Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Markus Brunfeldt

Automaatioverkkojen tietoturva-arvioinnin kohteet

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Opinnäytetyö

27.1.2020

Tekijä Otsikko Sivumäärä Aika	Markus Brunfeldt Automaatioverkkojen tietoturva arvioinnin kohteet 28 sivua 27.1.2020
Tutkinto	Insinööri
Tutkinto-ohjelma	Automaatiotekniikka
Suuntautumisvaihtoehto	Sähkö- ja automaatiotekniikka
Ohjaajat	Specialist, Cris Puchner Lehtori, Kimmo Sauren

Insinöörityö toteutettiin Sweco Industry Oy:lle. mikä on osa Sweco Oy konsernia. Insinöörityössä luotiin uusi palvelu ja ohjeistukset teollisuuden automaatioverkkojen tietoturvatarkastuksiin ja kuinka se toteutetaan asiakkaalle.

Insinöörityön teoriaosuudessa käsitellään teollisuuden automaatioverkkoja ja sen rakennetta sekä käydään läpi yleisiä automaatioverkon tiedonsiirtoprotokollia. Automaatioverkon arviointikohteissa on selitetty, miksi tietty osio luo verkkoon heikkouden ja miten syntyneeltä heikkoudelta suojaudutaan tai miten riski minimoidaan.

Sweco Insdustry Oy:lle luotiin ohjeistukset tarvittaviin työkaluihin ja toimintapoihin, että arviointi pystytään toteuttamaan järjestelmällisesti kaikkiin arviointikohteisiin. Ohjeistukset ovat tallennettu yrityksen verkkolevylle, että ne ovat aina saatavilla ja niitä pystyy hyödyntämään myös muut Swecon organisaatiot esimerkiksi suunnittelun tukena. Lopputuloksena syntyi automaatioverkkojen tietoturva-arviointi palvelu (TRAP), mikä on valmis tarjottavaksi asiakkaille.

Avainsanat	Cybersecurity, teollisuus, automaatio

Author(s) Title Number of Pages Date	Markus Brunfeldt Cybersecurity assessment for automation networks 28 pages 27.1.2020
Degree	Bachelor of engineer
Degree Programme	Electrical and automation engineering
Specialisation option	Automation Technology
Instructor(s)	Specialist - Cris Puchner Lecturer - Kimmo Sauren

The thesis work was made out for Sweco Industry Oy which is part of the Sweco Oy Group. The thesis work created a new service and instructions for security audits of industrial automation networks and how to implement it for the customer.

The theoretical part of the thesis deals with industrial automation networks and its structure as well as general communication protocols for automation networks. Automation network evaluation sites explain why a particular partition creates a vulnerability in the network, and how to protect against or mitigate the resulting vulnerability.

Sweco Insdustry Oy has been provided with the necessary tools and procedures to ensure that the assessment can be carried out systematically for all assessment sites. The instructions are stored on the company's cloud storage so that they are always available and can be used by other Sweco organizations, for example to support design. The result was an Automated Network Security Assessment Service and it is ready to be offered to customers.

Keywords	Cybersecurity, Automation, Safety, Industry

Sisällys

Lyhenteet

AES	*Advanced Encryption Standard.* Standardisoitu salaustapa.
ASCII	*American Standard Code for Information Interchange*. 7-bittinen, 128:n merkin laajuinen tietokonemerkistö.
DMZ	*Demilitarized zone*. Fyysinen tai looginen aliverkko, joka yhdistää eri tasoisia verkkoalueita.
HTTP	*HyperText Transfer Protocol.* Taustalla toimiva protokolla
IGMP	*Internet Group Management Protocol*. TCP/IP-pinon protokolla, joka mahdollistaa asiakkaiden liittymisen multicast-ryhmään. Arkkitehtuurisesti IGMP-protokolla toimii IP:n päällä.
IOT	*Internet of things*. Tarkoitetaan järjestelmiä, jotka perustuvat teknisten laitteiden suorittamaan automaattiseen tiedonsiirtoon sekä kyseisten laitteiden etäseurantaan ja -ohjaukseen Internet-verkon kautta
IP	*Internet Protocol*. Osoite, joita käytetään IP-verkoissa olevien laitteiden yksilöimiseen.
IPX	*Internetwork Packet Exchange.* Verkkokerroksen paketti protokolla, mikä lähettää tiedot siirtokerrokselle.
LAN	*Local Area Network*. Paikallinen lähiverkko.
MAC	*Media Access Control.* Yksilöllinen koodi, jonka valmistaja on määrittänyt tietylle verkkolaitteelle. Jokainen koodi on laitekohtainen.

NetBIOS	*Network Basic Input/Output System.* Se tarjoaa OSI-mallin istuntokerrokseen liittyviä palveluita, joiden avulla erillisten tietokoneiden sovellukset voivat kommunikoida lähiverkon kautta.
OPC/OPC UA	*Unified Architecture*. Eri laitteiden väliin tarkoitettu kommunikaatio protokolla.
PLC	*Programmable logic controller*. Ohjelmoitavat logiikka mikä ohjaa prosesseja.
QoS	*Quality of Service.* Tietoliikenteen luokittelua ja priorisointia.
RTU	*Remote terminal unit.* Mikroprosessoriohjattu elektroninen tietokone, joka liittää laitteen ohjausjärjestelmiin.
SCADA	*Supervisory Control and Data Acquisition.* Hajautettu toiminnan ja prosessien ohjausjärjestelmä.
SNMP	*Simple Network Management Protocol*. TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla. Protokollan avulla voidaan kysellä verkossa olevan laitteen tilaa tai laite voi itsenäisesti antaa hälytyksiä.
TCP/IP	*Transmission Control Protocol/Internet Protocol.* Internet laitteiden yhdistämiseen käytetty viestintäprotokolla.
VLAN	*Virtual LAN*. Tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin.
WEP	*Wired Equivalent Privacy*. Langattoman verkon salausprotokolla.
WPA/WPA2	*Wi-fi Protected Access.* Langattoman verkon kehittyneempi salausprotokolla.

1 Johdanto

Tämän vuosikymmenen aikana tapahtunut nopea tietoliikennetekniikan sekä sähköisen ja elektronisen tekniikan kehitys on tuonut erilaisia mahdollisuuksia teollisen prosessien kehitykselle. Tämä tuo teollisuuteen koko ajan uutta teknologiaa ja prosesseja pystytään seuraamaan ja halutaan seurata yhä tarkemmin. Energiatehokkuus, tuotannon optimointi, raaka-aineiden mahdollisimman hyvä käyttöaste vaativat sen, että prosessit ovat automaattisia ja mahdollisimman tehokkaita. Tämä teollisuudessa seuraava vallankumous on saanut nimityksen Industry 4.0. Industry 4.0 (Industrie 4.0) on alun perin Saksassa keksitty termi. Industry 4.0 kuvaa teollisuusprosessien sisäistä kommunikaatiota, kun kaikki laitteet pyritään yhdistämään toisiinsa ilman koko ajan tapahtuvaa valvontaa ja ne pystyvät analysoimaan itseään. Tehdyn analyysin avulla automaatio ja tekoäly säätää prosesseja ja näin päästään tehokkaampaan työskentelyyn ja tuotantoon. [1.] Industry 4.0. käyttää hyödykseen esimerkiksi esineiden internetiä (IoT), big dataa ja pilveen rakennettua ympäristöä.

Kun tietoa ja analytiikkaa kerätään paljon ja sitä halutaan koko ajan saataville yhä enemmän, ovat siitä mahdollisesti kiinnostuneet myös muutkin tahot kuin pelkästään yritys itse. Tiedon turvaamisen merkitys on nähty kauemmin sähköpostien, taloustietojen ja muiden vastaavien yritys- ja henkilösalaisuuksien osalta. Prosesseista kerättävä tieto on yhtä lailla liiketoiminnan ydin. Tiedon salassapidon ja oikeellisuuden lisäksi teollisissa prosesseissa turvallisuus nousee yhdeksi tärkeäksi kysymykseksi. Tietovuoto voi aiheuttaa taloudellisen riskin, mutta itse prosessiin liittyy monia niin ympäristö-, kuin henkilöturvallisuuskysymyksiä.

Kun automaatiojärjestelmässä laitteita yhdistetään toisiinsa, tulee verkkoympäristöön monia erilaisia tietoliikenne yhteyksiä. Luodut yhteydet ja laitteet luovat aina mahdollisia uusia riskejä tai uhkia väärinkäytöksille. Tämän takia tiedot, tiedon säilytys, ohjaukset, laitteet ja yhteydet sekä niiden yhteisvaikutukset tulisi tarkistaa tietoturvan näkökulmasta. Mikäli tietoturvasta muodostuvat riskit jätetään kokonaan huomioimatta, on kyberhyökkäys helpompi toteuttaa kohteeseen tai kohteisiin. Kyberhyökkäyksiä on monia erilaisia, ja ne voivat olla monenlaisia esimerkiksi tiedonkeräämistä, laitteiden manipulointia, prosessiarvojen vääristämistä, palvelunesto hyökkäykset, verkonhallintaan liittyvät hyökkäykset ja monia muita. Toteutustapoina kyberhyökkäyksissä voivat olla niin verkon yli tulevat hyökkäykset kuin fyysisesti paikan päällä tehdyt tiedon keruut, hyök-

käykset tai häirinnät. Kyberhyökkäykset voivat olla tahallisia tai tahattomia tekoja. Riskienhallinta kuuluu osaksi teollisuuden prosesseja jo entuudestaan, mutta Industry 4.0 ja digitalisuus tuovat tarpeen lisätä tietoturvauhat osaksi riskienhallintaa sekä tarkastusprosessia. Prosessiteollisuuden automaatiojärjestelmän turvallisuuteen liittyvä standardin SFS-EN 61511 Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille uusin versio antoi vaatimuksen tietoturvauhkien arvioinnille. [2.]

Tämän insinöörityön tilaajana on Sweco Industry Oy. Työssä on tarkoituksena selvittää, miten teollisuuden tietoturva-arviointi saadaan toteutettua olemassa oleville ja uusille asiakkaille sekä miksi arviointeja olisi syytä toteuttaa. Sweco on rakennetun ympäristön johtava teknisen turvallisuuden osaaja ja haluaa palvella jatkossakin asiakkaittensa tarpeita, joten teollisuuden tietoturva konsultointi sopii yrityksen portfolioon. Näin ollen uuden palvelukokonaisuuden kehittäminen tuo asiakkaiden saataville kokonaisvaltaisempaa teollisuuden teknisen turvallisuuden konsultointia.

Sweco Oy Ab ja Sweco Industry Oy

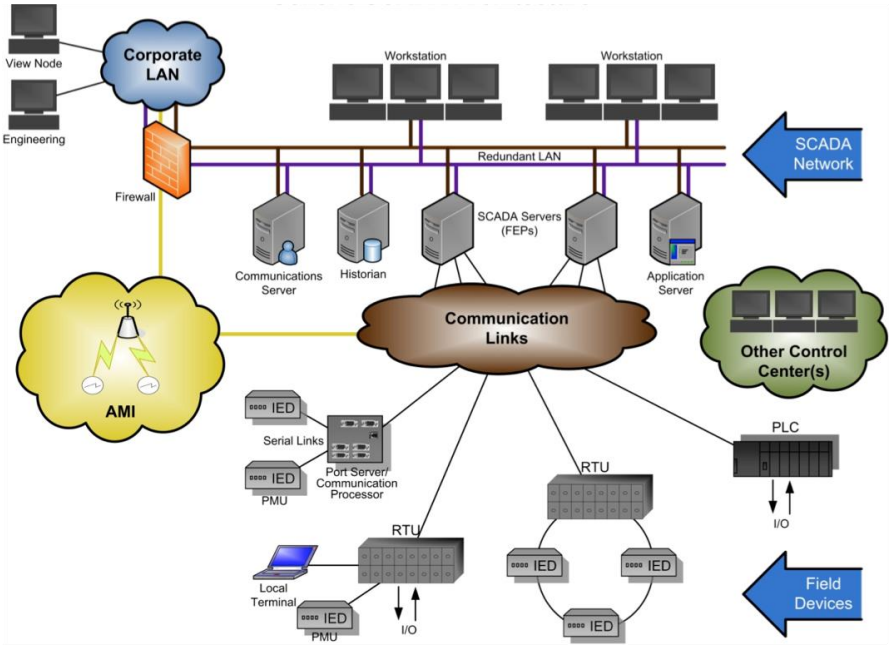
Sweco Industry Oy on osa Sweco AB konsernia. Ruotsissa perustettu rakennuskonsultointiin erikoistunut yritys työllistää noin 16000 henkilöä ja Suomessa noin 2400 henkilöä. Yritys toimii 12 eri maassa ja vuosittain toteutetaan projekteja noin 70 eri maahan. Konserniin kuuluu neljä alueellista organisaatiota: Sweco Sweden, Sweco Norway, Sweco Finland ja Sweco Central Europe. Suomessa Sweco Finlandin alla toimii Sweco Rakennetekniikka, Sweco Talotekniikka, Sweco Ympäristö, Sweco Industry, Sweco PM, Sweco Asiantuntijapalvelut sekä Sweco Architects. Sweco tarjoaa Suomessa suunnittelu- ja konsultointipalveluja rakennetekniikan, arkkitehtuurin, talotekniikan, teollisuuden sekä ympäristö- ja yhdyskuntatekniikan aloilla ja myös projektinjohto- ja rakennuttamispalveluita. [3.]

2 Automaatioverkko

Automaatioverkko toimii tuotantolaitoksen prosessin ohjausverkkona ja se on osa koko tehtaan tiedonsiirtoverkkoa. Tehtaan tiedonsiirtoverkko on tarkoitettu vain yrityksen omaan käyttöön ja tämän takia se pidetään yleensä pienenä LAN verkkona. Verkko on eritelty alueisiin, joissa kaikki toimintaan tarvittavat toiminnot voidaan toteuttaa. Liikennöinti verkosta ulospäin tapahtuu sovittujen sääntöjen ja pisteiden kautta, jotta tietoliikennettä pystytään valvomaan palomuureilla ja liikenteen suodatuksella. Verkon sisällä olevat toiminnot on varmennettu tai kahdennettu vaadituilta osin niin, että prosessin ohjaukset toimivat vikatilanteissakin suunnitellusti. Toimintojen varmennuksen tasot määritetään aina verkosta ja prosessista riippuen. Näin toimintavarmuus saadaan automaatioverkossa korkealle tasolle, koska tietyt prosessit ovat kriittisiä. Eritoten turva-automaatio ja sen käskyt pitää olla aina tavoitettavissa.

2.1 Automaatioverkon laitteet

Tietoliikenneverkon laitteiden tulee olla aina määritelty, jotta ymmärretään mitä pitää suojata ja kuinka suojaus tullaan toteuttamaan. Verkossa voi olla esimerkiksi reitittimiä, kytkimiä, prosessilaitteita, ohjausyksiköitä, PLC, palvelimia, palomuureja, toimilaitteita ja langattomia laitteita. Kuvassa 1 on esitetty tyypillinen automaatioyrityksen tietojärjestelmä.



Kuva 1. Automaatiojärjestelmän kuva ja mitä laitteita verkosta löytyy. [4.]

Älykkään tuotantolaitoksen kehityksen mukana laitteiden määrä lisääntyy ja uudistuu. Kun ymmärretään, mistä laitteista verkko rakentuu, pystytään ne suojaamaan oikein, sekä sijoittamaan verkossa arkkitehtuurin perusteella oikeaan paikkaan. Tavoitettavuus ja varmuus ovat suuressa roolissa myös verkossa, ja sen takia oikealla sijoittelulla niin fyysisesti kuin virtuaalisesti on suuri merkitys.

Verkossa on olemassa etähallittavia laitteita ja muutoksen sallivia laitteita, jotka tulisi suojata erillisen hallintaverkon taakse, koska hyökkääjän saadessa oikeudet pystyy hän luomaan uusia sääntöjä tai muuttamaan laitteita niin, että ne sallivat vahingollisen liikenteen. Mitä isompiin käyttöoikeuksiin hyökkääjät pääsevät käsiksi, on vahinko vaikeampi korjata sekä kustannukset kasvavat suuremmiksi.

Tämmöisiä hallittavia laitteita on esimerkiksi hallittava kytkin. Hallittavissa kytkimissä on käyttöliittymä, johon voidaan ottaa yhteyttä telnet- tai secure shell -protokollan avulla tai suoraan johdolla. Näitä kytkimiä voidaan useimmiten konfiguroida ja hallita kokonaisuuksina. Uudemmat kytkimet voivat tarjota myös internet selaimella toimivan konfigurointiliittymän. Hallittavat kytkimet ja niiden monet hallintaominaisuudet sopivat isoihin yritysverkkoihin, joissa valvottavien ja ohjattavien verkkolaitteiden määrä on suuri. Kuvassa 2 esitetty hallittava kytkin.

Kuva 2. Hallittava kytkin [5.]

Nykykytkimet sisältävät huomattavan paljon ominaisuuksia ja yhteyksiä, joilla vaikutetaan tietoturvaan esimerkiksi seuraavanlaisia ominaisuuksia [4]:

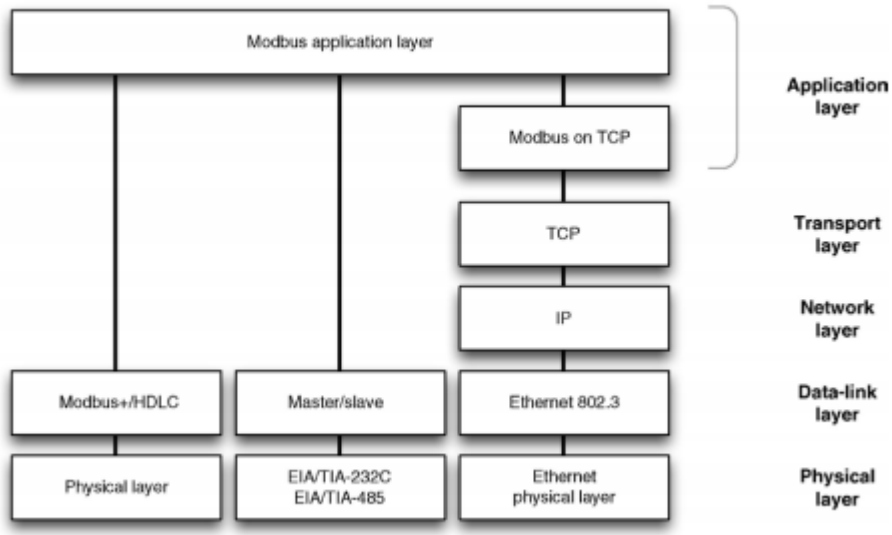
- SNMP-valvonta
- yksittäisten porttien käyttöönotto ja käytöstä poisto
- portin kaistanleveyden hallinta ja duplex-ohjaus
- IP-osoitteiden hallinta
- MAC-osoitteiden suodatus
- Spanning Tree -protokolla
- porttien peilaus verkkoliikenteen valvomiseksi
- porttien QoS-priorisointi
- VLAN-asetukset
- 802.1X verkkoon pääsyn valvonta
- IGMP-snooping -ominaisuus
- linkkien yhdistäminen tai trunking.

2.2 Tiedonsiirtoprotokollat

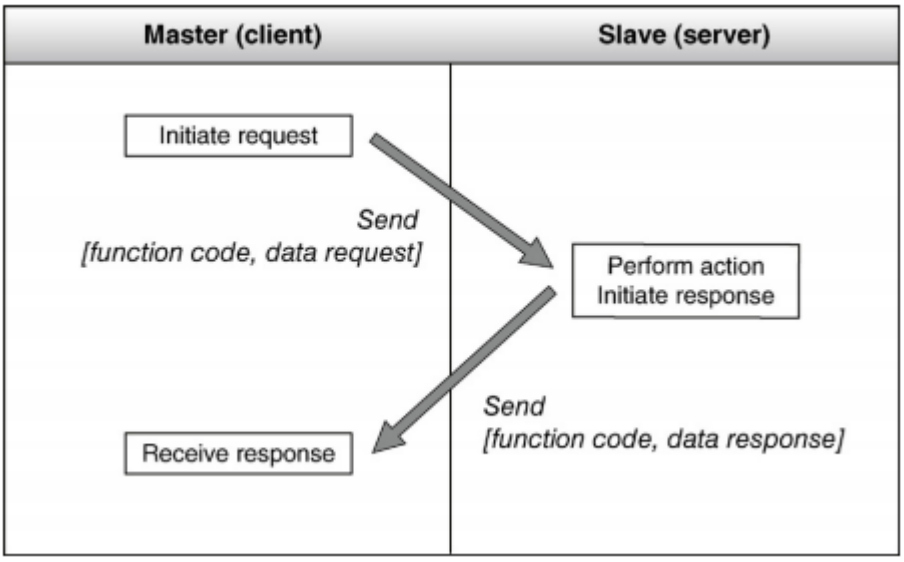
Kun halutaan ymmärtää, kuinka tietoturvahyökkäyksiltä suojaudutaan, on myös ymmärrettävä, minkälaista tietoliikenneprotokollaa teollisuuden laitteet käyttävät. Tiedonsiirtoprotokolla määrittää, mihin ja millä tavalla laitteet kommunikoivat keskenään verkossa. Teollisuudessa on olemassa monia erilaisia tiedonsiirtoprotokollia, kuten Modbus, OPC, Wireless HART, Profinet ja Profibus. Kaikille teollisuuden tiedonsiirtoprotokollille on yhteistä, että tiedonsiirron tulisi tapahtua nopeasti ja reaaliajassa sekä verkon pitää pystyä käsittelemään suurta määrää dataa luotettavasti. Teollisuuden protokollia on monia, ja seuraavaksi on listattu niistä osa sekä niihin liittyviä tietoturvaheikkouksia.

Modbus

Modbus-protokolla on kehitetty vuonna 1979 yhdistämään prosessin ohjauslaitteet tietokoneisiin. Siitä on myös syntynyt variaatioita, kuten Modbus RTU ja Modbus ASCII. Modbus on sovelluskerroksen viestintäprotokolla, kuva 3 selventää tiedonsiirtotapaa.



Kuva 3. Modbus-protokollan tiedonsiirtotasot [6.]



Kuva 4. Modbus-protokollan liikennöintitapa [6.]

Kun Modbus on niin sanottu vanhanaikainen protokolla, on siinä myös paljon heikkouksia tietoturvan osalta, kun liikennöintitapa on yksinkertainen. Kuva 4 näyttää yksinkertaisesti, kuinka Modbus-laitteet kommunikoivat keskenään. Modbus-protokollan tietoturvariskejä ovat seuraavat:

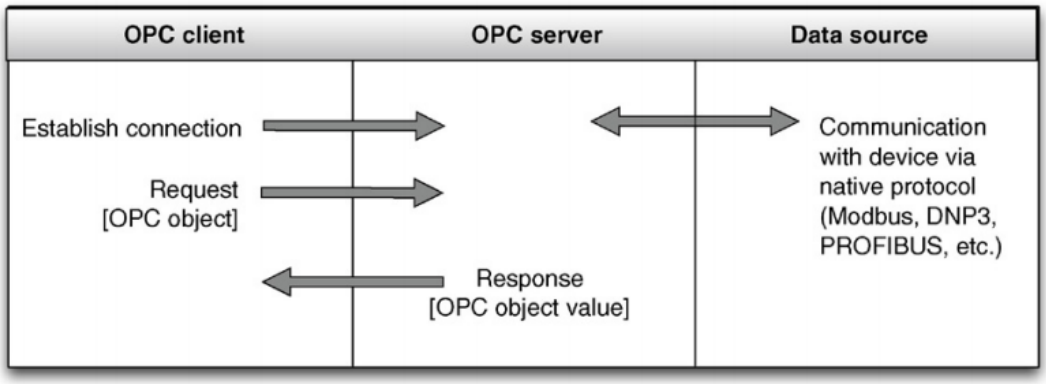
- Modbus-liikenteen autentikointi ei varmenna, mistä liikenne on peräisin, vaan pyytää koko ajan samaa osoitetta. Jos osoite on tiedossa, voidaan sen avulla luoda verkkoon vääränlainen laite, joka käyttää tätä verkko-osoitetta. Tämän avulla voidaan liikennettä helposti kaapata ja mahdollisesti muuttaa.

- Modbus-protokolla kulkee täysin selväkielisenä, jos liikennettä saa tallennettua, pystyy sen tulkitsemaan helposti, koska mitään salauksia ei ole.

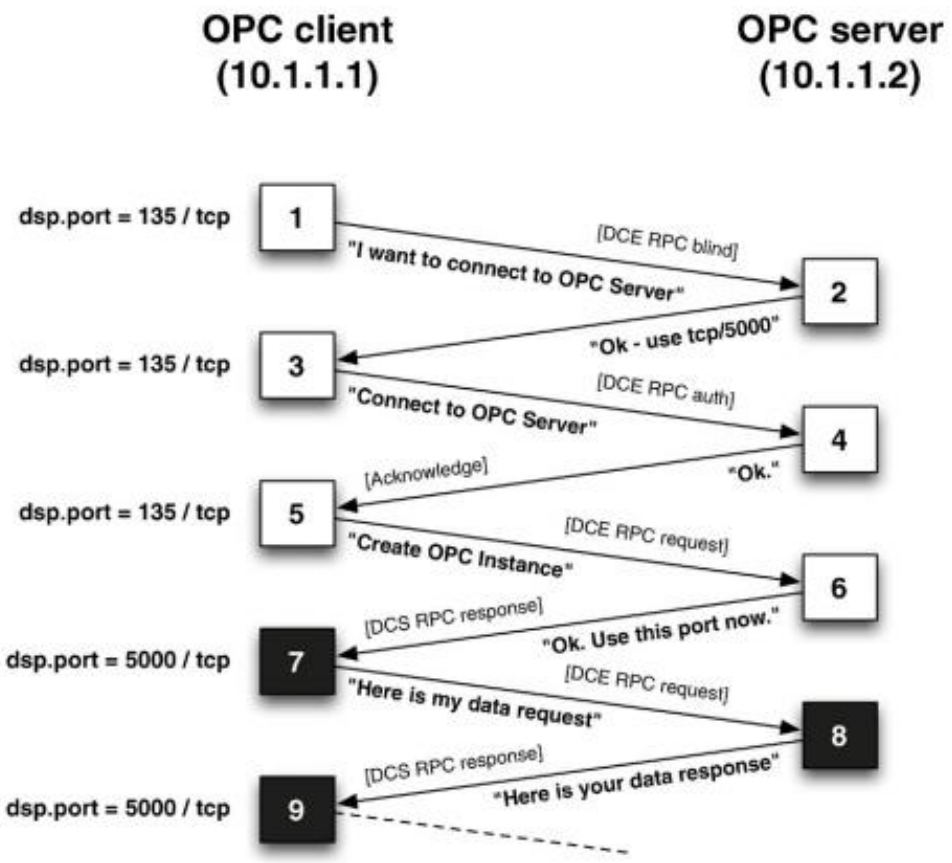
- Protokolla lähettää koko ajan kaikille laitteille viestejä, vaikka ne eivät olisi tarkoitettu vastaanottavalle laitteelle. Tämän avulla pystytään ylikuormittamaan laitteita ja niiden prosessointikykyä, näin ollen prosessi voi toimia hitaasti tai oikeata tietoa ei voida lukea. [6. s. 123–124.]

OPC

OPC- ja OPC-UA-protokollat on kehitetty nimenomaan sitä varten, että eri laitteet ja järjestelmät pystyisivät keskustelemaan keskenään verkon yli. Nykyisin protokollat ovat käytössä todella useasti, koska kaikki tehtaat ja muut tuotantolaitokset kootaan useista eri toimituksista. Näin saadaan helposti luotua yhteyksiä eri kokonaisuuksien välille. Kuvissa 5 ja 6 esitetty OPC-protokollan kommunikointitapa.



Kuva 5. OPC-kommunikointitapa [6.]



Kuva 6. OPC-protokollan kommunikointitapa. [6.]

OPC-protokolla on vanhempi, ja tämän takia se sisältää paljon enemmän tietoturvariskejä kuin OPC-UA. Olisi suotavaa käyttää näistä kahdesta vain OPC-UA-protokollaa. OPC sisältää seuraavanlaisia riskejä:

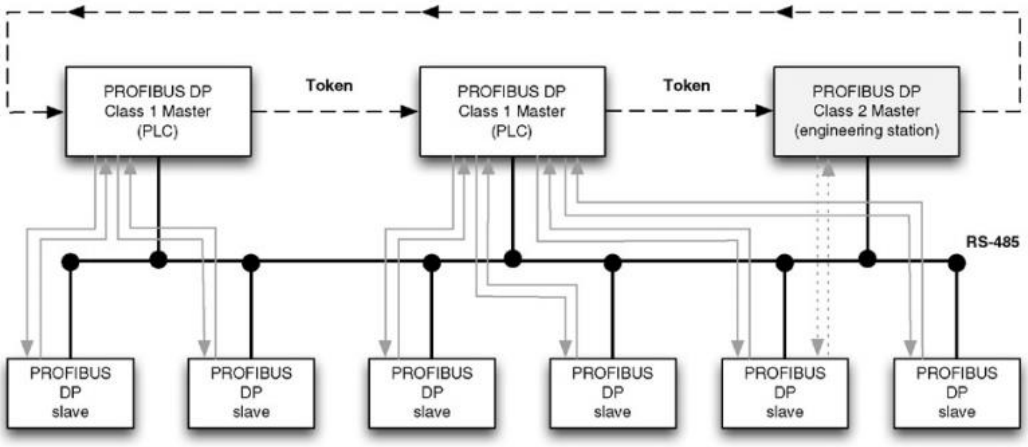
- Vanhanaikaiset autentikoinnit, mikäli päivityksiä ei ole hoidettu tai pystytty hoitamaan muusta vanhanaikaisesta ympäristöstä johtuen.

- Mahdollisesti paljon ylimääräisiä portteja ja palveluita auki, joita kautta avautuu hyökkääjille mahdollisia reittejä tunkeutua verkkoon. Esimerkiksi: HTTP, NetBIOS, NetBEUI, IPX.

- On mahdollista rinnalle luoda vääränlainen OPC-palvelin ja käyttää sitä tietojen kalasteluun tai haitallisen koodin asentamiseen. [6. s. 156–157.]

Profibus

PROcess FieldBUS eli Profibus on kehitetty 1980 luvulla Saksassa. Siitä on muotoutunut muutamia variaatioita esimerkiksi PROFIBUS PA (voidaan käyttää prosessin instrumentoinnissa), PROFIsafe (käytetään turva-automaatiossa ja turvallisuuteen liittyvissä kokonaisuuksissa) ja PROFIDrive (käytetään nopeata tiedonsiirtoa vaativissa kokonaisuuksissa). Profibus -protokolla toimii master-slave -menetelmällä, eli yksi isäntälaite hallinnoin tietoliikennettä ja orjalaitteet lähettävät pyydetyt tiedot isäntälaitteelle, joka ohjaa laitetta tai prosessia tarvittaessa. Väylään on mahdollista lisätä monia eri isäntälaitetta, kunhan orjalaitteille kerrotaan, minkä isännän kanssa se kommunikoi. Kuva 7 selventää kuinka, master-slave -liikennöintitekniikka toimii.



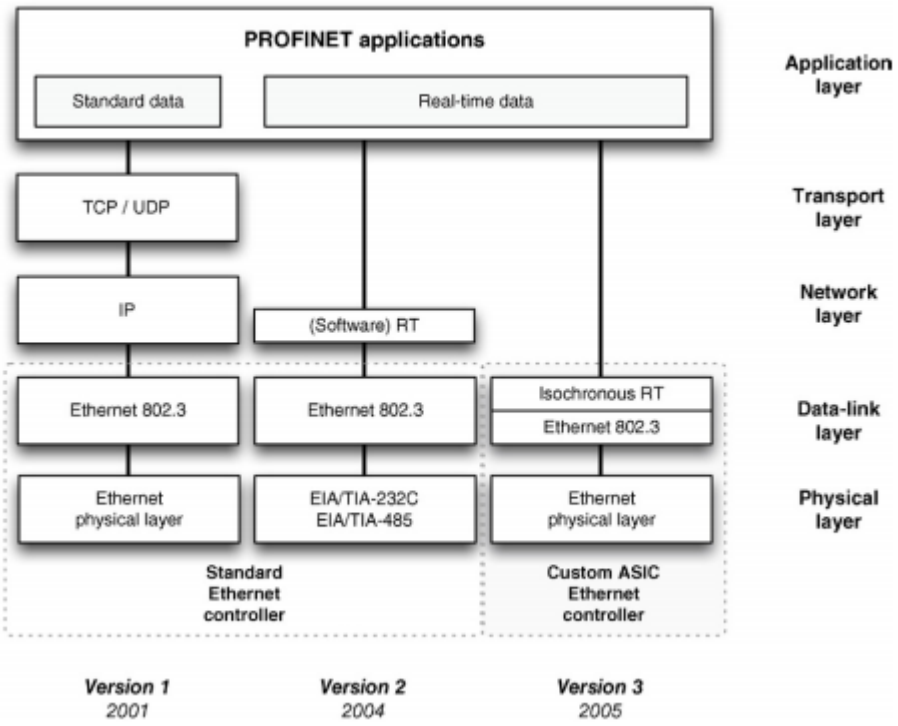
Kuva 7. Profibus master-slave-liikennöintapa [6.]

Profibus-protokollan mukana tulee tietoturvaan liittyviä riskejä. Profibus ei todenna liikennettään, joten vääränlaisen isäntälaitteen vieminen verkkoon on mahdollista. Yleensä tällainen hyökkäys vaatii fyysistä pääsyä Profibus DP -verkkoon, joten se on suojassa verkon yli tulevilta hyökkäyksiltä. Isäntälaite on yleensä aina yhteydessä Ethernet -verkkoon, joten sitä kautta voi hyökkäyksiä tehdä myös verkon yli hyödyntäen laitteen muita haavoittuvuuksia [6. s. 138 –141.]

Profinet

Profinet on avoin tehdasstandardi, jonka kehittivät Profibus-käyttäjät ja Siemens. Profinet on suunniteltu nimenomaan skaalautuvuutta varten. Profinet on reaaliaikainen Ethernet -protokolla ja sellaisenaan herkkä mille tahansa Ethernet-haavoittuvuudelle. Tietoturvariskin ja haavoittuvuuden laajuus riippuu suuresti käytetystä verkkoarkkitehtuurista, koska uudemmissa verkkolaitteissa on sisäistä diagnostiikkaa, joka huomaa yritykset tunkeutua verkkoon. Verkkoliikennettä voidaan siirtää ja käyttää IP:n yli. Mikäli näin toimitaan, altistuu se myös kaikille IP:n haavoittuvuuksille. PROFINET on myös altis palvelunestohyökkäyksille. Kun suuri määrä oikein määriteltyä UDP-liikennettä lähetään laitteille, saattaa laite ylikuormittua ja hidastua.

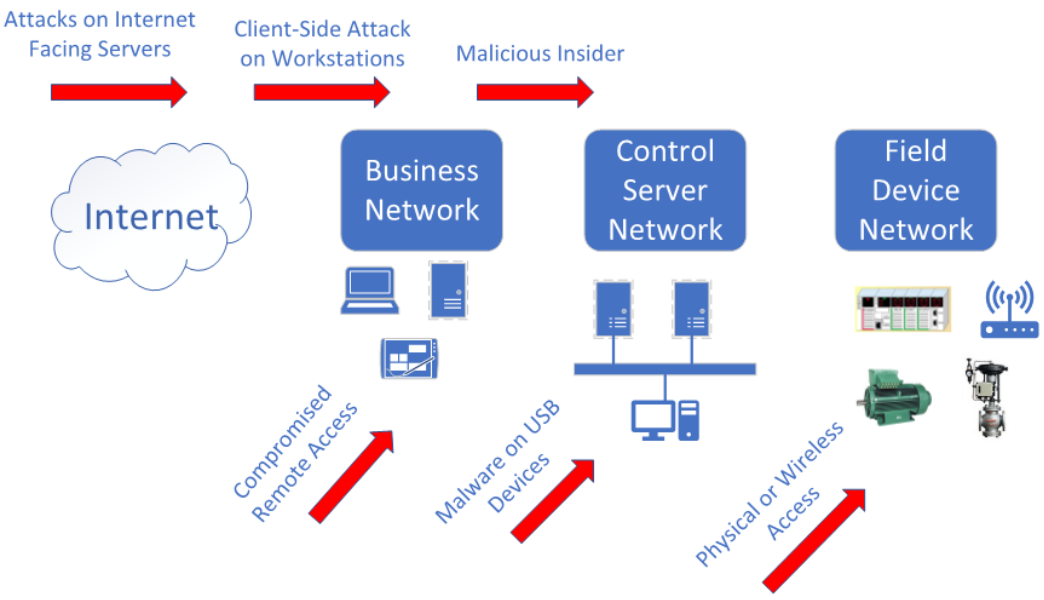
Kenttäväyläprotokollissa yhtenä riskinä on liikenteen varmennuksen puute ja niin on myös Profinetissä. Profinet-liikennettä voidaan siirtää suoraan normaalien toimistoverkkojen kautta, joten se tulisi nimenomaan suojata erittäin hyvin tai siirtää liikennettä vain varmasti tunnettujen verkkojen kautta. Profinetin liikennöintitapa esitetty kuvassa 8. [6. s. 146–148.]



Kuva 8. Profinet-protokollan toiminta [6.]

3 Tietoturva teollisuudessa

Teollisuudessa tietoturva on yleisesti huomattavasti jäljessä edelleen, ja vasta nyt aletaan ymmärtämään tietoturvan merkitys, kun tuotantolaitoksia on joutunut jo kyberhyökkäyksien kohteiksi. Kehittyneet ympäristöt ovat kaikki verkossa kiinni, joten samalla kun laitteet lisääntyvät syntyy myös aina uusia mahdollisia aukkoja verkkoon ja hyökkäys mahdollisuudet lisääntyvät. Kuvassa 9 on esitetty erilaisia hyökkäyskohteita ja menetelmiä. Kyberhyökkäyksien kohteet ja syyt voivat erota täysin toisistaan, on olemassa ilkivaltaa, tiedon kalastelua, häirintää sekä vahingoittamista tarkoituksessa ja monia muita. Kun jo tehtyjä hyökkäyksiä tutkitaan, saadaan niistä arvokasta tietoa estämään mahdollisia seuraavia hyökkäyksiä. Kun keinot löydettyjen uhkien ehkäisemiseksi on keksitty, hakkerit keksivätkin aina uusia keinoja toteuttaa hyökkäyksiään. Teollisuudessa onkin nähty jo monia erilaisia kyberhyökkäyksiä. Vaikutukset ovat olleet huomattavia ja kyberhyökkäykset ovatkin lisääntyneet koko ajan.



Kuva 9. Mahdollisia hyökkäysmenetelmiä

Prosessinohjausjärjestelmät ovat itsenäisiä, ja kun ne luodaan, on niiden tarkoitus luotujen ohjeiden ja määritysten mukaisesti jalostaa tuotetta, jotta saadaan lopputuotetta aikaiseksi. Kaikki järjestelmään tehdyt turvarajat on toteutettu pysäyttämään toiminta tur-

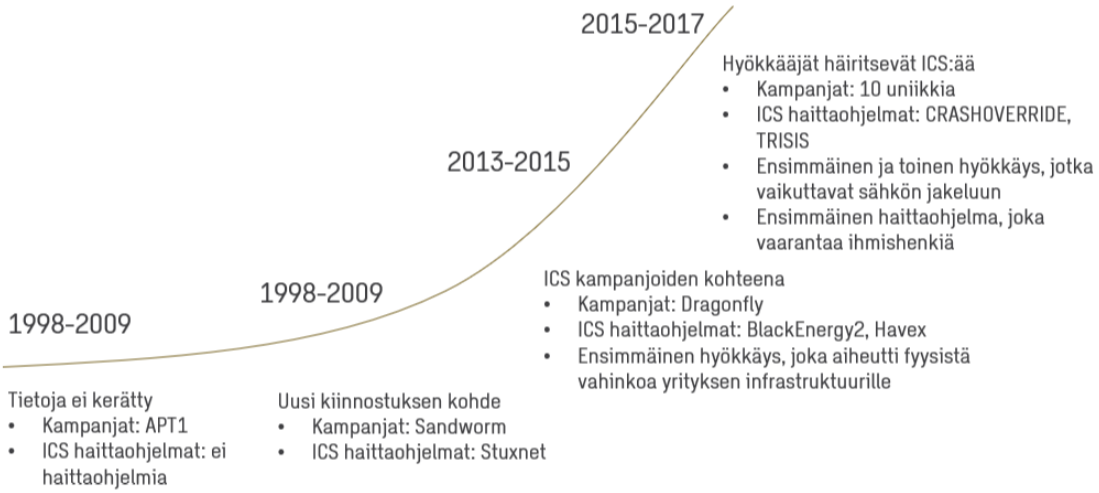
vallisesti, mikäli raja-arvot saavutetaan. Näin vältytään isommilta vahingoilta vikatilanteen sattuessa. Kyberhyökkäyksestä riippuen voi olla tarkoitus muuttaa prosessien toimivuutta tai esimerkiksi muuttaa raja-arvot niin, että prosessi tuhoutuu täysin. Toki tämmöinen hyökkäys vaatii paljon resursseja, mutta on mahdollinen. Tämän takia tulisi riskiarvioissa huomioida myös kyberuhat, jotta prosessi muutoksilta sekä suurilta vahingoilta vältytään. Esimerkkinä tämmöisistä prosessimuutoshyökkäyksistä on Stuxnet ja Triton/Trisis.

Stuxnet

Kun Stuxnet löydettiin 2010, oli se täysin uudenlainen ja erilainen kyberhyökkäys kuin mikään aikaisempi. Se tunkeutui vai tietynlaisiin Siemensin ohjausjärjestelmiin ja tarkasti ohjauksen perässä olevat laitteet; jos laitteet eivät olleet oikeat, ei haitallinen koodi tehnyt mitään. Tässä tapauksessa laite etsi uraaniin rikastamiseen liittyviä laitteita eli sentrifugeja ja pyrki muuttamaan niiden pyörimisnopeutta niin, että ne tärinän takia tuhoavat itsensä. Tarkoitus oli siis hidastaa uraanin valmistusta Iranissa. Haitallinen koodi toimi vielä niin, että se osasi näyttää kaiken olevan kunnossa prosessin valvomossa. Tämä täysin edistyksille haittakoodi avasikin teollisuuden silmiä, että kyberuhat ovat todellinen riski toiminnalle. [7.]

Triton/Trisis

Trisis -hyökkäys oli kohdennettu nimenomaan turva-automaatiota ohjaavaan laitteeseen nimeltä Triconex, joka on Schneider Electricin valmistama, ja se löydettiin vuonna 2017. Turva-automaation tarkoitus on ajaa tehdas pois tuotannosta, mikäli raja-arvot prosessissa saavutetaan. Hyökkäyksen tarkoitus oli löytää semmoiset laitteet, joihin oli jätetty ohjelmointimoodi päälle. Jos laiteessa oli RUN -moodi päällä, ei sitä pysty ohjelmallisesti muuttamaan. Valinta tapahtuu avaimella tai kytkimellä ohjainten luona. Haitallinen koodi uudelleenohjelmoi laitteet ja käynnisti tehtaissa turvatoiminnot joilla saatiin Petro Rabigin tehdas ajettua pois tuotannosta. Hyökkäyksen syyksi epäillään tiedon hankintaa uusia hyökkäyksiä vastaan. [8.]



Kuva 10. Kaavio, siitä kuinka paljon hyökkäykset ovat lisääntyneet teollisuudessa [9.]

Erittäin hyvän tietoturvan toteutuminen vaatii aina investointeja yritykseltä, mutta valitettavasti täydellisen kyberturvallisuuden toteuttaminen on mahdotonta, vaikka investointeja ja rahaa laitettaisiin loputtomasti. Tämän takia pitää tiedostaa, mikä on riittävä taso turvaamaan oman toiminnan lisääntyneiltä hyökkäyksiltä. Kuvassa 10 graafisesti esitetty, kuinka paljon kyberhyökkäykset ovat lisääntyneet 2000-luvulla.

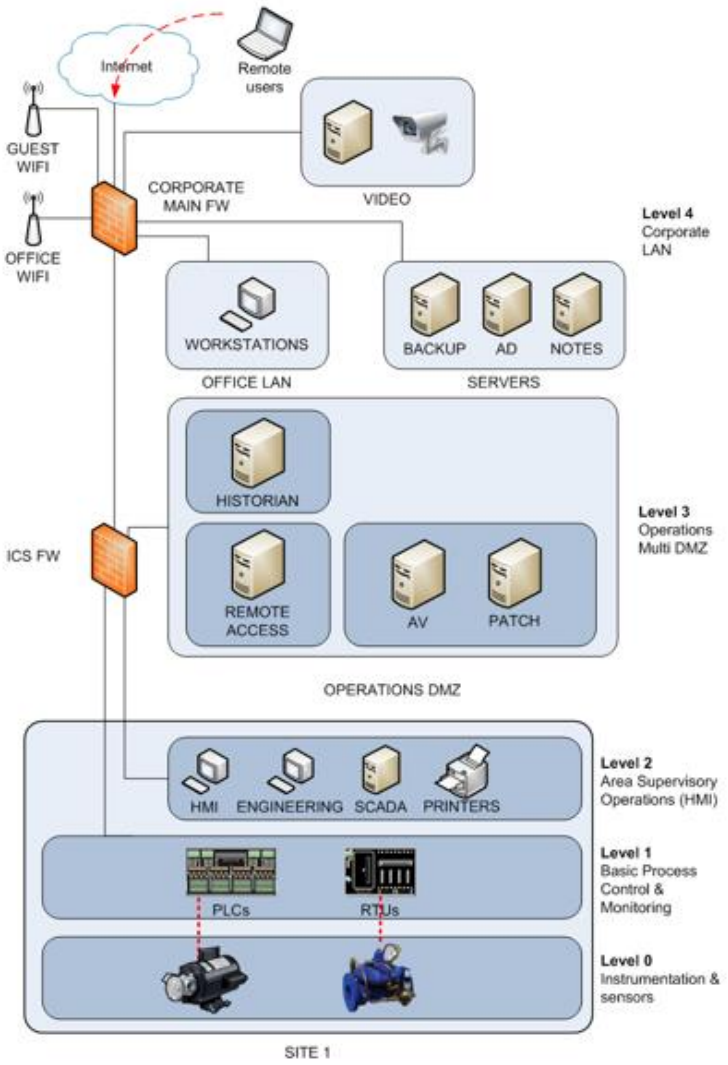
4 Arviointikohteet

Arviointikohteissa käydään läpi, miksi tietyt osa-alueet on tarkistettava ja miksi ne tekevät verkosta haavoittuvamman, mikäli niitä ei ole katsottu tietoturvan näkökulmasta. Arviointimenetelmillä ei pystytä varmistamaan, että järjestelmä tai verkko olisi murtovarma, mutta niillä todetaan, että mahdollisia heikkouksia tai aukkoja on olemassa. Yksittäiset löydökset eivät välttämättä tee verkosta heikkoa tai erittäin haavoittuvasta, mutta yhdessä monessa osassa oleva heikkous kasvattaa riskiä.

4.1 Verkkoarkkitehtuuri

Verkon hyvä rakenne on yksi suurimmista tekijöistä yrityksen suojaamiseksi tietoturva uhilta. Verkon segmentointi on pohja muulle tietoturvalle. Jos perustukset eivät ole kunnossa, ei muista toimenpiteistä saada yhtä hyvää hyötyä. Segmentoinnin tarkoituksena

on jaotella verkko osiin (segmentteihin). Segmenttien välistä tietoliikennettä rajoitetaan vain tarvittaviin yhteyksiin ja mahdollisesti tarkkailaan normaalista poikkeavaa liikennettä. Segmenttien välistä liikennettä rajoitetaan myös palomuurein sekä nykyään aktiivisilla verkkoliikenneseurantatyökaluilla, joista saadaan automatisoituja hälytyksiä tarvittaessa esimerkiksi jo tunnettujen hyökkäyksien ja niiden työkalujen aiheuttama tietoliikenne. Verkon eri segmenteillä hidastetaan haittaohjelman pääsemistä verkkoon ja mahdollista leviämistä kaikkiin verkon osiin sekä pystytään rajaamaan alueita tarvittaessa pois verkosta ilman, että koko tehdasta täytyy ajaa alas tuotannosta. Myös vahingon mahdollisuus poistetaan, koska segmentistä toiseen siirtymiseen tarvitaan käyttöoikeuksia, joita ei yleensä anneta kuin niille, jotka oikeuksia tarvitsevat. Tai kirjautuminen eri segmenteille mahdollistetaan vain tietyiltä koneilta. Kuva 11 on selventävä malli eri verkkoalueista.



Kuva 11. Esimerkki verkkotasoista ja hyvästä verkkoarkkitehtuurista.

Eri verkkoalueet luodaan helpottamaan ylläpitoa ja lisäämään tietoturvaa. Alueiden välissä olevat palomuurit suodattavat ja reitittävät liikenteen sääntöjen mukaisesti segmenteiltä toiselle.

Palomuuri on verkon suojaukseen tarkoitettu, ja se on ohjelmallisesti toteutettu laitteeseen. Palomuurin avulla estetään suora liikenne ulkoisesta verkosta tehtaan sisäiseen verkkoon. Palomuuri kerää lokitiedostoa kaikista yrityksistä kirjautua tuotantolaitoksen verkkoon ja siihen pystytään asettamaan hälytyksiä. Lokitiedoista nähdään myös, mistä IP-osoitteista tehtaaseen yritetään ottaa yhteyttä ja epämääräiset tai ei-haluttu liikenne estetään. Palomuurien on tarkoitus myös suodattaa sisäverkon liikennettä ja suojata verkon eri osia. Palomuurisäännöillä määritellään aina, mitä liikennettä saa kulkea eri verkkoalueiden välillä. Säännöt tai muutokset tulisi aina hyväksyttää ja tarkistaa verkosta vastaavalla henkilöllä. Palomuuriensäännöt pitäisi olla hyvän toimintatavan mukaisesti dokumentoitu sekä niistä tulisi selvitä, kuka palomuureja ylläpitää. Muutoksen hallinta olisi ehdottoman tärkeää. Sääntöjäkin voidaan konfiguroida väärin. Koska säännöt luetaan järjestyksessä, on mahdollista toisella säännöllä kumota aikaisempi ehto. Näitä väärin konfiguroituja sääntöjä hyökkäyksissä käytetään hyödyksi tai vastaavasti yritetään lisätä omia sääntöjä avaamaan liikennettä. Tämä aiheuttaa yleensä mahdollisia yhteysongelmia tai ei sallittua liikennettä väärän osoitteeseen.

Operatiivinen DMZ lisätään verkkoon estämään suorat yhteydet prosessiverkkoon. DMZ-tasolle yleensä sijoitetaan etäyhteyspalvelin. Sitä käytetään muun muassa etäyhteyksien luomiseen prosessitasolle, jotka tulevat sisäverkon ulkopuolelta. Etäyhteyspalvelimeen otetaan ensin yhteyttä ja kirjaudutaan sisään ja sitten otetaan erillinen yhteys prosessiverkkoon. Kaikki tiedot, joita prosessista tarvitaan esimerkiksi tuotannonohjauksissa, prosessin analysoinnissa tai historia tietoja, pyritään siirtämään prosessiverkosta automaatioverkon DMZ-palvelimille, mistä tiedot voidaan noutaa ilman yhteyttä prosessiverkkoon, näin vältytään ylimääräiseltä liikenteeltä kriittisen segmentin osiin. Päivityspaketit voidaan ajaa myös DMZ:n kautta, jos ne ovat sallittuja. Uudemmissa verkoissa on automaatiolaitetoimittajilla oma päivityspalvelin, joka kattaa vain heidän toimittamansa laitteet, joten muiden toimittamiin laitteisiin ja tietokoneisiin tarvitsee ajaa päivitykset erikseen tai rakentaa erillinen palvelin muiden toimittamia laitteita varten, jos sellainen on mahdollista. Yleensä tämmöinen järjestely on huomattavan kallis vanhoihin järjestelmiin verrattuna, joten on kustannustehokkaampaa ajaa päivitykset manuaalisesti järjestelmiin suoraan sisäverkosta.

Tuotantoverkko tarkoittaa tehtaan prosessiverkkoa. Prosessiverkko pitää sisällään kaikki prosessia ohjaavat laitteet ja tietokoneet sekä niiden hallintapaneelit. Tämä osio verkosta on todella kriittinen ja se pidetäänkin muusta verkosta erillään ja itsenäisenä.

4.2 Langattomat verkot

Langattomat verkot ovat yleistyneet myös teollisuudessa, ja se luo aina mahdollisen uuden tietoturvauhan yrityksen verkkoon. Langattomia verkkoja käytetään vielä vähän tehdasohjauksessa, koska ne eivät kata vaatimuksia datansiirtonopeuksien ja varmuuden takia, mutta esimerkiksi tiedon siirtoon ja ei -kriittisissä osissa langattomuutta käytetään paljonkin hyödyksi. Uhka muodostuu usein siinä vaiheessa, kun sisäverkkoon asennetaan ylimääräisiä tukiasemia, joihin saadaan ulkoverkosta suoraan yhteyksiä eikä näitä verkkoja ole määritelty verkkorakenteessa tai niistä ei olla tietoisia.

Langattomien verkkojen salaustavat muodostavat myös riskin yritykselle. Langattomien verkkojen salaustapoja on WEP, WAP ja WAP2, ja onkin yleisessä tiedossa, että eri tekniikat ovat vahvuuksiltaan huonompia kuin toiset. Salauksen ollessa huono pystytään se murtamaan käyttämällä esimerkiksi työkalua Aircrack-ng ja mahdollisesti kuuntelemaan liikennettä sekä näin keräämään kriittistä dataa yrityksestä ja sen toiminnasta. Tehtaalle langattomien verkkojen selvittäminen on tärkeää, ettei ylimääräisiä ole asennettu ja löydettyjä verkkoja pystytään vertaamaan yrityksen omaan listaan, mikäli semmoinen on toteutettu. Ylimääräiset verkot tulisi paikantaa, ymmärtää, miksi ne ovat tehdasalueella ja mihin verkon osaan se kytkeytyy.

WEP On kehitetty vuonna 1999 ja on erittäin paljon haavoittuvuuksia sisältävä langattoman verkon salaustapa. Vaikka korjausmuutoksia ja päivityksiä on tehty, tulisi se silti poistaa käytöstä ja päivittää toiseen salaustapaan. WEP -salaus on virallisesti poistettu salauskäytännöistä vuonna 2004. [10.]

WPA kehitettiin paikkaamaan WEP-salaus. WPA oli merkittävä parannus salaukseen. Salaustapa kehitettiin niin, että päivityksillä voidaan WEP-salausta päivittää parempaan, yhteensopivuuden takia jäi siihen huomattavia riskejä ja aukkoja eli WPA on myös hyökkäyksille altis ja murrettavissa. [10.]

802.11 turvastandardipohjainen *WPA2*-protokolla otettiin käyttöön vuonna 2004. WPA2 käyttää AES-tekniikkaa mikä on suuri parannus WPA:han ja WEP:iin verrattuna. On

mahdollista myös luoda hyökkäyksiä, vaikka käyttäisikin WPA2-salausta. Hyökkäys voidaan toteuttaa WPS:n kautta. Samaa hyökkäys tekniikkaa voidaan käyttää WPA-salattuihin verkkoihin. Hyökkäysaika on toki kohtuullisen pitkä 2–14 tuntia. WPS tulisi tukiasemista poistaa käytöstä, mikäli tämä mahdollisuus halutaan poistaa. Paras tapa suojata langaton verkko on käyttää nimenomaan WPA2 +AES -salausta. [10.]

4.3 Hallinnollinen tietoturva ja prosessit

Koko organisaatiossa pitää olla tieto siitä, miten yrityksen tietoturvaa toteutetaan. Tästä syystä luodaan prosessit. Prosessit auttavat tietoturvan toteutumista koko organisaatiossa. IEC62443-standardi onkin luotu nimenomaan ohjeistamaan teollisuuden tietoturvaa ja siihen liittyviä asioita. Hallinnollisen tietoturvan toteutuminen on ehdottoman tärkeää ja sen takia pitäisi nimetä dokumenttien ja prosessien hallintaan tietyt henkilöt ja niille varahenkilöt. Näin pystytään varmistamaan, että tietoturvakäytännöt ja ohjeet pysyvät ajan tasalla. Yleisesti onkin ongelmaksi kasautunut se, että vastuuhenkilöt puuttuvat.

Seuraavanlaiset asiat tulisi suorittaa ja dokumentoida [11]:

- nykytilan kartoitus
- riskienhallinta
- tietoturvakäytännöt ja politiikat
- erillinen tietoturvaohje yritykselle
- toiminnan jatkuvuuden hallinta ja suunnitelma
- henkilöstön tietoturvakoulutukset.

4.4 Fyysinen turvallisuus

Fyysinen turvallisuus tarkoittaa yritykselle fyysistä tapaa suojata tehdasta ja sen tietoliikenneverkkoa mahdollisilta haitoilta. Fyysinen turvallisuus on tehtaan aidat, kulkulupien hallintaa/seurantaa, ovien valvontaa, kameravalvontaa, lukituksia estämään verkkoon kytkeytyminen ilman avainta tai lupaa, hidastaminen tai että kukaan tuntematon ei pääse käsiksi vahingossa tai tarkoituksella esimerkiksi palvelinhuoneisiin ilman tietynlaisen pro-

sessin läpi käyntiä tai valvontaa. Fyysinen turvallisuus on suuressa roolissa myös kasvattamaan tuotantolaitoksen tietoturvaa. Fyysinen turvallisuus kattaa koko tuotantolaitoksen, ja sillä pyritään estämään yrityksen tietoja mahdollinen tuhoutuminen, vahingoittuminen tai vääriin käsiin joutuminen. Fyysinen turvallisuus takaa yritykselle turvallisen toimintaympäristön tietojen käsittelyyn. Eri alueet tulisi arvioida ja tarkastella minkä tasoiset suojaukset tulisi kyseiselle alueelle laittaa, että ei päädytä ylisuojaamaan tai alisuojaamaan alueita/tiloja. Palvelin- ja automaatiohuoneet sekä muut kriittiset kohteet tulee suojata vähintään varkauksilta, tulipalolta tai liialliselta lämpötilan nousulta, vedeltä, kosteudelta, sähköhäiriöiltä ja pölyltä. [12.]

Kriittistä dataa ei haluta menettää missään tilanteissa, on kyseessä sitten verkkohyökkäys tai niinkin tavallinen asia kuin tulipalo. Palvelinhuoneet sekä automaatiohuoneet tulisi suojata palolta erittäin hyvin savu- ja lämpötila-antureilla. Myös järjestelmän säännölliset tarkastukset ja testaukset pitäisi dokumentoida. Kun sähkölaitteet, palvelimet, automaatiologiikat, näytöt yms. vaurioituvat vedestä pahasti, on mahdollista käyttää muita sammutusmuotoja esimerkiksi kaasusammutusjärjestelmää, missä kaasua käytetään syrjäyttämään huoneessa oleva happi. Tämä sammutusmuoto on vain huomattavasti kalliimpi kuin normaali vesisammutusjärjestelmä. Hinnan takia se sijoitetaan usein vain kriittisiin kohteisiin ja muut kohteet tehtaasta toteutetaan vedellä, jos säädökset ja standardit sallivat sen. [12.]

Kaikki tilat tehtaassa sekä ympäristö sen ympäristö tulisi arvioida, että vesivahingolta suojaus pystytään toteuttamaan heti suunnittelun alkuvaiheessa eikä ylimääräisiä kustannuksia synny sen rakentamisesta jälkeenpäin. Automaatio- ja palvelinhuoneet on myös syytä kahdentaa ja sijoittaa fyysisesti eri lokaatioihin tehtaassa. Vaikka toinen tuhoutuisikin, pystytään tehdasta edelleen ajamaan tai se pystytään pysäyttämään turvallisesti. Veden kertymistä kriittisiin tiloihin tulisi välttää viemällä vesilinjat muuta kautta tai jos se ei ole mahdollista, niin ohjataan tiloihin mahdollisesti kertyvä vesi pois suunnitellusti. Palvelinhuoneet ja automaatio-ohjauslaitteet tulisi sijoittaa aina maatasoa korkeammalle esimerkiksi toiseen kerrokseen, että mahdolliset tulvat tai muuten noussut vesi ei heti saavuta kriittistä osaa tehtaasta. Jos sijoitus ylempiin kerroksiin ei ole mahdollista, tulee huoneissa olla korotettu lattia, joka antaa edes osittaisen suojan veden kertymistä vastaan. [12.]

Automaatiolaitteet ja palvelimet sekä muut sähkölaitteet tulisi sijoittaa myös pölyltä suojaan ja pyrkiä estämään pölyn kertyminen paikkoihin. Tämä aiheuttaa aina palokuormaa

sekä laitteiden vaurioitumista. Laitteita voidaan sijoittaa kaappeihin tai asennuskoteloihin, mitkä ovat suojattu tietylle tasolle. Suojauksia on eritasoisia ja yli- tai alisuojaaminen tuottaa myös todella paljon lisäkuluja, mikä ei ole suotavaa. Näin ollen alueen haitat tulisi arvioida pölyn, kaasun, roiskeiden tai räjähdyksen varalta ja suojata laitteet oikealla tavalla. Tällä hyödytään se, että tietojen menetysriski pienenee ja laitteiden käyttöikä kasvaa huomattavasti, eli samalla kustannukset pysyvät alempana. [12.]

Kaikki laitteet toimivat sähköllä, ja ne pitää olla koko ajan tavoitettavissa tai ohjattavissa tarvitsee laitteet suojata sähköhäiriöiltä. Jos häiriöitä tai sähkökatkoksia ilmenee, lisätään verkkoon akustoja tai generaattoreita pitämään yllä kriittisiä toimintoja. Myös ylijännitepiikeiltä on syytä suojautua. [12.]

Valvontajärjestelmän tulisi kattaa koko kohde niin, että jokainen kulkija voidaan tunnistaa, kun sinne saavutaan. Kriittisten kohteiden oviin tulisi asentaa lukot, jotka vaativat tunnisteen ja kameravalvonta lisäksi, että voidaan varmentaa kulkija. Kameravalvonnan tulisi kattaa koko tehdas niin, että sillä pystytään seuraamaan tarvittaessa tehtyjä liikkeitä sekä tallentaa historiatietoja kameravalvonnasta tarpeeksi pitkältä ajalta, että voidaan tutkia tietoja vielä jälkeenpäin. Yksityisyydensuoja pitää kuitenkin muistaa, eli kaikkialle kameravalvontaa ei voida asentaa. [12.]

4.5 Verkkoliikenteen analysointi prosessiverkkoon

Tietoliikenne ja automaatioverkko sisältää monia erilaisia tiedonsiirtoprotokollia, ja kaikkiin tiedonsiirtomuotoihin tehtaassa on mahdollista yhdistää saastunutta tai ei -haluttua liikennettä. Kriittisin hyökkäys on, jos tehtaan turvalaitteistoihin tai turva-automaatioon päästään lisäämään tai muuttamaan käskyjä. Tämän tapaiset hyökkäykset voivat aiheuttaa todella suurta haittaa tehtaalle, mikäli turvajärjestelmät eivät toimi niin kuin niiden kuuluisi.

Liikenteen analysointi tehdasverkkoon auttaa ymmärtämään, mitä liikennettä ja kuinka paljon sitä liikkuu verkon osissa. Moni verkkolaitetoimittaja tarjoaakin nykyään ratkaisuja jatkuvaan seurantaan ja niistä saadun datan analysointiin. Tämmöiset ovat toivottuja, kun uusitaan verkkoja tai rakennetaan täysin uutta kohdetta. Liikenteen analysoinnilla päästään käsiksi, jos verkossa kulkee liikennettä osoitteisiin, minne sitä ei ole määritelty. Mikäli ei -toivottua liikennettä, kirjautumisyrityksiä tai muutoksia ilmenee, pystytään se automaattisilla hälytyksillä ja rajoituksilla tuomaan nopeasti verkon ylläpitäjien tietoon ja eristys tapahtuu nopeasti ja suuremmilta ongelmilta mahdollisesti vältytään.

Automaattiset verkkoanalysaattorit ovat vasta tulossa tehdasympäristöihin, joten analysointi voidaan myös toteuttaa yksittäisestä kohdasta keräämällä liikennenäytteitä sekä analysoimalla se käsin. Edellä mainittua toimintatapaa voidaan käyttää tiettyjen kohtien tarkasteluun tai vanhemmissa verkkoympäristöissä, mihin ei ole vielä toteutettu seurantaa. Tietylle ajanjaksolle ajoitetussa näytteenotossa näkyy valitettavasti vain, mikäli epäsuotuisa liikenne on juuri silloin aktiivinen, joten tiettyjä paketteja voi jäädä saamatta. Haittaohjelmat tai muut häiriötekijät voivat aktivoitua vain tietyssä vaiheessa tai aikamääritteisesti. Tämän takia näytteenottoaika on suotavaa pyrkiä pitämään niin pitkänä, että tuotannon kaikki vaiheet olisi käyty läpi, eli pyritään samaan kaikista vaiheista liikennöintiä talteen.

4.6 Työasemien ja palvelinten turvallisuus

Vaikka operatiivisen teollisuusverkon pitäisi olla suljettu pois muusta verkosta, voi kuitenkin sisäverkon palvelimet ja työasemat olla konfiguroitu väärin tai ne ovat väärässä verkossa. Kun suljettuun teollisuusverkkoon lisätään laitteita, pitäisi kaikille olla aina samanlaiset prosessit, että vahingon tai unohduksen mahdollisuus pyritään pienentämään mahdollisimman pieneksi sekä pystytään olemaan myös varmoja, että kaikki laitteet ovat tietoturvakonfiguraatioiden osalta samalla tasolla.

Työasemat ja palvelimet tulisi tarkistaa säännöllisesti, vaikka automaatioverkko on erillinen. Niissä tulisi olla myös virustorjunta asennettuna sekä päivitettynä, koska haittaohjelmia voi myös tulla siirrettävien muistien mukana suljettuun verkkoon. Ongelmaksi yleensä muodostuu se, että verkkoon ei pystytä ajamaan päivityksiä mahdollisten vanhanaikaisen teknologian takia, mikä ei tue uusia päivityksiä. Vaikka tuki olisikin, päivityksiä ei yleensä ajeta automaattisesti tai jos sellainen halutaan toteuttaa, on se erittäin kallista, kun uusittavaksi tulisi suurin osa verkosta. Teollisuusympäristöissä on vielä paljon tietokoneita ja palvelimia, joihin on asennettuna käyttöjärjestelmä, joihin toimittajan tarjoama tuki on päättynyt ja tietoturvapäivityksiä ei julkaista. Päivityksissä on yleensä parannuksia niin suorituskykyyn kuin paikattuja tietoturvauhkia, joten niiden huomattava myöhästyminen tai kokonaan puuttuminen nostaa riskiä saada verkkoon mahdollisia häiriötekijöitä. Vanhojen tietoturva-aukkojen käyttö kyberhyökkääjille on kohtuullisen helppoa, joten muut verkon turvallisuustekijöiden pitää olla kunnossa ja pystyä estämään hyökkäys, ennen kuin se saavuttaa mahdollisia vanhentuneita palvelimia tai tietokoneita automaatioverkosta, jos niitä on vielä käytössä.

4.7 Tiedonkeruu julkisista lähteistä

Tiedot, joita yritys halutaan näyttää ulospäin internetin suuntaa, tulisi miettiä tarkkaan sekä arvioida niiden mahdolliset yhteisvaikutukset. Mitä suurempi määrä tietoa yrityksestä tai työntekijöistä annetaan saataville, pystytään niitä mahdollisesti hyödyntämään kyberhyökkäyksissä. Testauksessa pyritään keräämään mahdollisimman paljon tietoja yrityksestä julkisista lähteistä, minkä jälkeen käydään läpi, mitä niillä mahdollisesti pystyisi tekemään, esimerkiksi esiintymään yrityksen henkilönä tai arvaamaan yrityksen tunnuksia tietojen perusteella.

4.8 Ulkoinen haavoittuvuustestaus

Haavoittuvuustestaus kohdennetaan koko organisaation palveluihin, ja työkalujen avulla pyritään löytämään ulkoisia haavoittuvuuksia, joita hyväksikäyttäen mahdollisesti päästään yrityksen verkkoon. Ulkoiset testaukset tehdään ilman yrityksen tunnuksia, että laajuus ei kasva liian suureksi. Työssä käytetään porttiskannausmenetelmää. Sillä saadaan selville internetiin näkyvät palvelut ja avoimet portit. Porttiskannaukseen voidaan käyttää esimerkiksi Nmap-nimistä ohjelmaa. Ylimääräiset palvelut voidaan tämän perusteella poistaa näkyvistä eli pienennetään hyökkääjän kohteita. Palveluille, jotka jätetään ulkoverkkoon näkyviin, suoritetaan haavoittuvuusskannaus käyttämällä esimerkiksi Nessus-ohjelmaa ja pyritään löytämään tunnettuja haavoittuvuuksia. Löydettyjä haavoittuvuuksia voidaan käyttää mahdollisessa tietomurrossa. Tämä takia ulkoverkkoon näkyvät palvelut tulisi jättää mahdollisimman vähäisiksi.

4.9 Toimistoverkon haavoittuvuustestaus

Toimistoverkon haavoittuvuustestauksessa selvitetään toimistoverkon teknisen tietoturvan tilanne. Yrityksen toimistoverkko on aina kiinni internetissä, ja sieltä on yleensä yhteyksiä automaatioverkkoon, minkä takia se on yleensä ensimmäinen hyökkäyksen kohde. Toimistoverkossa palveluiden määrä on suuri, ja näin ollen haavoittuvuuksien määrä on suurempi. Ihmisten toiminta vaikuttaa myös suuresti tietoturvaan. Tämän takia hyökkäykset yleensä onnistuvatkin parhaiten toimistoverkon kautta nimenomaan ihmisen aiheuttaman vahingon kautta. Vahinkoja voi olla esimerkiksi epämääräisten sivustojen avaaminen tai ei tunnettujen liitteiden avaaminen. Tarkastuksessa tulisi myös tarkis-

taa, kuinka hyvin erilaiset sähköposti- ja web-suodattimet toimivat, että vahingon mahdollisuus saadaan tarpeeksi pieneksi. Tekninen haavoittuvuusskannaus voidaan suorittaa esimerkiksi Nessus-ohjelmalla. Sisäverkonskannaus vaatii yrityksen tunnukset, että saadaan kokonaisvaltainen kuva verkossa olevista palveluista ja laitteista sekä niiden haavoittuvuuksista. Haavoittuvuuksia voi olla esimerkiksi väärin konfiguroidut laitteet tai vanhentuneet päivitykset.

4.10 Jatkuvuussuunnittelu ja poikkeama hallinta

Yrityksen jatkuvuussuunnittelun ja poikkeamahallinnan tulisi kattaa myös tietoturva. Jatkuvuussuunnittelussa otetaan huomioon yrityksen toimintaympäristö ja siihen liittyvät riskit. Jatkuvuussuunnittelussa käydään läpi yrityksen varautumisen taso, valmiussuunnitelma, toipumissuunnitelma, toipumisaika, häiriötilanteet ja erilaisten häiriötilanteiden haittavaikutukset. Mikäli suunnitelmia ei ole tehty, toteutetaan ja/tai päivitetään nykyiset kattamaan myös tietoturva.

4.11 Automaatiolaitteiden tietoturvatestaus

Tarkempi laitteiden tietoturvatestaus voidaan toteuttaa, mikäli sille on tarvetta ja siihen saadaan lupa. Tarpeen yleensä määrittelee se, pystytäänkö laite suojaamaan tarpeeksi hyvin jo muilla toimenpiteillä. Laitteen testaus riippuu täysin siitä, minkälaisia yhteyksiä tai verkkorajapintoja laite käyttää. Tietoturvatestauksessa tehdään laitteeseen liittyvät verkkorajapintatestaukset, kuormitustestit, ohjelmiston testaus ja tarkastus. Laitteiden ohjeet ja käytännöt tulisi käydä läpi ja katsoa, onko niillä merkitystä tietoturvan osalta.

5 Tietoturva-arvioinnin hyödyt

Tietoturva-arvioinnit toteutetaan tiiviissä yhteistyössä tehtaan työntekijöiden ja johdon kanssa. Näin asiakasyritys pystyy seuraamaan, mitä arvioinnissa tapahtuu ja lisäämään arvioinnin aikana tietoa omasta verkosta. Työntekijöiden parempi tietämys verkosta ja sen toiminnasta on suora hyöty yritykselle. Verkonkuva selkeentyy työntekijöille paljon arvioinnin aikana sekä pystytään käymään läpi heikot kohdat ja se miksi ne ovat heikkouksia. Tietoturvan ymmärrys paranee ja jatkossa uusien verkkolisäyksien tai muutoksien tekeminen helpottuu. Arvioinnin hyödyt yleensä konkretisoituvat vasta arvioinnin lopussa, kun on saatu täysi käsitys verkosta ja sen toiminnasta sekä siinä olevista laitteista. Asiakas saa kattavan raportin, jossa on eritelty kaikki löydökset ja ne on lajiteltu

vaarallisuusasteikolla HIGH, MEDIUM, LOW JA INFO. Löydöksille annetaan myös arvio kuinka suuria tai vaikeita ne ovat paikata tai korjata asteikolla EASY, RELATIVELY EASY, MEDIUM, HARD. Kuva 12 on leike asiakkaalle toimitettavasta tietoturvaraportista.

Viite	Nimi	Riski	Korjaustoimen vaikeus	Kohde	Kuvaus ja suositus
1		HIGH MEDIUM LOW INFO	HARD MEDIUM RELATIVELY EASY EASY		**Havainto:** **Suositus:**

Kuva 12. Leike asiakkaalle tuotettavasta raportista.

Risk classification	Description
Info	An info risk may have an indirect impact on the company's business processes. In contrast, it may just indicate a nice-to-have feature.
Low	A low risk may affect the company's business processes. The low risk may also enable exploitation of other, higher level, issues.
Medium	With a medium risk, a serious disruption is possible in company's business processes. The medium risk may also indicate a serious inadequacy.
High	A high risk introduces a major business continuity issue.

Kuva 13. Riskiluokitustaulukko. [13.]

Mikäli verkon taso on todella huonolla tasolla, voivat investoinnit tulla hyvinkin hintaviksi. Asiakas pystyy raportista heti huomaamaan, mihin mahdollisia lisäyksiä tai muutoksia tarvitaan sekä laskemaan niille kustannukset. Kaikkia kohtia ei ole syytäkään korjata, koska hinta voi riskiin nähden nousta liian korkeaksi. Mutta pitää olla ymmärrys ja tiedostaa asia, että yksittäinen riski voidaan ottaa.

6 Yhteenveto

Opinnäytetyön tavoitteena oli kartoittaa ja luoda uusi tietoturva-arviointi palvelu Sweco industry Oy:lle. Tietoa teollisuuden tietoturvasta löytyi internetin hakukoneilla paljon, joten oikean tiedon löytäminen ja asiaan perehtyminen ei ollut ongelmana. Tietoa on myös kerryttänyt omat kokemukset aikaisemmasta työpaikasta, missä samanlaisia tarkastuksia tehtiin useampi.

Lopputuloksena saatiin kehitettyä asiakkaita varten palvelu, jossa tarkastellaan tehtaita tai muita teollisuuden toimintaympäristöjä tietoturvan näkökulmasta. Opinnäytetyössä esitellyt arviointikohteet ja -menetelmät on havaittu hyviksi aikaisemmista kokemuksista. Sweco Industrylle uuden palvelun kehitys tarkoitti myös sisäisiä koulutuksia, että yrityksen tietoturvaymmärrys saadaan samalle tasolle ja kaikille tieto uudesta palvelusta. Palvelu on tällä hetkellä valmis ja tietoisuuden vieminen organisaatioon on käynnissä. Asiakkaita on kontaktoitu ja heille on kerrottu uudesta palvelusta.

Lähteet

1. Industry 4.0, 2016. Verkkoaineisto. European Parliament, Policy department A: Economic and Scientific policy. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf. Luettu 21.11.2019.

2. IEC/TR 61511-0:2018:fi 2018 Helsinki SESKO ry.

3. Tietoa Swecosta 2019. Verkkoaineisto. Sweco Oy. https://www.sweco.fi/tietoa-swecosta/. Luettu 5.8.2019.

4. SCADA system layout 2019. Verkkoaineisto. https://rtidds.files.wordpress.com/2014/06/genericscadasystem.png. Luettu 1.11.2019.

5. Hallittava kytkin. 2019 Verkkoaineisto. BLACK BOX. https://www.blackbox.fi/fi-fi/page/26237/Resurssit/Tekniset-resurssit/Seikkaper%C3%A4iset%20selvityksset%20tekniikoista,%20termeist%C3%A4%20ja%20kytkenn%C3%B6ist%C3%A4./lan/erot-eihallittavien-hallittavien-ja-websmart-kytkinten-vlill. Luettu 24.11.2019.

6. D.Knapp Eric, Langlill Joel Thomas 2015. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and other Industrial Control Systems. Second editon. Elsevier Inc.

7. The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010. Verkkoaineisto. Congressional Research Service. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf. Luettu 14.11.2019.

8. TRITON/TRISIS fact sheet 2019 Verkkoaineisto PAS Global. https://cyber.pas.com/CyberIntegrity/media/Assets/Fact-Sheet-Cyber-Integrity-Triton-Trisis-Attack.pdf. Luettu 1.11.2019.

9. Dragos, RSA conference 2019. Verkkoaineisto. RSA Conference. https://www.youtube.com/watch?v=d__kbd-wlSQ. Luettu 10.11.2019.

10. Wireless Security Protocols: WEP, WPA, WPA2, and WPA3 2019. Verkkoaineisto. NetSpot. https://www.netspotapp.com/wifi-encryption-and-security.html. Luettu 1.11.2019.

11. Laakso, Matti 2010 PK-yrityksen tietoturvasuunnitelman laatiminen Opinnäytetyö. https://tietojesiturvaksi.fi/tietoturvasuunnitelma/hallinnollinen-tietoturva. Luettu 14.11.2019.

12. Fyysinen turvallisuus 2009 Verkkoaineisto Valtiovarainministeriö. https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus1. Luettu 12.10.2019.

13. OWASP Risk Rating Methodology 2019. Verkkoaineisto. OWASP. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. Luettu 8.9.2019.