusta lähtökohtien moninaisuudesta järjestelmän tietoturvaevaluaation voidaan katsoa koostuvan seuraavista päävaiheista:

1. evaluaatiokohteen määrittely (sis. evaluaation alaisten kohteiden rajaus)
2. evaluaatiokriteeristön määrittely (sis. vaatimukset vyöhykkeessä)

3. evaluaatiometodien ja työkalujen valitseminen sekä evaluaatio-ohjeen tarkempi määrittely (evaluaatiotyökalussa käytettävä profiili, skeletit, tarkistuslistat, jne. http://web.nvd.nist.gov/view/ncp/repository)
4. evaluointiaktiviteettien suorittaminen ja raportointi (esim. tietoturvatestaustyökalujen käyttö realistisessa testijärjestelmässä, ei tuotantokäytön aikana laitosjärjestelmissä)
5. evaluaation tulosten validointi.



Kuva 2. Määritelmä – automaatiojärjestelmän tietoturvaevaluaation päävaiheet.

3.3 Yleiskuvaus evaluaation vaiheista

Seuraavassa kuvataan lyhyesti **käyttöönotettavan** automaatiojärjestelmän evaluaatioon kuuluvat vaiheet.

Periaate 3. Evaluaation perusongelmana on teknisten yksityiskohtien voimakas tapauskohtaisuus.

Vakioidun evaluaation perusongelmana on se, että tehokkaan tietoturvaevaluaation yksityiskohtainen toteutus riippuu vahvasti evaluoitavan kohteen tyypistä, liiketoiminnan päätavoitteista sekä evaluaatiolle asetetuista tavoitteista. Yleispätevää, kaikkialle suoraan soveltuvaa tekniikkaa ei ole.

3.3.1 Evaluaatiokohteen määrittely

Käyttöönotettavasta järjestelmästä määritellään evaluoitava osuus. Koko järjestelmää ei ole välttämätöntä evaluoida, mikäli halutaan rajata evaluointi suppeammalle alueelle esimerkiksi työmäärän vähentämiseksi tai riittävän tarkkojen tulosten aikaansaamiseksi. Usein evaluaatio voidaan suorittaa tehokkaasti ja tarkasti, kun kohdistetaan tutkinta tiettyyn järjestelmän kohtaan (kuten vajavaisesti testattuun uuteen komponenttiin), joka on esimerkiksi prosessinomistajien ja vastaavien viiteryhmien kattavassa riskiarviointipalaverissa todettu kriittiseksi ja potentiaalisesti haavoittuvaksi. Toisaalta jossain muussa asiayhteydessä (esim. järjestelmäsuunnittelussa) voi olla jo valmiiksi dokumentoitu, että evaluoitavan moduulin merkitys koko järjestelmän oikealle toiminnalle on erityisen suuri. Eräs tapa voi olla selvittää, minkä komponentin tekniseen toteuttamiseen on liittynyt suuria epävarmuuksia – tiedetäänkö esimerkiksi, onko komponentin kehittämisessä käytetty teknologia-alusta vielä joiltain osin testaamaton.

Tärkeää on rajata mahdollisimman selkeästi evaluaatiokohteesta tutkittavat ominaisuudet. Käytännössä kohdetta rajattaessa voidaan määritellä, että tutkittavasta moduulista evaluoidaan ainoastaan esimerkiksi ulkoinen käyttäytyminen, ei moduulin sisältämän lähdekoodin tietoturvaominaisuuksia kokonaisuudessaan. Tietoturvaevaluaation kohteena on tällöin tietyn moduulin ulkoinen käyttäytyminen, ei se, miten tai millä säännöillä se on rakennettu (tai ohjelmoitu). Tällainen rajaus voi tulla kyseeseen esimerkiksi silloin, kun lähdekoodi ei ole saatavilla tai lähdekoodin tiedetään olevan hyvin laaja, jolloin sen kaikkia haavoittuvuuksia ei ehdittäisi kuitenkaan korjaamaan vaadittavassa ajassa. Tällaisessa tilanteessa kyseisen lähdekoodin vaikutusalue ei saisi tietenkään olla kokonaisjärjestelmän turvallisuuden kannalta kriittinen. Esimerkkejä mahdollisista evaluaatiota rajaavista valinnoista voisivat olla vaikkapa kohteen lähdekoodin tietoturvaominaisuudet,

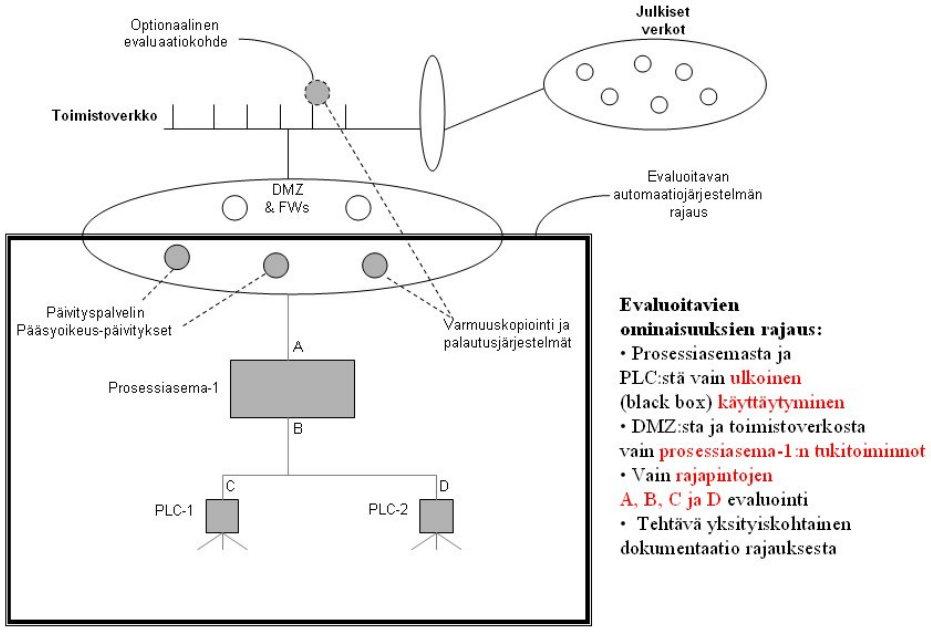
kohteen käyttäytymisen ulkoiset vaikutukset, järjestelmäasetusten oikeellisuus tai hyökkäysten vaikutukset järjestelmän suorituskykyyn.

Periaate 4. Evaluaatiokohteen määrittely.

Evaluaatiokohteen määrittely sisältää pääsääntöisesti seuraavia vaiheita:

1. Edellytys: Organisaatio on suorittanut tai tilannut (ja dokumentoinut) järjestelmän kokonaisriskiarvioinnin, jossa järjestelmän riskialtteimmat osat on tunnistettu. Riskiarvioinnin yhteydessä voidaan käyttää hyväksi järjestelmän teknistä skannausta tai sellaisten ominaisuuksien profilointia, jotka osoittavat järjestelmästä riskialttiita kohtia.
2. Organisaatio päättää muun muassa riskiarvioinnin ja muiden suunnitelmiensa ja tavoitteidensa perusteella, mitä evaluaatiokohteita kussakin tietoturvaevaluaatiossa tutkitaan.
3. Yksittäisessä evaluaatiossa organisaatio rajaa evaluaatiokohteiden tutkittavat ominaisuudet. Esimerkki: Kohteesta määritellään evaluoitavaksi ainoastaan ulkoinen (*black box*) käyttäytyminen järjestelmän ollessa tietoturvatestauksen alaisena. Käyttäytymisen on oltava todennettavissa standardimenetelmin (ja koskettava kokonaisjärjestelmän toimintakyvyn kannalta olennaiseksi todettua toimintoa).

Nämä vaiheet voidaan toteuttaa vapaamuotoisella, kullekin organisaatiolle sopivalla tavalla. Tulokset eli evaluaatiokohteen ja siitä tutkittavien ominaisuuksien rajaus tulee aina dokumentoida selkeästi ja mahdollisimman yksiselitteisesti.



Kuva 3. Esimerkki evaluoitavaksi valituista kohteista (harmaa väri) ja evaluoitavien ominaisuuksien rajauksesta.

3.3.2 Evaluaatiokriteeristön määrittely

Tämä vaihe eli kysymyksenasettelu on evaluaatioon liittyvistä määrittelyistä kenties vaikein: ”Mitä kriteeristöä vasten kulloistakin evaluaatiokohdetta tutkitaan?” Monissa aiemmissa yhteyksissä on havaittu, että on erittäin tärkeää määritellä ja todella ottaa käyttöön tarkoitukseen soveltuva kriteeristö evaluaation suorittamista varten. Mikäli kriteeristöä ei ole määritelty tarpeeksi tarkkaan tai se ei kohdistu tietoturvan kannalta oleellisiin järjestelmän seikkoihin, eivät evaluaatiotuloksetkaan vastaa tarkoitustaan eli järjestelmän ominaisuuksien todentamista sen tietoturvavaatimuksia vasten. Kuten todettu, soveltuva kriteeristö riippuu voimakkaasti evaluaatiokohteesta sekä tavoitteista, jotka järjestelmän toiminnalle on asetettu. Mitään sellaista kaikenkattavaa kriteeristöä ei ole olemassa, joka sopisi kaikkiin käyttötarkoituksiin suoraan, sillä kyse on yrityksen itsensä määrittelemästä asiasta.

Evaluoitavan yrityksen operatiivista toimintaa kuvaavien tietoturvamäärittelyjen ja -säännöstöjen tulee olla kunnossa. Mikäli näin ei ole, evaluoijat eivät voi tietää, mitkä ovat toimintaympäristön tarkat vaatimukset ja niiden täyttämiseksi

tarvittavat tietoturvakontrollit. (Evaluaatiota voitaisiin tietysti ajatella tehtävän vaikkapa jonkin yleistason mukaisesti, mutta tällöin ei tiedetä, miten evaluaation tulokset todella hyödyttäisivät kyseisen yrityksen operatiivisen toiminnan turvaamista.)

1. Kullakin automaatio- ja tietoliikennejärjestelmän evaluoitavalla osalla tulee olla operoivan organisaation erityisesti määräämä ja käytössä oleva tietoturvatason (*security level*) määrittely, johon kuuluvat kiinteästi sekä tietyt tietoturvakontrollit että yksityiskohtainen tekninen ja hallinnollinen tietoturvapolitiikka.
2. Lisäksi kokonaisjärjestelmän arkkitehtuurikuvauksessa on oltava määriteltynä suojattavien kohteiden vyöhykkeet, joissa kussakin vallitsee tietty tietoturvataso.

Yleisesti ottaen voidaan siis sanoa, että käyttöympäristöstä tulevat vaatimukset määräävät ehkä kaikkein voimakkaimmin valittavan evaluaatiokriteeristön yksityiskohdat sekä referenssitason, johon evaluoitavaa komponenttia verrataan. Lisäksi hyvän kriteeristön yleisiä ominaisuuksia ovat selkeys, yksiselitteisyys, käytettävyys sekä riittävä kattavuus. Tällöin kriteeristö sopii käyttötarkoitukseensa hyvin ja antaa edellytykset saavuttaa evaluaatiolle asetetut tavoitteet.

Monesti yritykset käyttävät omien tietoturvakontrolliensa ja niihin liittyvien säännöstöjensä määrittelytyön pohjana olemassa olevia tietoturvastandardeja ja parhaita käytäntöjä. Usein otetaan mallia standardien soveltuvista osista ja lisätään mukaan omien toimintatapojen, erikoisvaatimusten tai -säännöstöjen yksityiskohtia. Tavoitteena yleensä on, että tietoturvaohjeistus on yhteensopiva yrityksen olemassa olevaan säännöstökannan, laatukäsikirjojen ym. kanssa.

Automaatiojärjestelmän suojaamiseksi asetetaan usein muun muassa seuraavia vaatimuksia:

- järjestelmän saatavuuden ja käyttövarmuuden varmistaminen, resurssien käytön kontrollit
- vikatilanteista elpymisen suunnitelmat ja turvaaminen, toiminnan jatkuvuus
- valvontatiedon saannon ja prosessinohjauskyvyn turvaaminen
- pääsynvalvonnan kontrollit (esim. roolipohjainen), käyttäjätilien hallitseminen
- järjestelmän suojauksen ja eristämisen kontrollit

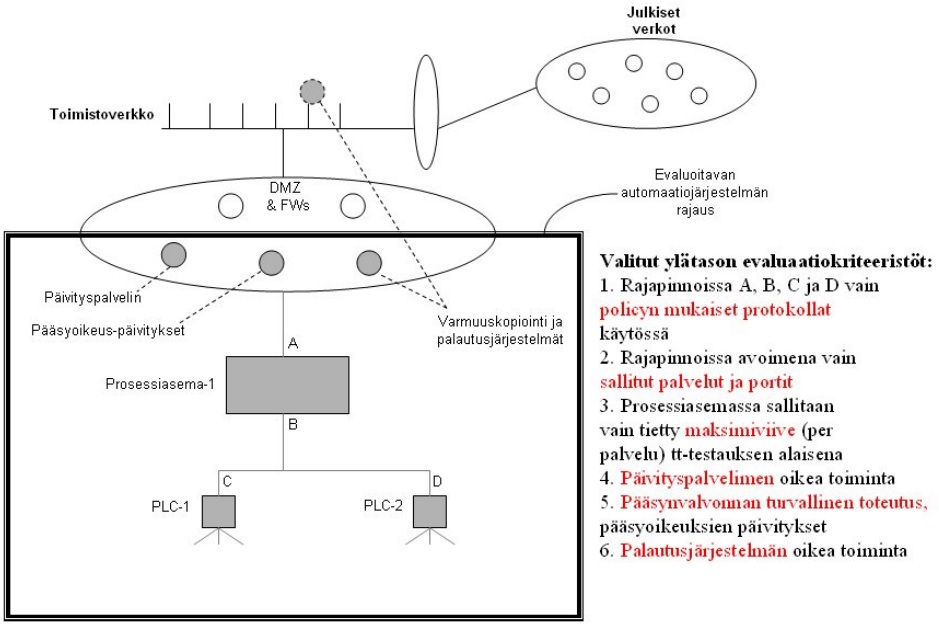
- järjestelmien kovennus, rajapintojen palveluiden rajoittaminen
- järjestelmään tallennetun datan ja viestien eheyden suojaaminen
- turvajärjestelmien signaloinnin (mm. hälytykset) varmistaminen
- tapahtumatiedon jäljitettävyys ongelmatilanteissa (*accountability*, ym.)
- haittaohjelmasuojauksen kontrollointi.

Käytännössä tällaisia vaatimuksia täytyy tarkentaa organisaatiotasolla, jotta riittävän tarkka evaluaatiokriteeristö saadaan johdettua voimassa olevista tietoturvavaatimuksista, -säännöistä ja -käytännöistä.

Alla on lueteltu teollisuusautomaatiojärjestelmien käyttöön soveltuvia tietoturvastandardeja ja -käytäntöjä (sis. valmiita kriteeristöjä ja vaatimuksia), joita voidaan käyttää hyväksi suunniteltaessa käyttöönotettavan automaatiojärjestelmän tietoturvaevaluaatiota.

Taulukko 14. Teollisuusautomaatiojärjestelmien turvaamiseen soveltuvia tietoturvakriteeristöjä.

Standardi / käytäntö	**Selitys**
American Petroleum Institute (API) Standard 1164, "Pipeline SCADA Security" [API-1164]	Sisältää mm. Annex A: Tarkistuslista SCADA-järjestelmän tietoturvan evaluointiin, Annex B: SCADA-järjestelmän tietoturvasuunnitelma (esimerkki).
IEEE 1686 - Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities [IEEE 1686]	Konkreettisia esimerkkivaatimuksia IED-laitteille.
ISA99 Industrial Automation and Control Systems Security Standards [ISA99]	ANSI/ISA-TR99.00.01: Sisältää mm. auditoinnin, mittaamisen ja monitoroinnin.
MSISAC/SANS: SCADA and Control Systems Procurement Language [PROC]	Turvallisten automaatiojärjestelmien hankkiminen. Mm. kovennus ja paljon muuta.
North American Electric Reliability Corporation (NERC) – CIP Standards [NERC]	Paljon hyviä toiminnallisia vaatimuksia mm. laitevalmistajille.



Kuva 4. Esimerkki ylätason evaluaatiokriteeristöstä.

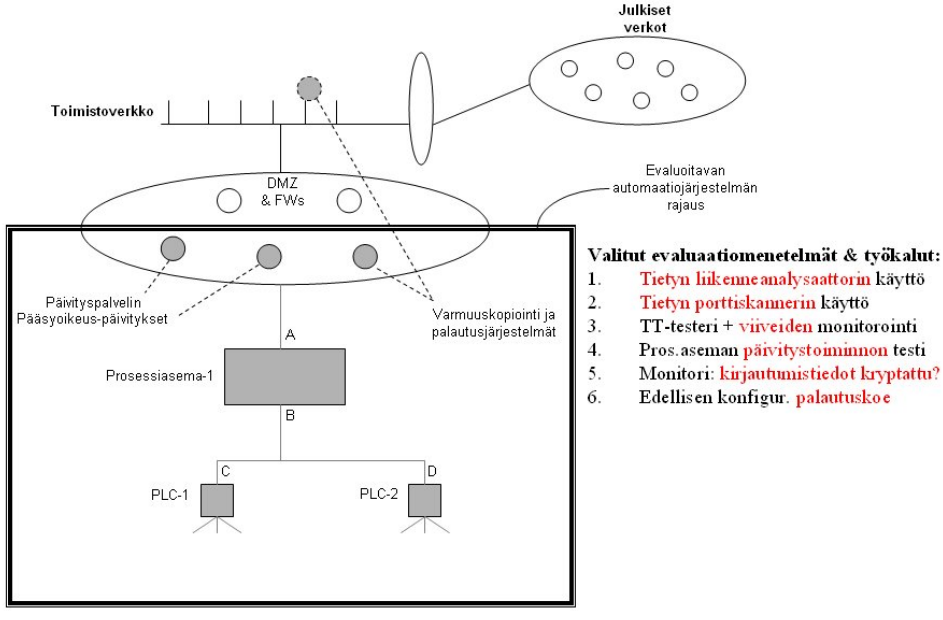
3.3.3 Evaluaatiometodien ja työkalujen valitseminen sekä toimintaohjeen määritteleminen

Ennen teknisten evaluaatioaktiviteettien aloittamista täytyy tarkistus- ja tietoteknisten evaluointiaktiviteettien yksityiskohdat määritellä tarkasti, selkeästi ja perustellusti. Tarvitaan selkeä lähtökohta (esim. yrityksen aiempien evaluaatioiden tulokset tai asetettu tavoitetila), johon kaikki evaluaatioaktiviteetit pohjautuvat. Esimerkiksi yksityiskohtaiset tarkistuslistat (jos niiden käyttö kuuluu evaluaatioon) on kiinnitettävä sekä järjestelmän ominaisuuksia tutkivat työkalut kuten penetraatiotesterit ja haavoittuvuusskannerit on yksityiskohtaisesti määriteltävä, kuten myös työkalujen käyttämät konfiguraatiot, laajennukset, haavoittuvuusprofiilit, *plug-in*-moduulit jne. Tähän tarvitaan usein syvällistä tietämystä tietoturvan teknisen evaluaation nykyaikaisista välineistä ja niihin kehitetyistä ominaisuuksista, joten ulkoisen asiantuntemuksen käyttö on usein paikallaan.

Evaluaatioon liittyviä tarkastuksia varten täytyy siis pohtia seuraavia kysymyksiä:

- Millä metodeilla ja työkaluilla evaluaation eri tarkastukset suoritetaan?
- Mitä testityökalujen asetuksia, laajennuksia, haavoittuvuuskantaa, tarkistuslistoja jne. evaluaation kussakin osatarkastuksessa käytetään?

Jäljempänä määritellään tarkemmin teollisuusautomaatiojärjestelmien evaluointiin ja testaamiseen soveltuvia metodeja ja työkaluja. Tärkeitä menetelmiä ovat muun muassa seuraavat: **Toimihenkilöiden haastattelu**: tarkastuslistojen käyttö, tietoturvakontrollien ja prosessikuvausten vertaaminen todelliseen tilanteeseen. **Haavoittuvuusanalyysi:** lähdekoodianalysaattorit, haavoittuvuusskannerit, koodikatselmoinnit. **Hyökkäysten sietoa testaavat menetelmät**: teollisuusympäristöihin soveltuvat tietoturvatesterit, esimerkiksi *Achilles Satellite*, penetraatiotesterit, *robustness*-testerit, testaus palvelunestohyökkäyksiä vastaan. **Järjestelmien konfiguraation selvittäminen** ja vertaaminen määriteltyyn: esimerkiksi verkkoskannerit, porttiskannerit, konfiguraatiotiedostojen tarkistus, palomuurisäännöstöjen ja eri järjestelmien pääsynvalvontasäännöstöjen läpikäynti.



Kuva 5. Esimerkki käytettävistä evaluaatiomenetelmistä.

3.3.4 Evaluointiaktiviteettien suorittaminen ja raportointi

Lopulta päästään itse evaluaation suorittamiseen eli evaluaation aikana tapahtuvien aktiviteettien kuvaukseen. Nämäkin aktiviteetit ovat tietenkin hyvin riippuvaisia tilanteesta eli niiden kokoonpano ja kuvaus mukautuvat siihen, millainen evaluaatio on valittu suoritettavaksi. Evaluoinnin yksityiskohdat määräytyvät käytettävien työkalujen mukaan. Seuraavassa kuvaillaan kuitenkin yleisluontoisesti järjestelmätestaamista automaatioteollisuusalueella.

3.3.4.1 Yleistä testaamisesta

Testauksen tulisi normaalisti sisältää joukko erityyppisiä lähestymistapoja, kuten järjestelmän sitkeyden (*robustness*) testaamisen, testauksen kuormituksen alaisena, testauksen hyökkäämällä (*penetration testing*), input/output-muuttujien validoinnin, verkon todellisen kokoonpanon selvittämisen, dataviestinnän mittaamisen ja vertailun määriteltyyn jne. Osa näistä lähestymistavoista vaatii pitkäjännitteistä kehitystyötä organisaatiossa, jotta kyseisestä testaustyypistä saatava hyöty olisi merkittävä.

Joidenkin yksittäisten testityökalujen käyttö saattaa joissain tapauksissa vaatia jopa vuosien perehtyneisyyden ja pohjatyön esimerkiksi tapahtumamallien ja laajennusten rakentamiseksi työkaluihin siten, että saadaan tarkka kuva järjestelmän normaalitoiminnoista. Perusteellisen työn tekemiseksi täytyy rakentaa mahdollisimman hyvin todellista vastaava testiverkko, asentaa testikohdejärjestelmät, konfiguroida tietoliikennegeneraattorit, kehittää testimenetelmiä ja työkaluja soveltuviksi jne. Tämä on monesti suuritöistä, koska tietoturvatestaamisella ei ole usein kovin pitkiä perinteitä monessakaan automaatioteollisuuden alalla toimivassa yrityksessä.

Käyttöönottotestaus

Käyttöönottotestaus tehdään ennen valmiin järjestelmän käyttöönottoa, jolloin kaikki tietoturvakomponentit on asennettu järjestelmään ja kaikki asetukset ja ympäristöolosuhteet ovat mahdollisimmat realistiset ja käytössä. Käyttöönottotestauksen tarkoitus on validoida, että tietoturvaan liittyvät toiminnot toimivat odotetulla tavalla, mm. että [ISA99-TR2]

- tietoturvaominaisuuksien asennukset on tehty oikein
- tietoturvaan liittyvä konfiguraatio on oikea

- tietoturvakontrollit toimivat spesifikaation mukaisesti
- tietoturvavaatimukset ja -politiikat toteutuvat oikein
- kokonaisjärjestelmä sekä turvallisuustoiminnot toimivat oikein.

3.3.4.2 Raportointi

Evaluaatioaktiviteettien tuloksena tulisi syntyä seuraavaa:

Periaate 6. Evaluaatioaktiviteettien aikana tai niiden jälkeen syntyviä tuloksia.

Evaluaation tuloksia:

Tiedostoja, joihin evaluaatiomenetelmien ja työkalujen tulokset on tallennettu. Nämä tiedostot on usein luokiteltava erittäin luottamuksellisiksi ja suojattava, sillä jos tieto esim. tietoturvapoikkeamista joutuu vääriin käsiin, saattaa järjestelmiin olla helppo tunkeutua sitä havaitsematta. Tulosten tulee olla vertailukelpoisessa muodossa vähintään siten, että vertailu mahdollistuu määriteltyyn tavoitetasoon sekä mielellään myös aikaisempaan tilanteeseen (*baseline*).

Raportteja, joissa on mm. evaluaatiokokonaisuuden tunnistetiedot, ennakkovaatimuksia (esim. käytetty kriteeristö, metodit ja työkalut), yhteenvetoja eri osuuksien tuloksista, tärkeimmät löydökset, mahdolliset kehityskohteet sekä parannusehdotukset. Erittäin luottamuksellisia.

Lisäksi, evaluaatioaktiviteettien tulisi olla helposti toistettavissa, toisin sanoen tulisi mm. valita evaluaatioita suorittavat henkilöt, evaluaatio-olosuhteet sekä käytettävät työkalut ja metodit sillä tavoin, että kyseinen evaluaatio ja sen tulokset eivät jää yksittäistapaukseksi. Evaluaation kokonaisuudelle tulisikin olla määriteltynä realistinen perusevaluaation toteuttamisen suoritustaso, jonka kustannukset ovat sopivalla tasolla, sekä lisäksi kehittämispolku, jonka mukaisesti pyritään suunnittelemaan parannuksia vuosittain.

3.3.5 Evaluaation tulosten validointi

Vaikka evaluaatio suoritettaisiinkin asianmukaisesti suunnitellen, toteuttaen ja raportoiden siihen liittyviä aktiviteetteja, olisi hyvä määritellä etukäteen mekanismi, jolla evaluaatiotuloksia voitaisiin validoida. Tulosten määrähän voi olla

valtava, tietenkin evaluaatiossa käytettyjen menetelmien ja työkalujen mukaan. Usein validointi ei ole yksinkertainen tehtävä, sillä se saattaa edellyttää sellaista tietoa tai kokemusta evaluaatiotuloksista, jota evaluaation suorittajilla ei ole ainakaan helposti käytettävissään. Usein uskottava validointi saattaa edellyttää tarkkaa tietoa edellisen evaluaation tuloksista ja tärkeimmistä muutoksista, joita kohdeympäristöön on mahdollisesti tullut. Vaikeammin saavutettavissa ovat ainakin aiemmin olleet riittävän tarkka tieto sekä aiemmin käytössä olleiden että uusien kaupallisten evaluaatiotyökalujen tarkkuudesta, tehokkuudesta ja kattavuudesta erityyppisten tietoturvaongelmien ja poikkeamien havaitsemisessa ja raportoinnissa juuri tietyssä kohdeympäristössä. Usein nämä seikat ovat epätäydellisesti tiedossa ja estävät kunnollisen tulosten validoinnin.

Jos tulosten validointi päätetään tietoisesti pääosin sivuuttaa, olisi joka tapauksessa hyvä silti edes jollain tasolla arvioida evaluointitulosten oikeellisuutta ja tarkkuutta. Tätä voidaan ainakin kartoittaa muutamilla yksinkertaisilla ja kevyillä tavoilla. Voidaan esimerkiksi

- Pyytää konsultointiapua alan asiantuntijalta, esim. kysyen: ”Puuttuuko löydöksistä jotain sellaista mitä niissä yleensä on?”, ”Ovatko löydöksemme tyypillisiä tällaisessa ympäristössä”, ”Onko saavutettu määrä tietoturvapoikkeamia normaalin rajoissa? Paljonko ”*false*-positiivisia” löydöksiä yleensä on?”, ”Millaisia tyypillisiä poikkeamia tai löydöksiä tietyn työkalun (ja asetuksen) olisi pitänyt löytää?”.
- Tehdä pistokokeita valittujen, helposti todennettavien löydösten paikkansapitävyydestä. Esimerkiksi jos katselmoinnissa ilmenee löydös, että tiettyjä tietoturvallisen koodauksen käytäntöjä ei ole sovellettu implementoinnin aikana (vaikka tällaisten käytäntöjen soveltamisen on määritelty kuuluvan tuotekehitysprosessiin), voidaan jonkin tunnetun moduulin koodille ajaa nopeasti lähdekoodianalyysi. Tuloksista voidaan sitten validoida, onko tietyntyyppisiä potentiaalisia haavoittuvuuksia todella olemassa järjestelmässä.

3.4 Evaluaatiomalleja ja ohjeita

Tässä luvussa esitämme konkreettisia evaluaatiovaatimuksia sekä samalla arvioimme saatavilla olevien kuvausten ja ohjeiden käyttökelpoisuutta teollisuusautomaatiojärjestelmien tietoturvan evaluoimiseksi.

3.4.1 Evaluaatiokriteeristöjä

Tätä osuutta valmisteltaessa olemme arvioineet paljon erilaisia lähtökohtia, vaatimuksia ja kriteeristöjä, joita käyttämällä automaatiojärjestelmien tietoturvaominaisuuksia voidaan määritellä ja arvioida. Aluksi määrittelemme muutamia tärkeitä referenssikonsepteja, jotka auttavat mm. evaluoitavan kokonaisuuden hahmottamisessa ja vaatimusten tarkassa kohdentamisessa. Jäljempänä keskitymme erityisesti sellaisten vaatimusten kuvaamiseen, joita voidaan soveltaa suojattavien kohteiden tietoturvavaatimusten määrittelyssä sekä tulevissa tietoturvaevaluoinneissa.

Kriteeristöjen koostamisessa olemme käyttäneet mm. seuraavia referenssejä: [NERC-005], [ISA99-1], [PROC], [ICSSEC], [IAONA], [ISA99-TR1], [FIPS112].

Myöhemmin seuraavissa taulukoissa käytämme struktuuria, joka sisältää erillisinä sarakkeinaan vaatimuksen **identiteettikoodin (ID)** vaatimusten erottelemiseksi toisistaan, vaatimuksen **kuvauksen**, ehdotuksen **pääevaluaatiomenetelmistä,** joilla kyseisen vaatimuksen toteutumista voidaan evaluoida sekä äärimmäisenä oikealla indikaattorin siitä, onko kyseessä pääasiassa **tekninen vai hallinnollinen** evaluaatio (vai molemmat).

3.4.1.1 Referenssikonseptit – suojattavien kohteiden vyöhyke, tietoturvataso

3.4.1.1.1 Suojattavien kohteiden vyöhyke – Security Zones

Yleistä

Teollisuusautomaation avulla suoritettuun tuotantoon tai prosessin ohjaukseen liitetyille laitteille ja ohjelmistolle asetaan hyvin erilaisia vaatimuksia eri käyttötarpeiden mukaan. Esimerkiksi toimistoverkon järjestelmien tulee usein olla yleiskäyttöisiä, *de facto* -standardien mukaisia IT-järjestelmiä, kuten MS-Windows -pohjaisia työasemia. Toisaalta automaatioverkossa on usein kovia reaaliaikavaatimuksia, mutta tällainen verkko eristetään yleisistä verkoista mahdollisimman tiukasti, jolloin varsinaisia toiminnallisia tietoturvaominaisuuksia ei tarvita niin paljon.

Näiden seikkojen takia yrityksen on syytä määritellä muutamia erilaisia vyöhykkeitä, ns. **suojattavien kohteiden vyöhykkeitä** (*Security Zones*), joissa määritellään ja listataan tarkasti kuhunkin vyöhykkeeseen kuuluvat tietopääomat.

Päätarkoituksena on konstruoida suojaus kunkin vyöhykkeen eksaktisti luetelluille tietopääomille määrätyillä vaatimuksilla ja tietoturvapolitiikoilla, joiden avulla pyritään saamaan kaikille vyöhykkeeseen kuuluville järjestelmille sopiva tietoturvataso (*Security Level*) [ISA99-1].

Security Zoneen kuuluvien **suojattavien tietopääomien** määrittely on looginen (Huom. usein on järkevää määritellä looginen ja fyysinen verkko tiettyyn rajaan asti yhteneväisesti), johon kuuluvat tietyt kriittiset tietopääomat, kuten [ISA99-1]

- Fyysisiä tietopääomia:
    - Tietokonelaitteet, verkkolaitteet, kytkimet, palomuurit, kommunikaatioväylät, modeemit, kaapelit jne.
    - Varmuuskopiointilaitteet ja -media, järjestelmäpalautuslaitteistot, muistit, varavoimalaitteet
    - Pääsynvalvontaan liittyvät laitteistot
    - Varaosat ja varaosavarastot
    - Ohjekirjat ja fyysinen dokumentaatio jne.
- Loogisia tietopääomia:
    - Käyttöjärjestelmät, tietokoneohjelmistot, tietokantaohjelmistot, rajapintamäärittelyt, kehitystyön ohjelmistot, analyysiohjelmistot jne.
    - Päivitykset, konfiguraatiotiedostot, tietokantatiedostot, varmuuskopiotiedostot
    - Järjestelmien suunnittelu- ja ylläpitotiedot
    - Tietoturvan suunnittelun ja ylläpidon tiedostot
    - Alihankkijoiden toimintaan liittyvät tiedostot ja resurssit jne.

Vyöhykkeet voidaan määritellä myös sisäkkäisiksi, jolloin sisimmäinen vyöhyke tarjoaa tiettyjen lisävaatimuksien avulla suojaa ympäröivän vyöhykkeen vaatimusten lisäksi. Yrityksen kontrollin ulkopuoliset vyöhykkeet luokitellaan yleensä **epäluotetuiksi vyöhykkeiksi (*Untrusted Zone*), joiden käyttäytymistä ei pystytä (ainakaan oleellisesti) kontrolloimaan.**

Oleellista vyöhykkeiden antamassa suojauksessa on niiden välisissä rajapinnoissa (liityntäpisteissä) sallittu toiminta. Jos henkilö tai tieto siirtyy vyöhyk-

keestä toiseen, tulee määritellä säännöstö menettelytavoista, esim. pääsynvalvontasäännöt ja sallitun tiedonsiirron määrittely. Vyöhyke voi olla **fyysinen vyöhyke (fyysisen paikan eristäminen)** tai **virtuaalinen vyöhyke (järjestelmien elektroninen suojaus).**

Yrityksen olisi hyvä määritellä suojattavien kohteiden vyöhykkeiden lisäksi vähintään kolme **tietoturvatasoa** (*Security Levels*). Nämä tietoturvatasot voivat olla esimerkiksi:

1 – alhainen tietoturva
2 – keskitason tietoturva
3 – korkea tietoturva.

Eräs konkreettinen esimerkki 3–4 erilaisesta tietoturvatasosta on esitelty dokumentissa *IAONA Handbook, Network Security* [IAONA]. Sen mukaan yksittäisen järjestelmän tai laitteen tietoturvatason (*”None”, ”Low-medium”, ”High”, ”Very-high”*) määrittelemiseksi pohditaan seuraavia tekijöitä:

- häiriön vaikutus tuotantoon
- häiriön vaikutus käyttäjien turvallisuuteen
- loukkauksen vaikutus yksityisyydensuojaan
- loukkauksen vaikutus yrityksen imagoon
- vahingon taloudellinen vaikutus
- vahingon merkitys sopimuksiin ja lakien noudattamiseen.

Tuloksen perusteella laite tai kyseinen alijärjestelmä osataan sijoittaa soveltuvaan suojattavien kohteiden vyöhykkeeseen jo alusta alkaen.

Kutakin tietoturvatasoa täytyy vastata lista tietoturvavaatimuksia ja tietoturvapolitiikkoja, joilla tietopääoma tai toiminta tullaan suojaamaan. Varsinkin uusituissa järjestelmäkokonaisuuksissa korkein tietoturvataso pyrkinee usein yhdistämään korkean tietoturvateknologian ja vahvat tietoturvakäytännöt yrityksen yksinkertaistettuihin toimintaprosesseihin. Korkean käytettävyyden ja saatavuuden järjestelmät yhdistetään sitten turvallisella tavalla näihin.

Tärkeintä on pyrkiä identifioimaan kaikki mahdolliset tietoturvaan ja käyttövarmuuteen vaikuttavat tietopääomat, määritellä mihin tietoturvavyöhykkeeseen ja tietoturvatasoon kukin niistä kuuluu sekä suojata kohteet näiden määrittelyiden mukaisilla tavoilla. Tällöin kukin tietoturvaan vaikuttava osatekijä saa hyvin määritellyn osuuden yrityksen toiminnoissa, joten voidaan arvioida, jos esim. järjestelmämuutoksen takia jokin alemmalla tietoturvatasolla oleva tietopääoma tulisi siirtää ylemmän tietoturvatason piiriin.

Tietoturvavaatimukset

Taulukko 15. Vaatimuksia suojattavien kohteiden vyöhykkeestä.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-SKV-001	Suojattavien kohteiden vyöhyke ja sen liityntäpisteet on tunnistettu: Kaikki kriittiset ja ei-kriittiset tietopääomat on tunnistettu ja suojattu niille määrätyllä tasolla, ml. pääsynvalvonta- ja monitorointijärjestelmät. Kommunikaatiolinkkien päätepisteet ovat liityntäpisteitä ko. vyöhykkeeseen.	Haastattelut, katselmoinnit	H
R-SKV-002	Liityntäpisteisiin pääsy on valvottu. Hallinnolliset ja tekniset kontrollimekanismit on määritelty: Liityntäpisteeseen on oletusarvoisesti kielletty pääsy. Järjestelmään on määriteltävä erityinen pääsyoikeus, kun pääsy halutaan sallia. Määritettynä: Pääsypyyntöjen (*access request*) ja valtuuttamisen (*authorization*) prosessit. Käytettävät käyttäjätunnistusmenetelmät. Valtuuksien jaon (*authorization rights*) prosessi. Liityntäpisteissä on aktivoituna ainoastaan operatiiviseen toimintaan tarvittavat portit ja palvelut. Sisään kirjauduttaessa tiedonanto (*banner*) käyttäjän edellisistä järjestelmään kirjautumisyrityksistä.	Haastattelut, Pääsynvalvonnan katselmointi, (porttiskannaus)	H/(T)
R-SKV-003	Ylläpidettävä pääsynvalvonnan lokia jatkuvasti (24/7) kaikissa vyöhykkeen liityntäpisteissä: Jos välitön hälytys tunkeutumisesta ei ole teknisesti mahdollista, täytyy loki katselmoida kolmen kuukauden välein laittoman tunkeutumisen havaitsemiseksi.	Haastattelut, lokikeräyksen katselmointi	H
R-SKV-004	Vähintään vuosittain tulee tehdä vyöhykkeen liityntäpisteiden haavoittuvuusanalyysi , jossa tulee - tarkistaa haavoittuvuusanalyysiprosessi	Haastattelut, katselmoinnit, (porttiskannaus),	H/T

	- tarkistaa, että vyöhykkeen liityntäpisteissä ainoastaan operatiiviseen toimintaan tarvittavat portit ja palvelut on aktivoituna – etsiä kaikki mahdolliset liityntäpisteet, joita vyöhykkeen sisälle pääsemiseksi on olemassa ja verrata tulosta dokumentoituihin liityntäpisteisiin - tutkia oletus (*default*) käyttäjätunnusten käyttö ja salasanat. Tarkistaa verkonhallintaan käytettävät tunnukset ja niiden käyttöoikeudet.	(verkkoskannaus), (haavoittuvuusskannaus)	
R-SKV-005	Dokumentaation on oltava katselmoitu ja ylläpidetty: Vastuullinen taho on tarkastanut vähintään vuosittain, että kaikki dokumentaatio vastaa nykyistä konfiguraatiota ja toimintaprosesseja. Päivitetty kolmen kuukauden kuluessa muutoksesta kaikki dokumentaatio siten, että se vastaa kaikkia verkkoon tai kontrolleihin tehtyjä muutoksia. Ylläpidetty pääsynvalvonnan lokia vähintään kolme kuukautta. Raportoitujen tietoturvatapahtumien dataa on säilytetty vähintään kolme vuotta.	Haastattelut, katselmoinnit	H

Päätoimenpiteet

- Inventoi ja ylläpidä tietoa kaikista laitteista, ohjelmistoista ym. tietopääomista, joilla järjestelmä on toteutettu ja joilla sen jatkuva toiminta varmistetaan.
- Määrittele suojattavien kohteiden vyöhykkeet, liityntäpisteet, tietoturvatasot sekä noudatettava tietoturvapolitiikka ja -vaatimukset.
- Määrittele hallinnolliset ja tekniset kontrollimekanismit pääsyn valvomiseksi liityntäpisteissä.

3.4.1.2 Verkkoarkkitehtuuri

Yleistä

Verkkolaitteita, kuten reitittimiä, keskittimiä, kytkimiä, palomuureja, IDS/IPS-laitteita sekä VPN-yhdyskäytäviä, käytetään verkon fyysiseen ja virtuaaliseen

muodostamiseen ja tiedon välittämiseen sekä verkon jakamiseen sopiviin hallittaviin osiin, esim. segmentteihin, joihin kytketyillä laitteilla on yhtenevä tietoturvataso. Lisäksi esim. kytkimen (portin) liikenne voidaan peilata toiseen porttiin, jota kuuntelemaan asetetaan verkkoa monitoroiva laite, esim. verkkoanalysaattori tai IDS.

Verkkoarkkitehtuurilla on suuri merkitys laitteiden välisen tietoliikenteen sujuvuuden ja turvallisuuden kannalta. Jos arkkitehtuuri on huonosti suunniteltu, tulee verkosta helposti fyysisesti ja loogisesti monimutkainen hallita ja, siinä kulkeva liikenne on vaikeasti hallittavaa ja siten turvatonta.

Verkko tulee jakaa toiminnallisesti eriytettyihin aliverkkoihin (*subnets*), joilla kullakin on oma mahdollisimman itsenäinen toimintansa. Aliverkkojen välissä käytetään usein kytkimiä, reitittimiä ja/tai palomuureja suodattamaan liikennettä. Aliverkot luokitellaan luokkiin (*Class* A, B tai C), joissa kussakin on laajempi tai suppeampi IP-osoiteavaruus. Lisäksi yksityisillä (*Private*) IP-osoitteilla on IANA:n (*Internet Assigned Number Authority*) määrittelemä oma osoiteavaruutensa, jota ei reititetä internetiin, mutta sitä ei yleensä ole tarpeen käyttää automaatioverkoissa.

Demilitarisoitu vyöhyke (DMZ) on erittäin tärkeä aliverkkotyyppi, jolla erotellaan vahvasti muita aliverkkoja toisistaan. Tyypillisesti DMZ:n eri puolille sijoitetaan eriytetyllä päätarkoituksella ja tietoturvatasolla varustettuja aliverkkoja (toimistoverkon toiminteet sijaitsevat yhdellä puolella ja automaatioverkon aliverkot toisella jne.). Organisaation ulkopuoliseen verkkoon luotetaan yleensä vähemmän kuin sisäiseen verkkoon. Mitä suurempi joukko aliverkossa on toimijoita, sitä vähäisempää luottamusta verkkoa kohtaan kannattaa osoittaa. Käytännössä automaatioverkossa olevia toimijoita kannattaa pyrkiä rajoittamaan ja kontrolloimaan tiukin tietoturvasäännöin, kun taas toimistoverkossa saatetaan sallia enemmän vapauksia esim. käytettyjen ohjelmistojen suhteen. Jos näiden verkkojen on oltava yhteydessä toisiinsa, niiden välissä on oltava DMZ, jossa oleviin palvelimiin on pääsy ainoastaan ennalta määritellyistä tietokoneista ja sovelluksista. Usein on parasta määritellä, että mitään tietoa ei saa siirtyä suoraan aliverkkojen välillä. Seurattavaksi tarkoitettu data (esim. Modbus) lähetetään automaatioverkosta päin (jos mahdollista tietoturvallisella) tiedonsiirtomenettelyllä DMZ:ssa olevaan palvelimeen, jossa se tallennetaan ja esikäsitellään. Kyseisten tietojen kyselyt ko. DMZ-palvelimelta sallitaan ainoastaan esim. käyttäjätunnistetulla HTTPS-yhteydellä toimistoverkon suunnasta, joten liikenne/hyökkäysyritykset toimistoverkosta automaatioverkkoon voidaan estää. Modbus-liikennettä ei sallita toimistoverkkoon tai toimistoverkosta. Eksplisiittinen, turvallinen pääsynvalvonta on oltava toteutettu sekä DMZ:n rajapintojen

palomuureissa (*default deny* -säännöt) että DMZ:n palvelinkoneissa (pääsynvalvontalistat).

Uhkat

Häiriöiden vaikutusalue: Jos esimerkiksi palvelinklusteria ei ole eristetty omaan aliverkkoonsa, saattaa vika toimistoverkon laitteessa aiheuttaa ongelmia palvelujen saatavuuteen kaikille käyttäjille. Samoin toimistoverkossa oleva tietokone saattaa aiheuttaa häiriöitä automaatioverkkoon, jos verkkoja ole eriytetty kunnolla toisistaan.

Jos kovin heterogeeninen tietoliikenne sallitaan aliverkkojen välillä, saattaa hyökkääjä päästä tunkeutumaan järjestelmiin, joihin hänellä ei ole pääsyoikeutta. Lisäksi esim. ohjelmistopäivitysten takia verkkoon voi kulkeutua sinne kuulumatonta tietoliikennettä, joka saattaa haitata luotetun verkon toimintaa. Jos aliverkoissa kulkevaa tietoliikennettä tai lokeja ei monitoroida, saattaa asiaton tunkeutuja jäädä havaitsematta ja laitteissa olevia mahdollisia haavoittuvuuksia saatetaan päästä hyödyntämään tuhoisin seurauksin. Samalla tavoin, mikäli DMZ:ssa sijaitsevan IDS:n tai muun monitorointijärjestelmän lokitietoja ei säännöllisesti tarkkailla ja sääntökantoja päivitetä, saatetaan järjestelmiin ajan kuluessa tunkeutua sitä havaitsematta.

Tietoturvavaatimukset

Taulukko 16. Verkkoarkkitehtuurin tietoturvavaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-VA-001	Turvallinen ja vikasietoinen tietoverkko-arkkitehtuuri aliverkkoineen on määritelty.	Haastattelut, verkkoarkkitehtuurikatselmoinnit	H/T
R-VA-002	Kaikki eri turvatasoilla olevien aliverkkojen väliset tietovuot on määritelty. Automaatio/toimistoverkkoliityntä: Tiedon turvallinen siirto DMZ:n palvelimen kautta. DMZ:ssa sallittu liikennöinti on rajattu, poikkeamat estetty, toteuma monitoroitu. Jokaisen sallitun tietovuon lähde (*source*) ja kohde (*destination*) on määritelty ja sellaisenaan toteutuva myös järjestelmän uudelleenkäynnistyksessä. Tietoturvataso on ylläpidetty verkon muutoksissa.	Haastattelut, tietoliikennedokumentaatio, konfiguraatio-, loki- ja monitorointitietojen katselmoinnit	H/T

R-VA-003	Aliverkkojen hätäirtikytkentä on suunniteltu ja prosessi verifioitu. Aliverkon sisäisen toiminnallisuuden tulee toimia itsenäisesti (testattu).	Hätäirtikytkennän ohjeen ja testien katselmoinnit	H/T
R-VA-004	Jokaisen suojattavien kohteiden vyöhykkeen (sis. DMZ) suodatussäännöt, monitorointi ja sääntökanta on määritelty hälytyslaukaisumääreineen. Ulospäin suuntautuva liikenne on suodatettu. Poikkeamista on suoritettu hälytykset.	Suodatussääntöjen ja monitoroinnin toiminteiden katselmoinnit	H/T
R-VA-005	DMZ on kahdennettu eri valmistajien laitteilla, mikäli se on tarpeen luotettavan toiminnan varmistamiseksi. Varmistettu, että varalla olevaa DMZ-järjestelmää voidaan korjata toiminnan häiriintymättä.	Varayhteys on määritelty ja testattu	H/T

Päätoimenpiteet

- Verkkoarkkitehtuurin, verkkosegmentoinnin, aliverkkoihin jaon, alitoimintojen jaon jne. tulee olla selkeästi määritettyjä ja loogisia.
- Jaa verkko yksinkertaisiin, helposti hallittavissa oleviin segmentteihin, joissa kussakin suoritetaan määriteltyä toimintaa ja joissa laitteiden ja ohjelmistojen toiminnallisuus sekä tietoturvavaatimukset ovat yhtenevät. Varmista että verkon toiminta on turvattu poikkeustilanteissa.
- Määrittele ja rajoita aliverkkojen keskinäiset sekä sisäiset tietovuot vain toiminnalle välttämättömiin. Suunnittele ja toteuta kaikki tietoturvatoiminnallisuudet siten, että ne eivät aiheuta riskiä välttämättömille toiminnoille.

3.4.1.3 Verkkolaitteet

Uhkat

Esim. verkon reitittimissä voi olla sulautettuna käyttöjärjestelmä, jossa on tietoturvahaavoittuvuuksia. Näin ollen verkkolaitteitakin on tarpeen päivittää ja päivitykset on tehtävä tietoturvallisesti, jottei järjestelmään tulisi uusia häiriötekijöitä. Verkkoon saatetaan lisätä asiattomia laitteita, mikäli verkkoon pääsyä ei ole

valvottu eri tasoilla. Aliverkkoihin voidaan yrittää syöttää suuria määriä häirintädataa, ellei liikennetulvaa pystytä estämään esim. palomuurissa, reitittimessä tms.

Tietoturvavaatimukset

Taulukko 17. Verkkolaitteiden tietoturvavaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-VL-001	Verkkolaitteita pystytään hallinnoimaan käytännöllisellä tavalla ja verkon kaikki konfigurointirajapinnat ovat tietoturvallisia. Kaikki tarpeettomat verkkokonfigurointi- ja hallinnointitoiminnot on poistettu käytöstä.	Laitehallintatoiminnan tarkistus, katselmoinnit, haavoittuvuus/ porttiskannaus	H/T
R-VL-002	Laitetoimittajan on esitettävä laitteidensa vaatimat pääsynvalvontalistat (ACLs) sekä porttien turvallinen konfiguraatio.	Pääsynvalvontasäännöstöjen katselmoinnit, konfiguraatiotiedot	H/T
R-VL-003	Laitetoimittajan on esitettävä laitteidensa toiminnan tarvitsemat palomuurisäännöt. Toimituksen yhteydessä toimitetaan spesifikaatio järjestelmän tietoliikenteestä, ml. protokollat, sisään ja ulos suuntautuva liikenne, sekä kaikkien niiden verkkoyhteyslaitteiden tunnukset joista yhteydenotot järjestelmän suuntaan on sallittu.	Palomuurisääntöjen katselmoinnit	H/T
R-VL-004	Toimittajan on esitettävä toimintojensa vaatima verkko-IDS laitteiden säännöstö sekä relevantit lokien seurantatyökalut.	Katselmoinnit	H/T
R-VL-005	VPN-palvelinten yhteistoiminta muiden verkkolaitteiden kanssa on varmistettu.	VPN-konfiguraation katselmoinnit	H/T
R-VL-006	Toimittaja on verifioinut laitteen tai ohjelmiston sovitun tietoturvatason.	Katselmoinnit	H
R-VL-007	Kokonaistoimittaja on tehnyt testiverkkoon porttiskannauksen ja dokumentoinut kaiken verkkoliikenteen alkuperän ja toiminnot porttitasolla.	Katselmoinnit	H/T
R-VL-008	Toimittaja on validoinut kaikki laitteen/ ohjelmiston tarvitsemat käyttöoikeudet ja tietoturva-asetukset baseline-järjestelmästä ennen päivitystä tai korvaavan laitteen asennusta.	Katselmoinnit	H

Päätoimenpiteet

- Verkkolaitteiden hankintojen ja toimitusten, hallinnan, asennuksen, konfiguroinnin, käytön ja ylläpidon tulee olla huolella suunniteltua.
- Toiminnan vaatiman tiedonsiirron spesifikaatioiden, tiedon suodattamisen säännöstöjen, sallittujen konfiguraatioiden ja laitteiden yhteistoiminnan tulee olla tarkkaan määriteltyä.
- Verkossa virtaa ainoastaan etukäteen määriteltyä tietoa, protokollia ja sovellusdataa sillä tavoin, että verkon toiminta kokonaisuutena on hyvin hallittavissa, riittävän yksinkertaista ja selkeää.

3.4.1.4 Verkon reunojen suojaus – palomuurit

Yleistä

Palomuuri on tärkeä väline, kun suojattavaan järjestelmään tai verkkoon tulevaa tai lähtevää asiaankuulumatonta tietoliikennettä halutaan rajoittaa (*blocking* / *filtering*). Se on kuitenkin vain yksi keino muiden joukossa erottaa turvallisia ja turvattomia järjestelmiä toisistaan. Palomuuri ei pysty havaitsemaan ja poistamaan sovellustasolla tai vasta sen yläpuolella havaittavissa olevaa epätoivottua verkkoliikennettä.

Uhkat

Palomuurilla voidaan estää tarpeettomat tietoliikenneyhteydet verkkojen väliltä. Valitettavasti on helppoa käyttää palomuureja myös turvattomilla tavoilla, mm. huolimattomuuden tai tietämättömyyden seurauksena, jolloin syntyy päinvastoin harhaanjohtava tunne hyvin turvatusta aliverkosta. Haitallista tietoliikennettä voi kulkea sallituissakin porteissa. Palomuuri ei tarjoa suojaa kaikilla tietoturvan osa-alueilla. Palomuurisääntöjen päivitys täytyy hoitaa vaarantamatta verkon suorituskykyä, sillä säännöstöt saattavat olla hyvin suurikokoisia varsinkin sovellustason palomuureissa ja IDS-järjestelmissä. Palomuurien toimintaa on tarve monitoroida, järjestää lokitapahtumaseuranta esim. myöhempää forensiikkatutkimustarvetta ajatellen.

Tietoturvavaatimukset

Taulukko 18. Palomuureihin liittyviä tietoturvavaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-FW-001	Toimittaja on määritellyt hyväksymänsä palomuurilaitteet ja palomuurisäännöt.	Säännöstöjen katselmointi	H/T
R-FW-002	Palomuurityypin ja -toiminnallisuuden vastattava tarvetta.	Haastattelut	H
R-FW-003	Palomuurisääntöjen pohjana oltava tietoliikenteen kielto (*deny all*), jonka lisäksi on määritelty ainoastaan järjestelmän vaatima, sallittu tietoliikenne.	Säännöstöjen katselmointi	H/T
R-FW-004	Palomuurisääntöjen päivitys on hoidettava vaarantamatta verkon suorituskykyä.	Ohjeiston katselmointi	H
R-FW-005	Automaatioverkkoon päin tuleva liikenne pitää kieltää. (Tieto siirretään DMZ-palvelimen välityksellä.)	Säännöstöjen katselmointi	T
R-FW-006	Automaatioverkosta ulospäin tuleva liikenne tulee rajoittaa vain välttämättömään, määrättyyn DMZ-palvelimeen lähetettävään tietoon (lähde/kohde, palvelu/portti).	Säännöstöjen katselmointi	T
R-FW-007	Käytä koeteltua lähtökohtaa palomuurisääntöjen määrittelemissä. Tee riskiarvio jokaisesta protokollasta.	Haastattelut, katselmointi	H
R-FW-008	Palomuurien lokitietoja on pystyttävä seuraamaan laitteelta säännöllisesti ja turvallisesti.	Katselmointi	T

Päätoimenpide

- Palomuurien käyttö täytyy suunnitella huolellisesti ja käytettävät säännöstöt on määriteltävä mahdollisimman rajoittaviksi ja sallia ainoastaan ennalta määrätty liikenne.
- Tärkeää on valita sopivin palomuurityyppi (*packet filter, stateful inspection, application level*) ja järjestää palomuurien lokitapahtumien seuranta.

3.4.1.5 Verkkoliikenteen seuranta

Yleistä

Verkko-IDS (eli NIDS) järjestelmillä pyritään tunnistamaan järjestelmään kuulumatonta verkkoliikennettä, jotta voitaisiin havaita järjestelmävikoja tai tunkeutumisyrityksiä verkottuneisiin järjestelmiin. NIDS-järjestelmän toiminta voi perustua verkkoliikenteen analyysiin joko

- tunnettuja haavoittuvuuksia ja haittaohjelmia tunnistamalla (*signature*-perusteinen) tai
- verkkoliikenteen havaittuihin poikkeavuuksiin normaalitilanteeseen verrattuna (*anomalia*-perusteinen).

NIDS ei ole perinteisesti ollut välttämätön osa automaatioverkkojen suojausta, mutta siitä on kehittymässä suhteellisen kevyt tapa monitoroida tietoverkon tapahtumia. Järjestelmälokien tarkkailu on ollut perinteinen tapa hoitaa tietoturvatilanteen seurantaa.

Uhkat

Järjestelmään kuulumaton verkkoliikenne on merkki järjestelmään tunkeutumisesta tai sen yrityksestä. Verkkoliikenteen seurannalla voidaan yleensä havaita ennalta tunnettuja ongelmia varsin hyvin. Lisäksi laiterikkoja ja väärin konfiguroituja laitteita saatetaan tunnistaa verkkoliikenteen seurannalla.

Tietoturvavaatimukset

Taulukko 19. Verkko IDS:ään liittyviä vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-MO-001	Verkkodatan keruupisteiden on oltava huolella valittuja. Esim. järjestelmän kriittiset pisteet / pisteet, joiden kautta kaikki liikenne kulkee.	IDS-järjestelmä-konfiguraation katselmointi	T/H
R-MO-002	Toimittajan on esitettävä järjestelmänsä sallitut liikennemäärät palveluittain sekä tunnetut signatuurit. Päivitysprosessi on määritetty.	Katselmoinnit	T/H
R-MO-003	NIDS-järjestelmän konfiguraatio on määritetty ja suojattu hyvin ulkopuolisilta.	Haastattelut	T/H

Päätoimenpide

- Verkkoliikenteen monitorointitarve selvitetään riskiarvioinnin avulla. Tarvittaessa suunnitellaan ja järjestetään soveltuva NIDS-järjestelmä, jonka toimintaa ja tuloksia seurataan, ylläpidetään ja turvataan.

3.4.1.6 Isäntäkoneiden seuranta

Yleistä

Erityisesti toimistoverkossa käytettävien palvelinten ja isäntäkoneiden toiminnallisuus on varsin mittavaa ja usein melko heterogeenistä. Tämä tarkoittaa samalla, että niiden turvallista konfiguraatiota voi olla vaikea hallita. Isäntäkoneisiin saattaa siirtyä haitallista koodia (esim. haittaohjelmia), jolla voi olla negatiivisia vaikutuksia alkuperäisiin käyttötarkoituksiin ja toimintoihin.

Uhkat

Toimistoverkon isäntäkoneet ovat alttiita haittaohjelmille ja hyökkääjien tunkeutumisyrityksille, joten tunkeutumisen havaitseminen on erittäin tärkeää vahinkojen minimoimiseksi. Sen sijaan automaatioverkossa itse tunkeutumisen havaitsemisjärjestelmät, esim. *Host-based IDS* (HIDS), saattavat aiheuttaa yllättäviä

viiveitä varsinaiseen toiminnallisuuteen, joten HIDS:n käyttöönoton edut ja haitat tulee punnita tarkoin.

Tietoturvavaatimukset

Taulukko 20. Host IDS:ään liittyviä suosituksia.

ID	Suosituksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-HO-001	HIDS-järjestelmän toimintaa määrittävän konfiguraation ja ohjeistuksen tulee sisältää: - Tiedostot, tarkkailtavat tiedostonimet, tiedostonnimijoukot (patterns). - Käyttäjätilit, järjestelmäkäyttäjätilit. - Oikeudet tarvittavien ohjelmien ajamiseksi, konfiguroimiseksi ja muu vastaava isäntäkoneen yhteistoiminta HIDS-järjestelmän kanssa.	Katselmoinnit	H/T
R-HO-002	Varmistettava, että käyttöönotettava HIDS-konfiguraatio ei häiritse käyttöjärjestelmän toimintaa eikä liiketoiminnan jatkuvuutta.	Katselmoinnit, haastattelut	H/T
R-HO-003	Kaikista käyttäjä- ja järjestelmäkäyttäjäistunnoista kerätään lokitietoa ja automaattinen hälytysten lähettäminen on mahdollista.	Katselmoinnit	H/T
R-HO-004	Lokianalyysi ja lokitulosten viestintä toimii käytännössä.	Katselmoinnit, haastattelut	H/T
R-HO-005	HIDS ei saa pystyä muuttamaan isäntäkoneen tai (oheislaitteiden) konfiguraatiota tai tiedostoja.	Katselmoinnit, haastattelut	H/T
R-HO-006	Järjestelmätoimittajan erikoistoimenpiteet: HIDS-ohjelmiston oikea toiminta testattava. ”*System image*” generoitava vertailukohdaksi. Operaattorin kanssa sovitulla tavalla / ajankohtana pitää päivittää HIDS-järjestelmän ohjelmisto ja sääntökanta ym. säilyttäen tietoturvan taso vakaana.	Katselmoinnit, haastattelut	H/T

Päätoimenpiteet

- Hallinnoitava ja kontrolloitava HIDS-järjestelmien käyttöä toimistoverkon isäntäkoneissa.
- Automaatioverkossa HIDS:n käyttöönoton ja käyttötapojen edut ja haitat tulee punnita erityisen tarkoin.

3.4.1.7 Käyttäjätilien hallinta ja pääsyn valvonta

Yleistä

Käyttäjätilien hallinnalla tarkoitetaan järjestelmiin pääsyn systemaattista kontrolloimista. Toisin sanoen: määritellään tarkasti kenellä on pääsyoikeus järjestelmään ja millä käyttäjäoikeuksilla. Taustalle tarvitaan tietenkin tietojärjestelmät, esim. Microsoft Active Directory, SELinux, FreeBSD, SAP R/3 -järjestelmät, jne., joissa on pääsynvalvonnan tuki. Yleensä pääsykontrolleissa kannattaa noudattaa minimioikeuksiin ja -tarpeeseen perustuvaa sääntöä, jolloin esim. käyttäjätiliin kohdistuneen onnistuneen hyökkäyksen vaikutusalue minimoituu.

Käyttäjäkohtaiseen pääsynvalvontaan liittyy seuraavien asioiden hallinnointia:

- Tunnistautuminen (*User Authentication*)
- Valtuutus (*Authorization*)
- Käyttäjätapahtumien kirjanpito (*Accounting*) tai (*Audit trail*).

3.4.1.7.1 Käyttäjätilien rajoittaminen

Yleistä

ICT-alueella on yleistä, että laitteet ja järjestelmät toimitetaan tilaajalle kokoonpanossa, jossa niihin on esim. asennuksen tai ylläpidon helpottamiseksi jätetty oletusarvoisia (*default*, *guest* tai *anonymous*) käyttäjätunnuksia ja salasanoja. Tällaiset tunnukset ovat yleisesti tiedossa, joten teollisuusautomaatiossa oletusarvoisten käyttäjätunnusten jättäminen toimitettavaan laitteeseen ei ole hyväksyttävää, sillä niiden passivoinnin unohtuessa seuraukset voisivat olla tuhoisat. Asennuksessa ja käyttöönotossa tarvittavat tunnukset on lähetettävä erikseen ja suojattuina.

Uhkat

Jos järjestelmään on jostain syystä jäänyt aktiiviseksi *default*-käyttäjätunnuksia, joihin liittyy yleisesti tunnettuja salasanoja tms., voidaan järjestelmää kohtaan helposti hyökätä ja tunkeutumista voi olla erittäin vaikea havaita. *Default*-tunnusta käyttämällä hyökkääjä voi tavoitella pääsyä jopa järjestelmäkäyttäjäksi.

Tietoturvavaatimukset

Taulukko 21. Käyttäjätilien rajoittamiseen liittyviä vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-KT-001	Välttämättömät, aktivoitavat käyttäjätunnukset on identifioitu.	Katselmoinnit	H
R-KT-002	Tarpeettomat, poistettavat käyttäjätunnukset on identifioitu.	Katselmoinnit	H
R-KT-003	Välttämättömät käyttäjätunnukset on aktivoitu.	Katselmoinnit	H/T
R-KT-004	Kaikki tarpeettomat käyttäjätunnukset on poistettu käytöstä viimeistään ennen käyttöönottoa.	Katselmoinnit	H/T
R-KT-005	Sallittujen ja kiellettyjen käyttäjätunnusten aktivointi, poisto, näiden ajankohta ja vastuullinen osapuoli on määritelty.	Katselmoinnit	H
R-KT-006	Käyttöön tulevat käyttäjätunnukset ja salasanat on toimitettu käyttöönottajalle salattuna, tietoturvallisella menettelyllä.	Katselmoinnit	H/T
R-KT-007	Uusia käyttäjätunnuksia ei luoda tai aktivoida ilman erityistä tilaajan/ käyttöönottajan vaatimusta.	Katselmoinnit	H/T

Päätoimenpiteet

- Uhkia aiheuttavat käyttäjätunnukset poistetaan käytöstä mahdollisimman varhaisessa vaiheessa järjestelmistä.
- Käytössä sallitaan ainoastaan tarpeelliset, hyvin määritellyt ja hallitut käyttäjätunnukset ja salasanat.

3.4.1.7.2 Istuntojen hallinta

Yleistä

Monissa vanhemmissa järjestelmissä saattaa olla käytössä yhteyskäytäntöjä kuten telnet, tai tiedonsiirtoprotokollia kuten FTP, joiden tietoturvaominaisuudet ovat heikot. Käyttäjää ei niissä tunnisteta luotettavasti, tietoja lähetetään salaamattomina tms. Tämä ei ole nykyään hyväksyttävää, sillä turvallisempia yhteys- ja tiedonsiirtomenetelmiä on usein helposti saatavilla.

Uhkat

Asiattomat henkilöt tai vakoiluohjelmat voivat päästä järjestelmiin ja niiden tietoihin käsiksi istuntoja nauhoittamalla tai kaappaamalla, mikäli turvallisia tiedonsiirtoprotokollia ei käytetä eikä istuntoja hallinnoida turvallisella tavalla. Erityisesti käyttäjätunnukset ja salasanat ovat tyypillisesti tiedustelun kohteina, sillä ne mahdollistavat pääsyn tietojärjestelmiin sisään.

Tietoturvavaatimukset

Taulukko 22. Istuntojen hallintaan liittyviä tietoturvavaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-LO-001	Järjestelmä ei lähetä käyttäjätunnus- ja salasanatietoja salaamattomina. Käytettävä yhteysprotokolla ja salausalgoritmi on valittu riittävän turvallisiksi, silti varmistaen riittävän käytettävyyden.	Katselmoinnit	H/T
R-LO-002	Järjestelmäistunto (*login*) on hallinnoitu turvallisesti. Tuplaistunnot, saman istunnon tietojen pidempiaikainen hyödyntäminen ja ”*auto-fill*” toiminnallisuus ovat yleensä turvattomia.	Katselmoinnit	H/T
R-LO-003	Peräkkäisten epäonnistuneiden kirjautumisyritysten määrää seurataan ja rajoitetaan pääsy rajan ylittyessä.	Katselmoinnit	H/T
R-LO-004	Istunnon pituutta ja automaattista uloskirjausta koskevat asetukset ovat käyttäjäkohtaisesti säädettävissä. Käytettävyydelle ja turvallisuudelle sopivimmat asetukset on aktivoitu kullekin käyttäjälle.	Katselmoinnit	H/T

Päätoimenpide

- Turvattomat protokollat poistetaan käytöstä, mikäli niille on turvallisempi vaihtoehto saatavilla. Turvattomat istuntojen hallintatavat poistetaan järjestelmän yhteyskäytännöistä.
- Tuloksena järjestelmässä on käytössä vain turvalliset tiedonsiirtoprotokollat ja -istunnot, kuten SFTP, HTTPS/TLS ja SSH, ja joiden käyttäjiä ja tunnuksia hallinnoidaan keskitetysti ja turvallisin menettelyin.

3.4.1.7.3 Käyttäjätunnuspolitiikka

Yleistä

Automaatiojärjestelmissä on usein vaatimuksena välitön pääsy järjestelmään esim. hätätilanteen sattuessa. Tästä voi aiheutua, että liian monen operatiivisen järjestelmän salasanakäytäntöihin liittyvä politiikka tai käytännöt ovat tarpeettoman sallivia ja turvattomia. Lisäksi valitut salasanat saattavat olla turvattomia.

Uhkat

Hyökkääjät pyrkivät selvittämään heikkoja salasanoja ns. ”*brute force*” - ja sanakirjahyökkäysten avulla, jolloin heikko salasana saattaa paljastua muutamissa minuuteissa. ”*Social engineering*” on yleinen uhka, jossa järjestelmän käyttäjiä harhautetaan paljastamaan salasanoja ja käyttäjätunnuksia hyökkääjiä edustavalle taholle.

Tietoturvavaatimukset

Taulukko 23. Käyttäjätunnuspolitiikkaan liittyviä vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-KP-001	Salasanat eivät saa esiintyä selväkielisenä ohjelman lähdekoodissa tai konfiguraatiotiedostoissa.	Käyttäjätunnuspolitiikan ja tiedostojen katselmoinnit	H/T
R-KP-002	Salasanan pituus ja kompleksisuus ovat turvallisella tavalla määrättyjä. Salasanan kelpoisuusaika ja uusiokäyttö ovat rajattuja. Sovellettava standardi on spesifioitu salasanojen vahvuudesta, esim. NIST, NERC tai ISA. Salasanojen käytön ohjeiston laatiminen voidaan perustaa esim. [FIPS112]-standardiin.	Käyttäjätunnuspolitiikan katselmointi	H/T
R-KP-003	Käyttäjätilien hallintajärjestelmään on hyvin määritelty ja rajoitettu pääsy. Laitevalmistaja ei voi tehdä muutoksia käyttäjätileihin ilman sovittua menettelyä.	Käyttäjätunnuspolitiikan katselmointi	H
R-KP-004	Hätätilanteita varten järjestelmään on määritelty nopeasti käyttöönotettavissa oleva rajattu pääsy (käyttäjältä unohtunut henkilökohtainen salasana).	Käyttäjätunnuspolitiikan katselmointi	H

Päätoimenpiteet

- Pääsynvalvontaan liittyviä käyttäjätilejä ja salasanoja tulee kontrolloida turvallisilla hallinnollisilla ja teknisillä prosesseilla. Kuitenkin on suunniteltava riittävä järjestelmään pääsy hätätilanteiden varalta.
- Päätuloksena on, että kaikkien käyttäjätilien ja salasanojen tiedot käsitellään aina luottamuksellisesti ja yhteisen menettelytavan mukaisesti. Tarpeettoman heikkoja salasanoja tai heikkoja salasanakäytäntöjä ei esiinny järjestelmässä.

3.4.1.7.4 Käyttäjäoikeudet

Yleistä

Käyttöjärjestelmät ja tiedostojärjestelmät toimitetaan usein oletusarvoiltaan (*default*) hyvin rajoittamattomilla (pääsy)oikeuksilla ja konfiguraatiolla. Kriittisiin käyttäjäoikeuksiin lukeutuvat käyttöjärjestelmätasolla usein mm. järjestelmän palautustoiminteet, etäyhteydet ja diagnostiikka.

Uhkat

Järjestelmän oletusasetukset ovat suuri uhka järjestelmän tietoturvalle, sillä ne voivat mahdollistaa tunkeutujalle pääsyn kriittisiin järjestelmätoimintoihin. Pääsyoikeudet täytyy määritellä ja pakottaa tehokkaasti myös käyttöjärjestelmätasolla.

Tietoturvavaatimukset

Taulukko 24. Käyttäjäoikeuksien minimimäärään liittyviä suosituksia.

ID	Suosituksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-OS-001	Järjestelmä tulee olla saatavana minimi-ominaisuuksilla ja -oikeuksilla, jotta tarvittavat palvelut ja oikeudet voidaan sallia vasta käyttöönottovaiheessa asennuskohteen säännöstön mukaisesti.	Käyttöjärjestelmäoikeuksien katselmointi, haastattelut	H/T
R-OS-002	Järjestelmäpalveluita on sallittava kullekin käyttäjälle vain hänen työssään tarvitsema minimimäärä. Tämä tulee toteutua päivitystenkin yhteydessä.	Käyttöjärjestelmäoikeuksien katselmointi, haastattelut	H/T

Päätoimenpide

- Järjestelmien oletusasetukset tulee rajoittaa sallimaan ainoastaan perustoiminnot. Kullekin käyttäjälle sallitaan ainoastaan vaaditut minimioikeudet järjestelmiin.

3.4.1.7.5 Käyttäjätilien seuranta

Yleistä

Käyttäjätilit on luotu, jotta järjestelmään pääsyä voitaisiin kontrolloida halutulla tavalla. Yleensä on lisäksi tarpeellista seurata, että luotuja käyttäjätilejä ei ajan kuluessa käytetä väärin. Tämä tehdään generoimalla lokitiedostoa eri käyttäjätileihin liittyvistä aktiviteeteista. Lokeja seuraamalla pyritään havaitsemaan tunkeutumisia, niiden yrityksiä tai muuta poikkeavaa sekä väärinkäytösten sattuessa kerättyä tietoa käytetään mm. erilaisiin forensiikkatarkoituksiin.

Uhkat

Asiaton järjestelmään tunkeutuminen hyväksytyillä käyttäjätunnuksilla on erittäin vakava uhka. Tunkeutuja voi pyrkiä peittämään jälkensä modifioimalla järjestelmälokeja tai muita tietoja, joilla järjestelmän käyttöä valvotaan.

Tietoturvavaatimukset

Taulukko 25. Käyttäjätilien seurantaan liittyviä tietoturvavaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-TS-001	Järjestelmä seuraa määriteltyjä käyttäjäaktiviteetteja ja politiikan muutoksia yksittäisen käyttäjän tarkkuudella tallentaen tapahtuman tarkan ajan (time stamp) ja ”paikan”.	Lokitietojen katselmointi	H
R-TS-002	Generoitu lokitiedosto tallennetaan siten, että sitä ei voida luvatta lukea eikä muokata (read-only media). Lokidataa seurataan säännöllisesti mahdollisten poikkeamien havaitsemiseksi.	Katselmointi, haastattelut	H/T
R-TS-003	Lokidatan keräys ja käsittely eivät saa vaarantaa järjestelmän suorituskykyä missään olosuhteissa.	Suorituskyvyn katselmointi	H/T

Päätoimenpide

- Väärinkäytösten varalta on tarpeellista seurata, että luotuja käyttäjätilejä ei ajan kuluessa käytetä väärin; ettei asiattomia tapahtumia tai käyttäjätilejä ei esiinny.
- Päätuloksena järjestelmässä tulee olla käytössä käytännöllinen seurantatoiminto, jossa tietoturvalle oleellisia tapahtumia seurataan jatkuvasti, aina yksittäisen käyttäjätilin tarkkuudella.

3.4.1.7.6 RBAC pääsynvalvonta

Yleistä

Vanhentunut tapa toteuttaa pääsynvalvonta perustuu ainoastaan yhteen pääsyoikeustasoon, jossa jokainen järjestelmän käyttäjä saa täydet oikeudet järjestelmän eri toimintojen käyttämiseksi. Vaikka tämä onkin käytössä joissakin tämänhetkisissä järjestelmissä (*legacy systems*), ei se uusissa järjestelmissä ole hyväksyttävää. Nykyään ymmärretään tarve määritellä tarvittavat käyttöoikeudet roolipohjaisesti käyttämällä ns. *Role-Based Access Control* (RBAC) -pohjaista järjestelmää. Tällaisessa järjestelmässä kullekin käyttäjälle voidaan määritellä hänen kulloisiinkin rooleihinsa sopivat käyttäjätunnukset, joiden käyttöoikeudet rajoitetaan ainoastaan hänen nykytehtävilleen tarpeellisiin oikeuksiin. Nykyään jo monet järjestelmät tukevat roolipohjaista pääsynvalvontaa mm. Microsoft Active Directory, SELinux, FreeBSD, Solaris, Oracle DBMS, SAP R/3 jne. kuuluvat näihin.

Uhkat

Mikäli roolipohjaista pääsynvalvontaa ei ole toteutettu, asiaton järjestelmään pääsy mahdollistaa hyökkääjälle kaikki mahdolliset järjestelmän väärinkäytön tavat. Tunkeutumisia on lisäksi vaikea havaita, koska käyttäjällä on valmiiksi laajat oikeudet toteuttaa mitä erityyppisimpiä tavoitteita.

Tietoturvavaatimukset

Taulukko 26. Roolipohjaiseen pääsynvalvontaan liittyviä vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-RB-001	Erityyppiset tehtävät on roolitettu ja kullekin roolille on määritetty tietyt, sallitut tehtävät. Eriyttää voidaan mm. ohjausjärjestelmän eri sovellukset, järjestelmäoperointi, tietyn tietokannan hallinta, käyttöliittymän ylläpito jne. Kullekin roolille on järjestelmään määritelty ainoastaan välttämättömiä (least privileged) pääsyoikeuksia rooliin kuuluvien tehtävien suorittamiseksi.	Haastattelut	H/T
R-RB-002	Roolit, niihin liittyvät käyttäjäoikeudet, sovellukset, käyttäjätilit, tunnukset ja muu informaatio on dokumentoitu ja suojattu asiattomalta pääsyltä tietoturvamenettelyin. Ainoastaan hyväksytyillä järjestelmäylläpitäjillä on oikeudet lukea ja muokata pääsyoikeuksienhallintajärjestelmää ja käyttäjien rooleja ja oikeuksia. Toimittaja ei saa tehdä muutoksia näihin ilman erityistä lupaa.	Käyttöoikeus- ja pääsynvalvontasäännöstö, haastattelut, katselmoinnit	H/T
R-RB-003	Järjestelmätasolla on määritelty laitteiden kommunikaatioprioriteetit, esim. kunkin kommunikaatiosekvenssin käynnistäjinä toimivat verkkolaitteet ja sovellukset, sekä sallitut kommunikaatioreitit.	Järjestelmäkonfiguraation katselmointi	H/T
R-RB-004	Käyttäjä ei voi lisätä itselleen käyttöoikeuksia kirjautumatta ensin laillisesti sisään jollain muulla lisäoikeuksia antavalla käyttäjätunnuksella.	Katselmoinnit	H/T

Päätoimenpiteet

- Uusien järjestelmien tulee käyttää roolipohjaista pääsynvalvontajärjestelmää, jossa kullakin käyttäjällä on aina ajantasaisesti määritelty rooli tai rooleja, joilla on tietyt rajatut käyttöoikeudet järjestelmän toimintoihin.
- Kukin käyttäjä on oikeutettu tekemään ainoastaan omassa työtehtävässä tarpeellisia toimintoja, jolloin väärinkäytösten mahdollisuus on minimoitu, samoin mahdollisten hyökkäysten vaikutusalue on rajattu.

3.4.1.7.7 SSO – ”Single Sign-On”

Yleistä

SSO eli ”*Single Sign-On*” on käyttäjätunnistukseen liittyvä järjestelmä, jossa käyttäjän suorittama yksittäinen hyväksytty sisäänkirjautuminen sallii hänelle (mm. roolipohjaisen pääsynvalvonnan RBAC:n avulla) pääsyn myös muihin hänelle sallittuihin järjestelmiin ilman erillistä sisäänkirjautumista kyseisiin järjestelmiin.

Uhkat

SSO-järjestelmä tuo mukavuutta useiden käyttäjätunnusten rasittamille käyttäjille, mutta toisaalta SSO-järjestelmän joissain toteutuksissa on ilmennyt tietoturvahaavoittuvuuksia, esim. selaimen evästeisiin liittyen. Nämä haavoittuvuudet saattavat helpottaa asiattomien tunkeutujien pääsyä kyseisiin järjestelmiin, joten järjestelmät on suunniteltava ja toteutettava huolella.

Tietoturvavaatimukset

Taulukko 27. SSO:hon liittyviä vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-SS-001	SSO-järjestelmä on toteutettava käyttäen roolipohjaista pääsynvalvontaa ja vahvaa käyttäjätunnistusta (mm. *two-factor authentication*). Heikosti hallinnoitujen yhtäaikaisten käyttäjäistuntojen mahdollisuus on eliminoitu.	SSO:n käyttöoikeus- ja pääsynvalvonta-tiedostojen läpikäynti	H
R-SS-002	Pääsynvalvonta SSO:ssa on oltava yhtä turvallinen kuin erilliset suorat RBAC-pohjaiset istunnot. Turvallisuus on validoitu testaamalla ja testitulokset on oltava saatavilla.	SSO:n pääsynvalvonta-tiedostojen katselmointi, testaus ja monitorointi	T/H
R-SS-003	SSO:hon liittyvät avaintiedostot ja pääsynvalvontalistat on suojattu asiattomalta pääsyltä. Konfiguraatio on määritelty, eikä sitä voi muokata ilman erityistä lupaa.	SSO:n käyttöoikeus- ja pääsynvalvonta-tiedostojen läpikäynti	H

Päätoimenpiteet

- Jos työntekijät käyttävät useita erillisiä järjestelmiä, kannattaa arvioida SSO-järjestelmän käyttöönottoa käytettävyyden lisäämiseksi ja salasanahallinnan yksinkertaistamiseksi.
- Mikäli SSO-järjestelmä otetaan käyttöön, on kokonaisuus toteutettava yhtä turvallisesti kuin erillisten järjestelmien roolipohjaiset pääsynvalvontajärjestelmät.

3.4.1.8 Järjestelmän kovennus

Yleistä

Kovennuksessa järjestelmien kokoonpanoa ja/tai konfiguraatiota rajoitetaan. Tällöin ICS-järjestelmälle tarpeettomien toiminnallisuuksien haavoittuvuudet eivät lisää tarpeettomasti riskejä.

3.4.1.8.1 Ylimääräisten ohjelmistojen ja palvelujen poisto

Yleistä

Esim. verkkolaitteissa on usein oletusarvoisesti aktiivisena toiminnallisuutta, jota ei kokonaisjärjestelmässä tarvita. Porttiskannaus on normaalikäytäntö avoimena olevien porttien selvittämiseksi. Tällöin skannattavan kohteen konfiguraation täytyy olla mahdollisimman lähellä normaalia käyttöympäristöä, ei kuitenkaan tuotantojärjestelmässä kiinni.

Uhkat

Avoimena olevissa palveluissa saattaa olla esim. haavoittuvuuksia, joita hyväksikäyttämällä hyökkääjä pääsee sisään kyseisen verkkolaitteen järjestelmään. Tällöin hyökkääjä saattaa pystyä muokkaamaan laitteen konfiguraatiota tai saattaa saada pääsyn edelleen muihin järjestelmiin.

Tietoturvavaatimukset

Taulukko 28. Ylimääräisten ohjelmistojen ja palvelujen poistoon liittyviä vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-KO-001	Kaikki tarpeettomat ja tietoturvaa uhkaavat sovellukset on poistettava, näihin lukeutuvat - tietokonepelit - pikaviestintäsovellukset - internet- palvelut - laiteajurit, joita ei käytetä - ohjelmistokääntäjät, järjestelmäkehityksen aikaiset ohjelmat - verkko- ja *datacom*-protokollat, joita ei käytetä - *utility*-, diagnostiikka-, verkonhallinta- ja järjestelmänhallintaohjelmistot - käyttämättömät konfiguraatiotiedostot ja data - esimerkkiohjelmat ja *scriptit* - tarpeettomat asiakirjahallinnan ohjelmistot - selaimen konfiguraation tarkistustoiminnot.	Katselmoinnit, haastattelut	H/T
R-KO-002	Järjestelmätoimittajan erikoistoimenpiteet: Listattu kaikki toimitettavassa järjestelmässä käytettävät palvelut ja portit (sis. normaalitoiminta ja hätätilatoiminta). Määritelty, miksi kukin palvelu ja portti on toiminnolle tarpeellinen sekä tarvittavien yhteyksien - lähettävän laitteen tunnus, IP- ja MAC-osoitteet. - vastaanottolaitteen tunnus, IP- ja MAC-osoitteet. - tietoliikenneprotokolla, portti tai porttiväli. Varmistettu, että kaikki toimituksen alaiset ohjelmistot ja palvelut on päivitetty sovittuun tilaan. Toimittaa ennalta sovitussa ajassa toimitukseen liittyvät päivitykset ylläpitäkseen sovittua tietoturvatasoa. Sopimuksen mukaisesti asentaa hyväksytyt ja testatut *firmware*-päivitykset ja ohjelmistojen korjauspäivitykset (*patches*).	Katselmoinnit, haastattelut	H/T

Päätoimenpide

- Poistaa ja estää järjestelmätoimituksesta tarpeettomat ohjelmistokomponentit, joita ei tarvita ICS-toiminnon käytössä ja ylläpidossa. Dokumentoida ja säilyttää tarkat tiedot siitä, mitä toimituksesta on poistettu ja disabloitu (ja mitä pitää olla toiminnassa).
- Suorittaa haavoittuvuusskannaus ja porttiskannaus (ei tuotannossa olevaan järjestelmään) porteille 1-65535 ja poistaa ylimääräiset palvelut. Verrata tulosta sallittujen palvelujen listaan.

3.4.1.8.2 HW konfigurointi

Uhkat

Järjestelmiä on tarpeen suojata tarpeettomalta pääsyltä ja mm. haittaohjelmilta poistamalla niistä käyttämättömät fyysiset liitynnät ja rajapinnat. Poistettaviin liityntöihin kuuluvat USB-portit, DVD-asemat, muistikorttiliitännät, käyttämättömät verkkokortit, liittimet jne. eli kaikki ylimääräiset tavat, joiden avulla järjestelmään voitaisiin päästä kiinni.

Laitteen toimintatilaa tarkkaileva/ylläpitävä *Heartbeat*-signalointi saattaa olla suojaamatonta ja haavoittuvaista tietoturvauhkille. Näin ollen sen yksityiskohdat tulee dokumentoida ja mahdollisesti monitoroida sen oikeaa toimintaa.

Tietoturvavaatimukset

Taulukko 29. Laitetason kovennuksen vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-HW-001	Jokaisen laitteen fyysiset liityntärajapinnat ja muut liitynnät on rajoitettu minimiin. *Autorun*-toiminto on poistettu käytöstä.	Katselmoinnit, haastattelut	H/T
R-HW-002	Järjestelmän tulee olla saatavana ja toimia normaalisti kokonaan poistetuilla tai rajoitetuilla ulkoisilla ja/tai sisäisillä liitynnöillä.	Katselmoinnit, haastattelut	H/T
R-HW-003	Järjestelmän BIOSin (tai vastaavan) konfigurointi on suojattu pääsynvalvonnalla.	Katselmoinnit, haastattelut	H/T
R-HW-004	Verkkoyhteydet on rajoitettu vain sallittuihin kohteisiin. Laite hylkää sanoman, jos lähettävän laitteen MAC-osoite ei ole sallittujen listalla.	Katselmoinnit, haastattelut	H/T

R-HW-005	Vain järjestelmävalvojalla tulee olla mahdollisuus ottaa poistettu liityntä uudelleen käyttöön, mikäli muutos on ohjelmallisesti tehtävissä.	Katselmoinnit, haastattelut	H/T
R-HW-006	Jos järjestelmässä on käytössä ns. *heartbeat*-signalointia, tulee se dokumentoida (portit, protokollat, liikennemäärät) ja arvioida sen tietoturvahaavoittuvuudet. Signaloinnin monitorointi saattaa olla tarpeen (mm. vrt. normaaliin *heartbeat*-signaloinnin määrään).	Katselmoinnit, haastattelut	H/T

Päätoimenpide

- Ylimääräiset liitynnät, kuten USB-portit, DVD-asemat, verkkokortit ja liittimet, tulee poistaa käyttöön tulevista automaatiojärjestelmistä.
- Sallitun *heartbeat*-signaloinnin yksityiskohdat tulee kontrolloida.

3.4.1.8.3 Ohjelmistojen asennus ja vikojen korjaaminen

Uhkat

Järjestelmien viat ja haavoittuvuudet, joihin ei ole asennettu korjausta, muodostavat konkreettisen uhan tietoturvalle ja luotettavalle toiminnalle. Kaikki ohjelmistojen asennukset ja vikojen korjaukset tulee kuitenkin tehdä kontrolloidusti, muutoin ajan myötä järjestelmään kantautuu uusia testaamattomia ominaisuuksia, haavoittuvuuksia ja vikoja.

Tietoturvavaatimukset

Taulukko 30. Vaatimuksia ohjelmistojen asennuksesta ja korjaamisesta.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-MU-001	Käytössä on korjaustenhallintaprosessi, jossa asiakkaalle toimitetun tuotteen korjausten asennus on kuvattu ja vastuutettu selkeästi. Lisäksi kaikki viat, korjaukset ja korjaavat toimenpiteet on rekisteröity ja ylläpidetty.	Katselmoinnit	H/T
R-MU-002	Toimittaja ilmoittaa järjestelmän ylläpitäjälle kaikki järjestelmään mahdollisesti vaikuttavat uudet julkaistut haavoittuvuudet. Seurannassa ovat mm. toimitettu järjestelmä, sen taustajärjestelmä, käyttöjärjestelmä, kolmannen osapuolen ohjelmisto jne. Ilmoitus sisältää haavoittuvuuden tietoturvavaikutukset, vian aiheuttajan ja korjaavat toimenpiteet.	Haastattelut, katselmoinnit	H/T
R-MU-003	On määritelty prosessi, jolla käyttäjä luottamuksellisesti kommunikoi havaitsemansa viat toimittajalle, joka vastaa käyttäjälle 24 tunnin kuluessa toimintasuunnitelmalla.	Haastattelut, katselmoinnit	H
R-MU-004	Toimittaja kehittää korjauksen haavoittuvuuteen. Korjauksen toiminnallisuus on testattu ja oikea toiminta osoitettu testijärjestelmässä ennen operatiiviseen järjestelmään asennusta.	Haastattelut, katselmoinnit	H/T
R-MU-005	Haavoittuvuus korjataan operatiiviseen järjestelmään sovitun ajan kuluessa ylläpitäjän kanssa sovittuna ajankohtana.	Haastattelut, katselmoinnit	H/T

Päätoimenpiteet

- Toimintaan vaikuttavia vikoja ja haavoittuvuuksia täytyy systemaattisesti seurata ja kehittää korjaukset sovitun ajan kuluessa.
- Korjaukset täytyy testata ja validoida oikea toiminta. Asennus kohdejärjestelmään suoritetaan ennalta määritellyn prosessin mukaisesti.

3.4.1.9 Koodauskäytännöt – Turvallisten ohjelmointisääntöjen käyttö ja seuranta

Yleistä

Turvallisten **ohjelmointisääntöjen** (*secure coding rules*) määrittely ja noudattamisen valvonta ovat ehkä parhaita tapoja parantaa ohjelmistojen laatua ja tietoturvaominaisuuksia. Ohjelmointisäännöillä fokusoidaan työ virheiden syntymisen lähteille, konkreettiseen työhön ja tuloksiin ajanjaksolta, jolloin ohjelmistot implementoidaan käytännössä. Koodaussääntöjen etuna on lisäksi, että sääntöjen noudattamista voidaan valvoa eri tavoin, mm. perinteisellä tavalla **koodikatselmoinnein**, mutta myös eritasoisesti automatisoiduilla **lähdekoodianalysaattoreilla** staattisen analyysin metodeja hyödyntäen. Koodin haavoittuvuudet voidaan tarkastaa tuotekehityksen aikana ja myöhemminkin, jos vain lähdekoodi on saatavilla. Tarkastukset tulee dokumentoida ja suojata hyvin, sillä tuloksia voidaan käyttää myöhemminkin hyväksi esim. tietoturvatestien hyödyllisimpiä kohteita ja menetelmiä määriteltäessä.

Uhkat

Hyökkääjä pääsee järjestelmiin sisälle haavoittuvuuksien kautta. Esim. syöttämällä haavoittuvan järjestelmän *input*-datakenttään liian pitkä arvo saadaan aikaan puskuriylivuoto, jonka seurauksena hyökkääjä saa asiattoman pääsyn järjestelmäkomentoihin. Komentoja voidaan yrittää syöttää suoraan *input*-muuttujiin, ja jos *input*-validointi on tehty ohjelmassa puutteellisesti, saattaa komento mennä asiattomasti suoritukseen. Tällaisia hyökkäyksiä on tyypillisesti vaikea havaita esim. palomuurien avulla.

Tietoturvavaatimukset

Taulukko 31. Lähdekoodianalyysiin liittyviä vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-CR-001	Toimittaja esittää kuvauksen turvallisista tuotekehityskäytännöistään ja koodaussäännöistään, joilla ohjelmisto (sis. *firmware*) kehitetään ja varmistetaan tietoturvalliseksi tuotteeksi.	Katselmoinnit, haastattelut	H/T
R-CR-002	Toimittaja esittää koodikatselmointien tulokset ennen käyttöönottoa.	Katselmoinnit, haastattelut	H/T
R-CR-003	Ylläpitovaiheen koodimuutokset (päivitykset, korjaukset) on koodikatselmoitu.	Katselmoinnit, haastattelut	H/T
R-CR-004	Ohjelmakoodista tarkastettavat asiat sisältävät mm. - *Input*/*Output*-arvojen oikeat tarkistustavat, ympäristömuuttujien ja signaalien oikeat määrittelytavat. - Puskuriylivuodot ehkäisty, turvallinen datan (mm. *arrays*, *strings*, *integers*) käsittely. - Web-lomakkeiden syötön tarkastus: poistettava mahdollisuus tehdä komennon lisäys, SQL-lisäys, *Cross-Site-Scripting* jne. - Muistin hallinta on tehty turvallisesti. - Lausekkeet, määrittelyt ja initialisoinnit on tehty oikein. - Asetukset ovat politiikan mukaiset, myös kaikkiin funktiokirjastoihin ja käyttöjärjestelmäparametreihin liittyen. - Lokitiedostojen eheys on varmistettu ennen lukua. - Tiedostojen ja tiedonsiirron salaus otettu käyttöön politiikan mukaisesti, erityisesti salasanat ja salausavaimet.	Lähdekoodin katselmointi, lähdekoodianalysaattorit	H/T
R-CR-005	Kriittisissä järjestelmissä tilaaja tai ennalta määrätty kolmas osapuoli analysoi tuotteessa käytetyn lähdekoodin ennen käyttöönottoa. Kolmannen osapuolen ohjelmistot, joita hyödynnetään toimitetussa järjestelmässä, tulee analysoida. Kokonaisjärjestelmää integroitaessa selvitetään kaikki järjestelmän todelliset haavoittuvuudet.	Lähdekoodin katselmointi, lähdekoodianalysaattorit, haavoittuvuusanalyysi	H/T

Päätoimenpiteet

- Käytettävät turvalliset koodaussäännöt, -käytännöt ja koodianalyysityökalut on määriteltävä selkeästi. Kaikki koodi on kehitettävä ja tarkastettava näiden sääntöjen mukaisesti.
- Päätuloksena kaikki kehitetty ja käyttöön tuleva ohjelmistokoodi, käytetyt koodikirjastot ja kolmannen osapuolten ohjelmistot on tarkistettu potentiaalisten haavoittuvuuksien löytämiseksi ja eliminoimiseksi.

Lisäinformaatiota

Yksityiskohdainen säännöstö kooditarkastuksia varten, katso mm.

https://www.securecoding.cert.org/confluence/display/seccode/CERT+Secure+Coding+Standards

Vaihtoehtoinen tietolähde on ”*Build Security In*” (U.S. DHS: *National Cyber Security Division*)

https://buildsecurityin.us-cert.gov/daisy/bsi/home.html

Yrityksessä tulee määritellä turvallisessa ohjelmoinnissa käytettävä sääntökanta, jota käytetään eri tuotteiden kehittämisessä ja koodikatselmoinneissa. Koska yksityiskohtaisia koodaussääntöjä on olemassa melko paljon ja koska ne ovat ohjelmointikielispesifisiä, kannattaa yrityksessä nostaa esiin tiettyjä sääntöjä siten, että ainakin liiketoiminnan kannalta tärkeimmät koodaussäännöt tulevat tarkastettua kriittisten tuotteiden osalta. Tämä vaatii jatkuvaa ylläpitoa ja seurantatyötä, joka luonnollisesti on osana yrityksen tuotteiden laadun ja tietoturvan varmistamisen prosesseja ja liittyy läheisesti tietoturvahaavoittuvuuksien seurantaan ja niiden hallintaan eri tuoteperheissä.

Hyviin koodianalyysityökaluihin lukeutuvat mm. *Coverity Prevent, Fortify Source Code Analysis, Grammatech CodeSonar, Klocwork K7, Ounce Labs Prexis/Engine*, sekä *Secure Software CodeAssure Workbench*. Kussakin työkalussa on toteutettuna tiettyjä sääntökantoja (*ruleset*), joita käyttämällä työkalu tekee koodianalyysin. Useimmissa työkaluissa tällaista sääntökantaa voi itse muokata ja laajentaa. *Fortifyn* ja *Coverityn* työkalut ovat yleiseen käyttöön erinomaisia, mutta käytännössä esteeksi saattaa tulla niiden hinta.

3.4.1.10 Haittaohjelmilta suojautuminen

Yleistä

Erityisesti nykyaikaisissa järjestelmissä esiintyy sinne kuulumattomia haittaohjelmia tai ainakin vaara saada tartuntoja vaarallisista ohjelmista. Haittaohjelmaksi luetaan tässä yhteydessä mikä tahansa ohjelma, joka voi vaarantaa järjestelmän alkuperäisen käyttötarkoituksen. Haittaohjelmia, kuten viruksia, matoja, botti-ohjelmia ja troijalaisia, pyritään havaitsemaan ja torjumaan verkon rajoilla ja/tai isäntäkoneissa. Haittaohjelmien torjunnan mekanismit onkin suunniteltava huolellisesti ja sopiviin kohtiin suojattavia verkkoja ja laitteita, jotta torjunnasta ei aiheutuisi haittaa järjestelmän oikealle toiminnalle missään olosuhteissa.

Uhkat

Haittaohjelmat voivat halvaannuttaa järjestelmän oikean toiminnan tai ohjata järjestelmää väärään toimintaan. Toisaalta haittaohjelmien torjuntaohjelmiston ylläpidosta saattaa aiheutua järjestelmän saatavuudelle ongelmia, esim. verkon jumittuminen automaattisen *signature*-päivityksen aikana tai viallisen päivityksen vaikutukset. Haittaohjelmat tai niiden torjuntaohjelmat eivät saa missään olosuhteissa poistaa järjestelmän toiminnalle elintärkeitä tiedostoja.

Tietoturvavaatimukset

Taulukko 32. Haittaohjelmilta suojautumiseen liittyviä vaatimuksia.

ID	Vaatimuksen kuvaus	Evaluaatio-menetelmä	Tekn. / Hallinn.
R-MW-001	Kaikki toimitettava ohjelmisto ja sen mukana tuleva materiaali on ennalta puhdistettu haittaohjelmien torjuntaohjelmistojen uusimmalla testatulla versiolla.	Katselmoinnit	H/T
R-MW-002	Toimittaja ilmoittaa tilaajalle kaikki takaportit, joita toimitettuun järjestelmään sisältyy, sekä syyt miksi niitä tarvitaan. Takaportteja ei tulisi järjestelmässä olla lainkaan.	Katselmoinnit	H/T
R-MW-003	A. Toimittaja on ohjeistanut, mitä ja miten haittaohjelmien torjunta-ohjelmistoja (mm. sallitut asetukset, versiot, päivitys) järjestelmässä tulee käyttää.	Katselmoinnit	H/T

	tai B. Toimitukseen kuuluu haittaohjelmien torjuntajärjestelmä, jonka vaikutukset isäntäkoneen suorituskykyyn on mitattu ja verifioitu.		
R-MW-004	Epäillyt tiedostot asetetaan karanteeniin (niitä ei deletoida välittömästi).	Katselmoinnit	H/T
R-MW-005	Luotettava ohjelmistojen ja signatuurien korjaus ja päivitys on järjestetty siten, että kunkin päivityksen vaikutukset on huolellisesti testattu. Testitulokset sisältävät vaikutukset verkkoyhteyksiin, CPU- ja muistikäyttöön sekä muut vaikutukset.	Katselmoinnit	H/T
R-MW-006	Torjuntaohjelmiston generoima lokitiedosto on suojattu ja sitä säilytetään ennalta sovittu aika.	Katselmoinnit	H/T

Päätoimenpiteet

- Järjestelmän toiminnan kannalta oleelliset haittaohjelmien torjuntaohjelmistot ja niiden toimintavaatimukset määritellään. Haittaohjelmien havaitseminen ja torjunta sijoitetaan tarkoituksenmukaisiin pisteisiin järjestelmässä.
- Järjestelmän oikeasta toiminnasta varmistutaan kaikissa olosuhteissa, torjuntajärjestelmät eivät saa vaarantaa suojattavaa järjestelmää millään tavoin. Päätuloksena suojattava järjestelmä ei saastu haitallisista ohjelmista, eikä sen toiminta häiriinny missään olosuhteissa. Jos saastumista kuitenkin sattuu, torjuntatoimet on ennalta suunniteltu huolella.

3.4.2 Toimihenkilöiden haastattelusta

Tärkeitä menetelmiä teollisuusautomaatiojärjestelmien tietoturvaevaluointiin ovat yleensä ainakin:

- toimihenkilöiden haastattelu
- katselmoinnit
- haavoittuvuusanalyysi

- hyökkäysten sietoa testaavat menetelmät (ei tuotannossa olevaan järjestelmään)
- järjestelmien konfiguraatiota selvittävät menetelmät.

Toimihenkilöiden haastattelua käytetään monissa evaluaation eri vaiheissa. Suora ihmistenvälinen kommunikaatio on yhä edelleen yksi tehokkaimmista tiedonvaihdon tavoista mm. valittaessa evaluaatiokohteita, suunniteltaessa evaluaation rajausta, katselmoinneissa, määrättäessä sovellettavia testaustyökaluja ja niiden asetuksia ja profiileja, hankittaessa evaluoitavaa materiaalia, tarkastettaessa käytössä olevia tietoturva- tai muita käytäntöjä ja niiden toteutumista, varmistettaessa raporttien oikeellisuutta ja laajuutta jne.

Haastatteluissa kannattaa yleensä käyttää jonkinlaista kysymyslistaa tai vaatimuslistaa, jonka toteutumista keskustelussa arvioidaan. Haastattelija tekee muistiinpanoja ja kirjaa ylös mm. kohteen (tietoturvan) hallinnassa käytettyjä toimintatapoja, suoritettuja osatehtäviä, tietoturvan varmistusaktiviteetteja, teknisiä proseduureja, työkalujen käytön yksityiskohtia jne. Erityisen tärkeää on kirjata poikkeamat vertailukohtaan nähden. Edellisessä kohdassa ”Evaluaatiokriteeristöjä” on esitetty paljon erilaisia tietoturvavaatimuksia, joita voidaan käyttää apuna evaluaatiokriteeristöä laadittaessa. Haastattelun on syytä sisältää seuraavia osuuksia:

- kyseessä olevan evaluaation tunnistetietojen merkitseminen: haastateltavan henkilön nimi, haastattelija, paikka ja päivämäärä
- haastattelun tavoitteen läpikäynti: esim. evaluoitavan kohteen kovennustoimenpiteiden selvittäminen
- evaluaatiokohteiden identifiointi: esim. laitetunnus, merkki ja malli, HW- ja SW-versionumerot
- evaluaatiokriteeristön toteutumisen arviointi (keskustellen): kovennusvaatimusten toteutumisen läpikäynti
- evidenssin kerääminen ja kirjaaminen kriteeristön täyttymisestä: esim. suoritettujen kovennustoimenpiteiden dokumentaatio, jossa toimenpiteiden suorittajat ja vastuuhenkilöt on nimetty
- muut asiaan vaikuttavat seikat: esim. Mitä muita tietoturvan toteutumiseen vaikuttavia seikkoja voisi mainita, vaikka niistä ei ole kriteeristöä?

Huom. Haastattelujen tulokset ovat hyvin arkaluontoista materiaalia, joten niitä on käsiteltävä erittäin luottamuksellisina ja suojattava ne vahvoin prosessein.

Seuraavassa mallilomake, jota voidaan käyttää vaikkapa kohteen koventamisen arviointiin. Haastattelijan tulisi käyttää kullekin evaluaatiokohteelle erillistä lomaketta.

Taulukko 33. Toimihenkilön haastattelulomake.

SALASSAPIDETTÄVÄ **Evaluaation tunnus:** <ID, yleensä osa suurempaa evaluaatiokokonaisuutta>		
Paikka ja päivämäärä:		
Haastateltavat henkilö(t) ja heidän tehtävänimikkeensä:		
Haastattelija(t):		
Haastattelun tavoitteet:	1.	
	2.	
Evaluaatiokohde	**Laitteen ja/tai ohjelmiston merkki ja malli**	**Laitteen tunnus, HW- ja SW-versionumerot**
<kohteen ID>		
Tarkentavaa kohteesta:		
Evaluoitavien ominaisuuksien rajaus	**Evaluoitavat <rajapinnat>**	**Evaluoitavat <toiminnot>**
1.		
2.		
Tarkentava rajaus:		
Evaluaatiokriteeri/-vaatimus	**Kriteerin toteutumisen arviointi**	**Evidenssi/Todentava dokumentaatio**
1.	<Erityisesti poikkeamat>	<Erityisesti toteumat>
2.		
3.		
Selvitettävää:		
Muut asiaan vaikuttavat seikat	**Selitys**	**Aiheen kontaktihenkilö?**
1.		
Muistiinpanoja:		

4. Tietoturvan testaaminen teollisuusautomaatiossa

4.1 Testimenetelmiä

4.1.1 Menetelmien yleisesittely

Aiempana mainittiinkin jo, että kunkin tietoturvaevaluaation tavoitteet ovat yksilölliset, samoin evaluaatiossa käytettävät metodit ja työkalut. Kaikki metodit ja työkalut eivät tietenkään sovellu kaikkiin tarkoituksiin. Seuraavassa annetaan muutama esimerkki työkalutyyppien soveltuvuudesta toimistoverkko- vs. automaatioverkkotestaukseen.

Useissa tapauksissa seuraavien työkalutyyppien käyttäminen on hyödyllistä *toimistoverkon* laitteiden ja ohjelmistojen testaamisessa (ei tyhjentävä lista):

- penetraatio-testerit
- *robustness*-testerit, *denial of service* -testerit
- työkalut verkon rakenteen ja palveluiden kartoitukseen
- haavoittuvuusskannerit
- applikaatiotesterit, mukaan lukien web-sovellukset
- lähdekoodianalysaattorit (sis. koodaussäännöt).

Vastaavasti *automaatioverkon* laitteiden ja ohjelmistojen testaamisessa hyödyllisiä ovat usein (ei tyhjentävä lista)

- penetraatio-testerit
- *robustness*-testerit, *denial of service* -testerit
- työkalut verkon rakenteen ja palveluiden kartoitukseen
- haavoittuvuusskannerit, automaatiolaitekohtainen konfiguraation tarkistus
- teollisuusautomaatiospesifiset testerit, esim. *achilles satellite*, sekä automaatiospesifisiä *plug-in*-moduleita tietoturvatestauksen eri työkaluissa

- monitorointityökalut suorituskyvyn tarkkailuun testauksen aikana
- (opt.: lähdekoodianalysaattorit, sis. koodaussäännöt).

4.1.2 Yksittäiset menetelmät

Seuraavassa esitämme lyhyet kuvaukset tietoturvatestauksen tärkeimmistä metodeista.

4.1.2.1 Fuzz-testaus

Fuzz-testaus on usein laajoissa ohjelmistoprojekteissa käytetty *black-box*-testausmenetelmä, jossa on suhteellisen hyvä kustannushyötysuhde. *Fuzz*-testauksen hyvä puoli on, ettei kohdejärjestelmästä tarvitse välttämättä tietää yksityiskohtia eikä lähdekoodia tarvitse olla saatavilla testien suorittamiseksi. Vasta kun löydettyjä virheitä aletaan korjata, lähdekoodin tulee olla saatavilla.

Tällä menetelmällä pyritään löytämään toteutusvirheitä kohdejärjestelmästä syöttämällä virheellisesti muokattua dataa sen protokollarajapintoihin. Monenlaisia syötteitä voidaan ”fuzzata” eli sekoittaa. Yleisimpiä kohteita tämän tyyppiselle testaukselle ovat verkkoprotokollat, mutta menetelmää voi soveltaa hyvin erityyppisiin tarkoituksiin. *Fuzz*-testaus on suhteellisen tehokas testausmetodi uusien haavoittuvuuksien löytämiseksi. Tämäntyyppisellä testauksella löydetyt haavoittuvuudet saavat kohdejärjestelmän toimimaan odottamattomalla tavalla (kaatuilu, muistivuodot). Tämän vuoksi *Fuzz*-testaus on erityisen hyödyllinen isoissa C- tai C++-sovelluksissa, joissa jokainen muistiturvallisuuteen vaikuttava virhe on todennäköisesti vakava haavoittuvuus.

Fuzz-testaus ei välttämättä riitä yksinään paljastamaan kaikkia muistiriippuvaisia haavoittuvuuksia teollisuusjärjestelmien protokollatoteutuksissa. Esimerkiksi huolellinen *data-flow* analyysi voi olla ainoa keino tiettyjen muistikorruptioon liittyvien haavoittuvuuksien löytämisessä. Lisäksi, *fuzz*-testaus ei välttämättä pysty tuottamaan tarvittavaa informaatiota, jonka avulla voitaisiin tunnistaa haavoittuvuusriippuvaisuuksia (*triggered vulnerabilities*). Tämä johtuu siitä, ettei *fuzz*-testauksessa havainnoida kohdejärjestelmän suoritusta muisti- ja keskusyksikkötasolla [BELLETT].

Testaustyökaluja on olemassa useantyyppisiä. Työläimmät tarjoavat testaajalle vain kehikon, jolla testitapaukset luodaan itse. Tämäntyyppinen testien rakentelu vaatii hyvän tuntemuksen testattavasta protokollasta ja suuria työmääriä. Yksinkertaisimmat *fuzz*-testaustyökalut lähettävät täysin satunnaista dataa testattavaan

kohteeseen. Satunnaisen datan käytöllä voi saada tuloksia aikaiseksi, mutta löydettyjen ongelmakohtien osoittaminen testauksen jälkeen on haastavaa, koska samaa testiä on vaikea ajaa uudestaan. Tehokas ja nopea *fuzz*-testausmenetelmä on työkalu, johon valmistaja on valmiiksi rakentanut testitapaukset.

Mitä tarkemmin testeri on erikoistunut tietyille protokollille, sitä vähemmän odottamattomia virheitä se löytää. Lisäksi, suoritettaessa *black-box*-testausta hyökätään yleensä suljettuun järjestelmään, mikä vaikeuttaa löydetyn haavoittuvuuden vaarallisuuden tai vaikutuksen arviointia ilman debuggausmahdollisuutta. Pääasiallinen haaste *fuzz*-testauksen virheiden etsinnässä on, että testeri yleensä löytää vain hyvin yksinkertaisia virheitä. Yksinkertaisessa testerissä voi olla huono koodikattavuus. Koodikattavuustyökaluja käytetään usein arvioimaan, miten hyvin testeri toimii, mutta nämä voivat tarjota vain suuntaviivoja testerin laadun arvioimiseen. Eri testerit löytävät samasta ohjelmistosta kukin erilaisen joukon virheitä.

Toisaalta, *fuzz*-testauksella löydetyt virheet ovat toisinaan vakavia ja kyseisiä virheitä hyväksikäyttämällä pystyttäisiin hyökkäämään järjestelmää vastaan. Hyökkääjät hyödyntävät samoja tekniikoita ja työkaluja kuin *fuzz*-testauksessa etsiessään turva-aukkoja, ja se tarjoaa *fuzz*-testaukselle etulyöntiaseman verrattuna binääriseen tai lähdekoodianalyysiin, tai jopa *fuzz*-testausta muistuttavaan *fault injection* –menetelmään. Se nojaa usein keinotekoisiin virhetilanteisiin, joita on vaikea tai mahdoton oikeasti hyväksikäyttää. *Fuzz*-testauksella pystytään usein löytämään erikoisia tai huomaamattomia virhetilanteita, joita tavallisen ihmistestaajan on hankala löytää ja joita tarkatkaan testisuunnittelijat eivät välttämättä osaisi suunnitella.

Fuzz-testaus ei voi korvata kattavaa tietoturvatestausta tai formaaleja menetelmiä, vaan se tarjoaa sattumanvaraisen näytteen järjestelmän käyttäytymisestä. Usein testin läpäisy kertoo vain, että ohjelma voi käsitellä poikkeuksia ilman kaatumista, eikä sitä että se toimii oikein. *Fuzz*-testausta voidaan siis pitää pikemminkin yleisen laadun mittarina kuin virheidenetsintämenetelmänä. Se antaa karkean arvion ohjelmiston luotettavuudesta ja voi ehdottaa mitä ohjelman osia pitäisi käsitellä koodianalyysillä, katselmoinnilla tai osittaisella uudelleenkirjoittamisella.

4.1.2.2 Porttiskannaus ja verkkotiedustelu

Verkkotiedustelulla tarkoitetaan tietoverkon avoimien palveluiden tunnistamista (porttiskannaus) ja verkossa olevien laitteiden tunnistamista (mm. osoite, käyttö-

järjestelmä). Verkkotiedustelun suorittaminen vaatii pääsyä samaan verkkoon, joko internetin kautta tai suoraan langattomalla/kaapeliyhteydellä. Aktiivisessa tiedustelussa lähetetään kohteeseen dataa ja tehdään johtopäätöksiä takaisin tulevasta vastauksesta. Passiivisessa verkkotiedustelussa ainoastaan kuunnellaan verkkoliikennettä, ja tehdään johtopäätökset liikennettä analysoimalla. Verkkotiedustelusta saatuja tietoja voidaan käyttää esimerkiksi hyökkäyksen rakentamiseen (hakkeri) tai järjestelmän suojaamiseen vaarallisia palveluita/versioita korjaamalla (ylläpitäjä).

Yksinkertaisimmillaan porttiskannausohjelma lähettää yhteyspyynnön kohteeseen järjestyksessä jokaiselle portille ja havainnoi, mitkä portit vastaavat tai vaikuttavat avoimilta. Vastauksen laadusta riippuen ohjelma päättelee käytetäänkö porttia, jolloin ohjelma tutkii ko. porttia tarkemmin ja yrittää etsiä siitä heikkoja kohtia. Jotkut ohjelmat päättelevät vastausten perusteella lisätietoja, kuten kohteen käyttöjärjestelmän tai porttikohtaiset sovellukset. Ohjelma ei pysty ilmoittamaan haavoittuvuuksista sinällään, vaan ylläpitäjän on itse osattava tulkita tuloksia.

Organisaatioiden kannattaa suorittaa verkkoskannaus seuraavista syistä [NIST-SP800-42]:

- tarkistaakseen, onko organisaation verkkoon liitytty luvattomasti
- tunnistaakseen haavoittuvat palvelut
- tunnistaakseen poikkeamat sallituista palveluista, jotka on määritetty organisaation tietoturvapolitiikassa
- valmistellakseen penetraatiotestausta
- avustaakseen tunkeutumisen havaitsemisjärjestelmän (IDS) konfiguroinnissa
- kerätäkseen todistusaineistoa verkkotietoturvan loukkauksista.

Erilaisia porttiskannaustapoja on useita, samoin kuin tapoja peittää porttiskannauksen todellinen lähde. Skannaus kuluttaa kaistanleveyttä ja hidastaa verkon vasteaikoja, joten se voi haitata verkon normaalitoimintaa. Ennen skannausta tuleekin varmistaa, voiko työkalujen lähettämästä datasta aiheutua haittaa järjestelmille. Sandian raportti *Penetration Testing of Industrial Control Systems* mainitsee tapauksen, jossa yksinkertainen ping sweep -tiedustelu SCADA-verkossa käynnisti yllättäen kolmimetristen robottikäsivarsien 180 asteen liikehdinnän. Käsivarsien ulottuvilla ei tapahtumahetkellä ollut onneksi ketään.

4.1.2.3 Haavoittuvuusskannaus

Haavoittuvuusskannaamisella tarkoitetaan yleisessä tiedossa olevien mahdollisten tietoturvaongelmien etsimistä kohdejärjestelmästä. Tällöin ei yleensä löydetä uusia, piilossa olevia haavoittuvuuksia, vaan löydösten kattavuus riippuu työkalun tietokantaan tallennettujen haavoittuvuustietojen laajuudesta ja ajantasaisuudesta.

Haavoittuvuudet voivat olla esimerkiksi vaaralliseksi todettuja ohjelmointivirheitä, turvattomia vanhoja ohjelmistoversioita tai vaarallisia avonaisia palveluita. Vaikka etsitäänkin jo maailmalla tiedossa olevia haavoittuvuuksia, skannaaminen on yksi tärkeimmistä tietoturvatestausmenetelmistä, koska teollisuusjärjestelmät käyttävät usein vanhoja, haavoittuvaisia ohjelmistoja. Skannerit voivat myös ohjeistaa, kuinka toimia löytyneiden haavoittuvuuksien jatkotoiminnan tai korjauksen suhteen, tai jopa korjata haavoittuvuuksia.

Haavoittuvuuksien identifiointi teollisuusautomaatiossa tarvitsee erilaisen lähestymistavan kuin perinteisissä IT-järjestelmissä. Kuten porttiskannauksessa, myös haavoittuvuuksien etsimisessä täytyy ensin varmistua, ettei testaaminen aiheuta ongelmia tai vaaratilanteita. Käytännössä tämä voidaan toteuttaa esimerkiksi irrottamalla testattava osa tuotantokäytössä olevasta järjestelmästä. Testien ajaminen tuotantokäytössä olevaan järjestelmään on vaarallista ja sitä tulee välttää. Esimerkiksi *Denial of Service* -tyyppiset testit voivat aiheuttaa suurta vahinkoa ennalta valmistautumatta.

Teollisuusautomaatiossa laite- ja ohjelmistokanta on usein vanhaa ja sisältää haavoittuvuuksia, joihin valmiita korjauksia ei välttämättä ole saatavilla. Kun haavoittuvuuksia löytyy, niitä ei aina välttämättä pystytä korjaamaan tai se ei ole taloudellisesti järkevää. Haavoittuvuuden korjaaminen ja järjestelmän päivittäminen voi erityisesti teollisuusautomaatiossa tulla hyvin kalliiksi, joten toteutumisriskiä tulee verrata korjaamisesta aiheutuviin kuluihin ja miettiä, voitaisiinko uhkan realisoituminen välttää jollain muulla suojauskeinolla.

Yleensä ottaen haavoittuvuuskannerit löytävät vain yksittäisiä riskejä eivätkä pysty arvioimaan verkon kokonaisriskitilannetta. Haavoittuvuuskannereilla voi olla korkea väärien positiivisten virheiden määrä, joten niiden tulosten tulkinta vaatii ammattitaitoa. Ne voivat myös hidastaa verkkoliikennettä kohtuuttomasti. Lisäksi, haavoittuvuustietokannat on pidettävä jatkuvasti ajan tasalla, koska tuloksien laatu on suoraan riippuvainen siitä. [NIST-SP800-42]

4.1.2.4 Penetraatiotestaus

Penetraatiotestauksessa arvioidaan järjestelmän tai verkon tietoturvan tasoa tekemällä hyökkäys järjestelmää vastaan testausmielessä. Samalla järjestelmässä mahdollisesti olevia haavoittuvuuksia monitoroidaan ja analysoidaan aktiivisesti. Haavoittuvuudet voivat johtua esimerkiksi epäsopivasta järjestelmän konfiguraatiosta, tunnetuista tai tuntemattomista laite- tai ohjelmistovioista tai tietoturvaongelmiin kohdistuvien (toiminnallisten/teknisten) vastatoimien heikkoudesta.

Analyysi voi sisältää haavoittuvuuksien aktiivista hyväksikäyttöä. Penetraatiotestauksen tulosten analysoinnissa pitäisi käydä läpi kaikki löytyneet haavoittuvuudet, samoin arvio niiden vaikutuksista mahdollisine korjausehdotuksineen. Penetraatiotestausta voidaankin pitää yhtenä tietoturvan auditointimenetelmänä, koska sen avulla pystytään testaamaan hyökkäyksen vaikutusta yrityksen liiketoimintaan.

Penetraatiotestejä voidaan suorittaa usealla tavalla. Black box -testauksessa ei tarvita aikaisempaa tietämystä testattavasta infrastruktuurista. Testaajien on ensin määritettävä järjestelmien sijainti ja laajuus ennen analyysin aloitusta. White box -testauksessa testaajilla on täydellinen tietämys testattavasta infrastruktuurista, kuten verkkorakenne, lähdekoodi ja IP-osoitetiedot. Black box -testaus simuloi hyökkäystä, jonka suorittaa sellainen, joka ei tunne järjestelmää. White box -testaus simuloi mitä voisi tapahtua sisäisen hyökkäyksen tai tietovuodon seurauksena, jolloin hyökkääjällä on pääsy lähdekoodiin, verkkorakenteeseen ja jopa joihinkin salasanoihin. Näiden kahden tekniikan välillä on useita välimuotoja.

White box -testauksen voi suorittaa usein täysin automatisoituna edullisena prosessina. Black box -penetraatiotestaus taas vaatii työtä ja ammattitaitoa, jotta riskit kohdejärjestelmälle osattaisiin minimoida. Se voi minimissään hidastaa organisaation verkon toimintaa verkko- ja haavoittuvuusskannauksen takia.

Näiden lisäksi testimenetelmät voidaan jakaa ”*Blue Teaming*” ja ”*Red Teaming*” -testaukseen. *Blue Teaming* -testauksessa testauksesta on tieto sekä organisaation tietojärjestelmävastaavilla että ylemmällä taholla. *Red Teaming* -menetelmällä hyökätään ilman että tietojärjestelmävastaavat tietävät hyökkäyksestä. Tällöin tieto testihyökkäyksestä on vain organisaation johdolla. Näistä *Blue Teaming* on halvempi ja yleisempi, mutta *Red Teaming* puolestaan mittaa totuudenmukaisemmin tietoturvan tasoa sekä toimintatapoja organisaatiossa. [NIST-SP800-42]

Penetraatiotestaus voi kohdistua järjestelmään sisäisesti tai ulkoisesti. Ulkoinen testaus suoritetaan realistisesti *black box*- testauksena palomuurien takaa. Sisäisessä testauksessa testaajat saavat käyttöoikeudet ja tietoa järjestelmästä jonkin roolin mukaan testin tavoitteista riippuen, esimerkiksi tavallisen työntekijän tai jopa ylläpitäjän oikeudet. [NIST-SP800-42]

Penetraatiotestaus on tehokas, joskin riskialtis ja huolellista suunnittelua vaativa testitapa. On mahdollista että järjestelmä vahingoittuu testauksen aikana toimintakelvottomaksi. Testausta onkin syytä edeltää huolellinen portti- ja haavoittuvuusskannaus sekä niiden tulosten käyttö penetraatiotestin valmistelussa.

4.1.2.5 Lähdekoodianalyysi

Lähdekoodianalyysi, automatisoitu tai manuaalinen, voi käsittää useita eri tekniikoita. Lähdekoodianalyysissä pyritään etsimään ohjelmiston lähdekoodista virheitä ilman ohjelman suorittamista. Analyysi voidaan suorittaa joko lähdekoodille tai joissain tapauksissa objektikoodille. Tyypillisesti automatisoitua lähdekoodianalyysiä kutsutaan staattiseksi analyysiksi.

Teollisuusautomaation järjestelmät on usein toteutettu erilaisin ohjelmistoratkaisuin, jolloin lähdekoodianalyysi soveltuu niiden tarkasteluun. Lähdekoodianalyysi on parhaimmillaan osana ohjelmistojen tuottajien omaa kehitysprosessia, jolloin ohjelmiston laatua ja virheiden syntymistä voidaan parhaiten hallita ja löytyneet ongelmat luontevasti korjata. Teollisuusautomaation tapauksessa on erityisen tärkeää, että koodiin jää mahdollisimman vähän toiminnallisuutta tai tietoturvaa vaarantavia ohjelmointivirheitä. Tähän tarkoitukseen lähdekoodianalyysi soveltuu hyvin yhtenä lisänä kokonaisuutta. Pelkästään lähdekoodianalyysin ja -työkalujen käyttäminen ei riitä varmentamaan riittävää ohjelmiston laatua, mutta se auttaa sen saavuttamisessa.

Lähdekoodianalyysin suorittamiseen on saatavilla tehokkaita kaupallisia ohjelmistoja, joista esimerkkeinä *Fortifyn*, *Klocworkin*, *Coverityn* ja *Ounce Labsin* tuotteet. Työkalut on tärkeä integroida osaksi ohjelmistokehitystyön eri vaiheita. Osa toimii yksittäisten ohjelmistokehittäjien työpöydällä itsenäisenä ohjelmistona, kun taas osa toimii yhteen erilaisten palvelinratkaisujen kanssa. Yksittäisten ohjelmistokehittäjien koneilla toimivien työkalujen tapauksessa analyysi jää yleensä selvästi kevyemmäksi kuin esimerkiksi buildiin integroidun työkalun ollessa kyseessä. Paras tulos saadaan, kun staattisen analyysin työkaluja käytetään johdonmukaisesti alusta alkaen avustamaan ohjelmistokehittäjien työtä.

Valmiinkin tuotteen lähdekoodin analyysillä voidaan saada kiinni ohjelmistovirheitä, mutta yleinen vaikutus koodin laatuun on pienempi. Avoimen lähdekoodin ja ilmaisen jakelun staattisen analyysin työkalut ovat tyypillisesti kevyempiä ratkaisuja verrattaessa niiden kaupallisiin kilpailijoihin. Osa on käyttöliittymiltään hyvin pelkistettyjä, ja osa taas hyvinkin monimutkaisia, maturiteetin mukaan. Ohjelmistokehittäjien harkitessa itselleen parhaiten soveltuvaa analyysityökalua on hyvä harkita tarkkaan käyttötarkoitus ja tavoitellut vaikutukset. Jos halutaan karsia hyvin rajattuja virheitä, voi osa avoimen koodin työkaluista tulla hyvinkin kyseeseen. Useamman kielen tehokkaasti kattavista ja laadukkaan tuen omaavista työkaluista joutuu tyypillisesti maksamaan verrattain suuria summia.

4.2 Työkalut

Tässä osassa evaluoimme tietoturvatestauksessa käytettäviä työkaluja, joita voi hyödyntää ICS-ympäristöissä. Evaluaation tarkoitus on antaa kuva eri menetelmille tyypillisistä työkaluista eikä siten olla täysin kattava esitys. Kaikkiaan 16 työkalua tai työkalukokoelmaa on evaluoitu ICS-ympäristöön sopivuuden kannalta. Yhteenveto työkaluista on esitetty taulukossa 34. Evaluoidut työkalut sisältävät penetraatiotestaustyökaluja, *fuzz*-testereitä, haavoittuvuusskannereita ja verkon monitorointityökaluja.

4.2.1 Monikäyttöiset ICS tietoturvatestaustyökalut

Tässä kategoriassa ovat työkalut, jotka on erityisesti tarkoitettu teollisuusautomaatiojärjestelmien tietoturvatestaukseen. Esimerkiksi *Wurldtech's Achilles Satellite* ja *Mu Dynamics Security Analyzer* kuuluvat tähän kategoriaan, ja niistä ensimmäinen evaluoidaan tässä. Nämä työkalut sisältävät erilaisia testimenetelmiä teollisuusautomaatiojärjestelmien luotettavuuden, kestävyyden (*robustness*) ja saatavuuden testaamiseen syöttämällä ei-sopivaa tai odottamatonta verkkoliikennettä testikohteeseen.

4.2.1.1 Wurldtech Achilles Satellite

Työkalu	Achilles Satellite
Luokitus	Monikäyttöinen työkalu erityisesti ICS-ympäristöjä varten. Protokolla- ja *fuzz*-testaus, verkkohyökkäyssimulointi, porttiskannaus, monitorointi.
Kehitysvaihekäyttö	Yksikkötestaus, integrointitestaus, systeemi/hyväksymistestaus.
Maksullisuus	Maksullinen.
Kypsyystaso	Käytetään useissa yrityksissä.
Alusta	Sisältää oman laitteiston ja Windows-pohjaisen asiakasohjelmiston.
Testikohde	Teollisuusautomaatiojärjestelmät.
Laajennukset	Erilliset protokollatesterit.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Erittäin automatisoitu.
Raportointi	Generoi pdf-raportit.
Soveltuvuus ICS-ympäristöön	Suunniteltu erityisesti ICS-ympäristölle. Tukee monia teollisuusautomaatioprotokollia.
Helppokäyttöisyys	Helppokäyttöinen graafinen käyttöliittymä. Hyvin dokumentoitu.
Muuta	Testilaite on teollisuus-PC (Ubuntu) erityisellä laitteistolla, testisovelluksilla ja datalla. Käytetään etänä vain Windowsille soveltuvalla asiakasohjelmistolla. Testit jaetaan seuraavasti: Skannaukset: Palvelujen haku porttiskannauksella. Storms: Kuormituksen testaus eri pakettimäärillä. Tason määritys, kuinka paljon paketteja kohde jaksaa käsitellä. Grammars: Generoi valideja ja invalideja viestejä testatakseen protokollatoteutusta tai protokollapinon toimintaa. Yksittäisiä *grammars*-testitapauksia ei voi tarkastella tai hallita käyttöliittymän kautta. Fuzzerit: Fuzzerit testaavat myös protokollatoteutuksia ja protokollapinojen toimintoja. Eroavaisuus verrattuna grammars-testitapauksiin on, että fuzzerit käyttävät mielivaltaisia otsikkotietoarvoja.

	Codenomicon Defensics: Jotkut Codenomiconin työkalut on integroitu Achillesiin. Käyttöliittymä näissä integroiduissa työkaluissa on huonompi kuin varsinaisissa Codenomiconin työkaluissa. Satellite sisältää testit vähintään seuraaville protokollille: ARP, BOOTP, CIP, DCOM, DHCP, DNP3, Ethernet/IP, FTP, HTTP, ICCP, ICMP IGMP, IPv4, LLDP/LLDP-MED, MODBUS/RTU, MODBUS/TCP, MMS, NTP, RPC, SNMPv1, SNMPv2c, SNMPv3, TACACS+, TCP, Telnet, UDP ja Vnet/IP. Testikohteen selviytymistä testeistä voidaan seurata mm. ARP-, ICMP- ja diskreettimonitoreiden avulla. *Achilles*-testaus myydään yleensä asiakkaalle palveluna. Satellite-testien läpäisy vaaditaan *Achilles Cyber Security* sertifikaattia varten. *Achilles Satellitessa* on kattava kokoelma testitapauksia eri protokollille, mutta laitteen hinnoittelu on melko korkea, jos laitteen hankkii itselleen. Pääasiallinen toimintatapa valmistajalla on kuitenkin myydä testaus- ja sertifiointipalvelua.

4.2.2 Fuzz-testaus

Fuzz-testaustyökaluja ja työkalutyyppejä löytyy vaihtelevasti; jotkut työkalut ovat vain kehysohjelmistoja, jotka vaativat että testaaja kokoaa testit itse. Jotkut työkalut saattavat vain lähettää satunnaista dataa testikohteelle. Tässä evaluoidut työkalut sisältävät valmiita testitapauksia, mikä helpottaa testaajan työtä huomattavasti.

4.2.2.1 Codenomicon Defensics

Työkalu	**Codenomicon Defensics**
Luokitus	Mallipohjainen fuzz-testaus.
Kehitysvaihekäyttö	Toteutus, testaus, käyttöönotto, ylläpito.
Maksullisuus	Maksullinen, hinnoittelu tapauskohtaista.
Kypsyystaso	Työkaluja on kehitetty noin 10 vuoden ajan.
Alusta	Linux, Windows, OS X.
Testikohde	Protokollarajapinnat.
Laajennukset	Katso kohta ”muuta”.
Uhkien vaikutuksen vähentäminen	Käyttäjä voi tarkastella jokaisen testitapauksen sisältöä. Kun kohdejärjestelmässä havaitaan epäilyttävää käyttäytymistä, eiläpimenneet testitapaukset merkitään selvästi lokeihin.

Automatisointi	Testitapaukset ajetaan automaattisesti.
Raportointi	Työkalu generoi testilokit ja yhteenvedon. Lokivaihtoehdot ovat kattavat (txt, xml, html, docx).
Soveltuvuus ICS-ympäristöön	Testiryhmät soveltuvat erinomaisesti ICS-ympäristölle. Modbus on ainoa testiryhmistä löytyvä ”puhdas” ICS-protokolla, mutta muita yleisiä protokollia käytetään laajalti ICS-ympäristössä (erityisesti IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP), HTML Server (verkkolaitekonfigurointiin) sekä SNMPv1/2c/3.
Helppokäyttöisyys	Työkalu on helppo käyttää ja ajaa. Työkalun pääominaisuuksien oppiminen vie vain muutaman tunnin. Sekä komentorivi- että graafinen käyttöliittymäversio ovat saatavilla.
Muuta	Sisältää työkaluja noin 130 eri protokollalle, jotka myydään itsenäisesti. Codenomiconin työkalut on tarkoitettu *robustness*-testaukseen ja etsimään vikoja protokollatoteutuksista. Myös tiedostomuodon toteutuksien testaamiseen löytyy työkaluja. Työkalut pyrkivät löytämään virheitä kohdejärjestelmästä syöttämällä sekoitettuja (*fuzzed*) protokollaviestejä tai viestinpätkiä kohdejärjestelmään. Testiryhmät sisältävät yleensä kymmeniätuhansia testitapauksia yhdelle protokollalle. Ympäristön ja kohteen mukaan testaus voi viedä melkoisesti aikaa. Testeistä aiheutuva kohdejärjestelmän kaatuminen tai hidastuminen yleensä vaikeuttaa tai pitkittää testityötä. Työkalu ‘*Traffic Capture Fuzzer’* ei vaadi protokollaspesifikaatioita. Testitapaukset generoidaan kohdejärjestelmän liikenteen pohjalta. Kyseinen työkalu laajentaa mahdollisten testikohteiden määrää suuresti, kuten omistusoikeudellisten ICS-protokol-lien tapauksessa. Työkalut ovat erittäin tehokkaita löytämään virheitä useista erityyppisistä kohteista. Työkalujen perusidea on pysynyt samankaltaisena kauan, mutta käytettävyys ja ominaisuudet ovat huomattavasti parantuneet ajan kuluessa.

4.2.2.2 JBROFuzz

Työkalu	**JBROFuzz**
Luokitus	Web-sovellus fuzzeri.
Kehitysvaihekäyttö	Toteutus, testaus.
Maksullisuus	Ilmainen.
Kypsyystaso	Version 1.6. aktiivinen kehittäminen käynnissä.
Alusta	Windows, Linux.
Testikohde	HTTP- ja HTTPS-rajapinnat.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Pyynnöt generoidaan ja lähetetään automaattisesti.
Raportointi	Vastaukset kirjoitetaan tiedostoon. Sisältää graafisen vaihto-ehdon vastauksille.
Soveltuvuus ICS-ympäristöön	Vähäinen. Pääfokus näyttää olevan julkisissa web-palvelimissa, mutta voidaan käyttää verkkolaitteiden konfigurointiin tarkoitettujen web-palvelimien testauksessa.
Helppokäyttöisyys	Tehokas käyttö vaatii paljon opettelua ja tietämystä http:sta. Sisältää hyvän tutoriaalin.
Muuta	OWASP-projekti (*Open Web Application Security Project*) Projektin web-sivuilta: *JBroFuzz generates requests, puts them on the wire and records the corresponding responses received back. It does not attempt to identify if a particular site is vulnerable or not; this requires further human analysis.* Työkalua käytettiin nopeasti http-palvelimelle kytkimessä. Epäilyttävää toimintaa ei havaittu kytkimessä tai palvelimessa. Kokeilu ei sisältänyt testausta kaikilla työkalun ominaisuuksilla.

4.2.3 Port scanning

Porttiskannauksen työkaluista evaluoimme Nmap-nimisen hyvin yleisesti käytetyn työkalun.

4.2.3.1 Nmap

Työkalu	**Nmap**
Luokitus	Porttiskannaus, verkkotiedustelu.
Kehitysvaihekäyttö	Toteutus, testaus, käyttöönotto, ylläpito.
Maksullisuus	Vapaa, GPL.
Kypsyystaso	Yli 10 vuoden kehitystyö. Nykyinen versio 5.0.
Alusta	Linux, Windows, BSD.
Testikohde	TCP/IP pohjaiset verkkolaitteet.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Osittainen.
Raportointi	Tulokset kirjoitetaan tekstitiedostoon.
Soveltuvuus ICS-ympäristöön	Riippuu ICS-verkossa käytettävistä laitteista. Soveltuu hyvin palveluiden, käyttöjärjestelmän ja porttien määrittämiseen.
Helppokäyttöisyys	Perusskannaus on helppoa, erityisesti graafisen liittymän kanssa. Edistyneempi käyttö kaikkien asetusten kanssa vaatii jonkin verran opiskelua.
Muuta	Monipuolinen perustyökalu tiedonkeruuseen, palvelujen määrittämiseen sekä käyttöjärjestelmän tunnistamiseen. Yleensä ensimmäinen työkalu, joka valitaan testaukseen. Zenmap on graafinen käyttöliittymä Nmapille. Zenmap sisältää seuraavat ominaisuudet: • Usein käytetyt skannaukset voidaan tallentaa profiileihin. • Tallennettuja skannaustuloksia voidaan vertailla keskenään. • Uusimpien skannausten tulokset tallennetaan tietokantaan, johon voidaan suorittaa hakuja. • Tuloksien visualisointi.

4.2.4 Haavoittuvuusskannaus

Haavoittuvuusskannereista evaluoimme Nessus- ja Nikto-nimiset työkalut.

4.2.5 Tenable Nessus

Työkalu	Tenable Nessus
Luokitus	Haavoittuvuusskanneri.
Kehitysvaihekäyttö	Toteutus, testaus.
Maksullisuus	Maksullinen kaupalliseen käyttöön, ilmainen kotikäyttäjille.
Kypsyystaso	Laajalti käytetty, kehitetty useita vuosia.
Alusta	Linux, Windows, OS X
Testikohde	Useita kohteita, pääasiassa verkottuneet järjestelmät.
Laajennukset	Plug-ineja useisiin käyttötarkoituksiin.
Uhkien vaikutuksen vähentäminen	Varoitukset vaarallisten palveluiden tai ohjelmistoversioiden varalta.
Automatisointi	Testien ajaminen on automatisoitu.
Raportointi	Raportin generointi html-muodossa.
Soveltuvuus ICS-ympäristöön	Testit ovat usein relevantteja ICS-ympäristössä. Nessus sisältää 39 tietoturvatarkistusta SCADA:lle.
Helppokäyttöisyys	Helppokäyttöinen graafinen käyttöliittymä.
Muuta	Haavoittuvuudet kirjoitetaan tietokantaan NASL-kielellä. Nessus ei pysty löytämään tuntemattomia haavoittuvuuksia kohdejärjestelmästä. Testit sisältävät porttiskannauksen ja joissain tapauksissa tarkemman tarkastelun, esim. jos ftp-portti on avoin, työkalu yrittää anonyymiä sisäänkirjautumista. Nessus koostuu palvelin- ja asiakasohjelmistosta. Palvelin hallinnoi plug-ineja ja voi hallita useita asiakasohjelmistoja, asiakaskäyttöliittymä on haavoittuvuusskannausta varten. Skannauksen kesto vaihtelee paljon. Ciscon reitittimen skannaus kesti yli 4 tuntia. Jotkin kohteet on skannattu alle 10 minuutissa. Nessus ei anna ”jäljellä oleva aika” -arviota skannaukselle. Nessus voi kutsua ulkopuolisia työkaluja, esim. Hydra, Nikto.

4.2.5.1 Nikto

Työkalu	**Nikto**
Luokitus	Haavoittuvuusskanneri Web-palvelinten testaukseen.
Kehitysvaihekäyttö	Toteutus, testaus, käyttöönotto, ylläpito.
Maksullisuus	Ilmainen, GPL.
Kypsyystaso	Kyllä, aktiivista kehitystä.
Alusta	Linux.
Testikohde	Web-palvelimet.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Varoittaa haavoittuvuuksista.
Automatisointi	Skannaus on automatisoitu.
Raportointi	Tekstitiedostoon.
Soveltuvuus ICS-ympäristöön	Monet ICS-laitteet (esim. kytkimet, prosessikontrollerit) sisältävät web-palvelimia konfigurointiin, mutta useat web-palvelimien haavoittuvuuksista eivät oleellisia ICS-ympäristössä.
Helppokäyttöisyys	Käyttö yksinkertaisen komentorivin avulla.
Muuta	Suorittaa useanlaisia kattavia testejä web-palvelimille. Sisältää yli 3 500 potentiaalisesti vaarallista tiedostoa/CGI:tä, versiot yli 900 palvelimesta ja versiospesifisiä ongelmia yli 250 palvelimesta.

4.2.6 Monitorointityökalut

Verkkomonitoroinnin työkaluista evaluoimme Nethawk iPron, Wiresharkin ja Clarified Analyzerin.

4.2.6.1 Nethawk iPro

Työkalu	**Nethawk iPro**
Luokitus	Verkkoliikenteen suorituskykyinen tallennus, monitorointi ja analyysi.
Kehitysvaihekäyttö	Toteutus, testaus, ylläpito.
Maksullisuus	Kyllä.
Kypsyystaso	Uusi tuote. Aktiivista kehitystä.
Alusta	Työkalun mukana erityinen laitteisto. *Flow*-analyysiin löytyy asiakasohjelma vain Windowsille.
Testikohde	Verkkoliikenne.
Laajennukset	*Flow*-analyysi, QoS ja Snort IDS.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Automaattinen *flow*-analyysi.
Raportointi	Visualisaatiot ja verkkotallenteet.
Soveltuvuus ICS-ympäristöön	Soveltuu ICS-verkon käyttäytymisen monitorointiin, esimerkiksi tietoturvatestauksen aikana.
Helppokäyttöisyys	Vaatii jonkin verran opiskelua. Web-pohjainen graafinen käyttöliittymä tai etä-SSH-yhteys.
Muuta	Koostuu *rack-size*-laiteratkaisusta. Tietokantapohjaiset verkon visualisointiominaisuudet. Työkalu sisältää monia edistyksellisiä ominaisuuksia eri käyttötarkoituksiin. Testasimme varhaisen version työkalua, joka sisälsi vain IDS:n ja liikenteen tallennusominaisuudet. Uusi iPro sisältää enemmän ominaisuuksia (esim. *flow*-analyysi, QoS-monitorointi).

4.2.6.2 Wireshark

Työkalu	**Wireshark**
Luokitus	Protokolla-analyysi.
Kehitysvaihekäyttö	Toteutus, testaus, käyttöönotto, ylläpito.
Maksullisuus	Vapaa, GPL.
Kypsyystaso	Ensimmäinen versio julkaistiin 1998. Nimi muuttui Etherealista Wiresharkiksi 2006. Nyt yli 500 osallistuvaa kehittäjää.
Alusta	Linux, Windows, BSD, OS X.
Testikohde	Verkkoliikenne.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Laajennetut suodatusvaihtoehdot tallennusta ja analysointia varten.
Raportointi	Reaaliaikainen loki, pcap, csv + eräitä muita formaatteja.
Soveltuvuus ICS-ympäristöön	Hyvä sovellettavuus. Suodattimet sisältävät joitain ICS-ympäristön protokollia, esim. UPC-UA Binary protocol, Modbus/TCP, DNP3, Common Industrial Protocol, Ethernet/IP, Profinet ja Foundation Fieldbus.
Helppokäyttöisyys	Helppokäyttöinen graafinen käyttöliittymä. Hyvin dokumentoitu. Suodattimet ja näkymät vaativat jonkin verran opettelua.
Muuta	Tukee satoja protokollia, yhdistyy vain yleisiin verkkoihin, kuten Ethernet, WLAN jne. Windows-versio aiheuttaa ajoittain koneen kaatumisen käynnistettäessä Wiresharkia. Vaatii koneelta paljon tehoa ja muistia käsitellessään laajoja tiedostoja.

4.2.6.3 Clarified Analyzer

Työkalu	**Clarified Analyzer**
Luokitus	Verkkoliikenteen visualisointi.
Kehitysvaihekäyttö	Toteutus, testaus.
Maksullisuus	Kyllä, erilaisia laskutusvaihtoehtoja.
Kypsyystaso	Työkalujen tutkimus ja kehitys alkoi 2002. Kaupallista työtä vuodesta 2006.
Alusta	Windows, Linux, OS X.
Testikohde	Online- tai offline-liikenteen analyysi.
Laajennukset	Logster – datan visualisointia lokeista. Voi käyttää yhdessä Wiresharkin kanssa.
Uhkien vaikutuksen vähentäminen	Liikenneanalyysi voi paljastaa viallisen laitteen tai vihamielisen yksikön verkosta.
Automatisointi	Visualisoinnit generoidaan automaattisesti. Käyttäjä voi valita eri vaihtoehdoista ja muuttaa visualisointivaihtoehtoja.
Raportointi	Pcap-tiedostot ja visualisoinnit. Tulokset voi myös siirtää Wiki-sivustolle.
Soveltuvuus ICS-ympäristöön	Riippuu ICS-verkosta. Voidaan käyttää esimerkiksi testihyökkäyksen visualisointiin.
Helppokäyttöisyys	Työkalua käytetään helppokäyttöisellä graafisella käyttöliittymällä.
Muuta	Käyttökelpoinen työkalu verkkoliikenteen visualisointiin. Sisältää erilaisia visualisaationäkymiä. Vaatii koneelta paljon tehoa ja muistia käsitellessään laajoja tiedostoja.

4.2.7 Lähdekoodianalyysi

Evaluoimme kaksi ilmaista lähdekoodianalyysityökalua: Cppcheck ja RATS. Kaupalliset lähdekoodianalysaattorit saattavat olla kovin kalliita pienissä projekteissa.

4.2.7.1 Cppcheck

Työkalu	**Cppcheck**
Luokitus	Työkalu staattiseen C/C++-koodianalyysiin, paikalliseen analyysiin, etsimään muistivuotoja jne.
Kehitysvaihekäyttö	Toteutus, testaus.
Maksullisuus	Vapaa, GPL.
Kypsyystaso	Korkea kehitys- ja ylläpitoaste.
Alusta	Linux.
Testikohde	C/C++-lähdekoodi, function-by-function-analyysi.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Ei sisäänrakennettuna, mutta helposti automatisoitavissa käyttäen skriptikieliä ym.
Raportointi	Yksinkertainen tekstiloki.
Soveltuvuus ICS-ympäristöön	Jos ICS-ohjelmisto on toteutettu C/C++:lla.
Helppokäyttöisyys	Erittäin helppokäyttöinen komentorivikäyttöliittymä, helppo ottaa käyttöön.
Muuta	Ohjelma yrittää löytää virheitä, joita C/C++-kääntäjä ei löydä. Se on kuitenkin optimoitu olemaan raportoimatta vääriä virheitä, mikä tarkoittaa samalla, että suhteellisen suuri määrä todellisia virheitä jäänee kuitenkin löytymättä.

4.2.7.2 RATS

Työkalu	RATS
Luokitus	Staattinen lähdekoodianalyysi. Karkean tason skannaukset lähdekoodille haavoittuvien funktioiden ym. varalta.
Kehitysvaihekäyttö	Toteutus, testaus.
Maksullisuus	Ilmainen, GPL, avoin lähdekoodi.
Kypsyystaso	Ei ylläpidetty, korkea kehitysaste, lähes vanhentunut.
Alusta	Linux, Windows.
Testikohde	C/C++, Perl, PHP ja Python lähdekoodianalyysi, line-by-line-analyysi.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Ei sisäänrakennettuna, mutta helposti automatisoitavissa käyttäen skriptikieliä jne.
Raportointi	Yksinkertainen tekstiloki.
Soveltuvuus ICS-ympäristöön	Rajoittunut soveltuvuus.
Helppokäyttöisyys	Erittäin helppokäyttöinen komentorivikäyttöliittymä, helppo ottaa käyttöön.
Muuta	Työkalu ei löydä kaikkia virheitä, mutta sillä voi karkeasti arvioida koodin lähtötasoa ja käyttää kohdistamaan tarkempia tietoturvakatselmointeja. Uusin versio on vuodelta 2002. RATSilla voi laskea kohdetiedoston ohjelmarivien lukumäärät.

4.2.8 Muut

Tämä osuus sisältää työkalut, joita ei voi kategorisoida tämän evaluaation muihin osioihin: Metasploit kehysohjelma haavoittuvuuksien etsintään, kaksi työkalukokoelmaa (Backtrack, Netwox/Netwag) ja kaksi yksittäistä protokollaspesifistä työkalua (SNMPWalk, Yersinia).

4.2.8.1 Metasploit Framework 3.2

Työkalu	**Metasploit Framework 3.2**
Luokitus	Haavoittuvuuksien etsinnän kehitys ja suoritus. Penetraatiotestaus.
Kehitysvaihekäyttö	Toteutus, testaus, käyttöönotto, ylläpito.
Maksullisuus	Ilmainen, BSD.
Kypsyystaso	Haavoittuvuuskartoituksen de facto kehitysympäristö/kehikko.
Alusta	Linux, Windows.
Testikohde	Useita kohteita.
Laajennukset	Kyllä.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Automatisoi haavoittuvuuksien hyväksikäytön.
Raportointi	Ei.
Soveltuvuus ICS-ympäristöön	Erinomaisesti soveltuva, erityisesti jos ICS käyttää haavoittuvia järjestelmiä. ICS-spesifisiä haavoittuvuuksia on julkisesti tiedossa hyvin vähän, mikä vähentää soveltuvuutta.
Helppokäyttöisyys	Helppokäyttöinen graafinen käyttöliittymä, mutta hyväksikäyttömoduulien rakentaminen vaatii kokemusta ja tietämystä haavoittuvuuksista.
Muuta	Sisältää yli 300 eri hyväksikäyttömoduulia Windows-, Unix/Linux- ja Mac OS X -järjestelmille. Työkalut pyrkivät hyväksikäyttämään kohdejärjestelmän turva-aukkoja. Prosessi etenee seuraavasti: 1. Hyväksikäyttömoduulin valinta: testaajan on löydettävä sopiva hyväksikäyttömoduuli, joka sopii järjestelmän haavoittuvuuteen. 2. Vaihtoehdot: Valitse, mitä vaihtoehtoja käytät hyväksikäyttömoduulin suhteen. 3. Valitse payload (shell code). 4. Konfiguroi payload paikallisella IP-osoitteella ja paikallisella portin numerolla. 5. Suorita hyväksikäyttömoduuli. Emme pystyneet suorittamaan onnistuneita hyökkäyksiä kohdejärjestelmäämme. Monissa tapauksissa payload riippuu käyttöjärjestelmästä, service pack -versiosta ja arkkitehtuurista. Tämä tarkoittaa, että osa Metasploitin payloadeista toimii vain tietyillä käyttöjärjestelmillä ja prosessoreilla. Onnistuneen hyökkäyksen suorittaminen vaatii haavoittuvaa versiota ohjelmistosta sekä payloadin vaihtoehtojen konfigurointiin perehtymistä.

4.2.8.2 Netwox/Netwag

Työkalu	**Netwox/Netwag**
Luokitus	Netwox sisältää 222 testityökalua jotka keräävät tietoa LANista tai laukaisevat erilaisia hyökkäyksiä. Netwag on graafinen käyttöliittymä Netwoxille.
Kehitysvaihekäyttö	Toteutus, testaus.
Maksullisuus	Ilmainen.
Kypsyystaso	Työkalut ovat täysin toimivia. Netwox/Netwag on saanut monia positiivisia arvosteluja ammattilaisilta.
Alusta	Linux, Windows.
Testikohde	Verkkorajapinnat esim. reitittimet, kytkimet, LAN-kortit.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Työkalut ajetaan automaattisesti, kun niiden suoritus on toteutettu oikeilla vaihtoehdoilla.
Raportointi	Vähäinen.
Soveltuvuus ICS-ympäristöön	Suunnattu administraattoreille. SNMP-, Telnet-, ja FTP-työkaluja voidaan soveltaa ICS-verkon mukaan.
Helppokäyttöisyys	Työkalut itsessään ovat helpohkoja käyttää, mutta sen ymmärtäminen, mitä eri työkalut tekevät, vaatii opiskelua. Linux-version graafista käyttöliittymää on helppo käyttää, mutta se ei ole kovin vakaa.
Muuta	Paljon työkaluja eri tarkoituksiin yhdistettynä yhteen pakettiin.

4.2.8.3 Backtrack

Työkalu	Backtrack
Luokitus	Työkalukokoelma tietoturvatestaukseen live CD/DVD:llä.
Kehitysvaihekäyttö	Riippuu työkalusta.
Maksullisuus	Ilmainen.
Kypsyystaso	Versio 4 suhteellisen kypsä.
Alusta	Live CD/DVD:ltä käynnistettävä.
Testikohde	Riippuu työkalusta.
Laajennukset	-
Uhkien vaikutuksen vähentäminen	-
Automatisointi	Riippuu työkalusta.
Raportointi	Riippuu työkalusta.
Soveltuvuus ICS-ympäristöön	Bactrack sisältää monia työkaluja, jotka soveltuvat ICS-testaukseen, mutta se ei sisällä erityisesti teollisuusautomaatioon suunnattuja työkaluja.
Helppokäyttöisyys	Riippuu työkalusta. Suurin osa on helppokäyttöisiä.
Muuta	Useimmat työkalut ovat vain komentorivipohjaisia.

4.2.8.4 Yersinia

Työkalu	Yersinia
Luokitus	Verkkoprotokollatestaus.
Kehitysvaihekäyttö	Toteutus, testaus, käyttöönotto, ylläpito.
Maksullisuus	Ilmainen.
Kypsyystaso	Ei kovin vakaa, harvoin päivitetty.
Alusta	Linux, Solaris, OS X 10.4.
Testikohde	Verkkolaitteisto.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Ei.
Raportointi	Ei.
Soveltuvuus ICS-ympäristöön	Ei sisällä testejä ICS-ympäristölle. Soveltuu teollisuusautomaatioon, jos verkko sisältää vanhoja Ciscon reitittimiä tai kytkimiä.

Helppokäyttöisyys	Sisältää graafisen käyttöliittymän, joka on melko yksinkertainen mutta ei siltikään helppokäyttöinen. Käyttöliittymä kaatuu usein.
Muuta	Yersinian tarkoitus on hyödyntää eri verkkoprotokollien heikkouksia. Tällä hetkellä seuraavien protokollien testit sisältyvät työkaluun: STP, CDP, DTP, DHCP, HSRP, 802.1Q, 802.1X, ISL, VTP. Emme pystyneet käyttämään Yersiniaa onnistuneesti dokumentoinnin ja testikohteiden puutteellisuuden takia. Tällä hetkellä työkalulle ei löydy käyttöohjeita ja testien vaikutus on epäselvä. Selvästikin testien pitäisi aiheuttaa epänormaalia käyttäytymistä verkkolaitteissa.

4.2.8.5 SNMPWalk

Työkalu	**SNMPWalk**
Luokitus	SNMP-spesifinen. Pyytää verkkokohteelta tietoa puumuodossa.
Kehitysvaihekäyttö	Toteutus, testaus.
Maksullisuus	Ilmainen.
Kypsyystaso	Erinomainen. Uusin päivitys vuonna 2002.
Alusta	Linux.
Testikohde	SNMP-agentit.
Laajennukset	Ei.
Uhkien vaikutuksen vähentäminen	Ei.
Automatisointi	Työkalut ajetaan automaattisesti, kun ne on suoritettu oikeilla valinnoilla.
Raportointi	Testitulokset on mahdollista tallentaa tekstitiedostoon.
Soveltuvuus ICS-ympäristöön	Soveltuu tiedonkeruuseen, jos SNMP-agentti on käytössä kohdejärjestelmässä.
Helppokäyttöisyys	Yksinkertainen komentorivityökalu. Dokumentaatio on rajoitettu.
Muuta	Joskus SNMP-kyselyt paljastavat yllättävän paljon tietoa kohdejärjestelmästä, esim. Windowsin snmp-daemon. Tulokset riippuvat SNMP-palvelimen konfiguraatiosta. Paljastunut tieto voi olla hyödyllistä hyökkäystä suunnittelevalle hakkerille.

4.2.9 Tietoturvatestaustyökalujen evaluoinnin yhteenveto

Taulukko 34. Tietoturvatestaustyökalujen evaluoinnin yhteenveto.

Luokitus	**Työkalun nimi**	**Saatavuus**	**Käyttö**	**Soveltuvuus ICS:lle 1–5 (1 = huono, 5 = hyvä)**	**Käyttötarkoitus**
Laaja ICS-tietoturvatestaus	Wurldtech Achilles Satellite	Maksullinen	GUI	5. Suunniteltu erityisesti ICS:lle. Tukee monia teollisuusautomaatioprotokollia.	Protokolla- ja fuzz-testaus, verkkohyökkäyssimulointi, porttiskannaus, monitorointi.
Fuzz-testaus	Codenomicon Defensics	Maksullinen	GUI + CMD	4. Erinomainen ICS-testaukseen.	Mallipohjainen fuzz-testaus.
	JBROFuzz	Avoin	GUI	1. Verkkolaitteiden web-palvelimien testaamiseen.	Web-sovellusfuzzeri.
Porttiskannaus	Nmap	Avoin	CMD	5. Riippuu ICS-verkon laitteista.	Porttiskannaus, verkkotiedustelu (palvelut, käyttöjärjestelmä).
Haavoittuvuusskannaus	Tenable Nessus	Maksullinen	GUI	3. Yleiskäyttöinen.	Haavoittuvuusskanneri.
	Nikto	Avoin	CMD	1. Useat haavoittuvuuksista eivät oleellisia ICS:ssä.	Haavoittuvuusskanneri Web-palvelinten testaukseen.
Monitorointityökalut	Nethawk iPro	Maksullinen	GUI	2. Esim. tietoturvatestausmonitorointi.	Verkkoliikenteen tallennus, monitorointi ja analyysi.
	Wireshark	Avoin	GUI	3. Joillekin ICS-protokollille.	Protokolla-analyysi.
	Clarified Analyzer	Maksullinen	GUI	3. Riippuu ICS-verkosta.	Verkkoliikenteen visualisointi.

Lähdekoodi-analyysi	Cppcheck	Avoin	CMD	2. Jos ohjelmisto toteutettu C/C++:lla.	C/C++-koodin staattinen analyysi, muisti-vuodot jne.
	RATS	Avoin	CMD	1. Rajoitettu sovellettavuus.	Staattinen koodianalyysi.
Muut	Metasploit Framework 3.2	Avoin	CMD + GUI	2. Soveltuu, jos testikohteesta löytyy työkalun listaamia haavoittuvuuksia.	Penetraatiotestaus. Haavoittuvuuksien hyväksikäyttö.
	Netwox/ Netwag	Avoin	CMD + GUI	2. Suunnattu administraattoreille.	Kerää tietoa LANista tai laukaisee hyök-käyksiä. SNMP-, Telnet-, ja FTP-työkaluja voidaan soveltaa.
	Backtrack	Avoin	CMD+ GUI	3. Sisältää useita potentiaalisia työ-kaluja.	Tietoturvatyökalukokoelma live CD/DVD:llä.
	Yersinia	Avoin	GUI	1. Ei ICS-spesifisiä testejä.	Verkkoprotokollatestaus.
	SNMPWalk	Avoin	CMD	2. Soveltuu tiedonkeruuseen SNMP-agenteilta.	SNMP-spesifinen. Pyytää verkossa oleval-ta kohteelta informaatiota.

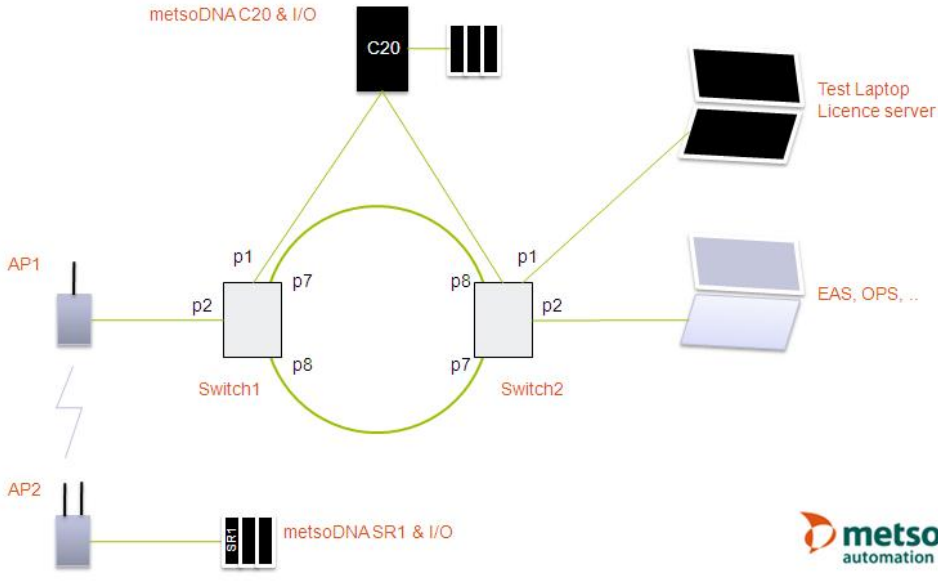
4.3 TITAN-hankkeen kokemuksia käytännön testaamisesta

Tässä osassa esitämme käytännön kokemuksia ICS-järjestelmän tietoturvatestauksesta TITAN-hankkeessa. Pääasiallisena testikohteena projektissa oli Metso Automationin MetsoDNA CR -järjestelmä. Testausta havainnollistetaan lisäksi yksinkertaistetulla logiikkaohjain-esimerkkitapauksella.

4.3.1 MetsoDNA CR -testauksen kokemuksia

TITANin tärkeimpänä testikohteena oli projektille räätälöity kokoonpano MetsoDNA CR -teollisuusautomaatioympäristöstä. MetsoDNA CR on skaalautuva teollisuusautomaatioalusta, joka soveltuu prosessinohjaukseen mm. puu-, paperi- ja energiateollisuudessa. Testauksen tavoitteena oli kohdejärjestelmän tietoturvan tason selvittäminen eri testimenetelmin, mahdollisten haavoittuvuuksien tunnistaminen sekä soveltuvimpien tietoturvatestausmenetelmien ja -työkalujen selvittäminen. Testijärjestelyssä oletettiin, että hyökkääjä on päässyt jo yrityksen palomuurien ja IDS/IPS-järjestelmien ohi ja on sisällä tehtaan verkossa.

MetsoDNA CR:n testaus alkoi kohdejärjestelmään tutustumisella, josta edettiin käynnissä olevien palveluiden, käyttöjärjestelmien ja niiden versioiden kartoittamiseen. Aluksi toimitetussa ympäristössä ei ollut kovennettuja laitteita, kovennettu valvomo toimitettiin myöhemmässä vaiheessa. Kovennetussa valvomossa oli käytössä ainoastaan tarvittavat verkkopalvelut, ja tämä vähensi potentiaalisia hyökkäyskohteita. Testeissä saatiin selvästi todennettua, että kovennuksilla saavutetaan huomattava tietoturvan parannus verrattuna koventamattomaan ympäristöön, ja kovennus on näin ollen yksi suositeltava tietoturvan parannuskeino.

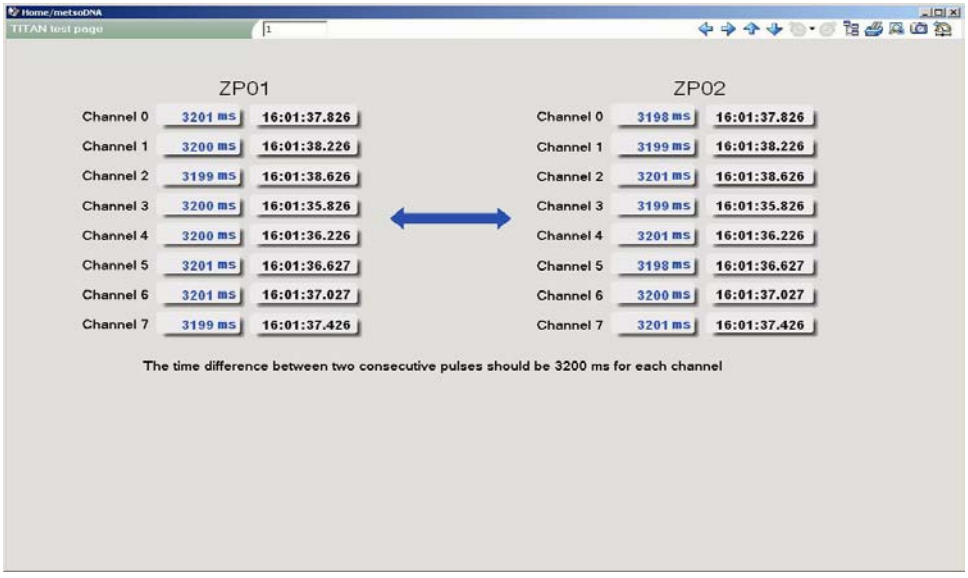


Kuva 6. MetsoDNA CR -teollisuusautomaatioympäristö.

VTT:lle toimitettu räätälöity pienikokoinen MetsoDNA CR -testijärjestelmä koostui seuraavista laitteista:

- Compaq Windows Laptop (EAS, OPS): Valvomo-PC
- Windows-PC: Valvomo -PC / Lisenssipalvelin
- Kaksi Metso Switch -teollisuuskytkintä (*Switch1 & Switch2*)
- Kaksi Wireless LAN Access Point (AP1, AP2)
- MetsoDNA-prosessiasema (malli ACN C20)
- MetsoDNA-prosessiasema (malli ACN SR1).

Kohdejärjestelmän testisovelluksessa prosessiasema ACN C20:lla sijaitseva laskuri lähettää pulsseja binäärisignaaleina järjestelmäväylän kautta prosessiasema ACN SR1:lle. Pulssin pituus on 400 ms, ja pulssit on numeroitu 1:sta 8:aan. Vain yksi pulssi kerrallaan on aktiivinen, joten jokainen yksittäinen pulssi kulkee aina 3 200 ms:n välein. Pulssien välisiä viiveitä käytettiin yhtenä indikaattorina järjestelmän viestiliikenteen toimivuudesta.



Kuva 7. MetsoDNA CR -testijärjestelmän valvomon näyttö.

Kohdejärjestelmässä kulkevaa verkkoliikennettä monitoroitiin eri työkalujen avulla. MetsoDNA CR -koejärjestelmän testaamiseen käytettiin mm. seuraavia työkaluja:

- **Nmap:** palveluiden ja verkon tiedustelu
- **Wireshark, Nethawk iPro:** liikenteen analysointi ja tallentaminen
- **Achilles Satellite:** porttien skannaus, verkkomonitorointi ja erilaiset verkkohyökkäykset
- **Codenomicon Defensics:** järjestelmän rajapintojen fuzz-testaus eri protokollatyökaluilla
- **Metasploit Framework:** valmiiden haavoittuvuuksia hyödyntävien työkalujen kokeilu
- **CPPCheck, RATS:** lähdekoodianalyysi
- **Nessus, Nikto:** haavoittuvuuksien skannaaminen
- **Netwox:** työkalupaketti, jossa useita pieniä työkaluja erilaisiin verkkotesteihin.

Verkkoon murtautumista testattiin Metson järjestelmätestausympäristössä. Automaatioverkko oli konfiguroitu asianmukaisesti, joten sisäänpääsy verkkoon ei onnistunut eikä automaatiojärjestelmään saatu aiheutettua häiriöitä. Työkalujen käytöstä ja soveltuvuudesta teollisuusautomaation testaamiseen saatiin hyviä kokemuksia. Käytettyjä työkaluja ei Satellitea lukuun ottamatta ole suunniteltu teollisuusautomaatiojärjestelmien testaamiseen, mutta ne soveltuivat siihen silti hyvin. Ilmaisia testityökaluja teollisuusautomaation sovelluskohtaisten protokollien testaamiseen löydettiin hyvin vähän.

4.3.2 Logiikkaohjaimen testaus

Tämän kohdan tarkoituksena on kuvata yksinkertainen esimerkki siitä, mitä työkaluja yksittäisen teollisuusautomaatiolaitteen testaamiseen voidaan käyttää. Esimerkki havainnollistaa miten vaarallista voi olla, jos hyökkääjä saa muodostettua suoran TCP/IP-yhteyden teollisuusautomaatiolaitteeseen.

Testikohteena oli Oulun seudun ammattikorkeakoululta lainattu ohjelmoitava logiikkaohjain (PLC). Laite on ollut opetuskäytössä, ja sitä on ohjelmoitu harjoitustöinä tekemään erilaisia tehtäviä kappaletavaralinjastolla. Testitilannetta varten laitteeseen ohjelmoitiin sovellus, joka avaa ja sulkee laitteen tuloja järjestyksessä. Kanavan aktivoitumisesta ja sulkeutumisesta on merkkinä vilkkuvat ledvalot laitteen paneelissa. Valojen tarkoituksena oli toimia yhtenä indikaattorina laitteen toimivuudelle testien aikana.

Testaustilanne ei ollut täysin realistinen, koska saimme suoran verkkoyhteyden laitteeseen jo valmiiksi. Automaatiolaitteet ovat yleensä useiden verkkoa turvaavien tietoturvamekanismien takana (palomuurit, DMZ, eriytetyt verkot). Oletuksena tässä testitilanteessa on siis, että hyökkääjä on onnistunut saamaan hallintaansa PC:n samasta verkosta. Hyökkääjä voi tässä tapauksessa olla esim. hakkeri, joka on kaapannut koneen käyttöjärjestelmän haavoittuvuutta hyväksikäyttäen.

Reititystauluja ja verkkorajapintaa tutkimalla saadaan selville verkon osoite. Testaus aloitetaan selvittämällä kohteen IP-osoite Nmap-työkalun ‘ping scan’ -komennolla. Komento käy yksitellen läpi verkko-osoitteet halutulta verkkoalueelta selvittäen ainoastaan saadaanko kohteeseen yhteys:

```
> nmap –sP 192.168.151.0/24
```

Haku paljastaa kohteen IP-osoitteeksi 192.168.151.15. Seuraavaksi selvitetään kohdelaitteen avoimet TCP- ja UDP-palvelut Nmap-työkalun porttiskannauksella.

```
> nmap -p- -vv -A 192.168.151.15
> nmap -sU -p 0-1024 -A -vv 192.168.151.15
```

Porttiskannaus paljastaa kohteesta paljon: avoimia UDP- ja TCP-portteja löytyy yhteensä yli 20. Näistä kiinnostavimmat olivat aluksi portit 80 ja 991, eli HTTP ja Telnet. Web-selaimella saatiin yhteys laitteen web-palvelimeen.

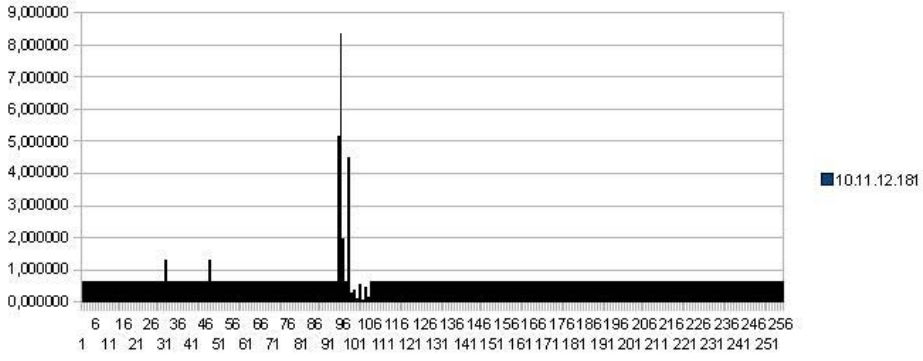
Palvelujen tunnistamisen jälkeen tehtiin hakuja logiikkaohjaimen verkkosivuille, josta löytyivät laitteen käyttöohjeet. Telnet-yhteydellä porttiin 991 pystyimme esimerkiksi syöttämään komennon S <enter>, joka pysäyttää laitteessa ajettavan sovelluksen (ja tässä tapauksessa sammutti led-valot). Telnet-yhteydellä pääsimme muokkaamaan mm. www-palvelimen sivuja.

Verkkohyökkäysten kokeileminen jumiutti laitteen resurssit välittömästi. Testityökaluina käytettiin hping2:sta ja Wurldtech Achilles Satellitea. Jo vähäinenkin liikenne testilaitteen verkkorajapintaan sai laitteen verkkorajapinnan ja sovellukset pysähtymään. Yhteenvetona voidaan sanoa, että murtautuminen testikohteelle on hyvin helppoa. Laitteessa ei ole turvamekanismeja, ja sillä on hyvin rajallinen suorituskapasiteetti. Laitteen tietoturvaa lisäisi merkittävästi pääsynvalvonnan (käyttäjätunnus ja salasana) turvallinen toteutus.

4.3.3 Tietoturvamonitorointi testauksen aikana

Tietoturvamonitoroinnilla tarkoitetaan tietoverkossa liikkuvan datan analysointia erilaisin menetelmin. Monitoroinnilla voidaan esimerkiksi havaita eri protokollia verkosta, salakuunnella kirjautumistietoja, visualisoida tietovoita ja havaita epätavallista käytöstä. Monitorointi on hyödyllistä myös tietoturvatestauksen aikana. Tällöin voidaan testikohteen liikenteestä havaita, aiheuttaako testaus ongelmia verkkorajapinnassa.

Alla olevassa esimerkkikuvassa näkyy erään testikohteen verkkoliikenteen käyttäytyminen pakettitasolla hyökkäyksen aikana. Vasemmalla näkyvä luku kuvaa yksittäisten pakettien välistä aikaa sekunneissa, ja alla oleva luku kertynyttä pakettien lukumäärää. Kuvaajassa näkyvät piikit ovat testauksen aiheuttamia häiriöitä.



Kuva 8. Esimerkki monitoroinnin hyödyntämisestä testauksen rinnalla TITAN-projektissa.

4.3.4 Huomioonotettavia asioita testauksesta

Tietoturvatestauksen pitäisi olla osa organisaation omaa turvallisuusohjelmaa, johon kuuluu oleellisena osana riskien, haavoittuvuuksien ja organisaation tietopääomien (*assets*) kartoitus. Uhkien toteutumisen varalta täytyisi määrittää vastaavat vastatoimet. On huomattava, että todennäköisimmät uhkat ICS-ympäristöissä ovat nimenomaan vahingossa tapahtuvat sattumukset ja sisäisesti tapahtuva vahingonteko (työntekijät, organisaation sidosryhmät), joskin eniten vahinkoa aikaan saavat kohdennetut hyökkäykset kohteeseen [ICSSEC].

Lisäksi, paitsi että hyökkäykset nykyisin ovat teknisesti edistyneempiä, myös se, mitkä haavoittuvuudet ovat relevantteja järjestelmälle, muuttuu jatkuvasti. Uhkia ei useinkaan ymmärretä tai ne sivuutetaan, eikä tietoturvallisen infrastruktuurin käsitettä ymmärretä. [HENTEA]

Teollisuusautomaatiojärjestelmien tietoturvatestauksen valmistelu ja läpivienti voi olla haastavaa, sillä spesifisiä testaustyökaluja on vaikea löytää teollisuusautomaatiossa paljon käytössä oleville kaupallisille suljetuille protokollille. Kaupalliset työkalut ovat usein helppokäyttöisiä ja hyvin dokumentoituja, mutta ne saattavat olla kalliita. Avoimella lähdekoodilla tehdyt testityökalut ovat vaatimattomampia ja työläitä käyttää, joskin edullisempia.

Teollisuusautomaation tietoturvatestaus vaatii paljon manuaalista työtä ja valvontaa, kuten perinteinenkin tietoturvatestaus. Testit on suunniteltava hyvin ja riittävä testikattavuus on arvioitava huolellisesti. Esimerkiksi *defense in depth* -periaatetta noudattaen myös sisäverkon laitteet tulee testata, vaikka hyökkääjän järjestelmään murtautumisen todennäköisyys olisikin pieni.

Testiohjelman apuna voi hyödyntää valmiita referenssejä. Esimerkiksi NISTiltä yleiskäyttöinen tietoturvatestaukseen liittyvä dokumentti on [NIST-SP800-42]. Tämän julkaisun osassa 2.2 on kuvailtu ICS-ympäristöön soveltuvia yleisiä tietoturvastandardeja ja -tarkistuslistoja, joiden avulla voidaan kehittää organisaation turvallisuusohjelmaa.

5. Esimerkki – älykkäät sähköverkot (*Smart Grids*)

Teollisuusautomaatio käsittää todellisuudessa erittäin laajan kentän erityyppisten toimintojen, prosessien ja teknologioiden soveltamista. Koska tietoturvan menestyksellinen hallinta ja ylläpitäminen usein edellyttävät vahvaa ”integraatiota” suojattavan kohdeympäristön kanssa, esitämme seuraavaksi esimerkin eräästä teknisesti hieman yhtenäisemmästä teollisuusautomaatiotoiminnan kohteesta. Kuvaamme joitakin lähtökohtia soveltuvien tietoturvastandardien ja -teknologioiden valinnasta älykkäiden sähköverkkojen (*Smart Grids*) vaatimiin tieto- ja tietoliikennejärjestelmiin. Älykkäiden sähköverkkojen vaatimusten määrittelyn kuvaus käy hyvästä esimerkistä erityisesti siksi, että tällaisten verkkojen oletetaan olevan maantieteellisesti laajoja, erittäin hajautettuja järjestelmiä, jotka vaativat paljon erilaisten tietoliikenneverkkojen soveltamista.

5.1 *Smart Grid* ICT:hen soveltuvia tietoturvastandardeja

Yleisesti ottaen voidaan todeta, että älykkäisiin sähköverkkoihin liittyvä tietoturvastandardointi on pidemmälle kehittynyttä Yhdysvalloissa kuin Euroopassa. Muun muassa seuraavat tietoturvaa pohtivat työryhmät ovat aloittaneet määrittelytyön Yhdysvalloissa jo muutamia vuosia sitten:

- ”*UCAIug AMI-SEC Task Force*”, jonka sivusto http://osgug.ucaiug.org/utilisec/amisec/,
    - AMI (*Advanced Metering Infrastructure*) määrittelytyötä.
    - Kehittää tietoturvasuosituksia ja käytäntöjä nykyaikaisten kulutusmittareiden etäluennan infrastruktuurin järjestelmäelementteihin.

- ”*Cyber Security Working Group* (CSWG)”, jonka työ löytyy sivustolta http://www.nist.gov/smartgrid/ ja joka toimii ”*Smart Grid Interoperability Panel* (SGIP)”:n alla.
    - Alun perin NISTin organisoima *Cyber Security Coordination Task Group* (CSCTG)
    - Muun muassa loistava tuore raportti ”NIST IR-7628 ”*DRAFT Smart Grid Cyber Security Strategy and Requirements*”.

Mainituissa työryhmissä saavutetut tulokset osoittavat, että geneeriseen käyttöön määriteltyjä tietoturvastandardeja ja -käytäntöjä (mm. luvussa 2 esitellyt standardit) täytyy soveltaa edelleen ja tarkentaa huomioiden erityiskohteiden tavoitteet ja käyttötarpeet.

Seuraavassa esitetään mm. edellä mainittujen työryhmien työhön perustuen esimerkinomainen luettelo älykkäiden sähköverkkojen ICT-järjestelmiin soveltuvista tietoturvastandardeista. Listaa voinee käyttää apuna esim. tietyn älykkäiden sähköverkkojen alijärjestelmän tietoturvavaatimuksia asetettaessa (jos lukija työskentelee mainittujen asioiden parissa.)

Taulukko 35. Älykkäiden sähköverkkojen tietoturvaan soveltuvia ICT-standardeja.

Lyhenne	**Standardin kuvaus**	**Työryhmä**
ANSI C12.22	*Meter and end device tables communications over any network.*	ANSI C12.22
INCITS 359	*Information Technology – Role Based Access Control.*	ANSI/INCITS
IEC 62351-1(-8)	*Information Security for Power System Control Operations (Network & system security, TCP/IP & MMS profiles, ICCP & Sub-station protection).*	IEC TC 57 WG15
802.1AE	*Media Access Control Security Standard.*	IEEE 802.1 WG
IEEE 1686-2007	*IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.*	IEEE
802.1X-2010	*Port Based Network Access Control.*	IEEE 802.1 WG
IEEE 802.11i	*Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements.*	IEEE 802.11 WG

SNMPv3	*Simple Network Management Protocol version 3 (Secure).*	IETF Network WG
TLS	*Transport Layer Security (TLS).*	IETF Network WG
DTLS	*Datagram Transport Layer Security (DTLS).*	IETF Network WG
IPSec	*Internet Protocol Security.*	IETF Network WG
CIP 002-009	*NERC Critical Infrastructure Protection (CIP standards).*	NERC reliability
SP 800-82	*Draft Guide to Industrial Control Systems (ICS) Security.*	NIST Computer security
FIPS 198	*The Keyed-Hash Message Authentication Code (HMAC).*	NIST Computer security
FIPS 197	*Advanced Encryption Standard (AES).*	NIST Computer security
FIPS 186-3	*Digital Signature Standard (DSS).*	NIST Computer security
PKCS #1, 3, 5, 12, 15	*RSA Public Key Cryptography Standards.*	NIST, RSA Laboratories
FIPS 140-2	*Security Requirements for Cryptographic modules.*	NIST Computer security
UtilityAMI HAN reqs	*UtilityAMI Home Area Network. System Requirements Specification.*	UCAIug AMI-SEC
Sec profile for AMI	*Security profile for advanced metering infrastructure (AMI).*	UCAIug AMI-SEC

5.2 *Smart Grid* ICT:lle asetettavia tietoturvavaatimuksia

Konkreettisten, noudatettavissa olevien vaatimusten asettaminen on yksi tärkeimmistä tietoturvaan liittyvistä tehtävistä. Tämä pätee myös sähköverkkojen automaatioon liittyen. Seuraavassa taulukossa esitetään esimerkinomaisesti tietoturvavaatimuksia, joita voi käyttää älykkäiden sähköverkkojen normaalitoimintojen vaatimien ICT-järjestelmien toiminnan turvaamiseksi.

Taulukko 36. Esimerkki tietoturvavaatimuksia älykkäiden sähköverkkojen ICT-järjestelmille.

Tyyppi	**Vaatimukset**
Järjestelmän ja tietoliikenteen suojaus	Järjestelmän komponenttien ja niiden välisen kommunikaation suojaaminen: + Hallintatoiminnallisuus erotettu muista palveluista. + Tietoturvatoiminnallisuus eriytetty. + Asiaankuulumaton tiedonsiirto estetty (esim. späm). + Palvelunestohyökkäykset estetty. + Kriittisten noodien resurssien käyttö priorisoitu. + Tietoliikenteen eheys ja autenttisuus varmistettu. + Tietoliikenne salattu (kun tarpeen). + Luotetut tiedonsiirtopolut määritelty. + Avaintenhallinnan infrastruktuuri (PKI) ja sertifikaatit määritelty. + Tietoturvaparametrien luotettava ja turvallinen siirto. + Vikasietoiset verkkonimien ja osoitteiden selvityspalvelut.
Järjestelmän ja tiedon eheys	Järjestelmävikojen tunnistaminen, raportointi ja korjaaminen: + Suojaus haittaohjelmilta järjestetty. + Tietoturvatapahtumien tallennus ja raportointi (mm. valtuuttamattomat järjestelmään pääsyn yritykset) toteutettu. + Tietoturvatoiminnallisuuden tilan (päällä/pois) varmistaminen. + Ohjelmistojen ja tiedon eheyden tarkistaminen ennen käyttöä. + Input datan rajoittaminen (autenttisuus, kelpoisuus). + Vikojen käsittely (rajoituksin).
Pääsynvalvonta	Käyttäjien ja laitteiden luotettava tunnistaminen ja resursseihin pääsyn rajoittaminen valtuutettuun henkilöstöön: + Käyttäjien tunnistus ja kontrolloidut pääsyoikeudet toteutettu. + Valtuutusten ja käyttöoikeuksien turvallinen hallinta. Vahva laite- ja käyttäjäntason tunnistus ylläpitotoimille. + Pääsynvalvonta toteutettu tietoturvapolitiikan ja roolien mukaisesti. + Kriittisimpiin toimintoihin on kaikkein rajoitetuimmat oikeudet.

	+ Tietovirrat on pakotettu tietoturvapolitiikan mukaisiksi. + Salasanojen kompleksisuus ja ainutkertaisuus on pakotettu. + Järjestelmä esittää käyttäjälle tiedotteen järjestelmän käytöstä ja edellisestä kirjautumisesta. + Järjestelmä rajoittaa aktiivisten istuntojen määrää ja pääsyjen lukumäärää. + Istunnon lukitus ja etäistunnon automatisoitu lopetus käytössä.
Seuranta ja jäljitettävyys	Järjestelmälokien ja tietoturvatapahtumien generointi ja validointi, jotta tietoturvamekanismit toimivat oikein: + Komponentti generoi aikaleimallisen tietoturvaseurannan tapahtumatiedon ml. tietoturvatapahtumat, kontrollitapahtumat ja konfiguraatiomuutokset. + Tapahtumatiedon generointi, siirto tai prosessointi ei saa heikentää järjestelmän operatiivista suorituskykyä. Kyky automaattiseen lokitiedon määrän vähentämiseen ja raportin muodostukseen. + Riittävä toiminta-aikaperustainen tapahtumatiedon tallennuskapasiteetti. + Tapahtumalokiprosessoinnin viasta lähetetään automaattisesti hälytys. + Tapahtumalokityökalut ja kerätty tieto ovat suojattuja valttuuttamattomalta pääsyltä, muokkaukselta ja poistolta.
Järjestelmän toimintakyky poikkeustilanteissa	Määritellyn toiminnan ja toimintakyvyn tulee säilyä riittävänä, vaikka järjestelmään kohdistuisi hyökkäys, sattuisi työtapaturma tai jokin komponentti vikaantuisi. + Järjestelmän toimintakykyä uhkaavat tapahtumat tunnistetaan ja pääjärjestelmän tila pidetään yllä tapahtumapaineen alaisena. + Hyökkäyksien, tapaturmien ja muun tapahtumapaineen estäminen ja toimintakyvyn säilyttäminen. + Hallittu alasajo paineen alaisena välttämättömät toiminnot ylläpitäen. + Järjestelmän nopea palautuminen.

Yllä kuvatussa taulukossa on käytetty lähteenä mm. [ASAP-SG].

5.3 *Smart Grid* -tietoliikenteessä sovellettavia tietoturvaprotokollia

Seuraavassa taulukossa on jälleen menty askel eteenpäin ja esitetty potentiaalisia tietoturvaratkaisuja, jotka voisivat soveltua osaratkaisuiksi edellä mainittuihin vaatimuksiin. Mitään tietoturvaratkaisuja ei voi koskaan soveltaa suoraviivaisesti, vaan järjestelmälle asetetut toiminnalliset vaatimukset tulee asettaa etusijalle. Jos ehdotettu tietoturvaprotokolla täyttää vaaditut toiminnalliset vaatimukset (testien jälkeen), se saattaa olla sopiva valinta esim. osajärjestelmien välisen päästä–päähän-tiedonsiirron turvaamiseksi.

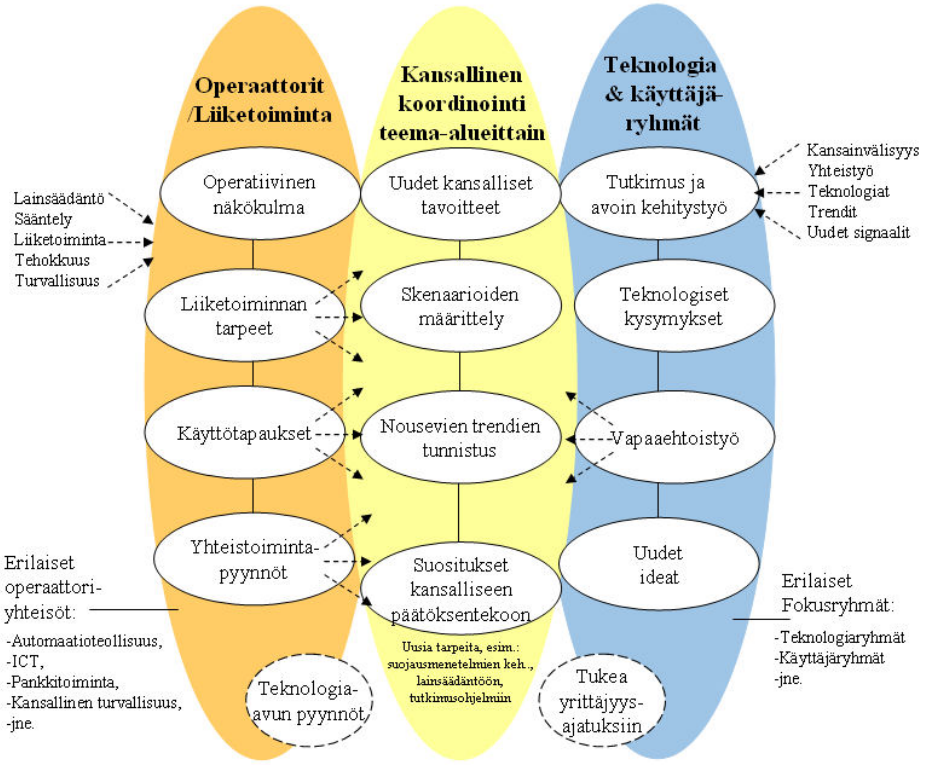
Taulukko 37. Tunnettuja tietoturvaprotokollia älykkäiden sähköverkkojen tietoturvavaatimuksiin.

	Järjestelmän ja tietoliikenteen suojaus	**Järjestelmän ja tiedon eheys**	**Pääsynvalvonta**
IPsec	IP-otsikosta asti suojaus	IP-otsikosta asti suojaus, estää asiattomat yhteydet	OK
SSL/TLS	TCP-datan suojaus	Suojatut datayhteydet	OK
X.509 (PKI)	Avaintenhall. ja tunnistus	Luottamuksen muodostaminen	Tunnistus ja valtuutus
XML salaus & allekirj.	Suojaus XML-tasolla	XML on haavoittuva	XML-otsikko ja data
SSH	Suojattu etäyhteys	Suojatut datayhteydet	OK
DIAMETER	Suojattu tunnistus valtuutus, jäljitettävyys	Signalointi suojattu	Tunnistus, valtuutus, jäljitettävyys

6. Tietoturvatilanteen hallinnasta kansallisella tasolla

Tuotekehitys on muuttunut kiihkeämmäksi, mukaan ovat tulleet lyhyet iteraatiot, *Agile, Lean* jne., joissa ohjelmoijat koodaavat toiminnallisuutta lyhyissä välittömästi testattavissa sykleissä. Tämä tarkoittaa, että kaikkien testityökalujen ja prosessien pitää olla helppokäyttöisiä ja tehokkaita. Koska tällainen ihannetila ei kuitenkaan aina toteudu, se merkitsee, että ohjelmistoihin jää testaamattomia ominaisuuksia, joiden tietoturvataso on epäselvä. Jos tällaisia ohjelmistoja kulkeutuu käytettäväksi teollisuusautomaation järjestelmiin, niiden negatiiviset seuraukset voivat olla ennalta-aavistamattomat.

Seuraavassa on esitetty luonnos siitä, millä tavoin kansallisella tasolla voitaisiin parantaa tiedonvaihtoa toimijoiden kesken ja ennakoida tulevaisuudessa väistämättä eteen tulevia ongelmia.



Kuva 9. Alustava ehdotus kansallisen ennakointiverkoston muodostamiseksi.

Suomessa tarvitaan lisää kansallista koordinointia teema-alueittain. Tulevaisuuden skenaarioita kannattaa työstää yhdessä ja tunnistaa niiden vaikutuksia kullekin liiketoiminta- ja teknologia-alueelle. Olisi ehkäpä jaettava vastuualueita eri alueiden asiantuntijoiden, käyttäjäryhmien ja operaattoreiden kesken. Tavoitteena voisi olla rakentaa verkosto, jossa asiantuntemus löytyy nopeasti kulloinkin esillä oleviin teknisiin, liiketoiminnallisiin tai epäjatkuvuutta aiheuttaviin tekijöihin. Teemaseminaarit ja työpajat tulisivat olemaan oleellinen osa tällaisen verkoston työtä ja toimintaa.

Tärkeä tietolähde Suomessa on CERT-FI:n sivusto: http://www.cert.fi/

7. Aihioita jatkotutkimuksille

Hankkeen yhteydessä on valmisteltu KROMI-nimistä jatkohanketta, jossa nyt kartoitetut, eniten kehitystyötä tarvitsevat tutkimusalueet käsiteltäisiin syvällisemmin. Tulevaisuudessa tulisi tutkia ja kehittää mm. kannettavia tietoturvan testiympäristöjä, joita voitaisiin käyttää hyväksi alan toimijoiden tietoturvatilanteen analysoinnissa ja kehittämisessä.

Yhteenvetoa jatkotutkimusten ylätason tavoitteista:

- Selvittää yksityiskohtaisemmin, miten standardit vaikuttavat tietoturvaan.
- Koostaa kannettava testiympäristö – yritysten ei tarvitsisi luovuttaa laitteita, vaan tutkijat voisivat mennä paikan päälle.
- Kehittää tutkimuksellinen pohja, jonka mukaisesti kannettava testi-/tutkimusympäristö kehitettäisiin ja ylläpidettäisiin.
- Levittää tietoa todelliseen ympäristöön – alan toimijoille, vahvaa disseminaatiota.

Seuraavassa on esitetty tiivistelmä jatkotutkimuksia tarvitsevista tutkimusaihioista.

7.1 Automaatiojärjestelmien tt-varmistamisen kokeelliset menetelmät ja toimintaohjeet

Jatkohankkeessa pääasiana olisi tutkia tarkemmin teollisuusautomaatioon soveltuvia tietoturvan varmistamisen menetelmiä ja tietoturvaratkaisuja. Lähtökohtina käytettäisiin aiemmin identifioituja *state-of-the-art*-menetelmiä, ratkaisuja ja työkaluja. Tutkimusmetodeihin kuuluisivat mm. haavoittuvuusanalyysi, lähdekoodianalyysi, penetraatiotestaus, *robustness*-testaus ja testattavan kohteen yksityiskohtainen tarkkailu testauksen alaisena.

Tutkimuksissa tulisi suorittaa mm. kokeellista, laajaa tietoturvaprofilointia tyypillisistä heikkouksista teollisuusautomaation ohjelmistoissa ja laitteissa. Testattavaksi ja analysoitavaksi koottaisiin laajasti ohjelmistoja, laitteita ja järjestelmiä, ja tätä kautta saataisiin tarkempaa tietoa laitteiden ja ohjelmistojen heikkouksista ja soveltuvista testimenetelmistä. Tavoitteena olisi tietoturvatestauksen ja -varmistamisen menetelmien sovittaminen ja syventäminen tietyille ylätason vaatimuksille, joita järjestelmille on asetettu, esim. ISA, NERC, ISO, IEC, NIST. Eniten jatkotyötä vaativia tutkimusalueita olisivat mm. kohteen selviytymisen yksityiskohtainen seuranta testauksen alaisena, tietoturva-analyysiin liittyvien välitulosraja-arvojen sekä mahdollisten instrumentointimetodien määrittely ja tietoturvatestausmenetelmien tehokkaampi ja tarkempi käyttö.

Tutkimukselliset lähtökohdat voidaan jakaa kolmeen osuuteen. Kukin osuus voisi käyttää tutkimuksessaan hyväkseen muiden osuuksien tuottamia välituloksia soveltuvin osin. Esimerkiksi järjestelmän yleisessä tietoturvatestauksessa voitaisiin käyttää apuna järjestelmän lähdekoodista analysoituja heikkouksia (jos kohteen lähdekoodi saatavilla).

7.1.1 Teollisuusautomaatiojärjestelmien käyttämien tietoverkkojen analysointi

Teollisuusautomaatiojärjestelmien käyttämien tietoverkkojen analyysissä olisi kaksi päätavoitetta.

Verkkoliikenteen analyysi ja normaalitila – Ensimmäisenä tavoitteena olisi selvittää verkkoliikenteen normaalitilat (baseline) tallentamalla dataliikennettä erilaisissa ympäristöissä. Yksityiskohtaisen normaalitilan ominaisuuksien tunteminen on perusvaatimus suurelle osalle analyysialgoritmeja, joita voidaan käyttää erilaisten liikennemallien tunnistamisessa. Jos normaalitila tunnetaan tarkasti, voidaan testattavan tilanteen eroavuudet normaalitilanteeseen mitata. Tavoitteena olisi myös tietoliikenteen yksittäisten osatekijöiden selvittäminen tunnistamalla liikennevuoanalyysin avulla eri komponenttien ja palveluiden aiheuttamat, mallinnetut liikennevuot. Näiden avulla tarkasteltavasta tietoliikenteen osasta voidaan tunnistaa tietyntyyppisiä laitteita tai palveluita ja esimerkiksi niiden tunnettuja käyttötiloja.

Verkkoliikenteen simulointi – Kerättyjä laite- ja palvelukohtaisia liikennetallenteita voitaisiin mallintaa ja käyttää tuottamaan simuloitua tietoliikennettä erilaisilla kokoonpanoilla, joissa voidaan yhdistää haluttu määrä komponentteja ja palveluita erilaisilla verkkoarkkitehtuureilla. Käyttämällä eri laitteiden ja pal-

veluiden liikennetallenteita ja liikennemalleja voidaan hallitusti toistaa paketteja kustakin liikennevuosta ja näin toteuttaa liikennesimulaatioita esim. spesifioidusta SCADA-verkosta. Kehitettyä liikennegeneraattoria voisi käyttää hyväksi myös muissa tutkimusprojekteissa, ja se mahdollistaisi mm. tietoturvatestaamisen virtuaalisessa tuotantoympäristössä sekä uusien laitteiden verkolle aiheuttaman riskin arvioinnin ennen niiden varsinaista käyttöönottoa, tai jopa ennen laitteen/ohjelmiston hankintaa.

7.1.2 Teollisuusautomaatiojärjestelmien ohjelmistokoodien ominaispiirteiden ja tietoturvavirheiden tutkimus

Teollisuusautomaatiojärjestelmien ohjelmakoodin tutkimuksen perusajatuksena olisi etsiä teollisuusautomaatiojärjestelmille ominaisia tietoturvahaavoittuvuuksia. Kattava tutkimus vaatisi, että ohjelmakoodia olisi saatavilla eri järjestelmistä ja riittävän paljon luotettavan analyysin suorittamiseksi. Koodi kuitenkin voidaan tarvittaessa hankkia paloittain eli riittäisi, jos usealta toimittajalta olisi saatavilla edes joitain moduuleita tai ohjelman osia. Tästä koodista voitaisiin sitten etsiä yhteisiä nimittäjiä, niin tietoturvahaavoittuvuuksien kuin ohjelmointitavankin osalta. Jos tutkimuksessa havaittaisiin yleisiä ja toistuvia virheitä, voitaisiin tämän tiedon pohjalta luoda teollisuusautomaatiospesifisiä ohjelmointisääntöjä ja/tai ohjeita, joita noudattamalla tämänkaltaiset ongelmat voitaisiin tulevaisuudessa paremmin välttää. Ohjelmistojen rakenteelliset erot – eivät pelkästään virheet – voisivat olla arvokasta tietoa. Vaikka suoranaisia ominaisia tietoturvahaavoittuvuuksia ei jostain ohjelmakoodista heti löytyisikään, jo tietyntyyppiset toistuvat rakenteet voisivat toimia vihjeinä mahdollisista riskeistä ja ongelmista ko. ohjelmistossa. Tutkimusvaiheina olisivat muun muassa

- lähdekoodien analyysi staattisen analyysin menetelmin virheiden löytämiseksi (manuaalinen ja mahdollisuuksien mukaan automaattinen)
- löydettyjen ohjelmointivirheiden ja ominaisrakenteiden analyysi ja tutkimus
- ohjelmointisääntöjen ja -ohjeiden luominen.

7.1.3 Teollisuusautomaatiojärjestelmien tietoturvatestausmetodien ja työkalujen tutkimus

Teollisuusautomaatiojärjestelmien, niiden osakokonaisuuksien tai yksittäisten laitteiden tietoturvatestaus on edelleen puutteellista. Niinpä tulisi systemaattisesti tutkia, minkätyyppisiä ongelmia ja uhkia laitteisiin ja järjestelmiin kohdistuu, vaikkapa silloin, jos hyökkääjä onnistuu saamaan yhteyden teollisuusautomaatioverkkoon. Tavoitteena voisi olla tietoturvatestata kattava valikoima erityyppisiä standardiprotokollilla kommunikoivia teollisuusautomaatiolaitteita. Tutkimusvaiheina olisivat muun muassa

- tiedon keräys testikohteista eri menetelmin, avoimien palveluiden ja haavoittuvaisten rajapintojen kartoittaminen. Tietoturvatestaustyökalujen soveltaminen kattavin testein.
- testikohteen tilan tarkkailu testauksen aikana ja epävakauden indikaattoreiden, analyysimenetelmien ja raja-arvojen selvittäminen
- yhteenvetotulosten mahdollisimman automatisoitu koostaminen eri menetelmien testituloksista.

Relevanttien työkalujen soveltuvia ominaisuuksia ja testausmetodeja tulisi analysoida. Lisäksi tarkasteltaisiin erilaisten haittaohjelmien aiheuttamia negatiivisia vaikutuksia järjestelmiin, mm. niiden mahdollisia hyökkäysvektoreita kriittisiin järjestelmiin. Työkalujen osalta tulisi tutkia mahdollisuuksia sulauttaa niitä yhtenäiseksi testikokonaisuudeksi, jotta yhtenäiseen testikäyttöön integroidut työkalut olisivat saatavilla kannettavassa PC:ssä kenttätutkimuksia varten.

Referenssejä

[API-1164] American Petroleum Institute (API) Standard 1164, ”Pipeline SCADA Security” (maksullinen).

[ASAP-SG] The Advanced Security Acceleration Project (ASAP-SG), SECURITY PROFILE FOR ADVANCED METERING INFRASTRUCTURE, v. 1.0.

[BELLETT] Vulnerability Analysis of SCADA Protocol Binaries through Detection of Memory Access Taintedness. Carlo Bellettini, Julian L. Rrushi. Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY 20–22 June 2007.

[FIPS112] FIPS PUB 112, Password Usage, (NIST).

[HENTEA] Improving Security for SCADA Control Systems. Interdisciplinary Journal of Information, Hentea Mariana. Knowledge and Management. Volume 3, 2008.

[IAONA] IAONA Handbook Network Security, Versio 1.5.

[ICSSEC] NIST SP 800-82 Final Public Draft, September 2008. Guide to Industrial Control Systems (ICS) Security.

[IEEE 1686] IEEE 1686 – Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities (maksullinen).

[ISA99] ISA99 Industrial Automation and Control Systems Security Standards (maksullisia standardeja).

[ISA99-1] ANSI/ISA-99.00.01-2007, Security for Industrial Automation Control Systems, Part 1: Terminology, Concepts and Models (maksullinen).

[ISA99-TR1] ANSI/ISA TR99.99.01-2007, Security Technologies for Industrial Automation and Control Systems (maksullinen).

[ISA99-TR2] ANSI/ISA-TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment (maksullinen).

[NERC] North American Electric Reliability Corporation (NERC) – CIP Standards.

[NERC-005] NERC CIP-005-2: Cyber Security – Electronic Security Perimeter.

[NIST-SP800-42] NIST SP 800-42 October 2003. Guideline on Network Security Testing.

[PROC] Department of Homeland Security: Cyber Security Procurement Language for Control systems, September 2009.

Julkaisun sarja, numero ja raporttikoodi

VTT Tiedotteita 2545
VTT-TIED-2545

Tekijä(t)
Pasi Ahonen

Nimeke

TITAN-käsikirja
VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa

Tiivistelmä

Tekesin Turvallisuusohjelman TITAN-hankkeen VTT:n osuuden tuloksia on koottu tähän käsikirjaan. Siinä esitellään tiiviisti tärkeimpiä teollisuusautomaation tietoturvaa sivuavia trendejä, standardeja, vaatimuksia, referenssimalleja, ohjeita, testausmenetelmiä ja -kokemuksia.

Tutkimuksissa on päädytty muun muassa seuraaviin johtopäätöksiin: Standardien mukaisen, turvallisen automaatiojärjestelmän hankinta on vaikeaa, joten yrityksen hankintaprosessin kehittämiseen kannattaa varata aikaa ja resursseja. Yhtenäisiä hankintakäytäntöjä täytyy edelleen kehittää. Lisäksi tietoturvan parantaminen vaatii selkeitä, helppokäyttöisiä ja tehokkaita työkaluja ja käytäntöjä, jotka voidaan ottaa käyttöön kaikilla tarvittavilla osa-alueilla kriittisten järjestelmien toiminnan jatkuvuuden varmistamiseksi. Tietoturvavaatimukset tulee työstää kehittäjien ja käyttäjien ymmärtämään muotoon.

Lisäksi näyttää siltä, että kansallisella tasolla tarvitaan lisää yhteistyöfoorumeita ja verkostoja tietoturvatilanteen kartoittamiseksi ja tulevaisuuden riskiskenaarioiden tunnistamiseksi. Mikään yksittäinen toimenpide ei turvaa Suomen automaatioteollisuuden tietoturvatilannetta kokonaisuutena, sillä kilpailu- ja toimintakyvyn varmistaminen tulevaisuudessa edellyttää avoimuuden ja monenkeskisen kommunikaation lisäämistä muun muassa operaattoreiden, laite- ja ohjelmistovalmistajien, automaatiojärjestelmätoimittajien, asiakkaiden, sääntelijöiden sekä jopa kuluttajien välisissä ja keskinäisissä verkostoissa.

ISBN
978-951-38-7642-5 (nid.)
978-951-38-7643-2 (URL: http://www.vtt.fi/publications/index.jsp)

Avainnimeke ja ISSN	Projektinumero
VTT Tiedotteita – Research Notes 1235-0605 (nid.) 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)	27823

Julkaisuaika	Kieli	Sivuja
Elokuu 2010	Suomi	152 s.

Projektin nimi	Toimeksiantaja(t)
Tietoturvaa teollisuusautomaatioon – TITAN	

Avainsanat	Julkaisija
Industrial systems, information security, security practices, security evaluation, security testing, standards	VTT PL 1000, 02044 VTT Puh. 020 722 4404 Faksi 020 722 4374

Tekesin Turvallisuusohjelmaan kuuluvan ”Tietoturvaa teollisuusautomaatioon” (TITAN) hankkeen VTT:n päätulokset on koottu tähän käsikirjaan. Siinä esitellään tiiviisti tärkeimpiä teollisuusautomaation tietoturvaa sivuavia trendejä, standardeja, vaatimuksia, referenssimalleja, ohjeita, testausmenetelmiä ja -kokemuksia.

Tutkimuksissa on päädytty muun muassa seuraaviin johtopäätöksiin: Standardien mukaisen, turvallisen automaatiojärjestelmän hankinta on vaikeaa, joten yrityksen hankintaprosessin kehittämiseen kannattaa varata aikaa ja resursseja. Yhtenäisiä hankintakäytäntöjä täytyy edelleen kehittää. Lisäksi tietoturvan parantaminen vaatii selkeitä, helppokäyttöisiä ja tehokkaita työkaluja ja käytäntöjä, jotka voidaan ottaa käyttöön kaikilla tarvittavilla osa-alueilla kriittisten järjestelmien toiminnan jatkuvuuden varmistamiseksi. Tietoturvavaatimukset tulee työstää kehittäjien ja käyttäjien ymmärtämään muotoon. Lisäksi näyttää siltä, että kansallisella tasolla tarvitaan lisää yhteistyöfoorumeita ja verkostoja tietoturvatilanteen kartoittamiseksi ja tulevaisuuden riskiskenaarioiden tunnistamiseksi.

Mikään yksittäinen toimenpide ei turvaa Suomen automaatioteollisuuden tietoturvatilannetta kokonaisuutena, sillä kilpailu- ja toimintakyvyn varmistaminen tulevaisuudessa edellyttää avoimuuden ja monenkeskisen kommunikaation lisäämistä muun muassa operaattoreiden, laite- ja ohjelmistovalmistajien, automaatiojärjestelmätoimittajien, asiakkaiden, sääntelijöiden sekä jopa kuluttajien välisissä ja keskinäisissä verkostoissa.

ISBN 978-951-38-7642-5 (nid.)
ISSN 1235-0605 (nid.)
ISBN 978-951-38-7643-2 (URL: http://www.vtt.fi/publications/index.jsp)
ISSN 1455-0865 (URL: http://www.vtt.fi/publications/index.jsp)