Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Jarmo Huovinen

Teollisuusverkkojen kybertietoturvallisuus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkötekniikka

Insinöörityö

23.5.2019

Tekijä Otsikko Sivumäärä Aika	Jarmo Huovinen Teollisuusverkkojen kybertietoturva 36 sivua 23.5.2019
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Sähkötekniikka
Ammatillinen pääaine	Sähkövoimatekniikka
Ohjaajat	Head of Network & Security Team Ilari Karinen Lehtori Jukka Karppinen

Insinöörityön aiheena oli tutkia teollisuusverkkojen kyberturvallisuutta sekä verkostoautomaatioon kohdistuvia tietoturvauhkia, haavoittuvuuksia, havainnointia ja suojaamista.

Työssä perehdyttiin teollisuuden tietoturvallisuutta käsitteleviin ohjeistuksiin sekä standardeihin IEC 62443 ja IEC 62254-1. Lisäksi tutustuttiin tietoturvavyöhykkeiden merkitykseen ja niiden suojaamiseen palomuureilla. Työssä selvitettiin tunkeutumisenesto- ja havainnointitekniikoiden toimintaa sekä niiden tuottamien lokitietojen ja tietoturvatapahtumien käsittelyä keskitetysti SIEM-järjestelmien avulla. Langattomien laitteiden käytöstä, hallinnoinnista, tietoturvasta ja haasteista käsiteltiin teollisuusympäristön IIoT-ratkaisuja. Lopuksi työssä esiteltiin esimerkein ohjelmia, joilla voidaan etsiä internettiin kytkettyjä iot-laitteita ja avoimeksi jääneitä palveluita.

Insinöörityö tuotti ohjeistusta automaatio-, sähkö- ja tietoturva-ammattilaisille teollisuuden kybertietoturvajärjestelmien suunnittelussa, testauksissa ja standardien soveltamisessa huomiotavista asioista.

Työn tuloksena todettiin, että teollisuuden tietoturvaratkaisuissa keskitytään yleensä suojaamiseen, havaitsemiseen ja korjaamiseen, jotka ovat ominaisuuksia, joilla pyritään tehokkaaseen uhkien ehkäisemiseen ja toiminnan jatkuvuuden varmistamiseen

Avainsanat	IIot, SCADA, IPS, IDS, SIEM, DMZ

Author	Jarmo Huovinen
Title	Cybersecurity for Industrial Control Systems
Number of Pages	36 pages
Date	23 May 2019
Degree	Bachelor of Engineering
Degree Programme	Electrical Engineering
Professional Major	Electrical Power Engineering
Instructors	Ilari Karinen, Head of Network & Security Team Jukka Karppinen, Senior Lecturer

The purpose of the thesis study was to investigate cyber security in industrial networks, security threats, vulnerabilities, detection and protection against network automation.

The first part discusses the guidelines for industry information security and standards IEC 62443 and IEC 62254-1. The second part of thesis introduces the importance of security zones and their protection with firewalls. After that the work explores the operation of intrusion prevention and detection techniques, as well as centralized processing of log data and security events produced by them using SIEM systems. The use, management, security, and challenges of wireless devices were addressed in IIoT industrial environment solutions. Finally the thesis gives examples of programs that were able to search for iot- devices connected to the Internet and open services.

This work was successful in providing guidance to automation, electrical and information security professionals in the design, testing and application of standards for industrial cyber security systems. As a result it was found that industrial security solutions tend to focus on protection, detection and repair, which are features that aim at effective threat prevention and operational continuity.

Keywords	IIot, SCADA, IPS, IDS, SIEM, DMZ

Sisällys

Lyhenteet

BYOD	Bring Your Own Device, Tietoverkkoon oma laite.
DCS	Distributed Control System, Hajautettu automaatiojärjestelmä.
DMZ	De-militarized Zone, Demilitarisoitu vyöhyke.
ERP	Enterprise Resource Planning, Toiminnanohjausjärjestelmä.
HMI	Human Machine Interface, Ihmisen ja ohjelmoitavan logiikan välinen käyttöliittymä.
ICS	Industrial Control System, Teollisuuden ohjausjärjestelmä.
IED	Intelligent Electronic Device, SCADA-järjestelmän laite.
IoT	Internet of Things, Teollinen internet, esineiden ja laitteiden, palveluiden, ohjelmistojen sekä järjestelmien liittämistä yhteen Internetin avulla.
IIoT	Industry Internet of Things, Teollinen internet.
IT	Information Technology, Informaatiotekniikka, tietotekniikka.
IDS	Intrusion Detection System, Hyökkäyksen ja tunkeutumisen tunnistus-järjestelmä.
IPS	Intrusion Protection System, Hyökkäyksen ja tunkeutumisen estojär-jestelmä.
ISA99	Instrumentation, Systems and Automation Society, Yhdysvaltalainen globaali automaatioteollisuuden asiantuntijoiden organisaatio.
MES	Manufacturing Execution System, MES-järjestelmä on tuotannon- tai val-

	mistuksen ohjausjärjestelmä, joka yhdistää ERP-järjestelmän varsinaiseen tehdasautomaatioon.
MODBUS	Sarjaliikenneprotokolla jota käytettään ohjelmoitavien logiikkapiirien kanssa.
NIST	National Institute of Standards and technology, Sähköalan standardointijärjestö.
NERC	North American Electric Reliability Corporation, Sähköalan järjestö.
PLC	Programmable Controller, Ohjelmoitava kontrolleri.
Profinet	Teollisuus-Ethernet-standardi.
Profibus	Avoin kenttäväyläjärjestelmä.
RDC	Remote Desktop Connection, Etätyöpöytäyhteys.
SCADA	Supervisory Control and Data Acquisition, Tiedonkeruu ja valvonta.
SSH	Secure Shell, Tietoliikenteeseen tarkoitettu protokolla.
SCP	Secure copy protocol, Salattuun tietoliikenteeseen tarkoitettu tiedonsiirto protokolla.
VPN	Virtual Private Network, loogisesti erotettu suojattu verkko-osa.
ZigBee	Lyhyen kantaman tietoliikenneverkko.

1 Johdanto

Teollisuusverkkojen tietoturvan kriittisyys on kasvanut ja kasvaa jatkuvasti. Yritykset ja järjestelmät verkottuvat kiihtyvää tahtia, jolloin niiden välille rakennetaan erilaisia tiedonsiirtoväyliä. Teollisuuden automaatiojärjestelmät suunniteltiin aluksi toimimaan eristettynä ja omina yksiköinään ja tietoturvalla tarkoitettiin enemminkin fyysistä kulunvalvontaa kuin tietoliikenteen valvontaa. Sähköverkkolaitteiden määrän huomattava kasvu ja sovellusten monimutkaistuminen sekä etätyöskentelyn yleistyminen Internet-verkon yli ovat asettaneet myös omat haasteensa automaatiojärjestelmien tietoturvalle. [1.]

Tämän opinnäytetyön tarkoituksena on täydentää ja syventää tietojani teollisuusverkojen- ja teollisen internetin kybertietoturvallisuuden suojaamisessa, joita käytän hyödyksi asiakkaiden toimeksiantojen ja toteutusten suunnitteluun.

Työn tavoitteena on tutkia teollisuusverkkojen tietoturvaa Purdue-viitekehysmallin mukaisesti, joka perustuu IEC 62443 (Teollisuuden tietoliikenneverkot, Verkkojen ja järjestelmien tietoturvallisuus) sekä automaatioalan järjestön ISA:n (International Society of Automation) viitekehysmalliin. Teollisuusverkon tietoturva-arkkitehtuuria määriteltäessä ovat verkon tietoturvavyöhykkeet ja segmentointi tärkeimmät kulmakivet, joiden perusteella pystytään suunnittelemaan muut tasot ja niiden väliset suhteet.

Tietoturvavyöhykkeiden suojaamiseen käytettään palomuureja, jotka ovat turvallisuusstrategioiden perusrakenne, jonka vuoksi opinnäytetyössä käsitellään niiden soveltamista verkkosegmenttien suojaamiseen.

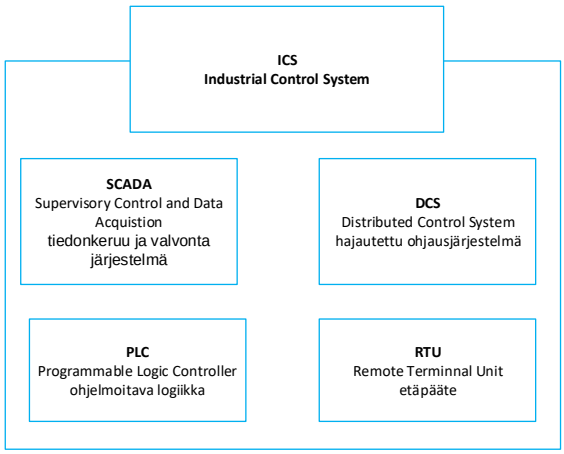
Etäyhteyksien kautta tulevien etäkäyttäjien tunnistamis- ja pääsynhallintamenetelmät ovat tapa varmistaa ja tunnistaa käyttäjät sekä liiketoiminnan kannalta tärkeät järjestelmät, jolloin julkisten verkkojen kautta liikkuvaa informaatiota suojataan käyttäen IPsec-tunnelointia, jota työssä tarkastellaan VPN-tunneloinnin yhteydessä.

2 Tavoitteena tietoturvallinen järjestelmäympäristö ja rakenne

Teollisen Internetin osalta riskit ovat jatkuvasti kasvava puheenaihe ja on helppo kuvitella uhkakuvia kuinka itsenäisesti toimivien anturien ja tekoälyyn perustuvien järjestelmien toimintaa voidaan uhata tietoverkkorikollisuudella.

Viestintätekniikan integrointi teollisuusjärjestelmiin ei ainoastaan anna uusia mahdollisuuksia vaan luo myös monia ennalta arvaamattomia haavoittuvuuksia. On erittäin haastavaa löytää sopivat keinot sellaisen ympäristön suojelemiseksi, joissa uhkamallit ja moninaiset asetukset ovat usein sidoksissa toisiinsa. Eräs suurimmista ongelmista automaatioalan ammattilaisilla on laitosten SCADA-järjestelmien ohjausjärjestelmät, jotka yhdistävät esimerkiksi sähkö-, öljy- ja kaasuputket, vedenjakelu- ja jätevedenkeräysjärjestelmät. Ne ovat suunniteltu avoimiksi ja kestäviksi sekä helppokäyttöisiksi mutta eivät välttämättä ole tietoturvallisia. [4.]

Teollisuusverkosta käytetään termiä ICS (kuva 1), jonka toimintaa voidaan ohjata monella eri tavalla riippuen sen käyttö tarkoituksesta.



Kuva 1. Industrial Control System toimii yleisenä terminä, joka kuvaa SCADA-, DCS-, PLC- ja RTU-järjestelmiä. [24.]

Karkea jako menee SCADA- ja DCS-järjestelmien välillä siten, että SCADA on suurempi kokonaisuus ja hajautettu laajemmalle alueelle, jossa voi olla pienempiä hallintakokonaisuuksia eli DCS-ympäristöjä.

DCS-ympäristö voi myös esiintyä itsenäisenä prosessin ohjausverkkona, joka ei välttämättä tarvitse suurempaa keskitettyä hallintaa ja sijaitsee yleensä maantieteellisesti pienellä alueella esimerkiksi tehdasrakennus.

Etäasemia (RTU) käytetään mittaustietojen keräämiseen järjestelmän ohjausyksikölle, joka suorittaa niiden perusteella järjestelmien säätötoimenpiteet ohjelmoitavien logiikkayksiköiden (PLC) toimesta.

Miten toteutetaan yhteydet teollisuuden ohjausjärjestelmien eri tasoille sekä suunnitellaan liityntä arkkitehtuurit konserni verkkoihin? Haasteina ovat usean toimittajan verkot ja liitynnät. Tietoturvauhkana ei nykyisin enää ole tavallinen kaupallisella virustorjuntaohjelmalla havaittava haittaohjelma vaan teknisesti kehittyneet ja monipuoliset verkkohyökkäystyökalut. Työkalujen ensimmäisenä tehtävänä on verkon tietyn osan haltuunotto ja seuraavana kehittyneimpien hyökkäyksellisten vakoilu- ja haittaohjelmien asentaminen. Vakoiluoperaatiot ovat ennakkoon ja tarkoin suunniteltu ja niillä on täsmällinen operatiivinen tehtävä talouteen ja teollisuuteen liittyvissä kohteissa.

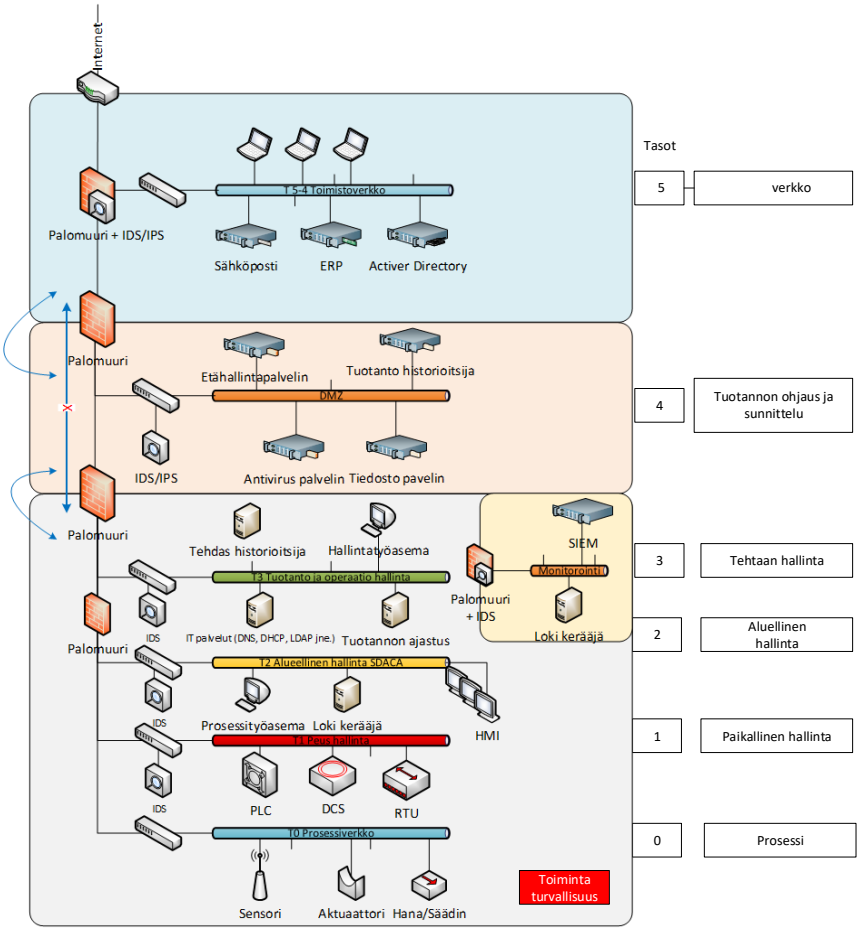
3 Teollisuuden ohjaus- ja automaatiojärjestelmien verkkoarkkitehtuuri

Puolustuksen syvyys, jota kutsutaan yleisesti myös kerrostetuksi puolustukseksi, on sotilaallinen käsite, jota on mukautettu tietotekniikkamaailmassa. Sitä käytetään nyt myös säännöllisesti ICS-maailmassa. Sotilaallisesti syvällisellä viittauksella tarkoitetaan joukkoa toisiaan tukevia puolustavia toimenpiteitä, joiden tarkoituksena on hidastaa vihollisen edistymistä pyrkimyksellä antaa puolustajalle enemmän aikaa vastata ja estää hyökkäys. Olemme kaikki kuulleet kliseen "jos hakkerit haluavat päästä sisään, he pääsevät sisään”. [9.]

Tämä pätee myös kyberturvallisuusmaailmaan, joissa puolustussyvyys hidastaa hyökkääjiä ja antaa puolustajalle enemmän aikaa vastata, kun puolustava kohde on vaarantunut. Ohjausjärjestelmien turvallisuuden paras puolustus on siten vankka verkkoarkkitehtuuri, joka eristää herkät ohjausjärjestelmät luontaisesti riskialttiilta yritysverkoilta. Ohjeistuksia ja standardeja erilaisiin tietoturvateknologioihin julkaisevat yhdysvaltalaiset National Institute of Standards and Technology (NIST) -organisaation Computer Security

sekä The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), joita käytetään pohjana teollisuudessa tietoturvallisten ratkaisujen suunnitellussa.

ISA99-valmistus- ja valvontakomitea on laatinut IACS-mallina tunnetun arkkitehtuurimallin, joka on rakennettu valvonnan hierarkian Purdue-malliin ISA99 / IEC-62443, jossa joukko vyöhykkeitä ja tasoja tunnistaa protokollasarjat, turvallisuusrajat ja tuotantolaitoksen toimintamalleja (kuva 2).



Kuva 2. Teollisuuden ohjaus- ja automaatiojärjestelmien verkkoarkkitehtuuri perustuu Yhdysvaltain turvallisuusviraston suosittelemaan malliin teollisuusverkkojen tietoturvasta. [9.]

Automaatioteollisuuden tueksi on kehitetty erityisiä ohjausprotokollia, jotka käyttävät tavanomaisia tietoliikenneprotokollia. Kolme suosituinta ohjausprotokollaa ovat EtherNet / IP, PROFINET ja Modbus / TCP. Kun koneet ja laitteet on liitetty alueiden vyöhykkeisiin, niiden turvallisuus on sen jälkeen ensiarvoisen tärkeää. Keskitetyn pääsynvalvonnan,

laitteen ja käyttäjän profiloinnin avulla on identiteettiin tunnistus suositeltavaa, ettei epäluotettavia tietokoneita tai laitteita käytetä teollisuusalueella verkoissa. [2.]

Turvallisuutta tulisi siis hallita kattavan ja syvällisen puolustusstrategian avulla, joka sisältää useita mekanismeja kuten käyttäjien todentamisen, salauksen, etäkäytön hallinnan, virustorjunnan ja käyttöjärjestelmäpäivitykset. Tärkein ero ICS-ympäristöissä verrattuna tietotekniikkaan on huomattavasti korkeammat käytettävyyden vaatimukset, jotka edellyttävät enemmän suunnittelua ja testausta, joilla varmistetaan prosessin onnistuminen.

4 Verkon segmentointi

Ensimmäinen askel suunnitella ICS/SCADA -verkon tietoturva-arkkitehtuuria on määritellä verkon segmentointi. Segmentoinnilla pyritään jakamaan verkkoa fyysisiin ja loogisiin alueisiin, joissa tavoitteena on saada häiriöalueet ja verkon käyttäjät rajattua pienenpiin alueisiin sekä niiden välille liikenteen valvontaa ja pääsypolitiikkoja. Tyypillinen ICS-verkko sisältää kuvassa 3 olevat vyöhykkeet, joilla on vastaavat luottamustasot.

Kuva 3. Tyypillisen ICS/SCADA-verkon sisältämät vyöhykkeiden luottamussuhteet. [9.]

Tällöin erilaisia tietoturvallisuusluokituksia on myös helpompi toteuttaa. Segmentointi liittyy entistä enemmän verkon tietoturvan parantamiseen ja on myös tehokas uhkien eh-

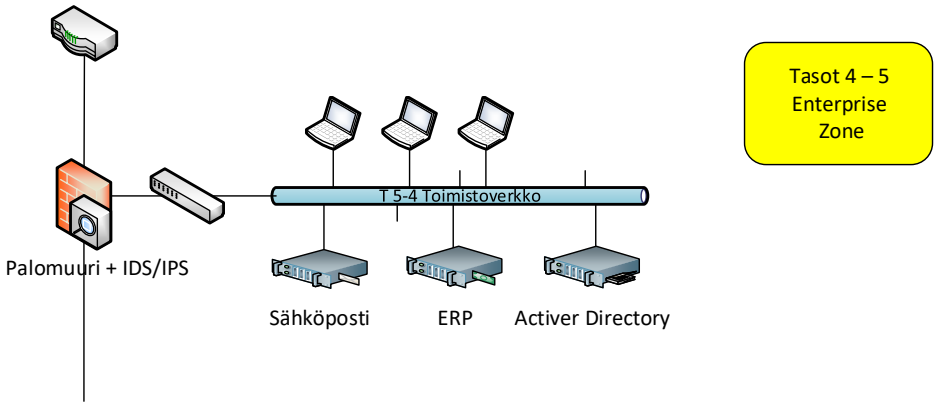
käisymenetelmä. Segmenttien välinen liikenne eristetään käyttämällä palomuureja, DMZ- alueita ja muita liikennesuodatusjärjestelmiä kuten yksisuuntaista suodatusta.

ICS-verkon puitteissa tuotantoverkkoa pidetään korkeimpana ja toimistoverkkoa matalimpana turvallisuustasovyöhykkeenä. Selkeästi määritelty segmentointi selkeyttää ja poistaa epäselvyyksiä uusien laitteiden tai järjestelmien sijoittamisessa eri turvallisuusvyöhykkeille. [3.]

4.1 Liiketoiminta- /yritystason vyöhyke

Käyttäjät ja järjestelmät vaativat usein Internet-yhteyksiä ja pääsyä yrityksen laajuisiin resursseihin kuten sähköpostiin ja Chatiin. Tyypillisesti tälle alueelle sijoitetaan toiminnanohjaus- ja tietokantajärjestelmiä, loppukäyttäjien työasemia ja etäkäyttöratkaisuja, kuten Citrix, VPN, SSH tai RDP.

Hallinta- ja toimistojärjestelmien suojauksilla pyritään sulkemaan ja rajaamaan tuotantoverkon turhat palvelut sekä laiteyhteydet, jolloin liikenne voidaan eristää esimerkiksi datadiodilla kulkemaan vain yhteen suuntaan. Palomuurin edessä oleva reititin tarjoaa pakettisuodatuksen peruspalvelut ja palomuuri pystyy käsittelemään monimutkaisempia ongelmia joko tilapäisen tarkastuksen tai välityspalvelimen avulla.

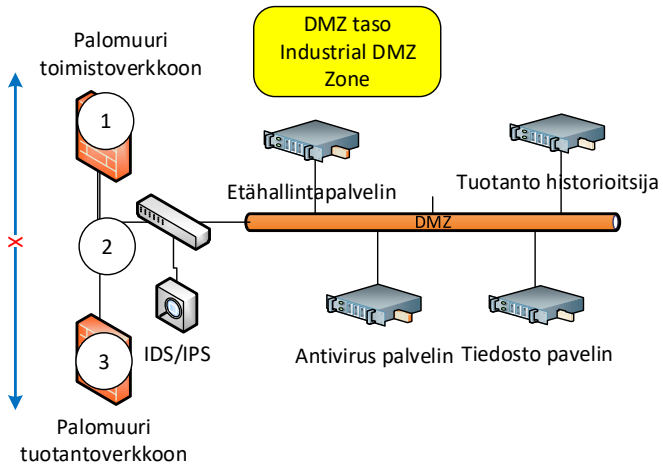


Kuva 4. Yritysverkon laitteita. [9.]

Tämäntyyppinen sijoittelu on erittäin suosittu internetiin suuntautuvissa palomuureissa, koska se mahdollistaa nopeamman reitittimen käsittelemään suurimman osan tulevista paketeista, erityisesti palveluestohyökkäyksissä, joka vähentää palomuurin kuormitusta. Se tarjoaa myös paremman puolustuksellisen syvyyssuojan, koska on olemassa kaksi erilaista laitetta, jotka hyökkääjän on ohitettava (kuva 4). [9.]

4.2 Demilitarisoitu vyöhyke

Demilitarisoitu vyöhyke (DMZ) on vyöhyke, joka sijaitsee teollisuus- ja yritysvyöhykkeiden välissä, jota käytetään turvallisten liikennevirtojen hallintaan vierekkäisillä alueilla. Tämä on myös se kohta, jossa palomuuri on tyypillisesti toteutettu liikennevirran ohjaamiseksi laitosverkkoon ja siitä ulos. Tyypillisesti DMZ-alueelta löytyy yksi tai useampi kriittinen komponentti kuten tuotannon historioitsija, joka sisältää arvokasta tietoa järjestelmien laadun- ja suorituskyvyn historiasta, langaton tukiasema tai etähallintapalvelin ja kolmansien osapuolten käyttöjärjestelmät (kuva 5). [9.]

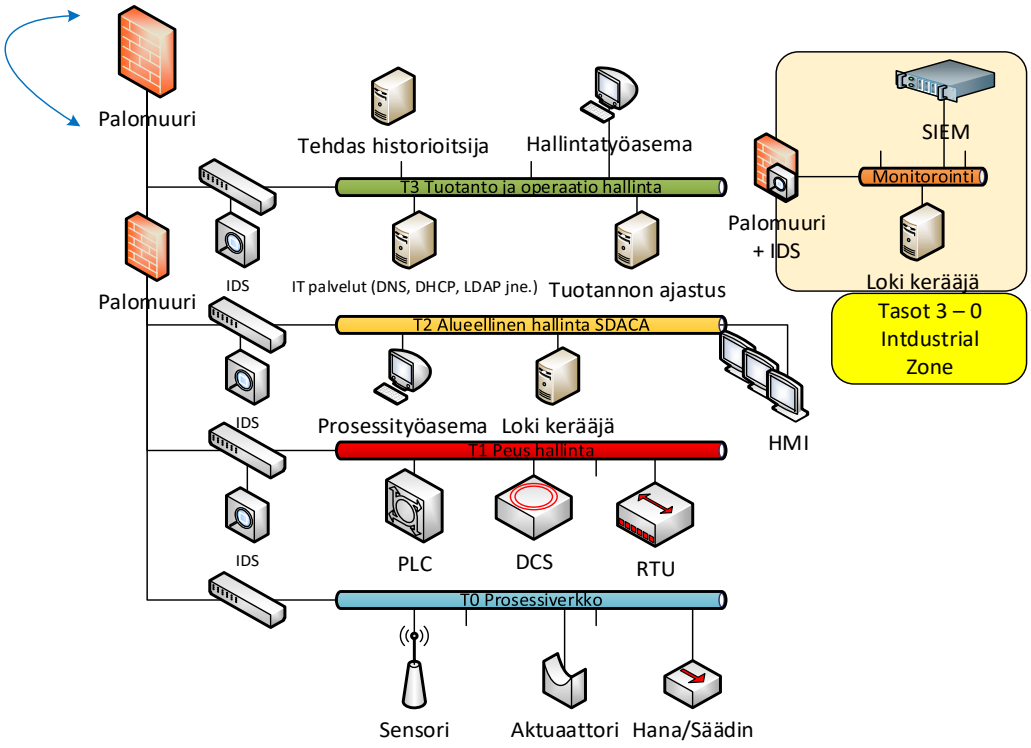


Kuva 5. DMZ-vyöhykkeen palvelimia. [9.]

Tuotanto- ja DMZ-verkon välinen liikenne sallitaan palomuurisäännöillä. Palomuurin lokitietoja seurataan jatkuvasti hallinnan kautta. DMZ-alueelle suositellaan sijoitettavaksi vain tallentavia tietoja olevia laitteita. DMZ-tietoturva on kriittinen laitosten toiminnan kannalta, koska se suojaa koneita haitalliselta liikenteeltä alemman luottamustason verkoista.

4.3 Tehdasverkkovyöhyke

Tehdasverkkoverkkoalueen eriyttäminen ja suojaaminen muista verkoista on tärkein osa verkon segmentointia, jonka vuoksi sillä on myös korkein suojaustaso. Tyypillisesti tehdasverkkoon sijoitetaan tuotantokriittiset järjestelmät kuten prosessinohjaus työasemia, palvelimia, tietokantoja ja automaatiota sekä instrumentointi- ja ohjauslaitteita (kuva 6). SFS-käsikirjassa 631-3 vyöhykkeestä käytetään myös nimeä turvajärjestelmävyöhyke. [19.]

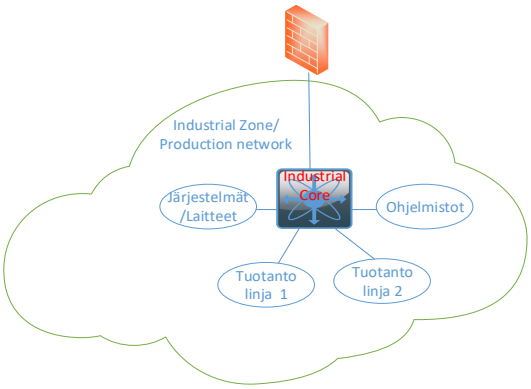


Kuva 6. Tehdasverkon laitteita. [9.]

4.4 Tehdasverkon erillisvyöhykkeet

Tietoturvan ja toiminnallisuuden kannalta tehdasverkon alueet tulisi jakaa edelleen erillisalueisiin, jolloin jokainen alue sisältää järjestelmät ja laitteet, joilla on yhteinen tehtävä

tai molemminpuolinen panos tuotantoprosessissa (kuva 7). Erillisalueilla tulisi olla selkeästi määritellyt rajat ja niiden välinen liikenne suodatettava käytön mukaisesti. Palvelut, protokollat ja sovellukset, jotka eivät ole olennaisia vyöhykkeen sisällä, tulisi poistaa.



Kuva 7. Tuotantoverkon erillisalueita, joilla on sama toiminnallisuus. [9.]

Teollisuusverkon protokollilla on lähtökohtaisesti erilaiset vaatimukset kuin muilla TCP/IP -perheeseen kuuluvilla protokollilla. Näistä keskeisimpiä ovat pienet viiveet tiedonsiirrossa, luotettavuus sekä luottamus siihen, että verkko, jossa toimitaan, on lähtökohtaisesti turvallinen.

Modus-TCP- tai DNP3-teollisuusverkon protokollat ovat pakollisia komponentteja prosessilaitteiden ohjaamiseen, mutta aina kun mahdollista, näiden protokollien pääsy alueen ulkopuolelle tulisi estää.

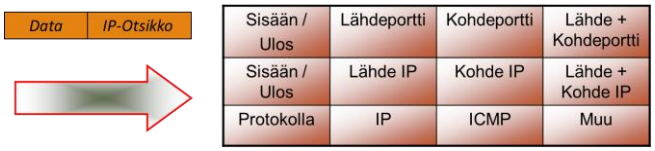
Jos tämä ei ole mahdollista, on toteutettava toimenpiteitä niiden suojaamiseksi hyökkäyksiltä tai väärinkäytöltä prosessinohjausverkon ulkopuolisista lähteistä, käyttämällä esimerkiksi palomuureja.

5 Palomuurit

Palomuurit ovat tärkeässä asemassa uhkien estämisessä, jotka voivat vaikuttaa turvallisuuteen ja luotettavuuteen sekä tuottavuuteen. Palomuureja käytetään yleisesti verkkojen suojaamiseen sekä eristämiseen eri segmenttien välillä. Mikäli yhteyksissä käytettään julkisia verkko-osoitteita, lähiverkot suositellaan suojattavaksi palomuurein, joissa verkostoautomaatioliikenteen VPN-tunnelointi on välttämätöntä. Julkisten verkkojen kautta välitettävä verkostoautomaatioliikenne on salattava ja salaus on suositeltavaa myös käytettäessä verkkoyhtiöiden omia tietoliikenneverkkoja. [1.]

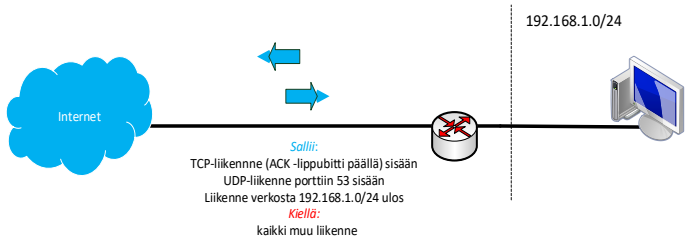
5.1 Pakettisuodatteiset palomuurit

Palomuurit luokitellaan neljään eri teknologiatyyppiin, joista ensimmäisenä pakettisuodatteiset palomuurit (Packet Filtering Firewall), jotka perustuvat pääsylistoihin ja päätöksiin pakettien sallimiseksi tai kieltämiseksi yksinkertaisilla suodatinperusteilla kuten lähde- ja kohde-IP-osoitteet viestissä (kuva 8).



Kuva 8. Pakettisuodatteinen palomuuri.

Kun suodatinperusteena on lähde- ja kohdeprotokollan numero, niin silloin tämän teknologian palomuureissa hyökkäykset eivät tyypillisesti ole estetty eikä havaittu (kuva 9).



Kuva 9. Esimerkki pakettisuodatteisen palomuurin liikenteestä.

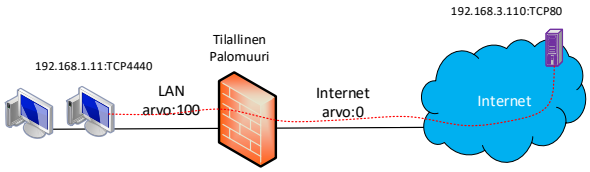
Pakettisuodatteisen palomuurin ensisijaisena etuna on alhaiset kustannukset ja vähäinen vaikutus verkon suorituskykyyn. Usein on hyödyllistä toteuttaa pakettisuodatus reitittimessä tilapäisen tarkastuspalomuurin edessä. Tällä on kaksi etua; se tarjoaa syvällisen puolustuksen ja vähentää tilallisen palomuurin työmäärää.

5.2 Tilalliset palomuurit

Tilalliset palomuurit (Stateful Firewall) ovat käytössä kaikkein yleisimpiä ja ne tunnetaan myös dynaamisina pakettisuodattimina, jotka valvovat yhteyksien tilaa ja tekevät määrityksiä siitä, minkä tyyppisiä tietopaketteja kuuluu tunnetulle aktiiviselle yhteydelle palomuurin läpi.

Yhteyksistä pidetään yllä erillistä tilataulua, jonka perusteella liikennettä suodatetaan. Algoritmi muodostaa automaattisesti tilataulun, joten suodatussääntöjen tekeminen on huomattavasti helpompaa kuin tilattomassa pakettisuodattimessa. Käytännössä jokainen paketti tarkastetaan ja verrataan sitä tilatietokantaan.

Olemassa oleviin yhteyksiin liittyvät paketit päästetään läpi ja tästä jälkeenpäin kaikki yhteyteen liittyvät paketit päästetään läpi niin kauan kuin yhteys on päällä. Kuvassa 10 on esitetty tilallisen palomuurin perustoimintaa.



Lähde	Lähdeportti	Kohde	Kohdeportti	Sallittu
192.168.1.11	TCP:4440	192.168.3.110	TCP:80	Kyllä (100-0)
192.168.3.110	TCP:80	192.168.1.11	TCP:4440	Kyllä, tilataulusta löytyy tieto

Kuva 10. Tilallinen palomuuri.

Useimmissa tapauksissa uusien yhteyksien on esiteltävä itsensä palomuurille, mitä useimmat asiantuntijat kutsuvat kädenpuristukseksi, ennen kuin ne sallitaan vakiintuneiden yhteyksien luetteloon.

Yhteys muodostuu lähiverkon puolelta, joka on määritelty palomuurissa luotettavaksi verkkoliittymäksi (kuvassa LAN, Arvo:100). Kun liikenne tulee palomuurille asti, algoritmi tekee tilatauluun tietueen ja palomuuri puhkaisee paluuliikenteelle reiän. Kun paluuliikenne saapuu muurille niin tutkitaan, onko tilataulussa vastaavaa tietuetta. Mikäli tietue löytyy, tilatauluun muodostetaan sallittu yhteys kahden eri laitteen välille. Palomuurissa oleva reikä suljetaan silloin kun yhteys katkeaa. Mikäli kyseessä on yhteydetön protokolla, reikä suljetaan halutun ajan kuluessa eli esimerkiksi UDP-pohjaisessa yhteydessä kahden minuutin kulutta viimeisen paketin saapumisesta.

Kuvassa 10 on reitittimen ulkoreunaan asennettu pakettisuodatin, jonka tarkoituksena on rajoittaa liikenne siten, että vain WWW-liikenne on sallittua (UDP 53 tarvitaan DNS-kyselyn läpimenemiseen) ja siten, että liikenne väärennetyllä IP- osoitteella on mahdotonta.

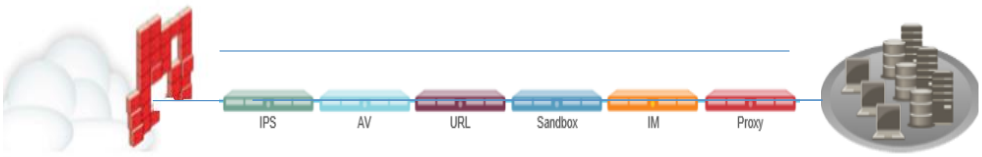
Täytyy muistaa, että kyseessä on karkean tason suodattaminen ja esimerkiksi TCP-portti 80 -liikennettä ei millään tavalla suodateta eli mikä tahansa sovellus menee läpi, kunhan se käyttää kommunikointiin TCP-protokollan porttia 80 ja on syntynyt sisäverkossa (ACK-bitti päällä). Tilalliset palomuurit ovat tehokkaampia uhkien havaitsemisessa mutta niillä on korkeammat kustannukset, suuremmat suorituskykyvaikutukset ja ne ovat monimutkaisempia konfiguroida ja käyttää.[1.]

5.3 Seuraavan sukupolven palomuuri

Seuraavan sukupolven palomuuri (Next-Generation Firewall) on kolmannen sukupolven palomuuriteknologiaa, joka yhdistää edellisten palomuurisukupolvien ominaisuudet sovellustunnistukseen perustuvaan suojaan (kuva 11).

Monitasoisen liikenteen suojauksessa palomuurin pitää osata monia toiminteita kuten haittaohjelmasuodatusta, sovellusten ja botnet-liikenteen tunnistusta, IDS/IPS- web-

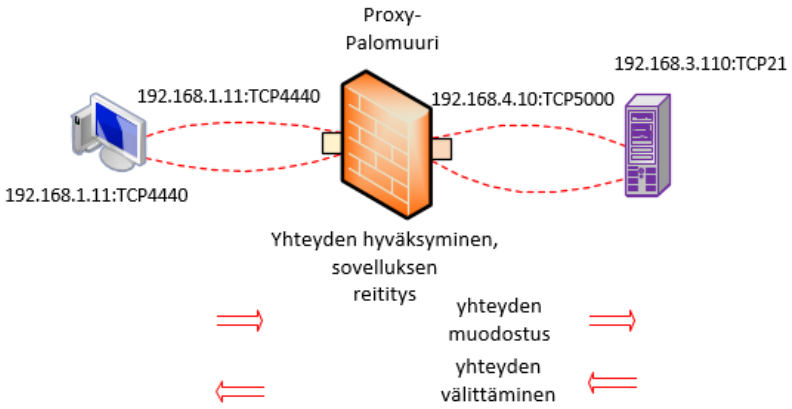
sivustojen suodatusta/estoa, SSL-liikenteen purkua sekä eritasoisia raportointeja. Käytännössä ulkoverkon reunalle viedään älykäs palomuuri, joka pystyy suojaamaan moni tasoisesti internetin ja sisäverkon välistä liikennettä. Monitasoista suojausta tarvitaan, koska haittaohjelmat voivat levitä myös turvalliseksi luokitellun luotettavan web-sivuston kautta, mikäli sisäverkosta vieraillaan tällaisella sivustolla. [14.]



Kuva 11. NGFW palomuurin ominaisuudet. [14.]

5.4 Sovelluskerroksen palomuurit

Sovelluskerroksen palomuureja (Proxy Firewall) kutsutaan myös Proxy-palvelimiksi, jotka lisäävät mahdollisuuden tutkia tiettyjä sovellusliikenteen palveluita (Web, FTP, telnet).



Kuva 12. Esimerkki Proxy-palomuuritopologiasta.

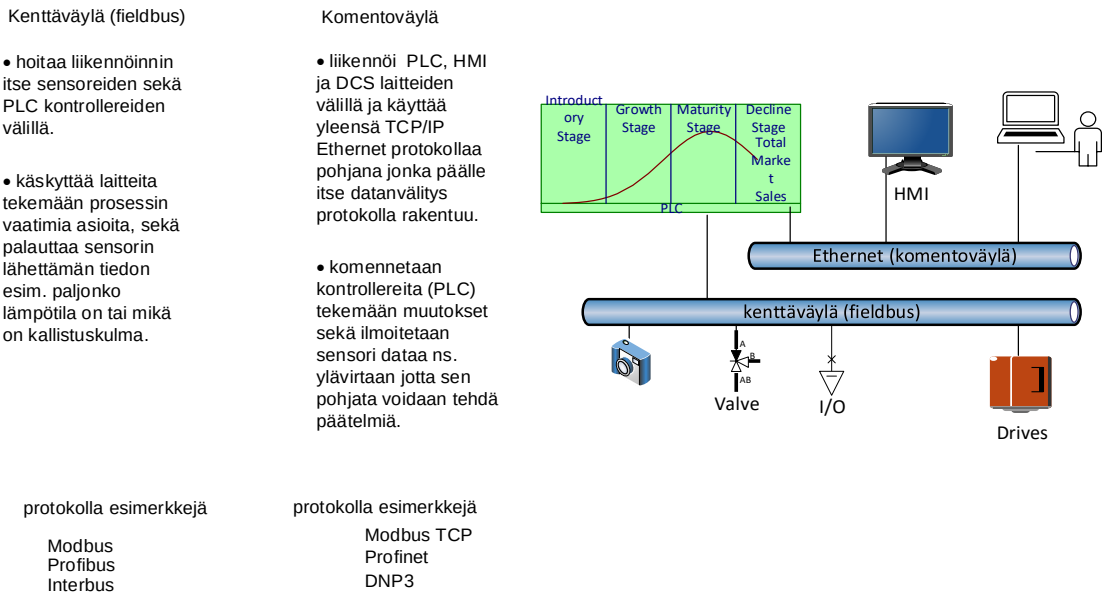
Kuvassa 12 on esimerkki Proxy-palomuurin toiminnasta, jossa käyttäjä ottaa ensin yhteyden Proxy-palomuuriin, joka puolestaan muodostaa jatkoyhteyden vastapään

koneeseen. Kyseessä on kaksi erillistä yhteyttä, asiakas -Proxy ja Proxy- kohde. Asiakaskonetta ei näy kohteen suuntaan vaan ainoastaan Proxy-palomuurin osoite, jolloin käyttäjän tiedot ovat turvassa. [14.]

Erilaisista palomuuriteknologiosta huolimatta palomuurit ovat turvallisuusstrategioiden perusrakenne. Palomuureja käytetään monimuotoisesti teollisuudessa sekä internetin laidalla, etä- ja konttoritoimistoissa, yrityksen ytimessä infrastruktuurin segmentoimiseksi mukaan lukien perinteiset ja virtualisoidut verkkoympäristöt. Nykyään kaupalliset palomuurit ovat yleensä hybridijärjestelmiä, joissa verkkotason perussuodatusta lisätään sovellustason yhdyskäytäväominaisuuksilla.

5.5 Teollisuusverkkojen protokollia

Kenttäväylätekniikan käyttö 1990-luvulla on ollut merkittävä innovaatio, joka on mahdollistanut automaatiojärjestelmien siirtymisen keskitetysti hajautettuihin järjestelmiin. Teollisuusverkkojen protokollat jakautuvat monessa tapauksessa kahteen osaan: kenttäväylään ja komentoväylään (kuva 13).



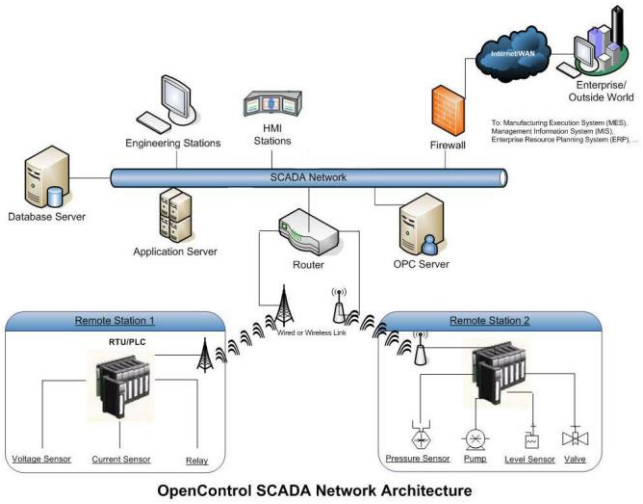
Kuva 13. Esimerkki kenttäväylän- ja komentoväylän eroista.

5.6 Komentoväylän yleisimpiä protokollia

Modbus

Modbus-protokollaa (kuva 14) käytetään yleisesti sähköteollisuuden SCADA- järjestelmissä, jolla yhdistetään valvontapääte (HMI) kentällä oleviin hallintapäätteisiin (RTU). Protokolla oli aluksi suunniteltu toimimaan pienillä nopeuksilla käyttäen kommunikointiin hitaita sarjaliikenne RS-232- ja RS-485-portteja. [2.]

Tästä syystä protokollaan itsessään ei sisälly mitään sisäänrakennettuja tietoturvaominaisuuksia tai käyttäjien tunnistusta. Protokollan yksi suurimmista heikkouksista on heikko tietoturva, koska liikenne on avointa ja salaamatonta. Protokollasta on olemassa sarjaportti Modbus- ja ethernet Modbus -TCP-versiot. Sarjaporttiversio tarvitsee monesti muuntimen väliin, jotta liikenne saadaan kulkemaan TCP/IP:n päällä. [3.]



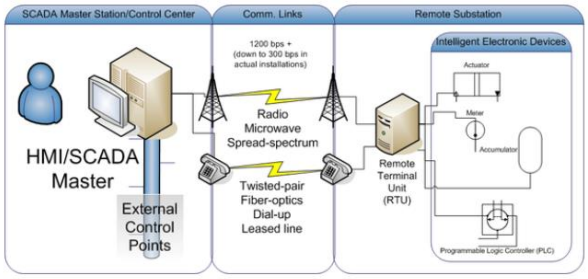
Kuva 14. Modbus-protokollan käyttöä. [3.]

Suojauksessa lähtökohtaisesti oletetaan, että tuotantoverkko on eristetty ja turvallinen eikä siellä ole haitallista liikennettä. Vaihtoehtoisesti liikenne voidaan salata käyttämällä TLS- liikennesalausta tai VPN-tunnelia päätelaitteiden välillä. Protokollan toimintavarmuus, luotettavuus ja yksinkertaisuus ovat suosineet teollisuudessa sen käyttöä vaikka heikkoudet tiedetään. [2.]

DNP3

DNP3-protokollaa (Distributed Network Protocol) käytetään pääasiassa sähkö- ja vesilaitoksissa ja se on kehitetty erityisesti tiedonsiirtoon eri tiedonkeruu- ja ohjauslaitteiden välille (HMI, RTU ja IED). Kuten muutkin teollisuusverkon protokollat DNP3 on haavoittuvainen salakuuntelulle sekä väärentämiselle.

IEC TC57 -komitea on saanut tehdä DNP3 :n tietoturvalliseksi, koska se on yksi yleisimmistä teollisuusverkoissa käytetyistä protokollista. [9.] DNP3-protokollalla toimivien päätelaitteidenvälille suositellaan IPSec/L2TP VPN- tunnelointia tai verkko eristetään ja rajataan tarkasti, minne liikennettä saa mennä. [7.]



Kuva 15. Esimerkki DNP3 protokollan käytöstä. [7.]

PROFINET

PROFINET on laajalti teollisuuden käytössä oleva Ethernet-protokolla, joka on PROFIBUS-käyttäjäorganisaation ja Siemensin kehittämä avoin standardi. PROFINET on reaaliaikainen Ethernet-protokolla, jota käytetään ohjainten ja laitteiden väliseen nopeaan tietojen vaihtamiseen, jossa aikavaateet voivat olla vain millisekunteja. Teknologia mahdollistaa myös langattoman tiedonsiirron. [10.]

Tietoturvan kannalta PROFINET välittää liikennettä yritys- ja teollisuusverkon välillä, jolloin liikenteen tulisi olla tiukasti valvottua. PROFINET :in käyttöönotto on suunniteltava erittäin huolellisesti, sillä se ei tue VLAN-segmentointia.

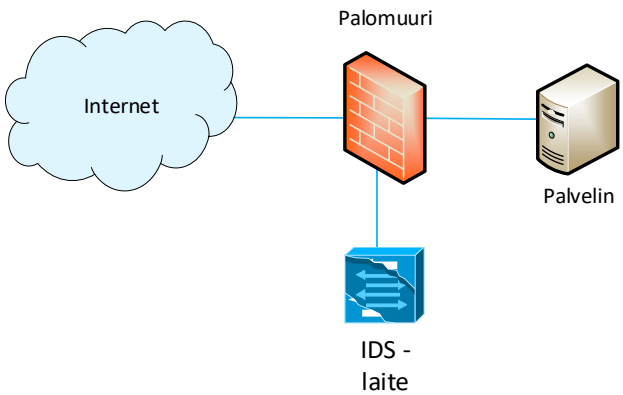
Suojauksissa palomuurit ja ICS-tietoiset tunkeutumisen estojärjestelmät olisi määritettävä siten, että ne estävät nimenomaan PROFINET-liikenteen määriteltyjen alueiden ja vyöhykkeiden ulkopuolelle. [10.]

6 Haavoittuvuuksien ja hyväksikäytön tunnistus- ja estojärjestelmät

6.1 Tunkeutumisen tunnistus- ja havaitsemisjärjestelmä

Tietoturvauhkien tunnistaminen jo aikaisessa vaiheessa on avain kykyyn puolustautua niitä vastaan ja varmistaa, ettei verkossa olevia tietojasi vaaranneta. Tietoturvavalvonnan tehtävänä on jatkuvasti seurata, arvioida ja vastata nopeasti tunkeutumisen havainnointitapahtumiin.

Tunnettujen verkkohyökkäysten havaitsemiseksi käytetään tunkeutumisen tunnistus- ja havaitsemisjärjestelmiä (IDS) (kuva 16), jotka on alun perin rakennettu haavoittuvuuksien havaitsemiseksi perustuu oletukseen, että järjestelmän haavoittuvuuksien hyväksikäyttö edellyttää poikkeavaa toimintaa kohdesovelluksia tai tietokoneita vastaan. IDS-laitteet seuraavat verkkoliikennettä ja käyttävät erilaisia havaitsemismenetelmiä, kuten liikenteen osia, vertaamalla tunnettujen hyökkäysten allekirjoituksiin. IDS on kuunteleva laite, joka valvoo liikennettä ja raportoi tuloksistaan järjestelmänvalvojalle, mutta se ei voi automaattisesti ryhtyä toimiin estääkseen havaittua poikkeamaa.



Kuva 16. IDS verkon reunalla. [15.]

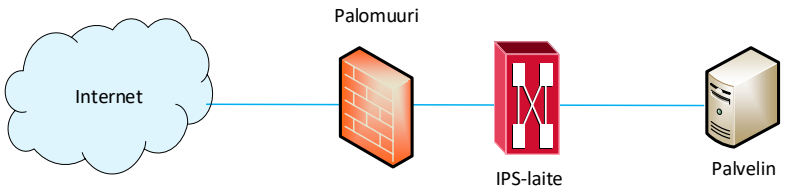
IDS perustuu verkkoliikenteen passiiviseen seurantaan ja poikkeamia käytetään hälytysten laukaisijoina. Yksinkertaisia sääntöjä voidaan kirjoittaa seuraamaan IP-lähteitä, kohteita, protokollia ja pakettien pituuksia. [15.]

6.2 Tunkeutumisen estojärjestelmä

Tunkeutumisen estojärjestelmä (IPS) (kuva 17) on osa verkon tietoturvatorjuntatekniikkaa, joka tutkii verkkoliikennettä haavoittuvuuksien hyödyntämiseksi ja estämiseksi. Tunkeutumisen estojärjestelmät analysoivat paketteja mutta voivat myös estää paketin toimittamisen sen perusteella, millaisia hyökkäyksiä se havaitsee.

IPS-laite sijaitsee usein palomuurin takana tai on integroituna suoraan palomuuriin, joka tarjoaa täydentävän analyysikerroksen estämään negatiivisesti vaarallisen sisällön siirtymistä verkkoon Toisin kuin edeltäjänsä, tunkeutumisen havaitsemisjärjestelmä on passiivinen järjestelmä, joka skannaa liikennettä ja raportoi uhkista.

Laitteet ovat olennainen osa puolustuksen syvällistä strategiaa ja tarjoavat automaattisen tavan valvoa ja vastata odottamattomiin uhkiin mutta kuitenkaan ne eivät voi tehdä kaikkea.

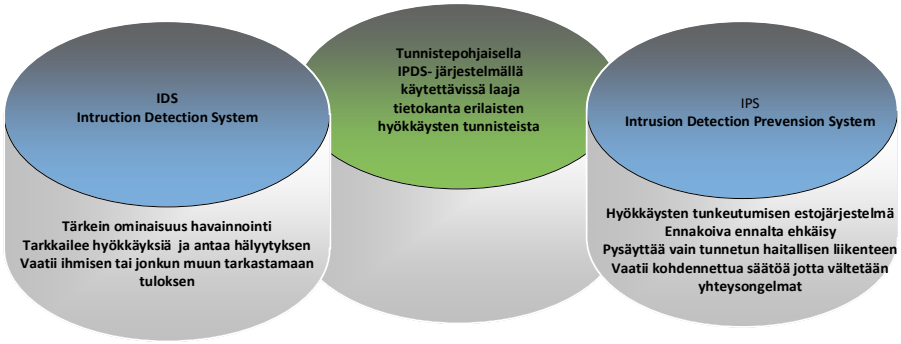


Kuva 17. IPS palomuurin takana. [16.]

IPS-ratkaisut ovat yhteensopivia palomuurien tai ICS/SCADA -laitteiden kanssa ja voivat toimia estämällä liikennettä, joka ei täytä määriteltyjä sääntöjä. Haitallisen verkkoliikenteen havainnointiin ja estämiseen on useita menetelmiä, joista allekirjoitukseen perustuva tunnistus ja tilastollinen poikkeavuuden havaitseminen ovat kaksi määräävää mekanismia.

Tunnisteisiin perustuva tekniikka on yksinkertaisin havainnointitapa, joka perustuu ennalta tunnettujen haavoittuvuuksien etsimiseen. Tekniikassa käytetään lähinnä laitevalmistajien laajoja hyökkäystietokantoja, joihin verkossa tapahtuvaa liikennettä verrataan mutta haasteena on ennalta tuntemattomien haavoittuvuuksien havaitseminen, joita ei vielä tunnisteta.

Tilastolliseen poikkeaman havaitsemiseen otetaan näytteitä verkkoliikenteestä sattumanvaraisesti ja verrataan niitä normaaliksi määriteltyyn verkkoliikenteeseen havaittuihin tapahtumiin etsien merkittäviä poikkeamia. Kun verkon liikennetoiminnan näyte on perusviestinnän parametrien ulkopuolella, IPS ryhtyy toimiin tilanteen käsittelemiseksi. IPS rakennettiin ja julkaistiin aluksi erillisenä laitteena 2000-luvun puolivälissä mutta se on tullut integroituna ratkaisuna nykyisiin palomuuriratkaisuihin yritystasolla. IPS- ja IDS-laitteet toimivat osana tietoturvaratkaisua (kuva 18).



Kuva 18. IDS- ja IPS-järjestelmät toimivat osana tietoturvaratkaisuja. [15;16.]

6.3 Haittaohjelmat ja suojaus

Teollisuusympäristöissä tietotekniikan päivittäminen ja muutosten tekeminen on tehty tarkoituksella yhä vaikeammaksi. Usein muutosten tekeminen onnistuu vain tuotantokatkojen yhteydessä. Virustentorjuntatyökalut toimivat tehokkaasti, kun ne asennetaan ja ylläpidetään kunnolla ja vaikka virustentorjuntatyökalut ovat yleinen käytäntö tietotekniikkajärjestelmissä, niiden käyttö ICS/SCADA:n kanssa saattaa edellyttää erityiskäytäntöjä, kuten yhteensopivuustarkistukset, muutoksenhallinnan ongelmat ja tehokkuusvaikutukset tuotantoon.

Suuret ICS/SCADA -järjestelmätoimittajat suosittelevat, jopa tukevat, tiettyjen virustentorjuntatyökalujen käyttöä ja joissakin tapauksissa valvontajärjestelmätoimittajat ovat saattaneet tehdä testaukseen oman työkalunsa tuotelinjansa tueksi ja siihen liittyvät asennukset. Usein pyritään lisäksi kehittämään yleisohjeita ja testausmenetelmiä, jossa keskitytään valvontaohjelmistojen suorituskykyyn, jotta ne täyttäisivät aukot, joissa ICS/SCADA- ja virustorjunta-asiantuntijan ohjeita ei ole saatavilla. [1;22.]

Valitettavasti viruksentorjunta suojausta ei ole aina mahdollista asentaa prosessinohjausjärjestelmiin, koska vanhojen järjestelmien ongelmana on käyttöjärjestelmien ikä. Teollisuusverkon tehokkaassa suojauksessa laitteet toimivat Internetissä erotetussa IP-verkossa, jolloin jokaisessa laitteessa on palomuuri. Vanhat suojaamattomat protokollat voidaan suojata kuljettamalla ne salatun tiedonsiirtokanavan yli (VPN), jolloin etälaite avaa VPN-putken palvelimelle ja valvomo saa tätä kautta turvallisen yhteyden kenttälaitteeseen. Miehittämättömät laitokset, joilla on suorat yhteydet järjestelmien ohjausyksiköihin, voidaan luokitella suuren riskin omaaviksi.

6.4 Prosessinohjausjärjestelmien tietoturvatestaus

Järjestelmän haavoittuvuuksien löytymiseen voidaan käyttää kahta menetelmää, joista ensimmäisenä vertailumenetelmä, jossa tuotannossa olevat ohjelmistot, laiteohjelmistot sekä käyttöjärjestelmän versiot voidaan viedä online-haavoittuvuustietokantoihin, joissa niitä verrataan aiemmin tunnistettuihin haavoittuvuuksiin. Vertailumenetelmässä tietojen kerääminen on melko työlästä mutta se ei aiheuta ICS/SCADA-verkkoon tuotannollisia riskejä tai vaaraa, koska tietoja ei lähetetä verkosta ulos eikä tietojen keräämiseen tarvita erikseen asenettavia ohjelmistoja.

Prosessinohjausjärjestelmien haavoittuvuustestausta on suunniteltava äärimmäisen varovasti, sillä toisessa menetelmässä eli haavoittuvuuksien skannaukseen asennettavat ohjelmistot voivat vaikuttaa haitallisesti moniin toimintoihin ja ohjauslaitteisiin.

Skannausmenetelmät ovat kyllä nopeampia ja paljon vähemmän työvoimavaltaisempia mutta tuovat myös paljon liikennettä ICS/SCADA-verkkoon ja siten voivat skannauksen tyypistä riippuen vaikuttaa negatiivisesti ICS-laitteisiin.

Koska ICS-laitteisiin voi kohdistua haitallisia vaikutuksia, on suositeltavaa, että skannaukset tehtäisiin testausta varten rakennetuissa erillisissä suljetuissa testaus- ympäristöissä.

Nykyään järjestelmät ja tietyt verkkolaitteet, kuten ohjaimet ja HMI:t, voidaan virtualisoida ja luoda tuotantoverkosta virtuaalinen testausympäristö ja siten skannata haavoittuvuuksia turvallisesti.

7 Langaton IIoT-ratkaisu teollisuusympäristöön

Nopeasti kehittyvät IIoT-ratkaisut tuovat uutta tehokkuutta teollisuuteen sekä uusia mahdollisuuksia tuotantolaitosten hallintaan, prosessien tehostamiseen ja laitteiden ennakoivaan ylläpitoon. Teollisuusmaailma yhdistää ja integroi nykyään teolliset ohjausjärjestelmät yritysjärjestelmiin, jossa on mukana liiketoimintaprosessit ja analytiikka. Kyseessä on liiketoimintaprosessien ja -mallien uudistaminen reaaliaikaisiksi ja yhä vahvemmin dataan pohjautuviksi.

IIoT-järjestelmät mahdollistavat siten merkittävää edistystä päätöksentekoon, toimintaan sekä yhteistyön optimointiin. IIoT:n tehokkuus perustuu isoon määrään kevyttä dataa, jota voidaan analysoida lähes reaaliaikaisesti erilaisten sensoreiden, kameroiden ja analytiikan avulla. Saatu tilannetieto voidaan valjastaa tuotekehityksen, palvelun ja liiketoiminnan tueksi.

Erilaiset tietolähteet on mahdollista yhdistää yhdeksi tilannekuvanäkymäksi, joka tukee laitteiden etähallintaa ja auttaa optimoimaan palveluiden ja prosessien toimintaa uudella tavalla. Yhden näkymän avulla on mahdollista ohjata jopa kokonaista tuotantolaitosta. Nykyaikaisten IIoT-ratkaisujen avulla teollisuuden toimijoiden on mahdollista saavuttaa merkittäviä säästöjä vuositasolla tuotantolaitoksen eri osa-alueilla.

Säästöt voivat muodostua esimerkiksi prosessien, varastonhallinnan ja kokonaistuotannon tehostumisesta sekä huoltotoiminnan oikeasta aikaistumisesta. [18.] Langattoman verkon nykyinen suunnittelu on osoittautunut tärkeäksi teollisen internetin hyötyjen toteuttamisessa. Nykyään laitokset käyttävät yhä enemmän langattomia verkkoja kriittisille

teollisuusautomaatio- ja ohjausjärjestelmille, jotka edellyttävät luotettavaa tiedonsiirtoa vähäisin viivein.

Langattomat lähiverkot poikkeavat merkittävästi perinteisistä kiinteistä lähiverkkoista käyttäessään jaettuja radiotaajuuksia ja ovat siten herkkiä häiriöihin ja kattavuuteen. Langattoman verkon käyttöönotto edellyttää harkittua suunnittelua sekä kaistanleveyden, läpäisykyvyn, luotettavuuden ja turvallisuuden osalta.

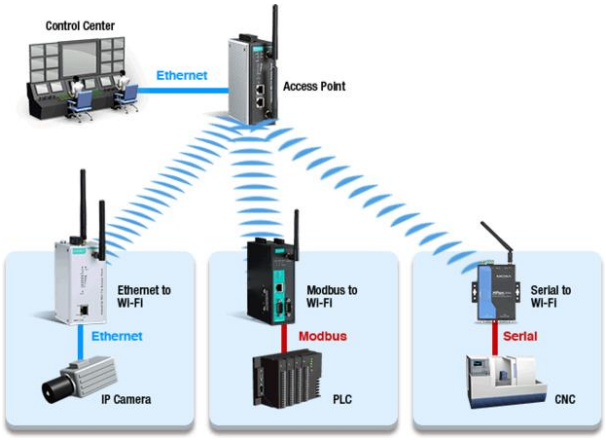
Teollisten tuotantolaitosten järjestelmävaatimukset painottuvat kestävyyteen, joustavuuteen ja saatavuuteen. Tietoverkkoturvallisuus on kuitenkin ratkaiseva tekijä digitaalisille ratkaisuille mutta sen toteuttaminen teollisuudessa vaatii erityistä huomiota. Tämä johtuu siitä, että teollisuuden tuotantojärjestelmissä ja -laitteissa on paljon pidemmät elinkaaret, jotka perustuvat usein vanhempaan teknologiaan, prosessoreihin ja käyttöjärjestelmiin, joita ei ole suunniteltu liitettäväksi internetin kautta ulkopuolisiin verkkoihin. Laiteet sijaisivat yleensä lähiverkoissa, jotka ovat suojattu ja eristetty ulkoisesta maailmasta palomuureilla.

IIoT-ratkaisujen on myös toimittava samassa ympäristössä, joissa on huomattava määrä vanhoja toimintatekniikoita. Niiden olisi myös oltava samanaikaisesti tietolähteinä erilaisten toimivien laitteiden kanssa kuten SCADA, PLC, DCS, joissa voi olla erilaiset protokollat ja tietokokonaisuudet. IIoT-ratkaisuissa käytetään yleensä erilaisia turvallisempia sekä joustavampia järjestelmäarkkitehtuureja, jotka koostuvat erikoistuneista piirisarjoista, salauksesta ja todentamisesta sekä uhkien havaitsemisesta. Tietoturvassa on siten olennaista, että se suunnitellaan alusta lähtien huolellisesti huomioiden turvallisuus, luotettavuus, kestävyys sekä kustannustehokkuus. [4.] Teollisuuden tuleva digitalisointi vaatii tehokkaita teollisia tiedonsiirtoverkkoja, joissa suurimpana haasteena toteutuksissa on tietoturvallinen ja helppo kommunikointi. Siirrettävän tiedon määrä kasvaa moninkertaiseksi seuraavan kymmenen vuoden kuluessa. Internet-verkkoon arvioidaan kytkeytyvän miljardeja laitteita, jotka yhdistyvät yhdeksi älykkääksi kokonaisuudeksi. Laitteiden tietoturvatasot voivat ovat vaihtelevia ja näin ollen tietoturvan rakentaminen IT- ja teollisuusjärjestelmiin tulee erittäin haastavaksi. [20.]

Teollisuuden langaton lähiverkkoarkkitehtuuri koostuu tukiasemista (Access Point) ja verkon liittyjistä (client), joita voidaan hallinnoida keskitetysti. Tukiasema voi toimia reitit-

timenä, jolloin se hoitaa langattoman verkon reitityksen sekä hallinnoinnin. Liittyjät muodostavat yhteyden langallisen laitteen ja langattoman verkon välille, jonne luodaan sovelluksen vaatima radiokenttä.

Teollisuuden automaatiomarkkinat ovat vuosien ajan toimineet ”tuo oma laite verkkoon” -periaatteella. Verkkoon kytkettyjen laitteiden hallinnan varmistamiseksi käytetään tunnistamis- ja pääsynhallintamenetelmiä. Kytkettäessä laite verkkoon, sitä voidaan seurata, hallita tai paikantaa etänä, joka mahdollistaa monien prosessien automatisoinnin ja toiminnan tehostamisen. Teollisilla sovelluksilla on usein erityisiä turvallisuusvaatimuksia ja siksi on tärkeää ymmärtää sovellusten ominaispiirteet ja arvioida niiden haavoittuvuudet ja riskit. Teollisuusympäristöt asettavat monet omat vaatimuksensa käytettäville ratkaisuille. [23.] Kuvassa 19 on esimerkkinä Siemensin teollisuuden langattoman verkon periaatteellinen toteutus.



Kuva 19. Siemensin esimerkki langattoman verkon toteutuksesta. [23.]

8 Teolliseen langattomaan internetiin liittyvät haasteet

Päätös langattoman teknologian käyttöönotosta sähkö- tai teollisuuslaitoksessa on strateginen valinta, jonka ansiosta infrastruktuuri tarjoaa merkittäviä etuja kuten alhaisemmat johdotuskustannukset. Oikea päätös voi parantaa turvallisuutta ja tehostaa laitoksen toimintaa. Kuten useimmissa kehittyvissä teknologioissa nykypäivän markkinat tarjoavat

langattomia ratkaisuja, jotka ratkaisevat teollisen liiketoiminnan tarpeet, mutta eivät välttämättä täytä tulevaisuuden vaatimuksia.

Langaton verkko on monimutkainen ja mahdollistava teknologia, mutta edellyttää tarkkaa harkintaa ennen laajaa käyttöönottoa.

Jotta kehitystoiminta pysyisi ajan tasalla ja auttaisi käyttäjiä löytämään parhaan ratkaisun sovelluksiinsa, ovat monet organisaatiot laatineet suosituksia ja standardeja sekä avoimia ratkaisuja, joita eri toimijat voivat hyödyntää omiin langattomiin ratkaisuihinsa.

Järjestelmien toimivuuden kannalta tulisi huomioida koko prosessin toiminta alusta loppuun. Teollisuudessa käytetään moninaisia tekniikoita sekä protokollia, jotka eivät ole yhteensopivia keskenään, jonka vuoksi suunnittelussa tulisi huomioida vanhojen laitteistojen ja uuden teknologian yhteensovittamisen integraatiovaikeudet.

Infrastruktuurivaatimukset edellyttävät luotettavia ja varmennettuja verkkoyhteyksiä.

9 Verkkoturvallisuuden tapahtumien valvonta

Kaikkia tietoturvauhkia ei enää pystytä havaitsemaan tai torjumaan pelkästään palomuureilla, IDS- tai IPS-laitteilla. Kehittyneiden haittaohjelmien taustalla ovat ammattimaiset tahot, jotka pyrkivät toimimaan huomaamattomasti pitkän ajan kuluessa.

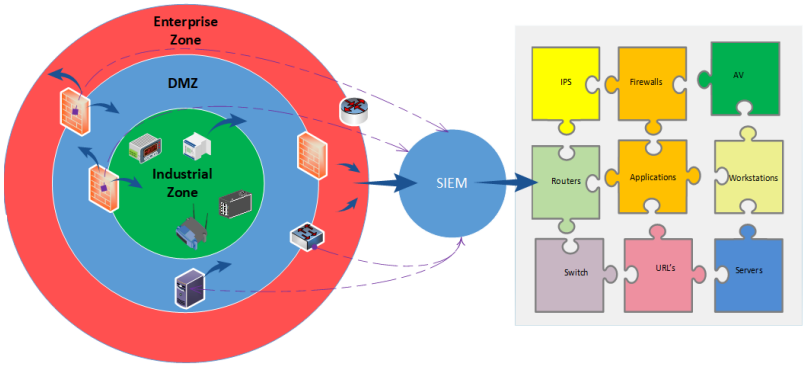
Ulkoisia hyökkäyksiäkin vaikeammin torjuttavia uhkia saattavat olla organisaation sisäiset väärinkäytökset tai tietovarkaudet, jolloin tietoturvainformaation ja tapahtumien hallinnan SIEM-tuotteet ovat keskeinen osa tietoverkkohyökkäysten tunnistamista ja niihin puuttumista.

Tapahtumalokit ovat arvokas resurssi vianmääritykseen ja vastauskäytäntöihin. Koska tietoturvallisuus koostuu monista kerroksista, olisi tärkeää saada yksittäinen näkymä kaikista tietoturvatapahtumista yhdestä paikkaa, johon SIEM-järjestelmät tuovat näkyvyyttä.

Vaikka SIEM-järjestelmän käyttöönotto ei ole helppoa, niin se on yksi tärkeimmistä indikaattoreista, että organisaatiolla on selkeästi määritelty tietoturvapolitiikka. SIEM:n ylivoimaiset lokien hallintaominaisuudet ovat tehneet tästä keskuksen, jossa se auttaa havaitsemaan hyökkäykset ja reagoimaan niihin nopeasti.

Useimmat tietoturvaohjelmat käsittelevät pienempiä uhkia mutta niiltä puuttuu isompi kuva tietoverkkohyökkäyksistä. Yksinään tunkeutumisen havainnointijärjestelmä voi harvoin tehdä enemmän kuin seurata paketteja ja IP-osoitteita. Samoin palvelulokit näyttävät vain käyttäjän istuntoja ja kokoonpanon muutoksia. [24.]

SIEM-teknologiat tukevat tapahtumaprosessia mutta ne voivat myös tukea ICS/SCDA -toimintoja, jolloin niiden tiedot oikein konfiguroituna ja analysoituna voivat auttaa laitteiden vika- ja kapasiteettitilanteiden ennustamiseen sekä tietoturvainformaation saamiseen. Vähintään palomuuri-, IDS/IPS-, reititin/kytkin- sekä käyttöjärjestelmän- ja sovellusten lokitiedot tulisi tallentaa (kuva 20). Lokitietoja siirretään useista järjestelmistä yhdeksi näkymäksi automaattisesti ja siten minimoidaan manuaalisten lokikatselmusten vaatimaa aikaa ja vaivaa.



Kuva 20. SIEM järjestelmä kerää lokeja eri lähteistä. [17.]

Skannaustulokset voidaan myös integroida SIEM -järjestelmiin, joiden avulla saadaan tuotettua hälytyksiä tunnistetuista liikennemalleista. SIEM: n analyysimoottori nopeuttaa tietojen käsittelyä ja muotoilua ja helpottaa toiminnallisten, operatiivisten ja turvallisuustietojen tarkastelua. Skannaustulokset voidaan myös integroida SIEM-järjestelmiin,

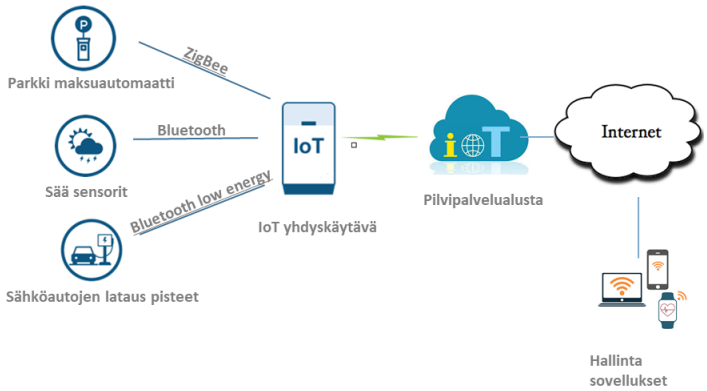
joista saadaan tuotettua hälytyksiä tunnistetuista liikennemalleista, joista sitten voidaan valita tiettyjä tapahtumia vaatimusten mukaiseen raportointiin, syyvaurioiden analysointiin sekä tapahtumien havaitsemiseen.

Käyttöönotosta voi aiheutua huomattavia kustannuksia, joten tämän vuoksi pienemmät organisaatiot ovat olleet vähemmän innostuneita järjestelmän käytöstä, jonka vuoksi useat pienet yritykset ulkoistavat lokien hallinnan palveluntarjoajille.

Nykyään hyödynnetään kehittyneempien SIEM-järjestelmien analytiikkaominaisuuksia kun etsitään tavallisuudesta poikkeavaa liikennettä tai käyttäjän toimia suuresta tietomäärästä.

10 Verkkoturvallisuuden hallinta

Tietoturva vaatii käytännössä kattavasti suojattua erillisverkkoratkaisua ja tarkasti määriteltyjä turvallisuuskäytäntöjä sekä korkealuokkaista tietoliikenneverkkojen rakenteellista turvallisuutta. Nykyään langattomat verkkotekniikat, kuten Bluetooth, WLAN- ja Zigbee (kuva 21), joita käytetään tiedonkeruussa ja -siirrossa sekä etähallinnoissa, ovat yleistyneet, jonka vuoksi internetin tietoturva asettaa uusia haasteita järjestelmien toteutuksiin. [20.]



Kuva 21. IIoT järjestelmän malli

Teollisuuden IIoT-järjestelmissä tietoa siirretään ja tallennetaan pilvipalveluihin, joissa

tietoturvaan ei useinkaan itse pystytä vaikuttamaan vaan tämä on toteutettu palvelun tarjoajan toimesta. Jotta tieto voidaan siirtää turvallisesti pilveen, pitää IoT-laitteen ja pilvipalvelun tunnistaa toisensa luotettavasti. Tämä mekanismi voi olla valmiiksi rakennettuna esimerkiksi Azure IoT Hubiin. [22.]

10.1 Etäkäytön tietoturva

Kriittisten järjestelmien etäkäyttö tarjoaa mahdollisuuden parantaa liiketoimintaa vähentämällä toimintakustannuksia sekä lisäämällä tuottavuutta. Etäyhteydet helpottavat pääsyä reaaliaikaisiin tietoihin, mutta miten verkkoturvallisuuden käytäntöjä sovelletaan liiketoiminnan tukemiin vaatimuksiin? Huomio tulisi kiinnittää ympäristöjen erojen tarkasteluun ja siihen, miten ne rajoittavat käytettävissä olevien teknologioiden valintoja.

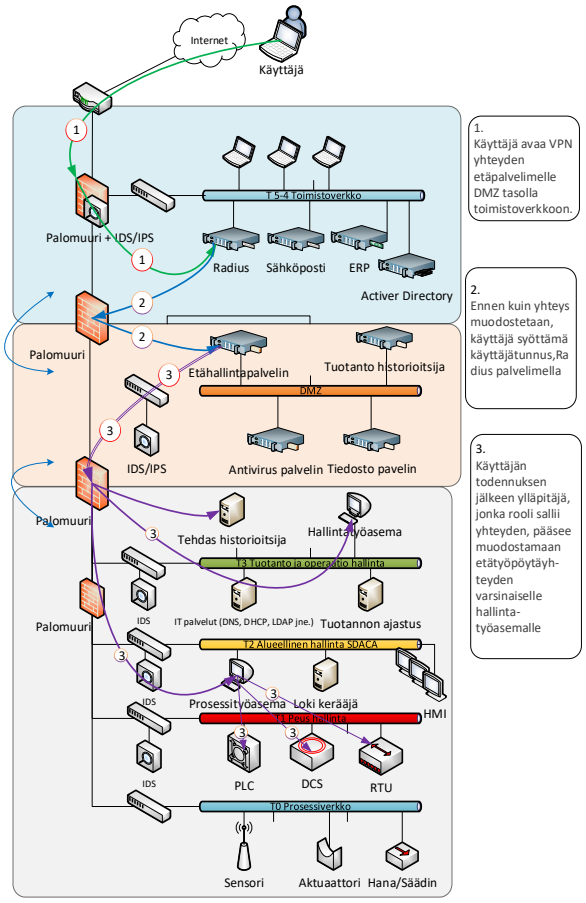
Etäyhteys ICS/SCADA -järjestelmiin avaa kuitenkin huomattavan riskin, vaikka monet kolmansien osapuolten palveluntarjoajat ja järjestelmien valmistajat ovat asettaneet etäkäytön perusedellytykseksi päivittäiseen toimintaan ja tukeen. [5;6.]

Etäkäytön tarve kasvaa edelleen sekä yrityksen työntekijöille että kolmannen osapuolen tuelle mutta valvontajärjestelmien etäkäyttöön liittyy yhä merkittäviä haasteita, joista tärkeimpinä ovat toimivat ja turvalliset yhteydet. Nykyaikaisissa ICS/SCADA -ympäristöissä on useita samankaltaisia tekniikoita kuin tieto- ja viestintätekniikassa ja siten myös samankaltaisia ratkaisuja. Pääsynvalvonta, verkkojen ja järjestelmien sekä haittaohjelmien aktiivinen seuranta ovat perusta Purdue-mallin mukaiseen puolustuksen. Yksittäistä etäkäyttöratkaisua, joka soveltuisi kaikkiin mahdollisiin arkkitehtuureihin, ei ole eikä mikään yksittäinen etäkäyttöratkaisu voi tarjota riittävää suojausta ilman puolustuksen perusteellista lähestymistapaa. Turvallisten etäkäyttöratkaisujen käyttöönotto ja ylläpito voidaan kuitenkin toteuttaa varovaisesti ja laadukkaiden analyysien perusteella tiukkojen vaatimusten luomisessa ja toteuttamisessa. [1.]

10.2 VPN-käyttö

VPN-yhteydet edustavat tunnettua teknologiaa, jota käytettään yleisesti ICS/SCADA -teollisuudessa. VPN perustuu tekniikkaan, jossa julkisten verkkojen kautta liikkuvaa informaatiota suojataan käyttäen IPsec-tunnelointia ja vahvoja salausavaimia yhdessä toistaiseksi murtamattomien salausmenetelmien kanssa. [19.]

VPN-pohjaiset ratkaisut ovat edelleen turvallinen lähestymistapa ICS/SCADA -verkkojen etäkäyttöön, vaikka se voi olla kallista asentaa ja ylläpitää. Kuvassa 22 on esimerkki VPN-yhteydenmuodistamisesta. [1;5]



Kuva 22. Esimerkki VPN-liikennöinnistä teollisuusverkossa. [1.]

Tyypillinen liitettävyys tapahtuu joko IPsec / SSL VPN -laitteen kautta mutta toisaalta monet yritykset käyttävät myös hybridiratkaisuja. Laitevalmistajat tarjoavat erilaisia

tapoja identiteetin tunnistuksen toteuttamiseen mutta yleensä tunnistus tapahtuu käyttäjähallintapalvelun kanssa, jossa käyttäjätiedot haetaan toimialueen Active Directorystä tai RADIUS, TACACS -palvelimelta. Kun käyttäjä on todennettu, tarkistetaan sovellus, lähde -IP ja -portti, kohde -IP ja -portti. Mikäli jokin näistä epäonnistuu, liikenne estetään. Jotta VPN-yhteydet toimisivat, kohdeorganisaation on pitänyt avata palomuurilta IPSec-portit (IP 50, UDP 500) ulkomaailmaan. Tämän jälkeen palomuureilla tehdään säännöt, mihin saadaan liikennöidä.

10.3 RDP-etätyöpöytäyhteydet

Myös RDP-etätyöpöytäyhteydet ovat hankalia, koska ne paljastavat laiteverkon tietokoneita julkiseen verkkoon ja luovat näin turvallisuusriskejä. Tietokoneet tarvitsevat säännöllisiä tietoturvakorjauksia, joita joudutaan päivittämään, kun ne muodostavat yhteyden julkisiin verkkoihin kuten laitoksen Wi-Fi-verkkoon. Tällöin tehtaan tietokoneet ovat sitten haavoittuvia julkisten verkkojen käyttöikkunoiden aikana (jos ne ovat myös avoinna RDC-ohjaukselle). Ne voivat joutua verkkohyökkäysten kohteiksi ja olla alttiita ransomware-injektioille.

Näiden turvallisuuskysymysten lieventäminen edellyttää lisäresursseja henkilöstöresurssien sekä ylläpidon kannalta. Perinteisten tekniikoiden lisäämä monimutkaisuus voi lisätä tietoturva-aukkoja, sillä teollisia ohjausjärjestelmiä ei ole yleensä suunniteltu liitettäväksi ulkoisiin tietoliikenneverkkoihin.

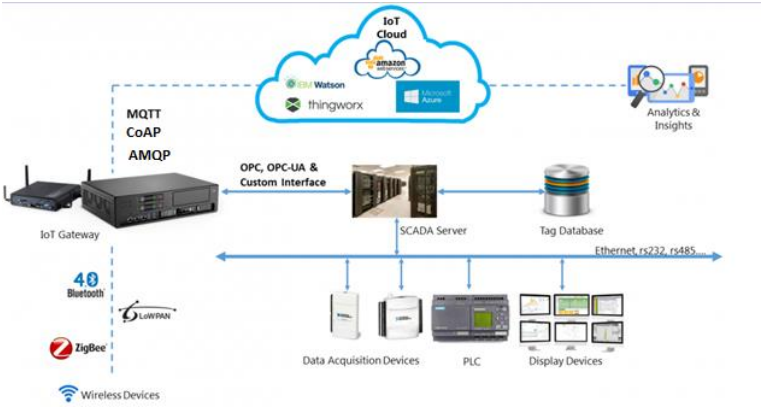
VPN:n käyttäminen yhdistää järjestelmän IT-verkkoon, mikä tarkoittaa myös sitä, että hakkerilla on pääsy johonkin järjestelmän pisteeseen, jota käytettiin esimerkiksi Ukrainan sähköverkkoa vastaan tehdyissä hyökkäyksissä vuonna 2016. [8.] Vaikka perinteistä VPN- ja etätyöpöytäyhteyksiä (RDP) käytetään laajalti ja ne sopivat etävalvonnalle ja -hallinnalle, ovat nämä teknologiat monimutkaisia sekä kalliita eikä ratkaisuissa kuitenkaan ole joustavuutta tai älykkyyttä erityistarpeiden tyydyttämiseksi.

10.4 Pilvipohjaiset etäkäyttöratkaisut

Monille ihmisille lauseet "etäkäyttö" ja "VPN" ovat synonyymejä. Yritykset ottavat kuitenkin nopeasti käyttöön pilvisovelluksia, jotka muuttavat turvallisuuden ja verkottumisen vaatimuksia. Käyttäjät ja sovellukset ovat alkaneet siirtyä käyttämään yhä enemmän internetin pilvipalveluita, jotka toimivat verkon ulkopuolelta ilman VPN- yhteyden muodostamista mistä tahansa laitteesta.

Yhdellä silmäyksellä näyttää, että pilvipohjainen turvallinen etäkäyttöratkaisu toimisi pääosin samalla tavalla kuin perinteinen VPN. Molemmat sallivat kahden IP-yhteensopivan laitteen kommunikoida turvallisesti keskenään etänä internetin välityksellä.

Etäyhdyskäytävät on liitetty kenttälaitteisiin, jotta niitä voidaan käyttää etäyhteyden kautta, jossa asiakasohjelmisto on asennettu asiantuntijan tietokoneeseen sekä pilvipalvelin voidaan asentaa pilvipohjaiseen alustaan kuten Amazon Web Serviceen tai Microsoft Azureen (kuva 23).



Kuva 23. Pilvipohjaiset etäkäyttöratkaisut. [20.]

Etäyhdyskäytävä ja asiakasohjelmisto käynnistävät molemmat lähtevän suojatun yhteyspyynnön pilvipalvelimelle. Pilvipalvelin kartoittaa kaksi yhteyspyyntöä ja onnistuneen todennuksen jälkeen molemmilta puolilta muodostetaan yhteys. Tämä voi aiheuttaa jonkinlaisen riskin ilman asianmukaisia suojausominaisuuksia.

11 Verkkolaitteiden haavoittuvuuksien etsintä internet-verkosta

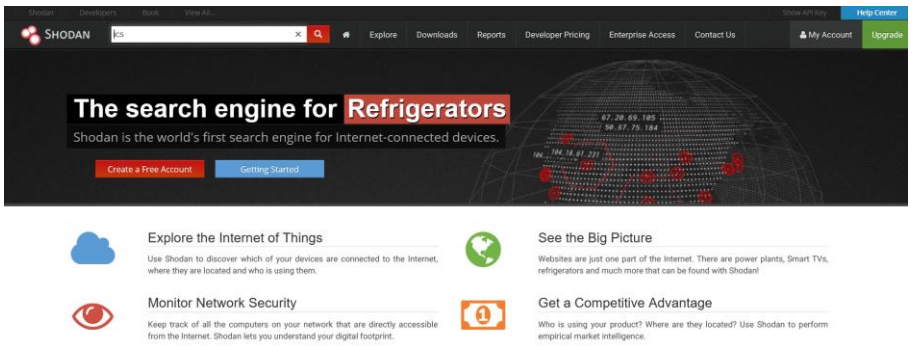
Lähtökohtaisesti ICS-laitteita ei pitäisi näkyä internetiin mutta valitettavasti suojaamattomia laitteita löytyy tietoturvaskannauksissa, joita hyödyntämällä hakkerit yrittävät etsiä järjestelmiin pääsyä eri menetelmillä sekä automaattisesti että manuaalisesti. Hakkereiden käytettävissä on siis paljon jo valmiita automatisoituja työkaluja, omia ohjelmia sekä koneille asennettavia haavoittuvuusskannereita. Lisäksi löytyy julkisia skannauspalveluita kuten perinteisiä hakukoneita. Erikoistuneet hakukoneet keskittyvät johonkin tiettyyn aihepiiriin toisin kuin yleiskäyttöiset hakukoneet. [11.] Shodan on yksi internetin hakukoneista, jonka peruskäyttö on ilmaista ja mahdollistaa kaikkien yleisessä verkossa olevien laitteiden löytämisen, jonka avulla voidaan löytää esimerkiksi web-kamerat, reitittimet, palvelimet ja internet-laitteet, jotka on liitetty internetiin. Pienellä lisämaksulla saadaan Shodaniin käyttöön hyödyllisiä lisäominaisuuksia kuten mm. laajemmat hakutulokset, komentorivikäyttö sekä karttahakuja.

Shodanilla on omat indeksointirobotit, jotka hakevat ja päivittävät jatkuvasti sen tietokantaa internettiin kytketyistä laitteista. Shodan-tietokanta sallii hakkerin etsiä IP-osoitteita ja aloittaa portin skannauksen tunnistaakseen mitä käyttöjärjestelmää kohteet käyttävät ja miten verkkoihin päästään sisään. Kun hakkeri tietää, mitkä ohjelmistosovellukset ovat käynnissä kohteen verkossa, hän voi kehittää tiettyjä työkaluja tunnettujen haavoittuvuuksien hyödyntämiseksi. Esimerkiksi jos hakkeri tietää, että kohteen valvontajärjestelmänä toimii Siemens ja sinne on raportoitu kaksi ohjelmiston haavoittuvuutta, ensimmäinen haavoittuvuus sallii onnistuneen etäisen hyökkäyksen ja toinen haavoittuvuus hakkerin paikallisen pääsyn muokkaamaan suojaustason salasanoja. Vaikka Siemensin ohjelmistopäivitys on käytettävissä, on todennäköistä, ettei sitä ei ole asennettu kaikkiin järjestelmiin. Esimerkkitapaus oli raportoitu vuonna 2015. [12.]

Shodan tutkii siis internetiä jatkuvasti ja yksi tärkeimmistä työkaluista, joka tekee verkkolaitteiden haavoittuvuuksien etsinnästä helppoa ja tuotetta kuvataan internetin ensimmäiseksi verkkoon kytkettyjen laitteiden hakukoneeksi

Palvelun kautta voidaan hakea esimerkiksi kaikki Suomessa verkkoon kytketyt FTP-palvelimet, jotka sallivat anonyymin kirjautumisen eli palvelimen käytön ilman salasanaa.

Shodania käytetään Web-käyttöliittymän (kuva 24) kautta kuten muitakin yleisimpiä hakukoneita. SHODAN toimii eri selaimissa, jota kuvailtu myös maailman vaarallisimmaksi hakukoneeksi eli hakkerien Googleksi.



Kuva 24. Esimerkki Shodan Web-käyttöliittymästä. [11.]

Tunkeutumiskokeiden testauksessa yleisimmin käytetty työkalu on Metasploit Framework, joka on avoimen lähdekoodin projekti ja tarjoaa myös tietoa tietoturva-aukoista. Muita yleisiä, vapaasti internetistä ladattavia hakukoneita ovat Google Hacking Diggity Project, Nmap, Snort, Kismet, Nessus, McAfee, Sophia ja Bandolier. [17.]

12 Yhteenveto

Tietoverkkohyökkäyksissä on havaittavissa selkeä kasvu, joissa usein kohteena ovat teollisuuden järjestelmät. Näin yritykset joutuvat arvioimaan uudelleen tietoturvamallinsa ja sen suojaukset.

Tunkeutumisreittien moninaisuus tarjoaa laajan valikoiman hyökkääjille haavoittuvuuksista ja problematiikkaa lisää vaikeus sulkea kaikkia tietoliikenneyhteyksiä. Yritysten tulisi ottaa käyttöön puolustuksen syvällinen strategia, jossa on useita kerroksia, jotka suojaavat toisiaan aina ohjauslaitteisiin saakka.

Saadaksemme verkon suojaukseen teolliseen käyttöön soveltuva ratkaisu, on järjestelmien suunnittelupuolella suositeltavaa käyttää enemmän sisäisiä vyöhykkeiden suojauksia ja tunkeutumisen havaitsemiseen tarvittavia analytiikkaohjelmistoja.

Valvontajärjestelmävalmistajilta edellytetään hyvää suunnittelua ja testausta ennen automaatiolaitteiden käyttöönottoa. SCADA- ja kontrolliprotokollien turvallisuus ominaisuuksia tulisi myös parantaa, sillä tällä hetkellä useimmat laitteet näyttävät olevan hyvin alttiita jopa pienille hyökkäyksille, koska niillä ei ole todentamis- tai valtuutusmekanismeja, joilla estetään väärennösten valvonta.

Muuttuviin haavoittuvuuksiin sopeutuminen ja niiden havaitseminen on valvontajärjestelmille haaste jossa virheet näkyvät ja tuloksena voisi helposti olla maineen menetys, ympäristövaikutukset, tuotannolliset ja taloudelliset menetykset.

Yhtä ja kaikille sopivaa malliratkaisua on vaikeaa kiteyttää ja löytää, koska useasti yritysten liiketoimintojen laajuus ja luonne sekä kumppaniverkostot vaihtelevat merkittävästi.

Opinnäytetyön lopputuloksena oli osoittaa arkkitehtuurisuunnittelun ja tietoturvauhkien havainnoinnin merkityksen tärkeyttä teollisuusverkkojen kybertietoturvariskien pienentämiseen sekä toiminnan jatkuvuuden varmistamiseen. Tietoturvan parantaminen on osa jatkuvaa ja kehitettävää toimintaprosessia, jonka on seurattava koko ajan aikaansa.

Lähteet

1 Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial. 2016. Verkkoaineisto. Department of Homeland Security. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf. Luettu 21.12.2019.

2 Alasdair,Gilchrist. 2018. The Industrial Internet of Things. O'Reilly Media, Inc. 1005 Gravenstein Highway North, Sebastopol, CA 95472, USA Industry 4.0. Luettu 11.11.2018

3 Cyber Security & Information Systems Information Analysis Center. 2016. Verkkoaineisto.The Efficacy and Challenges of SCADA and Smart Grid Integration.https://www.csiac.org/journal-article/the-efficacy-and-challenges-of-scada-and-smart-grid-integration/ .Luettu 23.3.2019

4 Pascal, Ackerman .2017. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies 2016. E-kirja. Packt Publishing. Luettu 23.9.2018

5 NIST Special Publication 800-82 . 2013. Verkkoaineisto. Guide to Industrial Control Systems (ICS) Security http://csrc.nist.gov/groups/SMA/fisma/ics/. Päivitetty 12.8.2015. Luettu 1.2.2019.

6 Prepared for the U.S. Department of Energy under Contract DE-AC05-76RL01830. 2011. Secure Data Transfer Guidance for Industrial Control and SCADA Systems. Verkkoaineisto. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf .Luettu 20.3.2019.

7 DNP3 2019. Verkkoaineisto. Wikipedia. https://en.wikipedia.org/wiki/DNP3. Päivitetty 18.1.2019. Luettu. 13.5.2019.

8 Yhdysvallat tutkii Ukrainan joulukuista sähkökatkosta. Verkkoaineisto. YLE . https://yle.fi/uutiset/3-8592656. Päivitetty 13.1.2016. Luettu 12.1.2019.

9 Pascal, Ackerman. 2017. Industrial Cybersecurity. E-kirja. Packt Publishing. Luettu 23.1.2019.

10 Siemens Teollinen tiedonsiirto. 2019. Verkkoaineisto. Väylämuunnokset. http://www.siemens.fi/fi/industry/teollisuuden_tuotteet_ja_ratkaisut/tuotesivut/automaatiotekniikka/teollinen_tiedonsiirto_esim_profinet/teollisuuden_langaton_tiedonsiirto.htm. Luettu 27.2.2019.

11 Shodan.io. 2019. Verkkoaineisto. Wikipedia. https://en.wikipedia.org/wiki/Shodan_(website). Päivitetty 25.1.2019. Luettu 14.11.2018.

12 Siemens : Security Vulnerabilities Published In 2015. 2015. Verkkoaineisto. https://www.cvedetails.com/vulnerability-list/vendor_id-109/year-2015/Siemens.html . Päivitetty 27.11.2015. Luettu 25.12.2018.

13 Knapp Eric D; Samani Raj; Langill Joel. Applied Cyber Security and the Smart Grid E-kirja. Syngress.

14 WHAT IS A FIREWALL?. 2019. Verkkoaineisto. Palo Alto Networks, Inc. https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall. Luettu 20.1.2019.

15 WHAT IS AN INTRUSION DETECTION SYSTEM ?. 2019. Verkkoaineisto. 2019 Palo Alto Networks, Inc. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids. Luettu 20.1.2019.

16 WHAT IS AN INTRUSION PREVENTION SYSTEM? 2019. Verkkoaineisto. 2019 Palo Alto Networks, Inc. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips. Luettu 20.1.2019.

17 Hilt Stephen; Wilhoit, Kyle; Shbeeb, Aaron; Singer, Bryan, Bodungen, Clint. 2016. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. Chapter 10. E-kirja. McGraw-Hill.

18 OWASP Internet of Things Project. 2019. Verkkoaineisto. 18.2.2019. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main. 18.2.2019. Luettu 1.3.2019.

19 SFS-käsikirja 631-3. Automaatio. Osa 3: Tietoturvallisuus. 2013. Helsinki: Suomen Standardisoimisliitto.

20 IoT. 2018. IoT enabled SCADA Solutions. Verkkoaineisto. http://www.travancoreanalytics.com/industrial-automation/iiot/. Luettu 23.4.2018.

21 Choosing the Right Industrial Wireless Network 2006. Verkkoaineisto. © 2006 Honeywell International Inc. http://www.lesmaninst.com/unleashd/catalog/wireless/Honeywell-XYR6000-OneWireless/hwwp_ChoosingWireless_0611.pdf. Luettu 25.3.2019.

22 ICS-CERT MONITOR. 2017. Verkkoaineisto. Updating Antivirus Software in Industrial Control Systems. Verkkoaineisto. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep-Oct2017_S508C.pdf.

23 Siemens Teollinen tiedonsiirto. 2018. Verkkoaineisto. Teollisuuden langaton tiedonsiirto. http://www.siemens.fi/fi/industry/teollisuuden_tuotteet_ja_ratkaisut/tuotesivut/automaatiotekniikka/teollinen_tiedonsiirto_esim_profinet/teollisuuden_langaton_tiedonsiirto.htm. Luettu 11.1.2018.

24 Gervais, Arthur. 2012. Security Analysis of Industrial Control Systems. Diplomityö. KTH Stockholm and Aalto University. Insinööritieteiden korkeakoulu. Aalto-doc-tietokanta.