Haanpää Kimmo

IEC 62443 -standardisarjan soveltaminen teollisuuden kyberturvallisuudessa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

12.2.2024

Tiivistelmä

Tekijä:	Kimmo Haanpää
Otsikko:	IEC 62443 -standardisarjan soveltaminen teollisuuden kyberturvallisuudessa
Sivumäärä:	64 sivua
Aika:	12.2.2024
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Monimuoto-opiskelu
Ohjaajat:	Vastuuarvioija Janne Salonen

Insinöörityössä tutustutaan IEC 62443 -standardisarjaan. Standardisarja keskittyy automaatio- ja ohjausjärjestelmien kyberturvallisuuteen. Työssä käydään läpi standardin neljä kategoriaa, jotka kattavat sekä tekniset että prosessipohjaiset näkökulmat kyberturvallisuuteen.

Työssä esitellään standardisarjan teknisiä liitteitä, jotka määrittelevät eri osapuolten roolit, vastuut ja vaatimukset kyberturvallisuuden varmistamiseksi. Lisäksi työssä perehdytään standardisarjan keskeisiin käsitteisiin ja määritelmiin, kuten turvallisuuden taso, turvallisuuden elinkaari ja turvallisuuden hallinta.

Työssä annetaan myös karkea kuvaus standardisarjan käyttämistä malleista ja prosesseista, kuten riskiperusteisesta lähestymistavasta sekä turvallisuuden suunnittelusta. Työn tavoitteena on lisätä lukijan ymmärrystä ja osaamista teollisuuden automaatio- ja ohjausjärjestelmien kyberturvallisuudesta ja sen merkityksestä eri teollisuudenaloilla. Työ perustuu IEC 62443 -standardisarjan dokumentteihin.

Työn luettuaan lukija pystyy syventämään tietämystään standardisarjan periaatteista ja soveltamisesta käytännössä, erityisesti automaatio- ja ohjausjärjestelmien turvallisuuden näkökulmasta.

Avainsanat: IEC 62443, tietoturva, kyberturva, IACS

Abstract

Author:	Kimmo Haanpää
Title:	Application of the IEC 62443 standard series in industrial cyber security.
Number of Pages:	64 pages
Date:	12 February 2024
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Blended learning
Supervisors:	Janne Salonen, Responsible Supervisor

The thesis introduces the topic of the IEC 62443 series of standards. This series of standards focuses on the cybersecurity of automation and control systems. The work goes through four parts that cover both technical and process-based perspectives on cybersecurity.

The work presents the technical appendices of the standard series, which define the roles, responsibilities and requirements of different parties to ensure cybersecurity. In addition, the work delves into the key concepts and definitions of the standard series, such as the level of security, the life cycle of security and security management.

The work also provides a rough description of the models and processes used by the standard series, such as a risk-based approach and security design. The aim of the work is to increase the student's understanding and competence in the cybersecurity of industrial automation and control systems and its significance in various industrial sectors. The work is based on the documents of the IEC 62443 series of standards.

After reading the work, the reader is able to deepen their knowledge of the principles of the standard series and its application in practice, especially from the perspective of the security of automation and control systems.

Keywords: IEC 62443, information security, cyber security, IACS

Sisällys

Lyhenteet

BIOS: *Basic Input-Output System.* Etsii ja lataa käyttöjärjestelmän keskusmuistiin sekä käynnistää käyttöjärjestelmän tietokoneen käynnistyessä. Se hoitaa myös matalan tason kommunikoinnin tietokonelaitteiston kanssa ja laitteiston hallinnan.

COTS: *Commercial off-the-shelf*. Valmis kaupallinen laite tai ohjelmisto, joka asennetaan ostavan organisaation tarpeisiin, eikä se ole organisaation tarpeisiin räätälöity tai tilaustyönä tehty ratkaisu.

CR: *Component requirement.* IEC 62443-4-2 standardissa määritelty komponenttivaatimus (CR).

DC: *Domain controller*. Microsoft-palvelimissa toimialueen ohjain on palvelintietokone, joka vastaa suojaustodennuspyyntöihin Windows-toimialueen sisällä.

DMZ: *Demilitarized zone*. Demilitarisoitu alue tarkoittaa fyysistä tai loogista aliverkkoa, joka yhdistää organisaation oman järjestelmän turvattomampaan alueeseen, esimerkiksi Internetiin.

EDR: *Embedded device requirement.* Sulautetun järjestelmän komponentin komponenttivaatimuksen (CR) nimi.

FR: *Foundational requirement.* IEC 62443-standardisarja määrittämä seitsemän perusvaatimusta (FR) teollisuuden automaatio- ja ohjausjärjestelmälle, sen alijärjestelmälle tai komponenteille.

HDR: *Host device requirement.* Isäntälaitekomponentin komponenttivaatimuksen (CR) nimi.

IACS: *Industrial automation and control system.* Teollisuuden automaatio- ja ohjausjärjestelmä, joka varmistaa tavaroiden ja palveluiden tuotantoon ja toimitukseen liittyvien prosessien valvonnan ja ohjauksen.

IDS: *Intrusion detection system.* Tunkeilijan havaitsemisjärjestelmä on tietoverkkoon asennettava järjestelmä, joka on ohjelmoitu tunnistamaan verkkoon suuntautuvat hyökkäysyritykset.

IEC: *International Electrotechnical Commission*. Kansainvälinen sähköalan standardointiorganisaatio. IEC:n tietotekniikka-alan standardit tehdään yhteistyössä ISO-standardointiorganisaation kanssa työryhmässä nimeltä JTC1 (Joint Technical Committee).

IEC TR: *IEC/Technical Report*. Standardointijärjestö IEC:n julkaisema tekninen raportti, joka kuvaa tietyn tuotteen, palvelun tai prosessin ominaisuuksia tai suorituskykyä. TR-raportteja käytetään usein uusien teknologioiden tai innovaatioiden arvioimiseen, kun taas standardit ovat yleensä laajempia ja kattavat useita erilaisia tuotteita tai palveluita.

IoT: *Internet of things*. Esineiden internetillä tarkoitetaan järjestelmiä, jotka perustuvat teknisten laitteiden suorittamaan automaattiseen tiedonsiirtoon sekä kyseisten laitteiden etäseurantaan ja -ohjaukseen internet-verkon kautta.

IP: *Internet Protocol*. Protokolla, joka huolehtii IP-pakettien toimittamisesta perille pakettikytkentäisessä tietokoneverkossa.

ISO: *International Organization for Standardization.* Itsenäinen, ei-valtiollinen kansainvälinen standardisoimisjärjestö.

IT: *Information technology*. Informaatiotekniikka tarkoittaa tietokoneiden ja digitaalisen tietoliikenteen avulla tehtävää tietojen muokkaamista, tallennusta ja hakua.

NDR: *Network device requirement.* Verkkolaitteen komponenttivaatimuksen (CR) nimi.

OS: *Operating system.* Käyttöjärjestelmä, joka hallinnoi tietokoneen laitteisto- ja ohjelmistoresursseja sekä tarjoaa yleisiä palveluita tietokoneohjelmille.

PLC: *Programmable logic controller*. Ohjelmoitava logiikka on teollisuustietokone, jossa on erilaisia syötteitä ja lähtöjä, ja sitä käytetään teollisuuslaitteiden ohjaamiseen ja valvontaan.

RE: *Requirement enhancement.* Järjestelmävaatimukset (SR) ja komponenttivaatimukset (CR) pitävät sisällään nolla tai useamman vaatimusten parannuksen (RE), joita täyttämällä teollisuuden automaatio- ja ohjausjärjestelmä, sen alijärjestelmä tai komponentin turvatasokyvykkyys määräytyy.

SAR: *Software application requirement.* Ohjelmistosovelluskomponentin komponenttivaatimuksen (CR) nimi.

SCADA: *Supervisory Control And Data Acquisition.* Tietokonepohjainen ohjelmisto- ja laitteistokokonaisuus, jota käytetään valvomaan ja ohjaamaan laajoja hajautettuja prosesseja ja järjestelmiä teollisuudessa.

SL: *Security level.* IEC 62443-standardisarjan määrittämä turvataso luokittelee ja määrittää, kuinka hyvin teollisuuden automaatio- ja ohjausjärjestelmä, sen alijärjestelmä tai komponentti on suojattu kyberuhilta. Se voi vaihdella alhaisesta korkeaan riippuen käytetyistä turvallisuuskäytännöistä ja -tekniikoista.

SL-A: *Achieved security level.* Saavutettu turvataso on todellinen turvallisuustaso, joka järjestelmälle on saavutettu.

SL-C: *Capability security level.* Turvatasokyvykkyys ilmoittaa, millaisen turvatason teollisuuden automaatio- ja ohjausjärjestelmä, sen alijärjestelmä tai komponentit voivat tarjota oikein määritettyinä.

SL-T: *Target security level.* Tavoiteturvataso edustaa haluttua turvatasoa tietylle teollisuuden automaatio- ja ohjausjärjestelmälle, sen alijärjestelmälle tai komponentille.

SPDS: *Safety Parameter Display System.* Prosessiarvojen seurantajärjestelmä toimii apuvälineenä ohjaamohenkilöstölle, kun he arvioivat tehtaan turvatilannetta poikkeavissa tilanteissa ja hätätilanteissa.

SQL: *Structured query language*. IBM:n kehittämä standardoitu kyselykieli, jolla relaatiotietokantaan voi tehdä erilaisia hakuja, muutoksia ja lisäyksiä.

SR: *System requirements.* IEC 62443-3-2 standardissa perusvaatimus (FR) pitää sisällään järjestelmävaatimuksia (SR), joilla täytetään perusvaatimus.

SuC: *System under consideration.* Tarkasteltavana oleva järjestelmä, joka voi olla teollisuuden automaatio- ja ohjausjärjestelmä tai sen alijärjestelmä, johon sovelletaan IEC 62443-standardisarjaa.

IEC/TS: IEC/Technical Specification. Standardointijärjestö IEC:n julkaisema tekninen eritelmä. Tekninen spesifikaatio kuvaa tietyn tuotteen, palvelun tai prosessin vaatimuksia. TS-eritelmiä käytetään usein uusien teknologioiden tai innovaatioiden määrittämiseen, kun taas standardit ovat yleensä laajempia ja kattavat useita erilaisia tuotteita tai palveluita.

USB: *Universal Serial Bus*. Sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi tietokoneeseen.

1 Johdanto

Nykyään yhä useammat laitteet ovat yhdistettyinä Internetiin ja varustettuina kasvavalla määrällä toiminnallisuuksia. Laitteet keräävät ja välittävät käyttötietoja, vastaanottavat asetuksia ja päivityksiä sekä kommunikoivat muiden laitteiden kanssa, joko suoraan tai palvelimen välityksellä ja kaikki tämä tapahtuu Internetin yli. Tätä kokonaisuutta kutsutaan esineiden internetiksi (IoT). Toinen merkittävä asia on laitteiden etäseuranta ja -ohjaus. Kaikki laitteet kehittyvät kohti älykkäämpiä ratkaisuja. Tietoturva-asiantuntija Mikko Hyppönen on esittänyt oman periaatteensa tietoturvaan liittyen:

Jos laiteessa on älyä, se on myös haavoittuva. (1)

Laitteiden tietoliikenteeseen liittyvät ominaisuudet lisäävät erilaisten hyökkäysvektoreiden määrää. Kotikäytössä olevat laitteet, jotka samalla ohjaavat turvallisuuden kannalta merkittäviä järjestelmiä, voivat muodostaa turvallisuusriskejä kodin sisällä. Esimerkiksi automaattinen kodin lukitusjärjestelmä, saunan etäohjaus tai muut kodinkoneiden etäohjaustoiminnot sekä turvakamerat voivat tarjota potentiaalisia reittejä haitallisten toimintojen toteuttamiseen. Laitteiden tietoturva-arkkitehtuuri on yleensä valmistajakohtainen mikä tarkoittaa, että yksittäisen laitteen kyberturvataso voi vaihdella merkittävästi eri valmistajien välillä. Vaikka yhden IoT-laitteen kyberturva olisi suunniteltu hyvin ja käyttäjä olisi huolehtinut laitteen päivityksistä, monimutkaistuvissa laitteissa haavoittuvuuksien määrä kasvaa, koska hyökkäys voidaan toteuttaa useiden eri vaiheiden kautta. Yhden laitteen hyvä tietoturvataso ei siis yksinään riitä, vaan tarvitaan kokonaisvaltaisesti riittävä tietoturvan taso.

Teollisuuslaitteistojen osalta kohdataan samankaltaisia haasteita. Teollisuusyritykset tavoittelevat mahdollisimman korkeaa automaatiotasoa laitteistoissaan. Laitteistojen tulee olla jatkuvassa yhteydessä palvelimiin yli internetin, ja niitä on kyettävä ohjaamaan mistä tahansa päin maailmaa, ei ainoastaan laitoksen ohjauskeskuksesta. Seurauksena on, että käytössä on useita eri

käyttöjärjestelmiä, sovelluksia ja laitteistokonfiguraatioita. Tämä johtaa mahdollisten kytkeytymispintojen määrän kasvuun ja hajautumiseen.

Osassa laitteita tietoturvasuunnittelu on korkealla tasolla, toisissa suunnittelu on heikompaa. Osassa laitteita tietoturvapäivitykset on pidetty ajan tasalla, kun taas toisissa päivitykset on jätetty kokonaan tekemättä. Ero johtuu laitteiden erilaisista käyttäjistä ja laitteita ylläpitävien organisaatioiden tietoturvapolitiikasta. Eri järjestelmät ja laitteet, jotka toimivat samassa ketjussa tietoliikenneyhteyden välityksellä, voivat olla peräisin eri organisaatioista. Tämä asettaa omat haasteensa tietoturvakäytäntöjen yhdenmukaistamiselle.

Teollisuusautomaatiojärjestelmien turvallisuus perustui pitkään ajatukseen, että järjestelmät pidettiin internetistä erossa. Laitekohtaisesti ei tarvinnut asettaa erityisen korkeita tietoturvavaatimuksia, koska niiden oletettiin olevan suojassa mahdollisilta verkkohyökkäyksiltä. Laitteet olivat erillään julkisesta internetistä teollisuuslaitoksen sisäverkossa. Nykyään on kuitenkin erittäin haastavaa luoda järjestelmä, joka olisi täysin eristyksissä julkisesta internetistä. Laite, joka toimii sisäisessä suljetussa verkossa, ei käytännössä ole irrallaan internetistä, jos sisäverkossa on minkäänlaisia yhteyksiä ulkomaailmaan, riippumatta siitä, kuinka monimutkainen tai epätodennäköinen kyseinen reitti on.

F-Securen Radar-verkkoskanneri suorittaa säännöllisiä tarkastuksia, joissa se etsii verkosta 3,7 miljardin julkisen osoitteen joukosta palveluita, jotka vastaanottavat PLC-laitteiden käyttämää Modbus-liikennettä, ja laitteita, jotka mahdollistavat etäkäytön ilman sisäänkirjautumista. Joka kerta paljastuu teollisuuslaitteistoja, jotka ovat alttiina verkossa, vaikka niiden ei pitäisi olla. Näitä laitoksia ovat muun muassa metallivalssaamot, leipomot, voimalaitokset, hiihtohissit, vesilaitokset, kerrostalojen kiinteistöhuoltojärjestelmät, terästehtaat, rautateiden liikenteenohjausjärjestelmät, kauppakeskusten pannuhuoneet ja sellutehtaat. (1)

Laitteiden turvallisuus on olennainen tekijä yhteiskunnan toimivuuden kannalta, koska laitteita käytetään käytännössä kaikissa yhteiskunnallisissa toiminnoissa. Erityisen kriittisiä alueita ovat esimerkiksi energiantuotanto ja -jakelu,

ruoantuotanto ja vesihuolto. Lisäksi viranomaisten käyttämät järjestelmät ja pankkijärjestelmät ovat äärimmäisen tärkeitä yhteiskunnan toiminnan kannalta, samoin niihin liittyvät oheislaitteistot, kuten jäähdytys- ja lämmitysjärjestelmät. Vaikka oheislaitteet eivät suoraan ole osa kriittisiä järjestelmiä ovat ne olennainen osa järjestelmien toimintaa. Esimerkkinä voidaan mainita palvelinkeskusten ilmanvaihtojärjestelmät tai ydinvoimaloiden varavoimajärjestelmät. Tietoturvan näkökulmasta on olennaista tarkastella järjestelmiä kokonaisuutena kaikkine oheistoimintoineen, jotta voidaan tunnistaa kaikki laitteiston kannalta kriittiset toiminnot.

Laitteiston tai laitteen kyberturvaan liittyy myös tietoliikenteen ulkopuoliset näkökulmat, kuten laitteen sijaintiin ja tiloihin liittyvät seikat. Missä laite tai laitteisto sijaitsee? Kuka laitetta saa käyttää? Miten laitetta käytetään? Minkälaiset turvatoimet ja -käytännöt tulee ottaa huomioon laitteen läheisyydessä? Miten laitteeseen voi kytkeytyä? Toisin sanoen laitteen tietoturvaa ei voi arvioida pelkästään ohjelmiston ja tietoliikenteen näkökulmasta vaan on huomioitava myös fyysiset ja käyttöön liittyvät tekijät. Tietoturvassa huomioidaan sekä kyberturvallisuus että tietoliikenteen ja tietojärjestelmien ulkopuoliset turvallisuutta koskevat näkökulmat.

Tietoliikenneverkot, joissa tietokoneet ovat keskenään yhteydessä, muodostavat verkoston. Verkostoteoriassa korostetaan, että verkosto voi tuottaa ominaisuuksia, joita yksittäisillä solmuilla ei ole. Ilmiötä kutsutaan emergenssiksi ja se viittaa uusien ominaisuuksien, ilmiöiden tai toiminnan tasojen syntymiseen, joita ei löydy yksittäiseltä solmulta. Heikossa emergenssissä ilmiö tai toiminto voidaan johtaa yksittäisten laitteiden keskinäisistä ominaisuuksista. (2)

Vastaavalla tavalla tietoturvahaasteet ovat järjestelmätasoisia kokonaisuuksia, jotka liittyvät moniin eri alajärjestelmiin. Tämän vuoksi tietoturva ei voi olla pelkästään yksittäisen laitteen haaste vaan se koskettaa toimijoita kokonaisuutena. Koko verkoston tietoturva muodostuu kaikkien yksittäisten solmujen tietoturvasta. Teollisuuslaitokset ja laitetoimittajat eivät voi yksinään vastata

tietoturvaan liittyviin haasteisiin. Sen sijaan tietoturvakäytänteiden on ulotuttava läpi koko laitteen ja laitoksen elinkaaren, kaikki sidosryhmät mukaan lukien.

Tietoturvallisuus ei enää koske ainoastaan yrityksiä tai yksityishenkilöitä vaan sillä on laajempi yhteiskunnallinen merkitys koko yhteiskunnan tasolla. Yhteiskuntamme on täysin riippuvainen tietoverkoista, automaatiosta sekä sähkön ja muiden energialähteiden toimintavarmuudesta. Yksittäinen laite kotona saattaa vaikuttaa merkityksettömältä yhteiskunnan tietoturvauhan kannalta, mutta kun yksittäisiä laitteita on satoja tai tuhansia, niistä voi yhdessä muodostua uhka, joka vaikuttaa merkittävästi yhteiskunnan toimintakykyyn. Useat laitteet voivat yhdessä muodostaa hyökkäysketjun, joka mahdollistaa kyberhyökkäyksen, vaikka yksittäisen laitteen haavoittuvuus ei itsessään mahdollistaisikaan hyökkäystä.

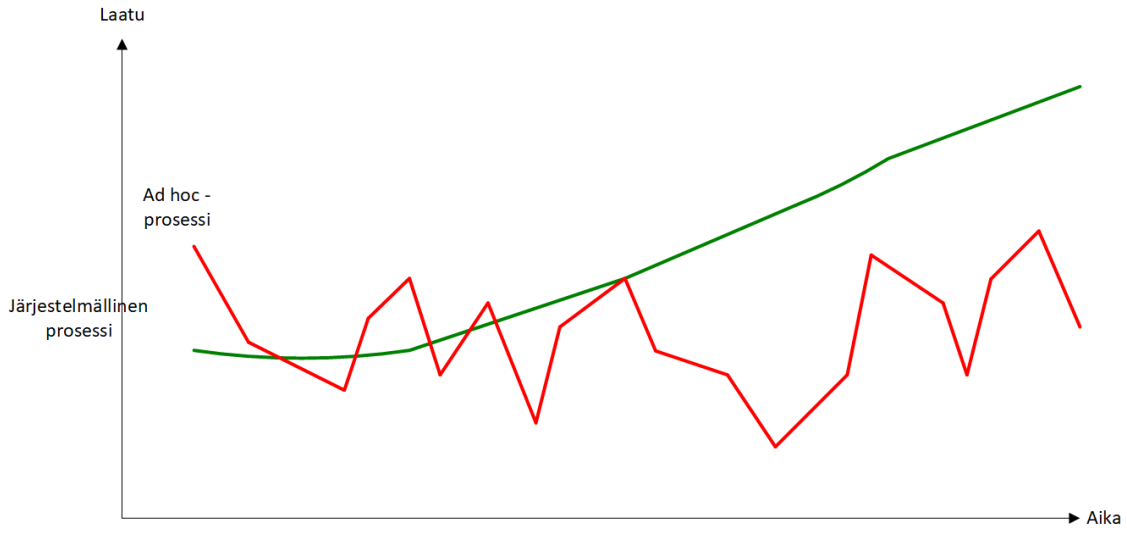
Kyberturva on jatkuvassa muutoksessa, uusien uhkien ja haavoittuvuuksien ilmestyessä kehittyvien teknologisten ratkaisujen myötä. Kyberturvan hallinnassa voi havaita samankaltaisuuden Tetris-pelin kanssa, jossa onnistumiset katoavat kuten rivit Tetriksessä, kun taas epäonnistumiset kasaantuvat ja ovat helposti havaittavissa (1).

Koska tietoturvallisuus ei ole pelkästään yksityisasia nykyisessä verkostoituneessa maailmassa, tarvitaan kansainvälisiä sopimuksia, lakeja ja asetuksia tietoturvan varmistamiseksi. Haavoittuvuuksia tulee aina esiintymään, eikä kaikkia uhkia voida ennustaa etukäteen. Tästä syystä tarvitaan yhteinen prosessi, joka tekee tietoturvallisuussuunnittelusta, ylläpidosta ja viestinnästä sidosryhmien välillä järjestelmällistä.

Tämä lähestymistapa ei poista kaikkia ongelmia eikä estä kaikkia loukkauksia, mutta se luo järjestelmällisen tavan analysoida niitä, tuottaa määrämuotoista tietoa ja korjata havaittuja ongelmia yhtenäisen prosessin kautta, jonka kaikki sidosryhmät ymmärtävät. Samalla tavalla toiminnallisen turvallisuuden standardit ovat luoneet käytäntöjä laitteistojen turvatoimintojen suunnitteluun, rakentamiseen ja ylläpitoon teollisuudessa.

Ilman järjestelmällistä tapaa tuottaa tietoturvallisuutta syntyy sattumanvaraista epävarmuutta. Epävarmuuden vuoksi tietoturvapuutteiden korjaaminen on ad hoc -tyyppistä, eikä kokonaisvaltaista suunnittelua ja ennakointia voida toteuttaa. Järjestelmällinen prosessi ei välttämättä tarkoita, että kyberturva olisi parempi yksittäisissä tapauksissa, vaan pikemminkin sitä, että eri tietoturvallisuusalueet ovat tekijöiden hallinnassa, ja analyysia tai kehitystä voidaan tarvittaessa säätää haluttuun suuntaan.

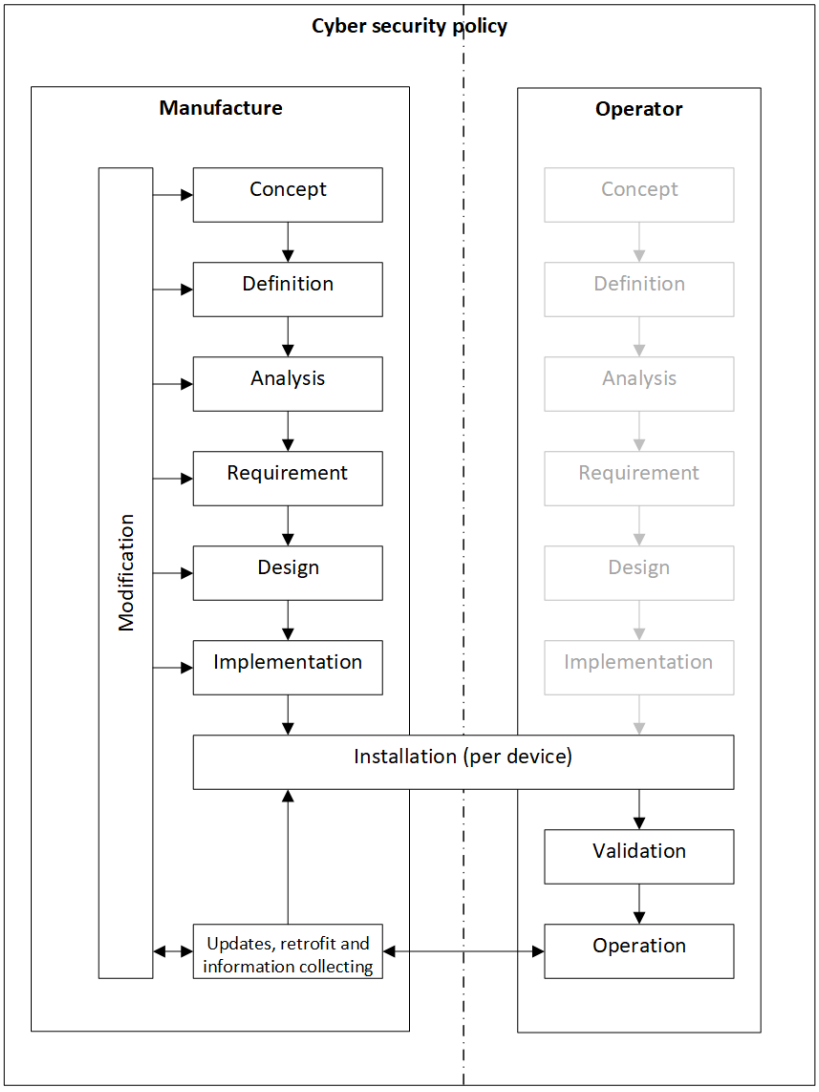
Voidaan jopa väittää, että järjestelmällinen prosessi, joka tuottaa heikkoa laatua, on parempi vaihtoehto kuin satunnaisten ongelmien paikkaamiseen perustuva prosessi, joka tuottaa yksittäistapauksessa hyvää laatua. Tämä johtuu siitä, että ensimmäisessä vaihtoehdossa prosessin osatekijöitä voidaan parantaa ja sillä tavalla parantaa tietoturvaa, kun taas jälkimmäisessä vaihtoehdossa laatu on sattumanvaraista. Järjestelmällisellä lähestymistavalla on mahdollista lopulta saavuttaa korkeampi laatu, kuten Kuva 1 on periaatteellisesti esitetty. Tästä syystä kyberturvan toteuttaminen ei ole projekti vaan prosessi, jossa aika mahdollistaa jatkuvan laadunparannuksen.



Kuva 1. Lopulta järjestelmällinen prosessi tuottaa parempaa laatua kuin ad hoc-tyyppinen sattumaan perustuva toiminta.

Kuten kaikessa turvallisuudessa, myös järjestelmän tai laitteen tietoturvallisuudessa, kyse ei ole pelkästään itsenäisestä tuotantoprosessista. Sen sijaan se muodostaa vertikaalisen kokonaisuuden, joka läpileikkaa koko rakennus- tai tuotantoprosessin. Järjestelmät tai myytävät laitteistot integroituvat toisen organisaation tietoturvaan, joten järjestelmiä rakentavat tai laitteita ja laitteistoja valmistavan organisaation tietoturvakäytännöt ja -menettelytavat tulee olla saumattomasti yhdistettävissä järjestelmiä tai laitteita käyttävien yritysten tietoturvaan.

Kuva 2 on esitetty laitteiston valmistavan organisaation ja sen käyttäjäorganisaation rajapinta suhteessa organisaatioiden elinkaareen.



Kuva 2. Tietoturvallisuutta tuottavat organisaatiot ja käyttäjäorganisaatiot linkittyvät elinkaarimallin asennusvaiheessa.

Teollisuudessa on aiemmin käytetty erityisiä tietoteknisiä laitteita automaatio- ja ohjausjärjestelmiin. Alun perin teollisuuslaitteet olivat liitettyinä laitoksen suljettuun verkkoon, mikä tarkoitti, että tietoturvakäytännöt olivat pääasiassa keskittyneet fyysiseen alueeseen, rakennusten turvallisuuskäytänteisiin sekä ihmisten liikkumisen rajoittamiseen alueella. Nykyään teollisuuslaitosten järjestelmät ovat kuitenkin liitetty internetiin, ja jopa yksi yhteys sisäverkosta internetiin altistaa teollisuuslaitoksen haavoittuvuudelle, riippumatta siitä, kuinka monimutkainen tai epätodennäköinen tuo yhteys on.

Nykyään teollisuuslaitosten automaatio- ja ohjausjärjestelmät rakennetaan kustannustehokkaasti kaupallisilla suoraan hyllyltä ostettavilla komponenteilla (COTS). Tässä yhteydessä termillä "komponentti" viitataan laitteeseen, joka hankitaan valmiina ratkaisuna. Komponentit integroidaan osaksi yrityksen tietojärjestelmiä, kuten liiketoimintajärjestelmiä, toiminnanohjausjärjestelmiä ja kustannusseurantajärjestelmiä. Integraatio mahdollistaa syvemmän käsityksen ohjausjärjestelmien toiminnoista, ja liiketoimintatasolla integroidut käsittelyjärjestelmät parantavat yrityksen kykyä suorittaa analyysejä tuotantokustannusten alentamiseksi, mikä puolestaan auttaa yritystä tehostamaan tuottavuuttaan. Lisäksi entistä saumattomammat tuotanto- ja ohjausjärjestelmät tarjoavat suoremman pääsyn yrityksen tietojärjestelmiin, parantaen näin yrityksen reagointikykyä muuttuvissa tilanteissa. Yhteiset rajapinnat vähentävät yleisiä tukikustannuksia ja mahdollistavat etätuen tuotantoprosessissa.

Haittapuolena on, että eri järjestelmien integrointi lisää verkostoitumista, mikä puolestaan kasvattaa järjestelmän kokonaiskompleksisuutta. Tämä lisää kyberturvauhkien määrää ja haavoittuvuuksien mahdollisuuksia, mikä lisää teollisuusyritysten työmäärää kyberturvan kehittämisessä ja ylläpitämisessä. Lisäksi suoraan hyllyltä ostettavien komponenttien valmistuksessa ei ole voitu huomioida yksittäisen teollisuuslaitoksen mahdollisia erityispiirteitä tietoturvan osalta.

Tämä korostaa tarvetta yhteisille pelisäännöille kaikille sidosryhmille, jotta hajautettu teollisuuslaitoksen integrointi olisi hallittavissa. Yksi ratkaisu tietoturvallisuuspolitiikan- ja käytäntöjen yhdenmukaistamiseen voi olla kansallisten ja

kansainvälisten standardien luonti. Tällä tavoin saadaan harmonisoitua ja yhteismitallistettua tietoturvallisuutta. On kuitenkin tärkeää ymmärtää, että standardien olemassaolo itsessään ei vielä tee laitteistosta kyberturvallista. Sen sijaan standardit luovat yhteisen viitekehyksen tai kielen, jonka avulla eri toimijat voivat saavuttaa keskenään hyväksyttävän tietoturvatason. Yksi esimerkki tällaisesta standardista on kansainvälinen IEC 62443 -standardisarja, joka käsittelee automaatio- ja ohjausjärjestelmien kyberturvallisuutta.

IEC62443 -standardisarjan tavoitteena on luoda yhteinen viitekehys teollisuuden toimijoille. Sarja tarjoaa tukea teollisuusyrityksille, laitteistojen ylläpitoyrityksille, laitoksia rakentaville yrityksille sekä komponenttivalmistajille kyberturvallisuustason suunnitteluun, rakentamiseen ja valmistamiseen.

Tämä insinöörityö johdattaa lukijan IEC 62443 -standardisarjaan. Työn sisältö jakautuu seuraaviin osioihin: Luvussa 0 esitellään tietoturvaloukkaustapauksia, joiden avulla havainnollistetaan tietoturvallisuuteen liittyviä elementtejä. Luvussa 0 tarkastellaan yrityksen johdon strategiaa komponenttikyberturvan valmistajan näkökulmasta. Luvussa 0 käsitellään IEC 62443 -standardisarjan osien sisältöä. Luvussa 5 käydään läpi IEC 62443 -standardisarjan keskeiset määritelmät ja käsitteet, joiden avulla lukijan on helpompi sisäistää standardisarjan tavoitteet ja vaatimukset. Työ tarjoaa lukijalle mahdollisuuden syventää tietämystään IEC 62443 -standardisarjasta.

2 Tietoturvaloukkaustapaukset

Tässä luvussa esitellään konkreettisia tilanteita, joissa tietoturvallisuuteen kohdistuvia uhkia ja haavoittuvuuksia on ilmennyt. Nämä käytännön esimerkit auttavat havainnollistamaan, miten tietoturvallisuuteen liittyvät elementit voivat ilmetä todellisissa tapauksissa. Luku tarjoaa syvemmän ymmärryksen tietouhkien monimuotoisuudesta ja korostaa tarvetta tehokkaille turvallisuuskäytännöille ja -strategioille sekä esittelee elementtejä, joita tietoturvallisuuteen liittyy. Tässä luvussa käsitellään kolmea tunnettua haittaohjelmaa, jotka ovat aiheuttaneet merkittäviä häiriöitä ja vahinkoja eri puolilla maailmaa. Nämä haittaohjelmat ovat Stuxnet mato, NotPetya ja SQL Slammer. Stuxnet-mato ja NotPetya-kuvaukset pohjautuvat lähteeseen (1).

2.1 Stuxnet-mato

Stuxnet oli edistyksellinen tietokoneohjelma, joka paljastui ensimmäistä kertaa vuonna 2010. Sen tarkoituksena oli aiheuttaa vahinkoa Iranin ydinohjelmalle, erityisesti Natanzin ydinvoimalan keskeiselle osalle, joka vastasi sentrifugien toiminnasta uraanin rikastamisessa.

Stuxnet erottui joukosta monimutkaisuudellaan, yhdistäen useita haittaohjelmatekniikoita. Se hyödynsi Windows-käyttöjärjestelmän neljää eri nollapäivän haavoittuvuutta, levisi USB-muistitikkujen välityksellä ja osasi piiloutua tehokkaasti. Lisäksi Stuxnet pystyi tunnistamaan tarkasti Iranin ydinohjelmaan liittyvät järjestelmät. Vaikka Stuxnetin alkuperäiset tekijät eivät ole virallisesti tunnustaneet vastuutaan, on vahva epäilys, että Yhdysvallat ja Israel olivat osallisina sen suunnittelussa (1).

Stuxnet toimi Windows-matona. Se kykeni leviämään organisaation sisäverkossa levyjakojen kautta ja vaikuttamaan minkä tahansa laitteen toimintaan, kunhan se kyettiin liittämään USB-porttiin. Stuxnet pystyi tunnistamaan ja manipuloimaan PLC-laitteita, erityisesti niitä, jotka liittyivät uraanin rikastamiseen sentrifugeissa.

Stuxnetin käyttämät taktiikat olivat äärimmäisen monimutkaisia, sillä se saastutti laitteet huomaamattomasti ja pystyi piiloutumaan pitkäksi aikaa, tehden tarkkoja muutoksia tuotantojärjestelmään. Nollapäivän haavoittuvuuksien käyttö ja allekirjoitetut digitaaliset sertifikaatit olivat osoitus Stuxnetin kehittäjien poikkeuksellisesta kyvykkyydestä ja tarkkuudesta.

Stuxnetin alkuperäinen leviämistapa näyttää liittyneen organisaation työntekijöiden koteihin murtautumiseen ja heidän henkilökohtaisten USB-tikkujensa saastuttamiseen, mikä mahdollisti tartunnan leviämisen teollisuuslaitokseen. (1)

Stuxnetin ilmaantuminen toi esille uudenlaisen uhan kybermaailmassa, missä haittaohjelmat eivät enää pelkästään kohdistuneet tietojärjestelmiin vaan myös fyysisiin laitteisiin ja infrastruktuuriin.

2.1.1 Opit Stuxnet-madon tapauksesta

Stuxnetin kyvyt olivat osoitus äärimmäisen monimutkaisesta ja korkeatasoisesta suunnittelusta. Mato hyödynsi useita nollapäivähaavoittuvuuksia, käytti digitaalisia allekirjoituksia haitallisten tiedostojen allekirjoittamiseen ja levisi nopeasti eri väyliä pitkin. Monimutkainen suunnittelu oli osoitus kyberaseiden kykyjen edistyksestä.

Stuxnet kohdistui teollisuuden ohjausjärjestelmiin, erityisesti SCADA-järjestelmiin, jotka ovat kriittisiä infrastruktuurin osia. Tämä korosti kriittisen infrastruktuurin haavoittuvuutta kyberhyökkäyksille ja digitaalisten keinojen mahdollista fyysistä vaikutusta.

Stuxnet suunniteltiin tiettyä kohdetta varten, mutta se aiheutti tahattomia seurauksia ja sivuvahinkoja maailmanlaajuisesti. Tapahtuma osoitti, miten vaikeaa on hallita edistyksellisen haittaohjelman leviämistä.

Stuxnetin uskottiin olevan valtion toimijan tuote, mikä herätti tietoisuuden hallitusten roolista kehittyneiden kyberaseiden käytössä ja hämärsi perinteisen sodankäynnin ja kybersodankäynnin välistä rajaa.

Attribuution haasteet korostuivat, kun pyrittiin tunnistamaan kyberhyökkäyksen takana olevat toimijat. Tämä toi esiin tarpeen parantaa attribuutiotaitoja vastuullisten osapuolten tunnistamiseksi.

Stuxnet-tapauksen myötä teollisuusjärjestelmien ja kriittisen infrastruktuurin tietoturvallisuus sai osakseen lisää huomiota. Organisaatiot ja hallitukset alkoivat tunnustaa tarpeen suojata paitsi perinteiset tietotekniikkajärjestelmät myös teollisuuden toiminnan teknologiat.

Stuxnet edisti maailmanlaajuista kyberaseiden kilpajuoksua, korostaen kyberaseiden tehokkuutta strategisten tavoitteiden saavuttamisessa. Tämä johti lisääntyneisiin investointeihin hyökkäys- ja puolustuskykyihin eri maiden keskuudessa.

Stuxnet haastoi oletuksen siitä, että internetistä eristetyt järjestelmät ovat immuuneja kyberuhkilta. Mato levisi USB-asemien kautta, mikä korosti ilman yhteyttä olevien järjestelmien haavoittuvuutta fyysisille tartuntavektoreille.

2.2 NotPetya

NotPetya oli Venäjän tukema kyberase, joka oli alun perin suunnattu Ukrainan valtiota vastaan (1). Hyökkäyksen alkuperäinen tavoite oli lamauttaa Ukrainan järjestelmiä, mutta se levisi hallitsemattomasti myös muihin maihin. NotPetya käytti hyväkseen MeDoc-nimisen kirjanpito-ohjelmiston päivitystä. Kiovassa venäläiset hakkerit murtautuivat MeDocin verkkoon ja upottivat haittaohjelman päivitystiedostoon. MeDocia käytetään laajasti Ukrainassa kirjanpitoon ja veroilmoitusten tekoon, mikä teki siitä ihanteellisen väylän hyökkäykselle.

Hyökkääjät kaappasivat MeDocin viralliset päivityspalvelimet ja toimittivat väärennetyn päivityksen, joka todellisuudessa sisälsi NotPetya-haittaohjelman. Koska monet Ukrainan yritykset käyttivät MeDocia, tämä johti NotPetyan laajaan leviämiseen. Se aiheutti mittavia vahinkoja ukrainalaisille yrityksille, ja vaikutukset ulottuivat myös Ukrainassa toimiviin länsimaisiin yrityksiin.

NotPetya aiheutti massiivisia tuhoja maailmanlaajuisesti, erityisesti Maersk-yhtiölle, joka raportoi yli 300 miljoonan dollarin menetyksistä (1). Maerskin konttisatamat jouduttiin sulkemaan NotPetya-tartunnan vuoksi, mikä aiheutti merkittäviä häiriöitä logistiikkaketjussa. Lisäksi Maerskin sisäiset järjestelmät, puhelinverkko, asiakaspalvelu ja internet-sivustot lamaantuivat.

2.2.1 Opit NotPetya haittaohjelman tapauksesta

NotPetya toi selkeästi esiin, että kyberuhka voi vaikuttaa laajasti paitsi tietojärjestelmiin myös fyysisiin toimintoihin, kuten satamien toimintaan. Yritykset kärsivät suurista tietojen menetyksistä ja merkittävistä taloudellisista tappioista. Tapahtuma korosti myös varmuuskopioiden merkitystä, sillä Maerskin DC-palvelimista ei ollut varmuuskopioita, ja identtiset palvelimet vaikeuttivat palauttamista. NotPetya toimi voimakkaana varoituksena yrityksille olla valppaina kyberuhkien varalta ja kehittää suunnitelmia mahdollisten laajamittaisten häiriöiden varalle.

Attribuutioiden haasteet NotPetya-iskun jälkeen olivat merkittävät, kun yritettiin määrittää haittaohjelman alkuperää. Aluksi sitä pidettiin taloudellista hyötyä varten suunniteltuna kiristyshaittaohjelmana, mutta myöhemmin paljastui, että kyseessä oli valtion tukema kyberase, jonka tavoitteena oli aiheuttaa laajaa häiriötä. Tämä korosti kykyä tehdä nopeita ja tarkkoja attribuutioita kyberhyökkäyksissä.

Yksi NotPetya-iskun keskeisiä opetuksia olivat sivuvahingot ja tahattomat seuraukset. Alun perin isku oli suunniteltu kohdistuvan Ukrainaan, mutta haittaohjelma levisi kuitenkin nopeasti maailmanlaajuisesti, vaikutti lukuisiin organisaatioihin ja aiheutti merkittäviä taloudellisia menetyksiä. Tapahtuma toi esille digitaalisen ekosysteemin keskinäiset riippuvuudet ja tarpeen arvioida riskejä laajemmassa kontekstissa.

NotPetya osoitti toimitusketjun riskit hyödyntäessään haavoittuvuuksia ukrainalaisessa kirjanpito-ohjelmassa levitäkseen. Isku osoitti, että yhden organisaation turvallisuuskompromissit voivat vaikuttaa myös muihin, mikä on osoitus

toimitusketjun riskeistä. Organisaatioiden on arvioitava ja lievennettävä riskejä laajemmassa ekosysteemissä.

Tapaus korosti säännöllisen paikkauksen kriittistä merkitystä. NotPetya hyödynsi Microsoftin Windows-käyttöjärjestelmän haavoittuvuutta, joka oli korjattu kuukausia ennen hyökkäystä. Tapahtuma korosti säännöllisen paikkauksen ja ohjelmistojen ajan tasalla pitämisen merkitystä tunnettujen haavoittuvuuksien hyväksikäytön estämiseksi.

NotPetyan nopea leviäminen ja tuhoavat kyvyt korostivat hyvin suunnitellun hallintasuunnitelman tärkeyttä. Organisaatioiden on pystyttävä havaitsemaan ja reagoimaan kyberturvahyökkäyksiin nopeasti minimoidakseen, jotta niiden vaikutukset toimintaan pystytään minimoimaan ja jotta palautuminen hyökkäyksen jälkeen olisi mahdollisimman tehokas.

Haittaohjelma teki tartunnan saaneista järjestelmistä saavuttamattomia, mikä johti toiminnallisiin häiriöihin. Tapahtuma korosti vahvan liiketoiminnan jatkuvuussuunnitelman ja säännöllisten varmuuskopioiden tärkeyttä.

NotPetya osoitti kyberuhkien globaalin luonteen, vaikuttaen organisaatioihin rajojen yli. Tämä korosti tarvetta kansainväliselle yhteistyölle uhkatiedon, parhaiden käytäntöjen jakamisen ja yhteisvastuullisen reagoinnin suhteen kyberhyökkäyksiin.

Isku korosti myös perusturvallisuuskäytäntöjen merkitystä, kuten vahvat salasanat, monivaiheinen tunnistautuminen ja käyttäjien tietoisuuden lisääminen kalasteluriskeistä. Näillä käytännöillä voidaan merkittävästi parantaa organisaation vastustuskykyä kyberuhkia vastaan.

2.3 SQL Slammer

Tammikuussa 2003 Slammer-mato, tunnettu myös nimellä Sapphire, teki ensiesiintymisensä internetin näyttämöllä. Mato hyödynsi haavoittuvuutta Microsoftin SQL Server 2000:ssa ja hyökkäsi suojaamattomiin Windows-pohjaisten

koneiden järjestelmiin. Se aiheutti puskurin ylivuodon ja levitti itseään satunnaisiin IP-osoitteisiin, lisäten leviämisen nopeutta eksponentiaalisesti. Ei kestänyt kauan, ennen kuin mato tarttui useisiin isäntiin, aiheuttaen laajaa verkkoruuhkaa pysäyttäen lopulta internet-liikenteen. (3; 4; 5)

Helmikuussa 2003 Slammer löysi tiensä Davis-Besse-ydinvoimalan verkkoon Yhdysvalloissa. Vaikka mato ei uhannut voimalan turvajärjestelmiä tai aiheuttanut fyysistä vahinkoa, sillä oli merkittävä vaikutus laitoksen toimintaan. Mato soluttautui voimalan verkkoon aliurakoitsijan tietokoneen kautta, joka oli yhteydessä internetiin kiertäen palomuurin. Slammer-mato levisi sitten prosessinohjausverkkoon tartuttaen lopulta voimalan prosessiarvojen seurantajärjestelmän (SPDS) ja prosessitietokoneen. (3; 4)

SPDS valvoo laitoksessa kaikkein kriittisimpiä turvallisuusosoittimia, kuten jäähdytysjärjestelmiä, ytimen lämpötila-antureita ja ulkoisia säteilyantureita. Monet näistä vaativat tarkkaa valvontaa jopa silloin, kun voimala ei ole käytössä. Lähes viiden tunnin ajan SPDS oli poissa käytöstä, mikä esti voimalan valvomon operaattoreita saamasta pääsyä kriittisiin turvallisuustietoihin. Vaikka voimala oli polttoaineen lataustauolla eikä tuottanut sähköä tuolloin, SPDS:n menetys olisi voinut olla vakavia seurauksia, jos voimala olisi ollut käynnissä. Mato sammutti myös voimalan prosessitietokoneen yli kuudeksi tunniksi, mikä johti tilapäiseen datan menetykseen. (3; 4)

2.3.1 Opit Slammer-madon tapauksesta

Ohjelmistopäivitysten hallinta on kriittinen näkökohta, jonka tämä tapaus toi esiin. On tärkeää asentaa ohjelmistojen uusimmat versiot ja korjaustiedostot viipymättä. Tämä auttaa vähentämään turvallisuusriskejä ja optimoimaan ohjelmistojen toiminnallisuuden ja suorituskyvyn. Slammer-mato hyödynsi Microsoftin ohjelmistossa olevaa haavoittuvuutta, mikä oli korjattu jo aikaisemmin. (4)

Jaettu verkko voi edistää tehokkuutta ja yhteistyötä, mutta jos verkko ei ole hyvin suojattu, järjestelmä voi olla altis ulkopuolisille hyökkäyksille. Ydinvoimalan

hyökkäys osoitti, että haittaohjelmilta voi suojautua tehokkaasti eristämällä kriittiset ja ei-kriittiset järjestelmät ja rajoittamalla verkkoyhteyksiä. (4)

Lisäksi tapaus paljasti tarpeen parantaa toimittajien ja alihankkijoiden käytäntöjä ja ohjeita. Mato pääsi ydinvoimalan verkkoon alihankkijan tietokoneen kautta, mikä edellyttää kolmansien osapuolten tarkempaa valvontaa. Organisaatioiden on määriteltävä selkeät turvallisuusmenettelyt kaikille ulkopuolisille toimijoille, jotka käyttävät niiden verkkoa. (4)

Davis-Bessenin tapaus osoitti, että hyvin suunniteltu tapahtumien hallintasuunnitelma on välttämätön. Organisaatioiden on kyettävä havaitsemaan, reagoimaan ja palautumaan turvallisuusloukkauksista nopeasti. (4)

Myös työntekijöiden koulutus ja tietoisuus ovat tärkeitä, koska monet turvallisuusuhkat liittyvät inhimillisiin virheisiin, huolimattomuuteen tai tietämättömyyteen. Jos työntekijät ovat tietoisia uusimmista turvallisuusuhista ja parhaista käytännöistä, he voivat välttää samankaltaisia hyökkäyksiä. (4)

Myös jatkuvan valvonnan ja havaitsemisen tarve korostui. Jatkuva valvonta ja havaitseminen tarkoittaa, että organisaatioiden on seurattava jatkuvasti verkkojensa ja järjestelmiensä tilaa ja toimintaa ja käytettävä erilaisia työkaluja ja menetelmiä poikkeamien ja epäilyttävien toimintojen havaitsemiseksi. Reaaliaikaiset valvonta- ja havaitsemistyökalut voivat auttaa havaitsemaan uhkia aikaisemmin. (4)

2.4 Tapausten yhteenveto

Edellisistä tapauksista voidaan havaita viisi haavoittuvuuskategoriaa: järjestelmien heikkouksien hyödyntäminen, leviämistavat, ulkopuolisten järjestelmien kautta tapahtuva hyökkäys, tietoliikenneverkkoalueiden segmentointi ja mahdollisuudet vaikuttaa järjestelmään.

2.4.1 Järjestelmien haavoittuvuuksien hyödyntäminen

Windows toimii lähes itsestään selvänä hyökkäyspintana, jonka haavoittuvuuksia hyödynnetään laajalti erilaisissa hyökkäyksissä, sillä sen käyttöjärjestelmän laaja levinneisyys organisaatioiden tietojärjestelmissä tekee siitä houkuttelevan kohteen. Lisäksi SQL Serverit ja muut palvelut luovat merkittävän hyökkäysvektorin järjestelmiin. Stuxnet-madon tapaus paljasti, että teollisuusautomaatiolaitteet, kuten PLC-laitteet, eivät enää ole immuuneja uhkille.

Uhkien minimoiminen vaatii laadukasta laitteistosuunnittelua, jossa tutkitaan ja arvioidaan syvällisesti erilaisten hyökkäysvektoreiden mahdollista olemassaoloa. Riskejä on poistettava huolellisella suunnittelulla ja tehokkaalla toteutuksella. Lisäksi laitteiden päivityskäytännöt tulisi automatisoida, jotta turvapäivitykset voidaan asentaa välittömästi niiden julkaisun jälkeen.

Kuten NotPetya-haittaohjelman tapaus osoitti, itse päivitykset voivat kuitenkin muodostaa leviämisreitin, jos päivityksiä toteuttaneeseen yritykseen kohdistuu tietomurto. Siksi on äärimmäisen tärkeää, että päivitysprotokollat ja organisaation sisäiset tietoturvallisuuskäytännöt kehittyvät ja päivittyvät jatkuvasti vastaamaan muuttuvia uhkakuvia.

2.4.2 Leviämistavat

Käyttöjärjestelmien ja ohjelmistojen kautta leviävät haittaohjelmat voivat hyödyntää tietokoneita, joihin ei ole asennettu tarvittavia päivityksiä, joissa ohjelmistot ovat huonosti konfiguroitua tai joissa on nollapäivähaavoittuvuuksia. Tarvittavien päivitysten asentaminen ja väärän konfiguroinnin aiheuttamiin haavoittuvuuksiin voidaan vaikuttaa tehokkailla tietoturvakäytännöillä ja niistä johdetuilla menetelmillä sekä organisaation turvakulttuurilla. Nollapäivähaavoittuvuuksiin vaikuttaminen on kuitenkin vaikeampaa, koska ne ovat määritelmän mukaan haavoittuvuuksia, jotka eivät ole laajalti tiedossa. Automaattiset ja välittömät päivityskäytännöt ovat tässä avainasemassa, sillä ne poistavat mahdollisen haavoittuvuuden heti, kun se on tullut julkiseksi tiedoksi.

Haittaohjelmien leviämisen torjunta USB-tikun tai aliurakoitsijan tietokoneiden kautta edellyttää tarkkaa suunnittelua tietoturvapolitiikan ja -menetelmien osalta. On tärkeää asettaa tarkat vaatimukset sille, millä ehdoin laitteet tai komponentit saavat kytkeytyä teollisuuslaitoksen sisäverkkoon. Lisäksi sisäverkon rakenne tulisi olla jaettu eri alueisiin, joilla on omat turvallisuustasot. Eri turvallisuustasojen välille on luotava palomuureja ja turva-automaatioverkossa tulisi käyttää yksisuuntaista yhdyskäytävää. Yhdyskäytävä sallii tietojen liikkumisen ainoastaan turva-automaatioverkossa ulospäin, estäen samalla tietojen liikkumisen turva-automaatioverkkoon.

2.4.3 Tietoliikenneverkkoalueiden segmentointi

Edellä korostettiin organisaation verkkojen eriyttämisen tärkeyttä eri toiminnallisiin kokonaisuuksiin. Yritysverkko voi kattaa esimerkiksi yhtiön laajemman verkon, josta on yhteys yrityksen tehtaiden verkkoihin. Tehtaan verkko puolestaan jakautuu ohjauskeskuksen, prosessiohjauksen ja turva-automaatiojärjestelmän verkkoihin (katso Kuva 6). Lisäksi näiden verkkojen välillä voi olla demilitarisoituja alueita (DMZ). Jokaiselle näistä verkon osista tulee määrittää turvallisuustaso, ja niiden väliset suhteet on arvioitava ja analysoitava mahdollisten uhkien varalta. Tämän pohjalta on laadittava vaatimukset verkon laitteille ja toimintatavoille, jotta verkossa voidaan täyttää asetetut tietoturvavaatimukset.

IEC 62443-standardisarjassa otetaan huomioon kaikki yllä mainitut näkökulmat.

3 Yrityksen johto tieturvakäytännön perustana

Tässä luvussa tarkastellaan keskeisiä tietoturvajohtamisen elementtejä yritysjohdon näkökulmasta. Luku perustuu tekijän näkemyksiin yrityksen johdon tietoturvakäytännöstä, joka toimii organisaation tietoturvallisuuden perustana.

Tietoturvakäytäntö asettaa selkeät suuntaviivat ja käytännöt tietojen suojaamiseksi ja riskien hallitsemiseksi. Se kattaa laajan valikoiman aiheita, kuten tietojen keräämisen, käytön, tallentamisen ja jakamisen sääntelyn sekä henkilöstön koulutuksen ja tietoturvallisuusmenetelmät. Tehokas tietoturvakäytäntö ei ainoastaan suojaa yrityksen arkaluontoisia tietoja, vaan myös edistää luottamusta sidosryhmien keskuudessa ja voi toimia kilpailuetuna markkinoilla.

Yrityksen hallituksen ensisijainen tehtävä on määritellä organisaation arvot, missio ja strategia. Nämä muodostavat yrityskulttuurin perustan, joka lopulta ohjaa sitä, miten korkealaatuisia tuotteita ja palveluja yritys kykenee tuottamaan.

Operatiivinen johto puolestaan vastaa toimintaohjelmista ja tietoturvakäytäntöjen luomisesta hallituksen asettamien päämäärien pohjalta. Tietoturvakäytännöt toimivat ohjenuorana, jonka avulla määritellään toimintatavat ja -ohjeet. Käytäntöjen avulla yritys pyrkii toteuttamaan riittävän laadukkaita laitteita ja ohjelmistoja, jotka vastaavat asetettuihin turvallisuustavoitteisiin.

3.1 Hallituksen lähtökohtana olevat oletukset

Yrityksen hallituksen tulee olla täysin tietoinen tietoturvaympäristön realiteeteista, jotta se voi asettaa operatiiviselle johdolle sellaiset vaatimukset, jotka mahdollistavat laadukkaan tietoturvapolitiikan, jolla voidaan saavuttaa myyntituottojen tavoitetaso. Alla on muutamia toimintaympäristöön liittyviä oletuksia, jotka yrityksen hallituksen tulisi tiedostaa, kun se muodostaa yrityksen arvot, mission ja strategian:

- Jokaisessa järjestelmässä on aina yksi tai useampi virhe tai haavoittuvuus.

- Ohjelmistokomponenteissa esiintyy aina yksi tai useampi haavoittuvuus.
- Laitteistokomponenteissa ilmenee aina yksi tai useampi vika.
- Käyttöjärjestelmiin (ytimessä), ohjelmistokomponentteihin ja laitteistokomponentteihin kohdistuu aina uhkia toimintaympäristöstä riippumatta.
- Kyberturvan tuottaminen on prosessi.
- Uusia haavoittuvuuksia paljastuu jatkuvasti.
- Lopulta totuus paljastuu aina.

Edellä mainitut oletukset luovat toimintaympäristön, jossa tietoturvasuunnittelun ja -toteutuksen realiteetit tulee otetuksi huomioon oikeassa suhteessa. Hyvään tietoturvan tasoon pyrkivän yrityksen suurin riski on olettaa, että sen laitteet ja ohjelmistot ovat virheettömiä tai että niihin ei kohdistu mitään uhkia käyttöympäristössä. Liiallinen itsevarmuus tietoturvan laadusta voi sokeuttaa, jolloin omissa laitteissa ja ohjelmistoissa mahdollisesti esiintyviä haavoittuvuuksia ei havaita. Turvallisuusalla pieni annos pessimismiä on hyve.

3.2 Yrityksen hallituksen vaatimukset

Tässä esitellään esimerkin omaisesti yrityksen hallituksen määrittelemiä arvoja, visiota ja strategioita. Näiden pohjalta yrityksen operatiivinen johto voi laatia tietoturvapolitiikan vaatimukset ja toimintaohjeet. Tarkoituksena on luoda yrityskulttuuri, joka mahdollistaa tarvittavan tietoturvatason saavuttamisen yrityksen tuottamissa tuotteissa. On huomioitava, että esimerkit ovat yleisiä eivätkä välttämättä vastaa kaikkien yritysten toimintaympäristöä tai kaupallista sektoria.

Seuraavassa on manifestin tapaan laadittu mahdolliset arvot, missio ja strategia, jotka yrityksen hallitus voisi määritellä.

Arvot

Yrityksemme vahva sitoutuminen avoimuuteen ja rehellisyyteen ulottuu niin sidosryhmien kuin sisäisen toimintaympäristömme suuntaan. Ymmärrämme tietoturvaan liittyvän vastuumme jatkuvasti muuttuvassa toimintaympäristössä ja

ylläpidämme jatkuvaa vuoropuhelua tuotteidemme käyttäjien kanssa niiden koko elinkaaren ajan. Luomme avoimen työympäristön, jossa voimme rohkeasti ja rehellisesti keskustella tietoturvaan liittyvistä laatukysymyksistä, ja kannustamme avoimuuteen tuomalla rohkeasti esille tietoturvaan liittyviä haasteita ja ongelmakohtia.

Missio

Yrityksemme missiona on ylläpitää avointa ja rehellistä viestintää kaikkien sidosryhmiensä kanssa tietoturvan liittyvistä aiheista. Tavoitteenamme on tiedottaa avoimesti, rehellisesti ja välittömästi kaikista laitteisiimme kohdistuvista tietoturvahaavoittuvuuksista ja -uhista. Avoimuus uhkien suhteen on keskeinen osa tietoturvasuunnittelua. Se luo ilmapiirin, jossa jokainen yrityksen työntekijä voi osallistua tietoturvahaavoittuvuuksien tunnistamiseen ja raportointiin. Pyrimme edistämään luottamuksen kasvua sidosryhmiimme ja vahvistamaan yrityksemme tuotteiden brändiarvoa. Laadukas tietoturvan taso laitteistossamme on avoimen ja järjestelmällisen toiminnan lopputulos. Tavoitteenamme on vahvistaa yrityksemme asemaa tietoturvallisuuden maailmanlaajuisena toimijana ja toimia aktiivisena osana tässä yhteisössä.

Strategia

Yrityksemme hallitus vahvistaa tietoturvan keskeiseksi elementiksi laitteiston strategiassa. Tarkoituksena on varmistaa, että vastaamme sidosryhmiemme tarpeisiin asianmukaisesti ja että laitteistomme tietoturvataso vastaa asiakkaidemme vaatimuksia. Strategiamme perustuu huolellisesti dokumentoituihin ja määrämuotoisiin prosesseihin, joiden joustavuus ja päivitettävyys ovat keskeisiä tekijöitä. Hallitus korostaa avointa viestintää sekä yrityksen sidosryhmien että sisäisten toimijoiden kanssa, edistäen tietoturvallisuuden ymmärryksen kasvua organisaatiossamme.

Lisäksi hallitus sitoutuu luomaan ja ylläpitämään avoimia kommunikaatiokanavia, jotka edistävät tietoturvaan liittyvien asioiden avointa keskustelua. Aktiivinen osallistuminen tietoturvayhteisön tapahtumiin sekä oman panoksemme

antaminen yhteisölle ovat keskeinen osa strategiaamme. Tämä sitoutuminen yhteisöön, avoin viestintäkulttuuri ja jatkuva kehitys tukevat hallituksen asettamaa tavoitetta ylläpitää ja parantaa yrityksemme laitteistojen kyberturvaa jatkuvasti muuttuvassa toimintaympäristössä. Keskeisenä strategisen tavoitteena on varmistaa, että yrityksen laitteet ovat maailman johtavien tietoturvavaatimusten mukaisia, mahdollistaen tuotteiden myynnin eri maissa ja vastaten tarvittaviin säädöksiin ja standardeihin.

3.3 Tietoturvakäytännöt

Laitteiden tietoturvan toteutusta varten operatiivinen johto laatii tietoturvakäytännöt, joka perustuu hallituksen asettamiin arvoihin, visioon ja strategiaan. Nämä käytännöt muodostavat kattavan suunnitelman hyväksyttävän turvallisuustason saavuttamiseksi laitteistossa, joka käsittää eri organisaatiotasoilla määritellyt käytännöt. Näitä käytäntöjä tarkastellaan säännöllisesti turvallisuusauditointien yhteydessä. Politiikassa otetaan huomioon kaikki sovellettavat lainsäädännöt, asetukset ja sopimusvelvoitteet, ja siinä voidaan määrittää, että yrityksen tulee sertifioida tuotteensa IEC 62443 -standardisarjaan.

Yrityksen eri osien tietoturvapolitiikat ja käytännöt täytyy integroida saumattomasti, vaikka kyseessä onkin laitteiston valmistus. Rakenteellinen johdonmukaisuus edistää kokonaisvaltaista yhdenmukaisuutta. Käytännöt ovat yksityiskohtaisia menettelytapoja, jotka liittyvät tiettyihin tietoturvatoimenpiteisiin.

Toteutuksen eri elinkaaren vaiheissa esiintyy erilaisia turvallisuusongelmien profiileja ja näihin haasteisiin vastataan sekä turvallisuuspolitiikalla- että käytännöillä. Nämä pitävät sisällään ohjeet vaatimustenmukaisuuden arvioimiseen ja käytäntöjen päivittämiseen.

Tietoturvakäytännössä- ja -menetelmissä tulee huomioida myös odottamattomat tilanteet. Organisaatiolla täytyy olla selkeä käsitys siitä, mikä on vaatimus ja mikä valinnainen ohjeistus. Käytännöt ja toimintatavat tietoturvaohjelman

käynnistämiseksi muodostavat vankan perustan, joka kattaa yrityksen nykyiset valmiudet ja toimii pohjana yrityksen kyvylle vastata kasvaviin kyberuhkiin.

Proaktiivinen lähestymistapa on olennainen osa tietoturvan hallintaa ja IT- ja tuotanto-organisaatioiden tulisi tiivistää yhteistyötään turvallisuusongelmien ratkaisemiseksi. Operatiivisen johdon tulee päivittää tietoturvamääräykset vastaamaan organisaation muutoksia ja turvallisuusuhkia.

Yritystason politiikassa määritellään vastuualueet ja suhteet, ja käytännöissä eritellään turvallisuustavoitteet eri osa-alueille. Johdon on viestittävä käytännöistä selkeästi ja laajasti koko organisaatiolle.

3.3.1 IEC 62443-sarjan kypsyysmalli

Tämä luku on koottu lähteiden (6, s. 39–45; 7, s. 15; 8, s. 19–20) perusteella.

Standardi IEC 62443-4-1 sisältää kypsyysmallin, joka tarjoaa organisaatioille vertailukohdan standardin vaatimusten täyttämiseksi. Malli tunnustaa, että organisaatiot eivät välttämättä saavuta haluttua tasoa prosesseissaan välittömästi, vaan kehittyvät ajan myötä. Organisaatiot etenevät kohti tavoitetasoa ja edistymistä voidaan käyttää viestimään sidosryhmille organisaation kehittymisestä.

Kypsyystasot tarjoavat lisätietoja siitä, kuinka perusteellisesti organisaatio on täyttänyt IEC 62443-4-1 standardin vaatimukset. Tasot muodostavat arvioinnin perustan, jonka avulla sidosryhmät voivat arvioida tuotteen kehittämisen laadun tasoa.

Kypsyystasojen tarkoitus on tarjota organisaatiolle mahdollisuus määrittää, mikä organisaation valmius on hyödyntää prosessejaan ja menettelytapojaan kyberturvallisen tuotteen suunnitteluun ja toteuttamiseen. Vertailun avulla organisaatio voi tunnistaa kehityskohteita ja parantaa tuotetta.

On odotettavissa, että ajan myötä tuotetoimittajan kyvyt kehittyvät korkeammalle tasolle, kun se hankkii asiantuntemusta vaatimusten täyttämisessä.

Jatkuvaa parantamista mittausten perusteella pidetään keskeisenä tekijänä tuotetoimittajan kypsyystason nostamisessa. Hyvien käytäntöjen kehittyminen kyberturvallisen tuotteen kehittämisessä edellyttää, että tuotetoimittaja on aktiivinen, etsii uusia käytäntöjä ja toteuttaa niitä.

4 IEC 62443 -standardisarja

Tämän luvun ja aliluvun tiedot perustuvat lähteisiin (5–16).

IEC 62443 on standardisarja, joka käsittelee teollisuuden automaatio- ja ohjausjärjestelmien kyberturvaa. Se sisältää liiketoiminnan, yritysten IT-järjestelmien ja teollisuuden automaatio- ja ohjausjärjestelmien kyberturvan näkökulmat. Tämä tekninen määritelmä on suunnattu kaikille, jotka ovat osallisina tai vaikuttavat järjestelmän tietoturvaan, sekä teollisuuden automaatio- ja ohjausjärjestelmien ja yritysverkkojen yhteensovittamiseen. IEC 62443 edellyttää, että nykyisiä turvallisuusjärjestelmiä ja -käytäntöjä kehitetään, jotta teollisuuden automaatio- ja ohjausjärjestelmät saavat riittävän turvallisuustason ja jäännösriski on hyväksyttävissä rajoissa.

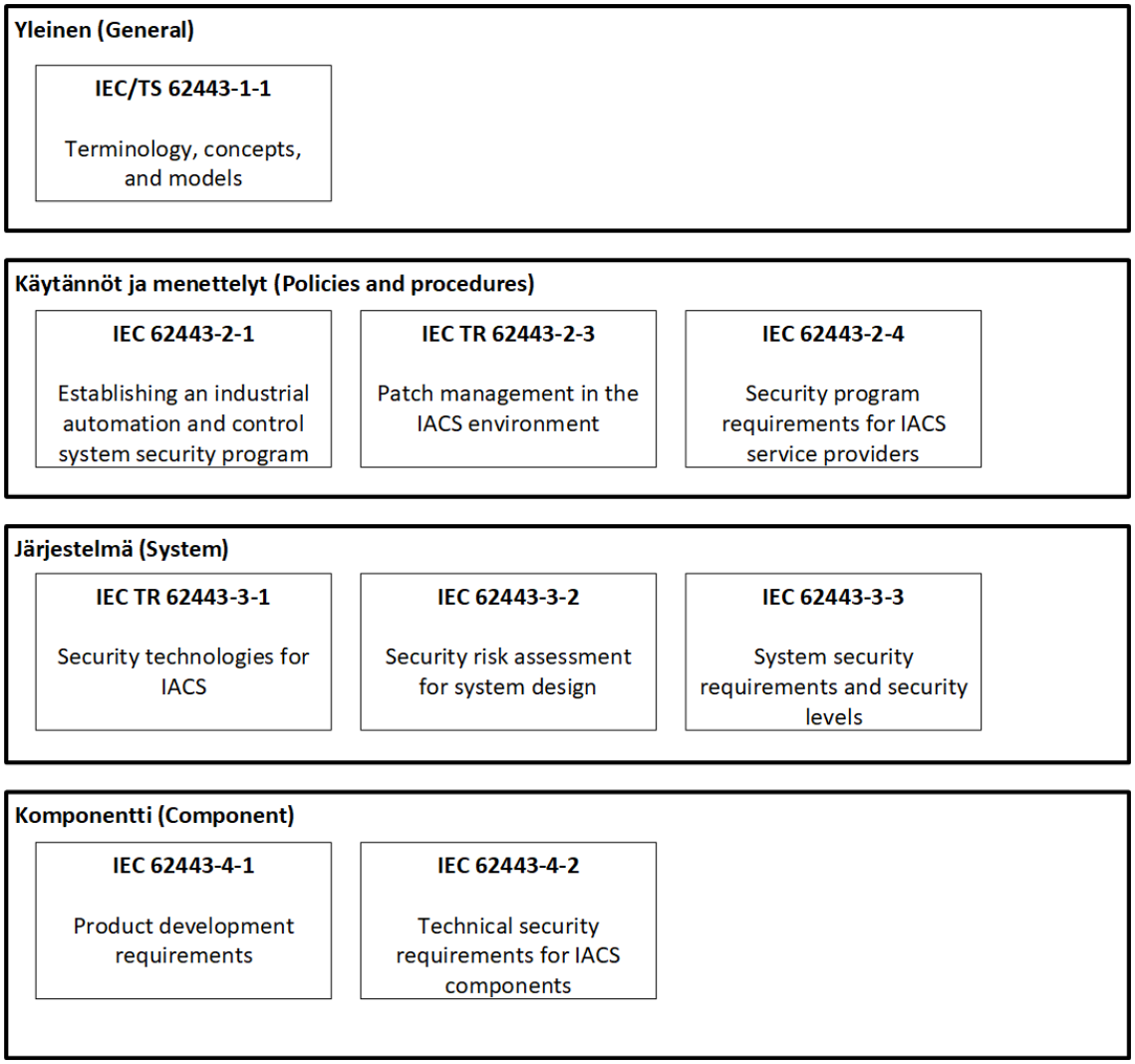
Standardi antaa ohjeita teollisuuden prosesseihin liittyvien järjestelmien turvallisuuteen, suojaukseen ja luotettavuuteen liittyen. Standardi varmistaa, että järjestelmät noudattavat tarpeellisia turvallisuusvaatimuksia. IEC 62443 -standardisarja on kattava viitekehys teollisuuden automaatio- ja ohjausjärjestelmien turvallisuudelle. Sen tavoitteena on lisätä turvallisuutta teollisuuden automaatioympäristöissä. IEC 62443 -standardin noudattaminen jakaa vastuun automaation kyberturvasta eri osapuolille. Standardi asettaa vaatimukset suojattavien kohteiden omistajille, järjestelmäintegraattoreille, tuotetoimittajille ja järjestelmän ylläpitäjille. Standardisarja mahdollistaa yhtenäisen sertifiointijärjestelmän, jota monet yritykset tarjoavat. Standardi keskittyy pääasiassa teollisuusautomaatioon ja ohjaukseen. Se ei ota kantaa liiketoiminnan suunnitteluun ja logistiikkaan, mutta ottaa huomioon liiketoiminta- ja teollisuusjärjestelmien välisen tiedon eheyden. Teollisuusautomaatio ja ohjaus käsittävät erilaisia valvontakomponentteja, joita käytetään tyypillisesti prosessiteollisuudessa, kuten SCADA-järjestelmät. SCADA-järjestelmät ovat yleisiä organisaatioissa, jotka toimivat esimerkiksi

sähkönsiirron- ja jakelun, kaasu- ja vesihuollon, öljyn- ja kaasuntuotannon tai kaasu- ja nestemäisten siirtojohtojen aloilla.

Tekninen eritelmä koskee teollisuuden automaatio- ja ohjausjärjestelmiä, jotka ovat olennaisia teollisten prosessien turvallisuudelle, suojaukselle ja luotettavuudelle. Näitä ovat muun muassa erilaiset ohjausjärjestelmät, viestintäverkot ja mittaus- ja valvontajärjestelmät. Standardin tarkoituksena on määritellä näiden järjestelmien turvallisuusvaatimukset. IEC 62443 -standardisarja esittää automaatio- ja ohjausjärjestelmien kyberturvallisuuden tekniset ja prosessuaaliset näkökohdat. Se antaa ohjeita eri osapuolille turvallisten teollisuusautomaatiojärjestelmien suunnitteluun ja ylläpitoon. Standardisarja täydentää IT-turvallisuuteen keskittyvää ISO 27001-standardia. IEC 62443-standardisarja määrittelee kyberturvan parhaat käytännöt ja vertailuarvot teollisuusautomaation käyttäjille. Se pyrkii yhdistämään toiminnan, tietotekniikan, prosessiturvallisuuden ja tietoturvan. Standardisarja on saanut kansainvälisen hyväksynnän ja tunnustuksen ja sitä sovelletaan monilla teollisuudenaloilla.

IEC 62443-standardisarja ei tarjoa yleispätevää ratkaisua, vaan se edellyttää yksilöllistä lähestymistapaa yrityksen tarpeiden ja olosuhteiden mukaan. Turvallisen automaatioratkaisun luomiseksi on tehtävä uhka- ja riskianalyysit, joiden perusteella määritellään järjestelmän ja komponenttien vaatimukset. Lisäksi on tärkeää toteuttaa jatkuvaa valvontaa ja henkilökunnan koulutusta turvallisuuden varmistamiseksi. IEC 62443 -standardisarjan käyttöönotto edellyttää jaetun vastuun periaatteen noudattamista automaation kyberturvallisuudessa, ja standardisarja asettaa vaatimukset keskeisille sidosryhmille, kuten suojattavien kohteiden omistajille, järjestelmäintegraattoreille, tuotetoimittajille ja järjestelmän ylläpitäjille.

Standardisarja koostuu neljästä kategoriasta: Yleinen (General), Käytännöt ja menettelyt (Policies and procedures), Järjestelmä (System) ja Komponentti (Component). IEC 62443-standardiperheen dokumentit on esitetty kuvassa 3.



Kuva 3. IEC 62443 -sarjan osat.

4.1 Yleinen -kategoria

Kirjoitushetkellä ainoa saatavilla oleva dokumentti yleisestä kategoriasta on IEC/TS 62443-1-1 tekninen spesifikaatio.

4.1.1 IEC/TS 62443-1-1 Terminology, concepts, and models

Tämä osa IEC 62443 -sarjaa on tekninen spesifikaatio, joka määrittelee käsitteet ja mallit teollisuuden automaatio- ja ohjausjärjestelmän turvallisuudelle. Se luo perustan muille IEC 62443 -sarjan standardeille ja teknisille eritelmille.

4.2 Käytännöt ja menettelyt -kategoria

Tämä standardisarjan kategoria määrittelee olennaiset osat teollisuuden automaatio- ja ohjausjärjestelmien (IACS) kyberturvallisuuden hallintajärjestelmän rakentamiseksi ja tarjoaa ohjeet niiden kehittämiseen. Sen vaatimukset noudattavat ISO/IEC 27001 -standardin vastaavia vaatimuksia ja se kattaa myös suunnitteluprosessin ohjelmalliset näkökohdat sekä valmistustoimintoihin liittyvät toiminnot. Lisäksi kategoriassa käsitellään teollisuuden automaatio- ja ohjausjärjestelmien kyberturvallisuuden korjauspäivitysten hallintaa, sekä se tarjoaa suosituksia ja vaatimuksia suojattavien kohteiden omistajille ja tuotteiden toimittajille. Kategoria asettaa myös turvallisuusvaatimukset integraatio- ja ylläpitopalveluja tarjoaville teollisuuden automaatio- ja ohjausjärjestelmien palveluntarjoajille ja se mahdollistaa profiilien sovittamisen erilaisiin ympäristöihin.

4.2.1 IEC 62443-2-1 Establishing an industrial automation and control system security program

Standardi määrittelee ne elementit, jotka ovat tarpeen kyberturvallisuuden hallintajärjestelmän perustamiseksi teollisuuden automaatio- ja ohjausjärjestelmille (IACS). Lisäksi standardi antaa ohjeita elementtien kehittämiseen.

Standardin vaatimukset ovat hyvin samankaltaisia kuin ISO/IEC 27001 vaatimukset. Standardi antaa ohjeita suunnitteluprosessin ohjelmallisiin näkökohtiin. Standardi sisältää kriteerit valmistustoimintoihin liittyvien toimintojen määrittelemiseksi. Tässä määritellään elementit, jotka ovat tarpeen teollisuuden automaatio- ja ohjausjärjestelmien kyberturvallisuuden hallintajärjestelmän perustamiseksi, ja antaa ohjeita elementtien kehittämiseen. Standardissa kuvatut kyberturvallisuuden hallintajärjestelmän elementit liittyvät enimmäkseen käytäntöön, menettelyyn ja henkilöstöön, ja ne kuvaavat, mitä organisaation lopulliseen kyberturvallisuuden hallintajärjestelmän tulee tai pitäisi sisällyttää. Standardin soveltajien tulee soveltaa tämän standardin ohjeita kehittääkseen asianmukaisen kyberturvallisuuden hallintajärjestelmän organisaatioonsa. Tässä standardissa käsitellyt periaatteet ja menettelytavat tulee räätälöidä

organisaation tarpeiden mukaan eli vain yhtä tapaa toteuttaa standardin vaatimuksia ei ole.

4.2.2 IEC TR 62443-2-3 Patch management in the IACS environment

Tämä tekninen raportti käsittelee teollisuuden automaatio- ja ohjausjärjestelmän kyberturvallisuuden korjauspäivitysten hallintaa. Korjauspäivitysten hallinta on osa kattavaa kyberturvallisuusstrategiaa. Korjaustiedostoja kutsutaan ohjelmistopäivityksiksi, laiteohjelmistopäivityksiksi, Service Pack-päivityksiksi ja hotfix-korjauksiksi. Korjaustiedostoilla ratkaistaan vikoja, parannetaan käytettävyyttä ja luotettavuutta sekä korjataan kyberturvallisuuteen liittyviä haavoittuvuuksia perussyöttöjärjestelmän (BIOS) päivitysten ja muiden päivitysten yhteydessä. Tekninen raportti esittelee monia teollisuuden automaatio- ja ohjausjärjestelmän korjausten hallintaan liittyviä ongelmia ja alan huolenaiheita suojattavien kohteiden omistajille ja teollisuuden automaatio- ja ohjausjärjestelmätuotteiden toimittajille.

Teknisessä raportissa kuvataan vaatimuksia suojattavien kohteiden omistajille ja teollisuusautomaatio- ja ohjausjärjestelmien tuotteiden toimittajille, jotka ovat perustaneet ja ylläpitävät korjauspäivitysten hallintaohjelmia. Standardissa suositellaan määriteltyä muotoa tietoturvakorjauskorjaustietojen jakamiseen suojattavien kohteiden omistajilta, joidenkin tuotteiden toimittajien korjauspäivitystietojen kehittämiseen liittyvien toimintojen määrittelyä sekä korjaustiedostojen käyttöönottoa ja asennusta. Raportti ei tee eroa käyttöjärjestelmille (OS), sovelluksille tai laitteille saatavilla olevien korjaustiedostojen välillä. Siinä ei tehdä eroa infrastruktuurikomponenttien tai teollisuuden automaatio- ja ohjausjärjestelmäsovelluksia toimittavien tuotteiden toimittajien välillä. Se antaa ohjeita kaikille teollisuuden automaatio- ja ohjausjärjestelmään sovellettaville korjaustiedostoille.

4.2.3 IEC 62443-2-4 Security program requirements for IACS service providers

Standardi IEC 62443-2-4 sisältää turvallisuusvaatimukset teollisuuden automaatio- ja ohjausjärjestelmien integraatio- ja ylläpitopalvelujen tarjoajille.

Standardi määrittelee kattavan joukon vaatimuksia teollisuuden automaatio- ja ohjausjärjestelmien palveluntarjoajille. Vaatimukset koskevat turvallisuusominaisuuksia, joita palveluntarjoajat voivat tarjota suojattavan kohteiden omistajille automaatioratkaisujen integraatio- ja ylläpitotoimien aikana. Koska kaikki vaatimukset eivät päde kaikkiin teollisuuden aloihin ja organisaatioihin, on mahdollista kehittää profiileja, jotka mahdollistavat vaatimusten osajoukkojen luomisen. Profiileja käytetään sovittamaan standardin vaatimukset erilaisiin ympäristöihin, mukaan lukien ympäristöt, jotka eivät perustu teollisuuden automaatio- ja ohjausjärjestelmiin.

Standardissa määritellään vaatimukset suojausominaisuuksille, joita integraatio- ja ylläpitopalvelujen tarjoajien tietoturvaohjelmat tukevat. Ominaisuuksien tuki tarkoittaa, että palveluntarjoaja voi pyynnöstä toimittaa suojausominaisuudet suojattavien kohteiden omistajalle. Ominaisuuksien tarjoamisen ehdot eivät kuulu standardin soveltamisalaan. Lisäksi teollisuuden automaatio- ja ohjausjärjestelmän palveluntarjoajat voivat käyttää IEC 62443-2-4 -standardia turvaohjelmiensa jäsentämiseen ja parantamiseen. Palveluntarjoajat voivat myös käyttää standardeja IEC 62443-3-3 ja IEC 62443-4-2 yhdessä standardin IEC 62443-2-4 kanssa työskennellessään taustalla olevien teollisuuden automaatio- ja ohjausjärjestelmien tai komponenttien toimittajien kanssa.

Suojattavien kohteiden omistajat voivat käyttää IEC 62443-2-4 -standardia vaatiakseen tiettyjä tietosuojausominaisuuksia palveluntarjoajalta. Tarkemmin sanottuna suojattavien kohteiden omistajat voivat käyttää IEC 62443-2-4 -standardia ennen tällaista pyyntöä määrittääkseen, sisältääkö tietyn palveluntarjoajan tietosuojausohjelma suojattavien kohteiden omistajan tarvitsemat ominaisuudet.

4.3 Järjestelmä -kategoria

IEC 62443 -standardisarjan tässä kategoriassa tarjotaan suosituksia ja ohjeita tietoturvateknologioiden ja lieventämismenetelmien käyttöön teollisuuden automaatio- ja ohjausjärjestelmäympäristöissä. Painopiste on tietoturvakäytäntöjen kehittämisessä haavoittuvuuksien tunnistamiseksi ja riskien vähentämiseksi. Osa käsittelee myös elektronisen kyberturvan teknologioita ja antaa ohjeita niiden kehittämiseen, käyttöönottoon ja ylläpitoon. Tämän lisäksi keskitytään organisaatioiden riskeihin arvioinnissa ja turvallisuusvastatoimien soveltamisessa teollisuuden automaatio- ja ohjausjärjestelmiin.

4.3.1 IEC TR 62443-3-1 Security technologies for IACS

Tämä tekninen raportti tarjoaa ehdotuksia ja ohjeita kyberturvateknologioiden ja lieventämismenetelmien käyttöön. Se sisältää myös tietoja, jotka on otettava huomioon kehitettäessä organisaation tietoturvakäytäntöjä, -ohjelmia ja menettelytapoja teollisuuden automaatio- ja ohjausjärjestelmäympäristöä varten.

Tekninen raportti auttaa tunnistamaan ja käsittelemään haavoittuvuuksia. Sen lisäksi se tarjoaa mahdollisuuden kehittää menetelmiä, joilla erilaiset tietohyökkäysten riskitekijät voidaan tunnistaa ja niiden vaikutuksia pienentää. Tämän avulla voidaan varmistaa, että saavutetaan hyväksyttävä riskitaso. Raportti toimii tehokkaana työkaluna luottamuksellisten tietojen suojaamiseksi ja estääkseen mahdollisia vahinkoja ihmisille ja ympäristölle.

Tekninen raportti auttaa tunnistamaan ja käsittelemään haavoittuvuuksia sekä auttaa luomaan menetelmän, jolla voidaan tunnistaa eri tietohyökkäyksen riskitekijät ja pienentämään riskiä, joka voisi vaarantaa luottamukselliset tiedot tai aiheuttaa ihmisille ja ympäristölle vahinkoa. Tekninen raportti auttaa myös tunnistamaan ja käsittelemään teollisen verkon tai ohjausjärjestelmien ja niiden valvomien ja säätämien teollisuuden ja infrastruktuurin kriittisten omaisuuserien toimintahäiriöitä.

Raportti arvioi monia nykyisiä elektroniseen kyberturvaan liittyviä teknologioita, lieventämismenetelmiä ja työkaluja, jotka voivat soveltua teollisuuden automaatio- ja ohjausjärjestelmän ympäristön tietohyökkäysten ja iskujen suojaamiseen. Raportti käsittelee näiden teknologioiden, menetelmien ja työkalujen kehitystä, käyttöönottoa, toimintaa, ylläpitoa, suunnittelua ja muita käyttäjäpalveluita. Lisäksi raportti tarjoaa ohjeita teknologisista vaihtoehdoista ja vastatoimista teollisuuden automaatio- ja ohjausjärjestelmien (ja niihin liittyvien teollisuusverkkojen) suojaamiseen tietoturvahyökkäyksiltä. Ohjeita voivat hyödyntää valmistajat, myyjät ja tietoturvakäytäntöjen harjoittajat loppukäyttäjien organisaatioissa, laitoksissa ja teollisuudessa.

Teknisen raportin ohjeistus tunnistaa ne toimet, jotka ovat tyypillisesti tärkeitä tietosuojattujen ohjausjärjestelmien tarjoamiseksi, mutta joiden soveltaminen ei aina ole yhteensopiva järjestelmän tehokkaan toiminnan tai ylläpidon kanssa. Ohjeistus sisältää ehdotuksia ja suosituksia asianmukaisten tietoturvasovellusten käytöstä tietyissä ohjausjärjestelmissä. Tietyn järjestelmän ja siihen liittyvän teollisuusverkon erityisten tietoturva-aktiviteettien ja käytäntöjen valitseminen ja käyttöönotto on järjestelmän omistajan vastuulla.

4.3.2 IEC 62443-3-2 Security risk assessment for system design

Standardi määrittelee joukon toimenpiteitä, jotka ohjaavat organisaatiota prosessissa, jossa arvioidaan tietyn teollisuuden automaatio- ja ohjausjärjestelmään liittyviä riskejä ja tunnistetaan sekä sovelletaan turvallisuusvastatoimia riskien vähentämiseksi siedettävälle tasolle. Standardin keskeinen käsite on teollisuuden automaatio- ja ohjausjärjestelmän turvavyöhykkeiden ja väylien soveltaminen. Vyöhykkeet ja väylät esitellään IEC TS 62443-1-1:ssa. Standardin kohdeyleisöön kuuluvat suojattavien kohteiden omistajat, järjestelmäintegraattorit, tuotetoimittaja, palveluntarjoaja ja viranomaiset. Standardi tarjoaa perustan turvallisuusvastatoimien määrittelylle yhdistämällä standardissa tunnistetut tavoiteturvatasot (SL-T) IEC 62443-3-3:ssa määriteltyihin vaadittuihin turvatasokyvykkyyksiin (SL-C). IEC 62443-sarjan tämä osa määrittelee vaatimukset tarkasteltavana olevalle järjestelmälle (SuC), ja jakaa järjestelmän vyöhykkeisiin ja

väyliin, arvioi riskin kullekin vyöhykkeelle ja väylälle, asettaa kullekin vyöhykkeelle ja väylälle tavoiteturvallisuustason (SL-T) ja dokumentoi turvallisuusvaatimukset.

4.3.3 IEC 62443-3-3 System security requirements and security levels

Standardi edellyttää, että tietoturvallisuusohjelma on perustettu ja toimii IEC 62443-2-1:n mukaisesti. Lisäksi oletetaan, että korjauspäivitysten hallinta on toteutettu johdonmukaisesti IEC/TR 62443-2-3:ssa esitettyjen suositusten mukaisesti käyttäen asianmukaisia järjestelmävaatimuksia ja vaatimusten lisäyksiä. IEC 62443-3-2 kuvaa, miten projekti määrittelee riskiperusteiset turvatasot (SL), joita käytetään tuotteiden valinnassa standardin yksityiskohtaisesti kuvattujen teknisten tietoturvakyvykkyyksien perusteella. Standardi tarjoaa yksityiskohtaisia teknisiä järjestelmävaatimuksia (SR), jotka liittyvät seitsemään perusvaatimukseen (FR), kuten on kuvattu IEC 62443-1-1:ssä, järjestelmän turvatasokyvykkyys (SL-C) vaatimukset mukaan lukien.

IEC 62443-1-1:ssä on määritelty yhteensä seitsemän perusvaatimusta (FR), jotka ovat tunnistus ja todennus, käytön hallinta, järjestelmän eheys, tietojen luottamuksellisuus, rajoitettu tietovirta, ajoissa tapahtuva vaste tapahtumaan ja resurssien saatavuus. Nämä seitsemän vaatimusta ovat perusta teollisuuden automaatio- ja ohjausjärjestelmän turvatasokyvykkyydelle (SL-C). Standardin tavoite ja tarkoitus on määritellä turvatasokyvykkyys (SL-C) teollisuuden automaatio- ja ohjausjärjestelmälle, toisin kuin tavoiteturvataso (SL-T) tai saavutettu turvataso (SL-A), jotka eivät kuulu tämän standardin soveltamisalaan.

4.4 Komponentti-kategoria

IEC 62443 -standardisarjan tässä kategoriassa käsitellään tietoturvallisuuteen liittyviä elinkaarivaatimuksia teollisuusautomaatio- ja ohjausjärjestelmäympäristössä käytettäville tuotteille. Standardi tarjoaa ohjeita turvallisten tuotteiden kehittämiseen, määritellen kyberturvavaatimukset automaatio- ja ohjausjärjestelmätuotteiden kehittäjille. Se sisältää tekniset vaatimukset komponenteille, kuten

sulautetuille laitteille, verkkolaitteille ja ohjelmistosovelluksille, ja johtaa turvatasokyvykkyydet, joiden avulla komponentit voivat torjua uhkia ja saavuttaa tietyn turvallisuustason. Standardi on suunnattu järjestelmäintegraattoreille, tuotetoimittajille ja viranomaisille, auttaen ymmärtämään ja täyttämään kyberturvaan liittyvät vaatimukset tuotteiden osalta teollisuusautomaatio- ja ohjausjärjestelmissä.

4.4.1 IEC 62443-4-1 Product development requirements

Standardissa kuvataan kyberturvallisuuteen liittyvät tuotekehityksen elinkaarivaatimukset teollisuusautomaatio- ja ohjausjärjestelmäympäristössä käytettäville tuotteille ja annetaan ohjeita vaatimusten täyttämiseksi. Standardi sisältää kyberturvavaatimukset kaikille automaatio- ja ohjaustuotteiden kehittäjille, joissa kyberturva on huomioitava. Standardi määrittelee prosessivaatimukset turvallisten tuotteiden kehittämiseksi teollisuuden automaatio- ja ohjausjärjestelmiin. Se määrittelee kyberturvatuotteiden kehityksen elinkaaren kyberturvatuotteiden kehittämiseksi ja ylläpitämiseksi. Elinkaari sisältää kyberturvavaatimusten määrittelyn, turvallisen suunnittelun ja toteutuksen, jolla voidaan täyttää vaatimukset turvatasosta.

4.4.2 IEC 62443-4-2 Technical security requirements for IACS components

Standardi määrittelee kyberturvallisuustekniset vaatimukset komponenteille, jotka muodostavat teollisuuden automaatio- ja ohjausjärjestelmän. Näitä komponentteja ovat sulautettu laite, verkkolaite, isäntälaite ja ohjelmistosovellus. Standardi johtaa vaatimuksensa teollisuuden automaatio- ja kyberturvavaatimuksista, kuten on kuvattu IEC 62443-3-3:ssa. Standardin määritetään tietoturvakyvykkyys, jonka avulla komponenteilla on kyky torjua uhkia, tiettyyn turvallisuustasoon (SL) ilman korvaavia vastatoimia.

Järjestelmäintegraattorit, tuotetoimittajat ja tarvittaessa myös viranomaiset ovat tämän standardin kohderyhmä. Järjestelmäintegraattorit käyttävät standardia

apuna ohjausjärjestelmäkomponenttien hankinnassa. Ohjausjärjestelmäkomponentit muodostavat teollisuuden automaatio- ja ohjausjärjestelmän ratkaisun. Integraattorit määrittävät yksittäisten komponenttien riittävän turvatasokyvykkyyden. Tuotetoimittajat puolestaan käyttävät standardia ymmärtääkseen, millaisia vaatimuksia asetetaan ohjausjärjestelmäkomponenteille niiden turvatasokyvykkyyden mukaan. Komponentti saattaa olla suunniteltu niin, ettei se tarjoa vaadittua kyvykkyyttä itsessään, vaan se voi olla suunniteltu integroitumaan korkeamman tason yksikön kanssa ja hyötyvän tämän yksikön kyvykkyydestä.

Standardi opastaa tuotetoimittajia siinä, mitkä turvavaatimukset voidaan kohdentaa ylemmän tason järjestelmälle ja mitkä vaatimukset tulisi olla luontaisia komponenteissa. Tuotetoimittaja tarjoaa dokumentaatiota siitä, miten komponentti voidaan integroida asianmukaisesti järjestelmään saavuttaakseen tietyn tavoiteturvallisuustason (SL-T). Standardin komponenttivaatimukset (CR) johdetaan IEC 62443-3-3:n järjestelmävaatimuksista (SR). Vaatimukset IEC 62443-3-3:ssa ovat nimeltään järjestelmävaatimukset (SR), jotka johdetaan IEC 62443-1-1:ssä määritellyistä yleisistä perusvaatimuksista (FR). Järjestelmävaatimukset voivat myös sisältää joukon vaatimuksen parannuksia (RE). Komponenttivaatimusten ja vaatimusten parannusten yhdistelmä määrittää, millä turvallisuustasolla komponentti voidaan esittää kykenevän toimimaan. Komponenttityypin komponenttivaatimukset ovat:

- Ohjelmistosovellusvaatimukset (SAR),
- Sulautetun laitteen vaatimukset (EDR),
- Isäntälaitteen vaatimukset (HDR),
- Verkkolaitteen vaatimukset (NDR)

Seitsemän perusvaatimusta (FR), jotka on määritelty IEC/TR 62443-1-1:ssä, ovat perusta ohjausjärjestelmän turvatasokyvykkyyksien määrittelylle. Tämän teknisen raportin tavoite ja tarkoitus on määritellä ohjausjärjestelmäkomponentin turvatasokyvykkyydet (SL-C).

5 Käsitteet ja soveltaminen

Tämän luvun ja aliluvun tiedot perustuvat lähteisiin (5–16).

Tässä osiossa tarkastellaan IEC 62443 -standardisarjan keskeisiä käsitteitä ja niiden määritelmiä. Ymmärtämällä nämä käsitteet voi tehokkaasti omaksua standardisarjan vaatimukset ja hyödyntää niitä. Tämä vastaa kielen opiskelua, jossa sanastoa opitaan muodostamaan merkityksellisiä lauseita.

5.1 Toimijat

IEC 62443-standardisarja määrittelee kolme keskeistä toimijaa: suojattavien kohteiden omistajan, järjestelmäintegraattorin ja tuotetoimittajan.

Suojattavien kohteiden omistaja vastaa yhdestä tai useammasta teollisuuden automaatio- ja ohjausjärjestelmästä, huolehtien niiden operatiivisesta toiminnasta ja ylläpidosta. IEC 62443-2-1 ja IEC 62443-2-4 -standardit asettavat vaatimuksia teollisuuden automaatio- ja ohjausjärjestelmään, mikä puolestaan asettaa vaatimuksia suojattavien kohteiden omistajalle.

Järjestelmäintegraattori yhdistää komponentit ja alijärjestelmät yhdeksi kokonaisuudeksi, muodostaen teollisuuden automaatio- ja ohjausjärjestelmän. Integraattori varmistaa, että kaikki komponentit ja alijärjestelmät toimivat projektin määritysten mukaisesti. Järjestelmäintegraattorilla on kyky suorittaa integraatioprosessi, joka sisältää suunnittelun ja käyttöönoton. IEC 62443-2-4- ja IEC 62443-3-2-standardit asettavat vaatimuksia järjestelmien integroinnille, ja siten järjestelmäintegraattorille kohdistuvia vaatimuksia.

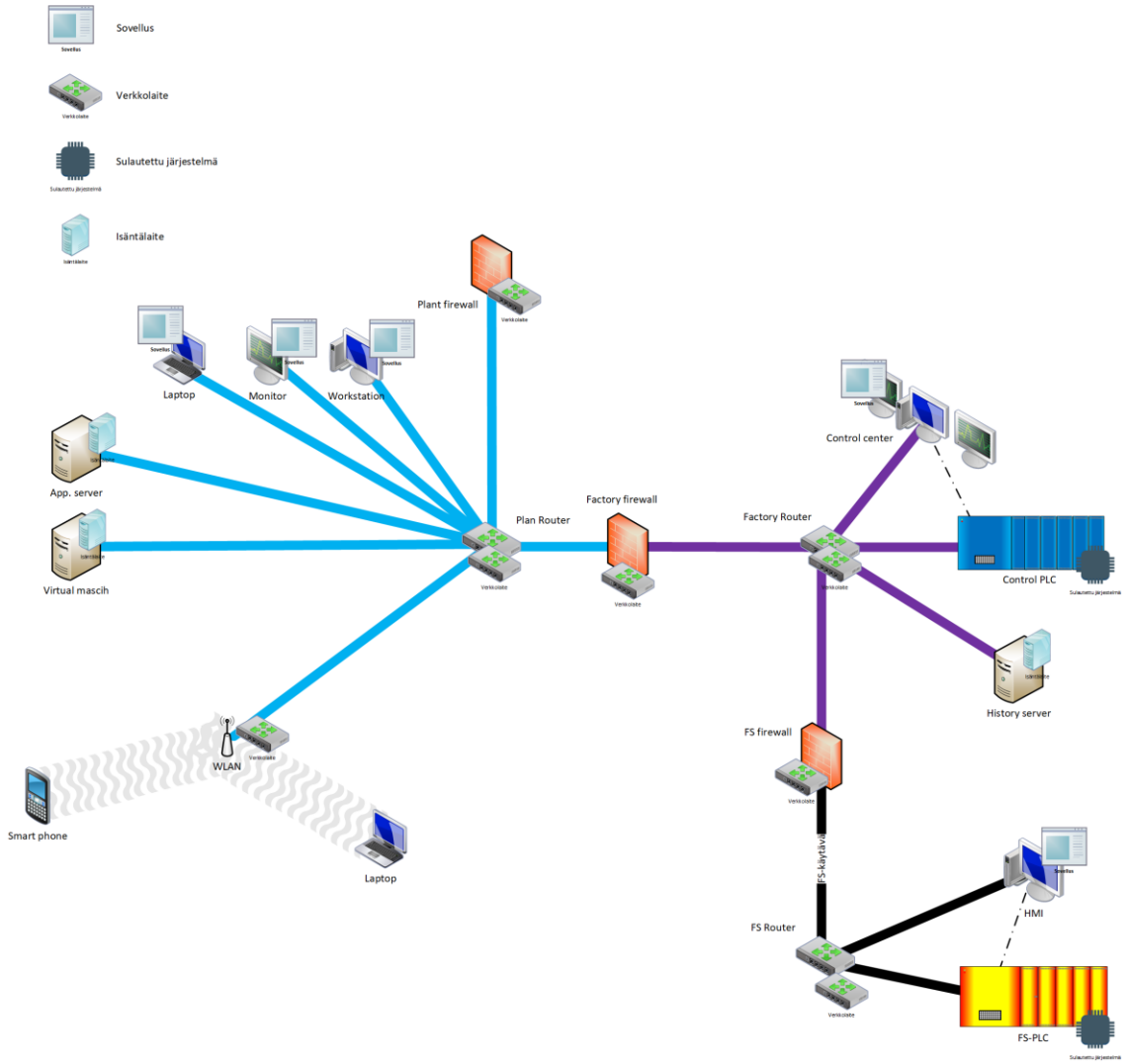
Tuotetoimittaja on laitteiston tai ohjelmistotuotteen valmistaja. Standardisarjan mukaan tuotetoimittaja valmistaa komponentteja, joista teollisuuden automaatio- ja ohjausjärjestelmät koostuvat. Tuotetoimittajalla on prosessi ja kyvykkyys tuottaa komponenteille tietty turvallisuustaso. IEC 62443-4-1 asettavat vaatimuksia komponenttien kehitykselle ja siten tuotetoimittajille.

5.2 Komponentti

Komponentti on tuotetoimittajan valmistama laitteisto tai ohjelmistotuote. IEC 62443-standardisarja määrittelee neljä eri komponenttityyppiä: ohjelmistosovellus, sulautettu järjestelmä, verkkolaite ja isäntälaite. Komponenteille asetetaan vaatimuksia IEC 62443-4-2-standardissa.

5.3 Teollisuuden automaatio- ja ohjausjärjestelmä

IEC 62443-standardisarjan mukaan teollisuuden automaatio- ja ohjausjärjestelmä rakentuu neljästä komponentista: ohjelmistosovelluksista, sulautetuista järjestelmistä, verkkolaitteista ja isäntälaitteista. Kuva 4 esitetyssä verkkoarkkitehtuurissa havainnollistetaan selkeästi, miten nämä komponentit jaetaan eri osiin standardin viitekehyksessä. Järjestelmän jakaminen eri komponentteihin mahdollistaa tehokkaamman tietoturvan hallinnan ja avaa mahdollisuuden tunnistaa potentiaaliset riskit kussakin osassa. IEC 62443-3-3 -standardi asettaa järjestelmän tekniset turvallisuusvaatimukset teollisuusautomaatio- ja ohjausjärjestelmille, varmistaen näin koko järjestelmän turvallisen toiminnan.



Kuva 4. IEC 62443-standardisarjassa teollisuuden automaatio- ja ohjausjärjestelmä koostuu neljästä komponentista: sovellukset, verkkolaiteet, sulautetut järjestelmät ja isäntälaiteet.

5.4 Turvallisuus

Turvallisuudella IEC 62443-standardisarjassa viitataan vapauteen sietämättömästä riskistä. Käsite sisältää laittoman tai ei-toivotun toiminnan, kuten tunkeutumisen, tarkoituksellisen tai tahattoman häirinnän ja sopimattoman pääsyn estämisen teollisuuden automaatio- ja ohjausjärjestelmän luottamuksellisiin tietoihin.

5.5 Haavoittuvuus

Haavoittuvuus määritellään puutteeksi tai heikkoudeksi järjestelmän suunnittelussa, toteutuksessa, toiminnassa ja hallinnassa, joka mahdollistaa järjestelmän eheyden tai tietoturvapolitiikan vaatimus en rikkomisen.

5.6 Loukkaus

Ulkoisen toimijan tunkeutumisen tai hyväntahtoisen sisäpiiriläisen toiminnan seurauksena tapahtuva toiminta tai tapahtuma, joka rikkoo tietoturvapolitiikan vaatimuksia.

5.7 Tunkeutuminen

Tunkeutuminen tapahtuu, kun käyttäjä saa pääsyn järjestelmään (tai sen resursseihin) ilman asianmukaista valtuutusta.

5.8 Hyökkäys

Toimi, joka on tarkoituksellinen yritys (erityisesti menetelmän tai tekniikan näkökulmasta) välttää turvatoimenpiteitä ja rikkoa järjestelmän tietoturvakäytäntöjä.

5.8.1 Hyökkäysluokat

Hyökkäyksillä on erilaisia tunnustettuja luokkia. Aktiivinen hyökkäys pyrkii muuttamaan järjestelmän resursseja tai vaikuttamaan niiden toimintaan. Passiivinen hyökkäys taas tavoittelee järjestelmän tietojen oppimista tai hyödyntämistä ilman vaikutusta resursseihin. Sisäinen hyökkäys käynnistyy organisaation sisältä, tyypillisesti sisäverkosta sisäpiirin toimesta, ja käyttää hyväksi resursseja ilman asianmukaista valtuutusta. Ulkopuolisen hyökkäyksen alkuperä on järjestelmän ulkopuolelta (internetistä tai organisaation eri verkkoalueelta), luvattomalta tai laittomalta käyttäjältä. Hyökkäys saattaa olla sisäpiiriläisen tekemä tai avustama, mutta hyökkäykselle on ominaista toimia sisäverkon ulkopuolelta.

Ulkopuoliset hyökkääjät voivat vaihdella amatööreistä järjestäytyneisiin rikollisiin, kansainvälisiin terroristeihin ja vihamielisiin valtioihin. Kuva 5 on esimerkkejä, jotka on esitetty hyökkäysluokan nelikentässä.

	Passiivinen	Aktiivinen
Sisäinen	Työntekijä joka jättää monitorointilaitteen yrityksen sisäverkkoon.	Alihankkija pyrkii tuhomaan yrityksen sisäverkossa olevan tiedoston.
Ulkopuolinen	Turvallisuuspalvelu, joka on saanut välitettyä haittaohjelman yrityksen verkkoon, joka kuuntelee liikennettä.	Rikollisjärjestö on saanut toimitettua lunnastroijalaisen yrityksen tietojärjestelmään.

Kuva 5. Hyökkäysluokkia on passiivinen ja aktiivinen sekä sisäinen ja ulkopuolinen.

5.9 Uhka

Uhka on potentiaalinen turvallisuusloukkaus, ja se ilmenee, kun olosuhde, kyvykkyys, toiminta tai tapahtuma voi rikkoa turvallisuutta ja aiheuttaa haittaa. Joitakin esimerkkejä uhkista on:

- Hyvää tarkoittava sisäpuolinen työntekijä saa fyysisen pääsyn prosessinohjausalueelle ja liittää USB-muistitikun johonkin tietokoneista.
- Hyvää tarkoittava ulkopuolinen työntekijä (aliurakoitsija) pääsee prosessinohjausalueelle tartunnan saaneella kannettavalla tietokoneella.
- Hyvää tarkoittava sisäinen työntekijä avaa tietojenkalasteluviestin, joka vaarantaa hänen käyttöoikeustietonsa.

Uhkan onnistumiseksi on hyödynnettävä yhtä tai useampaa haavoittuvuutta. Siksi on välttämätöntä tunnistaa laitteisiin ja ohjelmistoihin liittyvät tunnetut haavoittuvuudet, jotta voidaan estää tai vaikeuttaa turvaloukkauksen tapahtumista.

5.10 Loukkauksen toteutumisen todennäköisyys

Kun arvioidaan loukkauksen toteutumisen todennäköisyyttä, otetaan huomioon sekä uhan realisoitumisen todennäköisyys että mahdollisen haavoittuvuuden hyödyntämisen todennäköisyys. Esimerkiksi viruksen vaikutusta verkon toimintaan arvioitaessa tulee ensin arvioida, miten todennäköistä on, että virus saa pääsyn verkkoon, ja sen jälkeen arvioida, miten todennäköistä on, että virus kykenee kiertämään verkon virustorjuntaohjelmat. Loukkauksen todennäköisyys voidaan ilmaista seuraavalla kaavalla:

$$P_{Loukkaus} = P_{Uhka,loukkaus} \times P_{Haavoittuus,loukkaus} \quad (1)$$

, jossa $P_{Loukkaus}$ on loukkauksen todennäköisyys, $P_{Uhka,loukkaus}$ on uhan realisoitumisen todennäköisyys ja $P_{Haavoittuus,loukkaus}$ on haavoittuvuuden hyödyntämisen todennäköisyys. Kaavassa (1) merkki × viittaa joko kvantitatiiviseen tulomerkintään, joka perustuu todennäköisyysjakaumiin, tai kvalitatiiviseen tulomerkintään, joka perustuu epävarmuuden määrään arvioon. Tyypillisesti kvantitatiivisessa tilanteessa käytetään heuristisia menetelmiä epävarmuuden tason arvioimiseksi.

Kirjoitushetkellä IEC 62443-standardisarja ei sisällä kvalitatiivista menetelmää todennäköisyyden ja siten riskien arvioimiseen.

5.11 Loukkauksen vakavuus

Uhkien ja haavoittuvuuksien lisäksi on arvioitava loukkauksen seurauksen vakavuus, joka ilmenee negatiivisena vaikutuksena organisaation omaisuuteen tai toimintaan. Tämä voi konkretisoitua esimerkiksi tuotantolaitoksen prosessin keskeytymisenä, mikä johtaa taloudellisiin menetyksiin. Lisäksi loukkaus voi

aiheuttaa henkilövahinkoja tai ympäristöongelmia, jotka usein muunnetaan rahallisiksi menetyksiksi, jotta kaikki mahdolliset vaikutukset voidaan yhdistää saman vakavuuden mittapuun alle. Suojattavien kohteiden omistajien on myös otettava huomioon riskien vähentämiseen tai korjaamiseen liittyvät kustannukset.

5.12 Riski

Riski on yhdistelmä loukkauksen todennäköisyyttä ja sen aiheuttaman vahingon vakavuutta. Riski koostuu uhasta, haavoittuvuudesta ja loukkauksen vakavuudesta. Uhka- ja haavoittuvuuskomponentit voivat ilmetä todennäköisyysarvioina. Riski voidaan tarkemmin määritellä odotusarvoksi tappiolle, joka ilmaistaan todennäköisyytenä, että tietty uhka käyttää hyväkseen tiettyä haavoittuvuutta (eli loukkaus) tietyllä seurauksella. Riski voidaan määrittää sekä kvantitatiivisesti että kvalitatiivisesti (yleensä heuristisesti) seurauksen ja loukkauksen todennäköisyyden tulona (kaava 2).

$$R_{loukkaus} = S_{loukkaus} \times P_{Loukkaus} \quad (2)$$

, jossa $R_{loukkaus}$ on tapahtuman riskin määrä, $S_{loukkaus}$ on loukkauksen seuraus eli tappion määrä ja $P_{Loukkaus}$ loukkauksen toteutumisen todennäköisyys. Riskinarvioinnissa usein luodaan riskimatriisi, jossa pystyrivit kuvaavat tapahtuman todennäköisyyttä (esim. epätodennäköinen, mahdollinen tai todennäköinen) ja vaakarivit kuvaavat tapahtuman seurausta eli tappion määrää (esim. vähäinen, haitallinen tai vakava). Kenttiin merkitään riskin sieto seuraavilla arvoilla: merkityksetön riski, vähäinen riski, kohtalainen riski, merkityksellinen riski ja sietämätön riski.

Taulukko 1. Eräs esimerkki riskimatriisista.

Tapahtuman todennäköisyys	Tapahtuman seuraus		
	Vähäiset	Haitalliset	Vakavat
Epätodennäköinen	Merkityksetön	Vähäinen	Kohtalainen
Mahdollinen	Vähäinen	Kohtalainen	Merkittävä
Todennäköinen	Kohtalainen	Merkittävä	Sietämätön

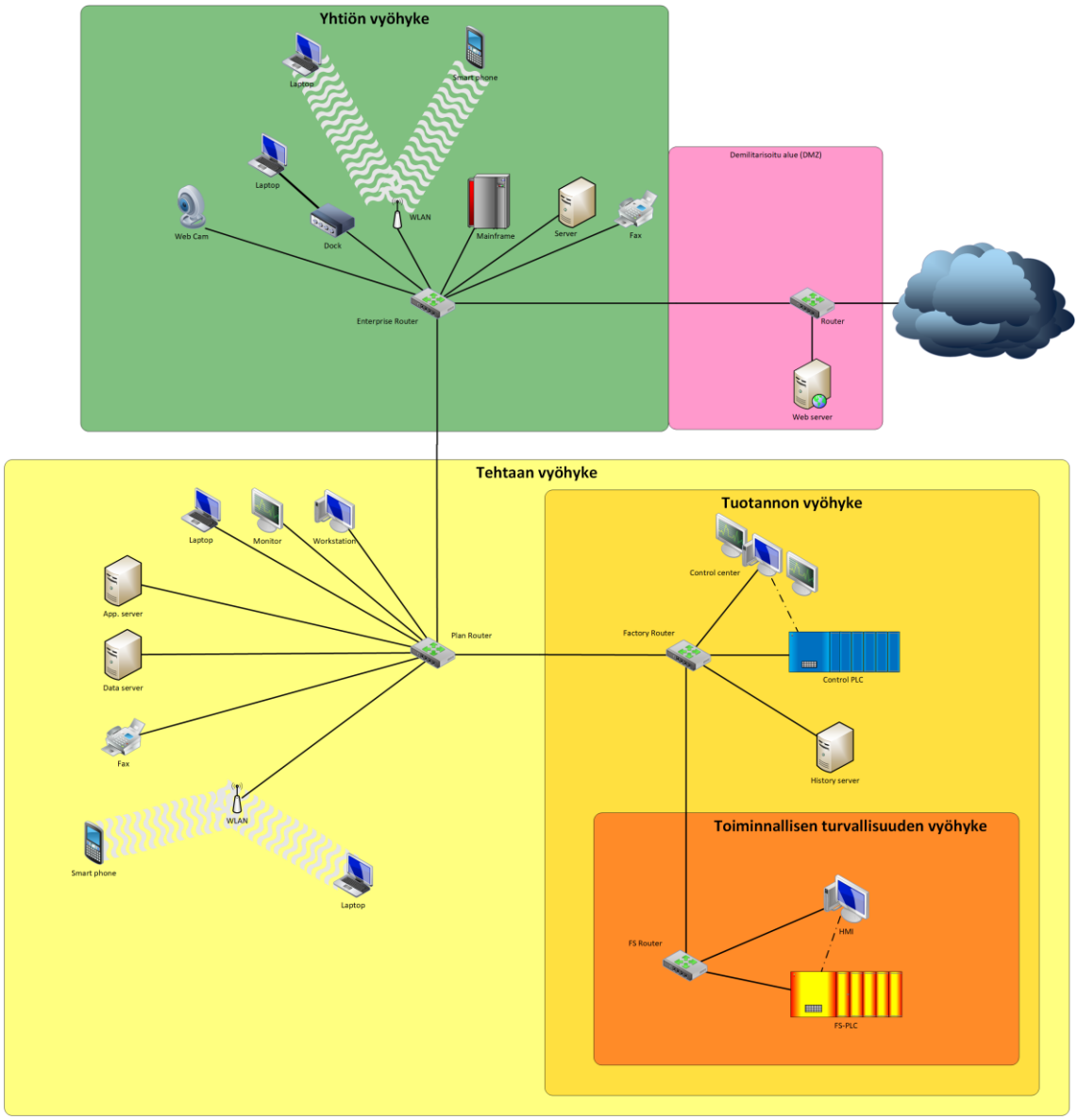
Riskimatriisista yritys voi päätellä, mikä on yrityksen riskin sietokyky ja asettaa tavoitteen, mihin kohtaan matriisia halutaan asettaa tavoitteet tapahtuman riskin suhteen. Prosessi auttaa organisaatiota hahmottamaan, miten se suhtautuu riskeihin ja määrittelemään, millä tasolla se haluaa pitää eri riskit. Käytännössä tavoitteet voivat vaihdella organisaation tyypistä, liiketoiminnasta ja sidosryhmistä riippuen. Tavoitteiden asettamisen avulla organisaatio pyrkii hallitsemaan riskejä tehokkaasti ja tekemään strategisia päätöksiä riskienhallinnan suhteen.

5.13 Turvavyöhykkeet

Turvallisuustasot vaihtelevat tilanteiden mukaan, ja yksi suojataso ei ole yleispätevä kaikille järjestelmän osille. Tämän vuoksi turvallisuutta hallitaan turvavyöhykkeen käsitteellä. Turvavyöhyke on käytännössä looginen ryhmittely fyysisistä laitteista, joilla on samanlaiset suojausvaatimukset. Turvavyöhykkeiden käyttö helpottaa turvallisuusympäristön hallintaa, kun tiettyjä järjestelmiä ryhmitellään turvavyöhykkeisiin, ja toiset pidetään vyöhykkeiden ulkopuolella. Turvavyöhykkeiden sisällä voi myös olla alivyöhykkeitä, jotka tarjoavat lisäkerroksen turvallisuutta erilaisiin turvallisuusvaatimuksiin vastaamiseksi.

Suurten järjestelmien suojaamiseksi saatetaan tarvita monimutkaisia suojaustoimia. Tehokas turvallisuusstrategia voidaan toteuttaa noudattamalla syvyyssuuntaisen turvallisuussuunnittelun periaatetta (Defense in Depth), jossa käytetään useita vastatoimia kerrostetusti tai vaiheittain. Esimerkiksi tunkeutumisen havaitsemisjärjestelmät voivat havaita ja raportoida mahdolliset verkkoon tunkeutumiset.

Turvavyöhykkeellä on selkeästi määritelty raja, joka erottaa siihen sisältyvät ja poissuljetut elementit. Pääsy vyöhykkeen resursseihin on hallittava sekä sisältä että ulkopuolelta. Tämä säätelee tiedonsiirtoa ja pääsyä vyöhykkeen suojattaviin kohteisiin ja mahdollistaa täten tiedon ja ihmisten liikkumisen turvavyöhykkeiden sisällä ja välillä asianmukaisia valtuusrajoituksia noudattaen. Jokaisella vyöhykkeellä on omat attribuutit, kuten turvallisuuskäytännöt, omaisuusluettelo, pääsyvaatimukset, uhkat ja haavoittuvuudet, loukkauksen seuraukset, hyväksytyt tekniikat sekä muutoksenhallintaprosessit. Vyöhykkeet voivat olla luotettavia tai epäluotettavia ja ne voidaan määritellä fyysisesti tai loogisesti. Fyysiset vyöhykkeet järjestetään omaisuuden fyysisen sijainnin perusteella, kun taas loogiset vyöhykkeet määritellään toimintojen tai muiden ominaisuuksien perusteella. Fyysisen vyöhykkeen perusteella järjestetty esimerkki teollisuusyrityksen turvavyöhykkeistä on havainnollistettu Kuva 6.



Kuva 6. Havainnollistava esimerkki yrityksen verkon eri vyöhykkeistä.

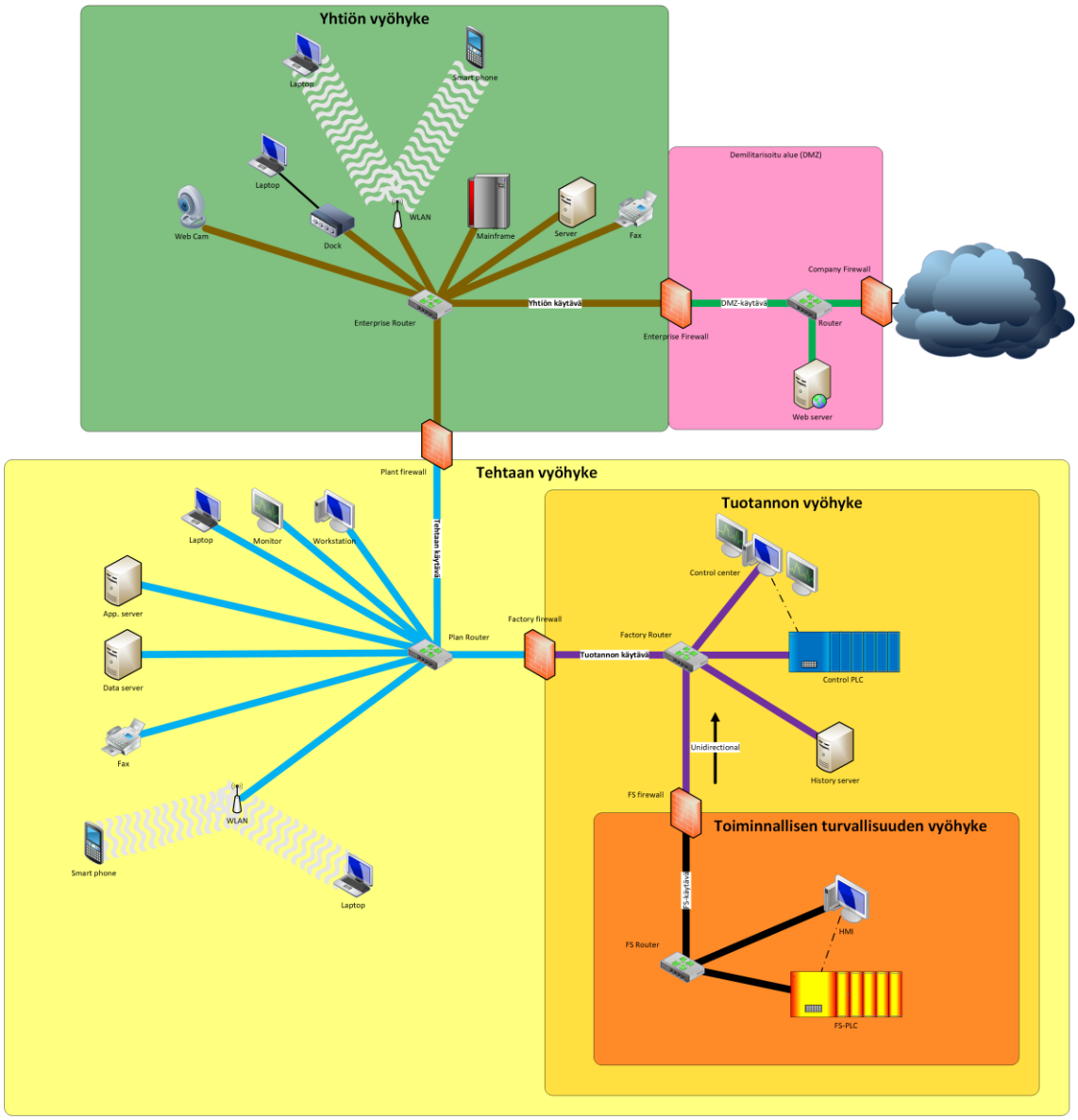
5.14 Käytävä

Käytävä on erityinen turvavyöhykkeen tyyppi, joka ryhmittelee viestinnän loogisesti organisoitavissa oleviin tietovirtoihin turvavyöhykkeen sisällä ja sen ulkopuolella. Se voi olla yksittäinen palvelu, kuten yksi Ethernet-verkko, tai koostua useista tietokantajista, kuten useista verkkokaapeleista ja suorista fyysisistä pääsyistä. Kuten turvavyöhykkeet, se voi koostua sekä fyysisistä että loogisista

rakenteista. Käytävät voivat yhdistää laitteita vyöhykkeen sisällä tai yhdistää eri turvavyöhykkeet.

Kuten turvavyöhykkeet, myös käytävät voivat olla joko luotettavia tai epäluotettavia. Vyöhykkeiden sisällä pysyvät kanavat ovat yleensä luotettavia vyöhykkeen sisällä viestivien prosessien toimesta. Luotettavien kanavien ylittäessä vyöhykerajoja on käytettävä päästä päähän olevaa turvallista prosessia.

Epäluotettavia kanavia ovat ne, jotka eivät ole samalla turvatasolla kuin vyöhykkeen päätepiste. Tässä tapauksessa itse viestinnän turvallisuus on yksittäisen kanavan vastuulla. Kuva 7 on esimerkkiyrityksen tietoliikennearkkitehtuuri, johon on merkitty käytävät ja niitä erottavat palomuurit.



Kuva 7. Havainnollistava esimerkki yrityksen vyöhykkeiden käytävistä.

5.15 Kanava

Kanavat ovat tietynlaisia viestintäyhteyksiä, jotka luodaan viestintäkäytävässä. Ne perivät käytetyn käytävän turvallisuusominaisuudet ja säilyttävät turvatun käytävän tarjoaman turvallisuustason. Kanavat voivat olla joko luotettavia tai epäluotettavia. Luotettavat kanavat mahdollistavat turvallisen viestinnän muiden turvavyöhykkeiden kanssa. Ne voivat myös laajentaa loogista turvavyöhykettä sisältäen laitteita fyysisen turvavyöhykkeen ulkopuolella.

Epäluotettavat kanavat ovat viestintäpolkuja, jotka eivät ylläpidä samanlaista turvatasoa kuin vertailtava turvavyöhyke. Viestintä viitevyöhykkeestä (alue, joka määrittelee viestinnän ei-turvalliseksi) vaatii tietojen validoinnin ennen niiden hyväksymistä.

5.16 Turvataso

Turvataso heijastaa vyöhykkeen tai käytävän vastatoimien vaadittua tehokkuutta sekä laitteiden ja järjestelmien luontaisia turvallisuusominaisuuksia riskinarvioinnin perusteella. Turvataso mahdollistaa vyöhykkeen tai käytävän riskin luokittelun ja auttaa määrittämään tarvittavan tehokkuuden vastatoimille, joita käytetään luvattoman toiminnan estämiseen.

Turvataso nähdään vyöhykkeen tai käytävän ominaisuutena, ei niinkään yksittäisen laitteen, järjestelmän tai osan ominaisuutena. Ajan myötä tietoturvan taso voi laskea vastatoimien heikkenemisen, uusien haavoittuvuuksien, mukautettujen uhkien tai hyökkäysmenetelmien, tietoturvakerrosten murtumisen sekä laitteiden ja järjestelmien luontaisten suojausominaisuuksien vuoksi.

Laitteiden tai järjestelmien luontaisten turvallisuusominaisuuksien heikkeneminen voi johtua uusien haavoittuvuuksien löytämisestä, parantuneista hyökkääjien taidoista, hyökkääjän tuntemuksesta olemassa olevista vastatoimista sekä hyökkääjien paremmista resursseista.

Suojaustasot jaetaan kolmeen tyyppiin: tavoiteturvataso (SL-T), saavutettu turvallisuustaso (SL-A) ja turvatasokyvykkyys (SL-C). Näitä tasoja sovelletaan tietoturvan elinkaaren eri vaiheissa IEC 62443 -standardisarjan mukaisesti.

Tavoiteturvataso (SL-T) kuvastaa haluttua turvallisuustasoa tietylle teollisuuden automaatio- ja ohjausjärjestelmälle ja määritellään yleensä riskinarvioinnin perusteella. Saavutettu turvataso (SL-A) puolestaan edustaa todellista turvallisuustasoa, kun järjestelmä on otettu käyttöön (on huomioitava, että

tietoturvataso laskee ajan myötä uusien haavoittuvuuksien ilmaantuessa ja järjestelmien vanhetessa). Turvatasokyvykkyys (SL-C) ilmoittaa, millaisen turvallisuustason komponentit voivat tarjota asianmukaisesti määritettyinä.

Turvatasot luokitellaan neljään kategoriaan: SL1, SL2, SL3 ja SL4, joista SL1 tarjoaa heikointa suojaa ja SL4 parasta suojaa. Näiden suojausluokkien kuvaukset vaihtelevat satunnaisista rikkomuksista (SL1) tahallisiin loukkauksiin kehittyneillä keinoilla, laajoilla resursseilla ja korkealla motivaatiolla (SL4). Suojaustasot tarjoavat kattavan viitekehyksen vyöhykkeen turvallisuuden hallintaan ja soveltuvat laajasti eri organisaatioille ja toimialoille. Taulukko 2 on esitetty turvatasojen kuvaukset taulukkomuodossa.

Taulukko 2. Turvatason neljä kategoriaa.

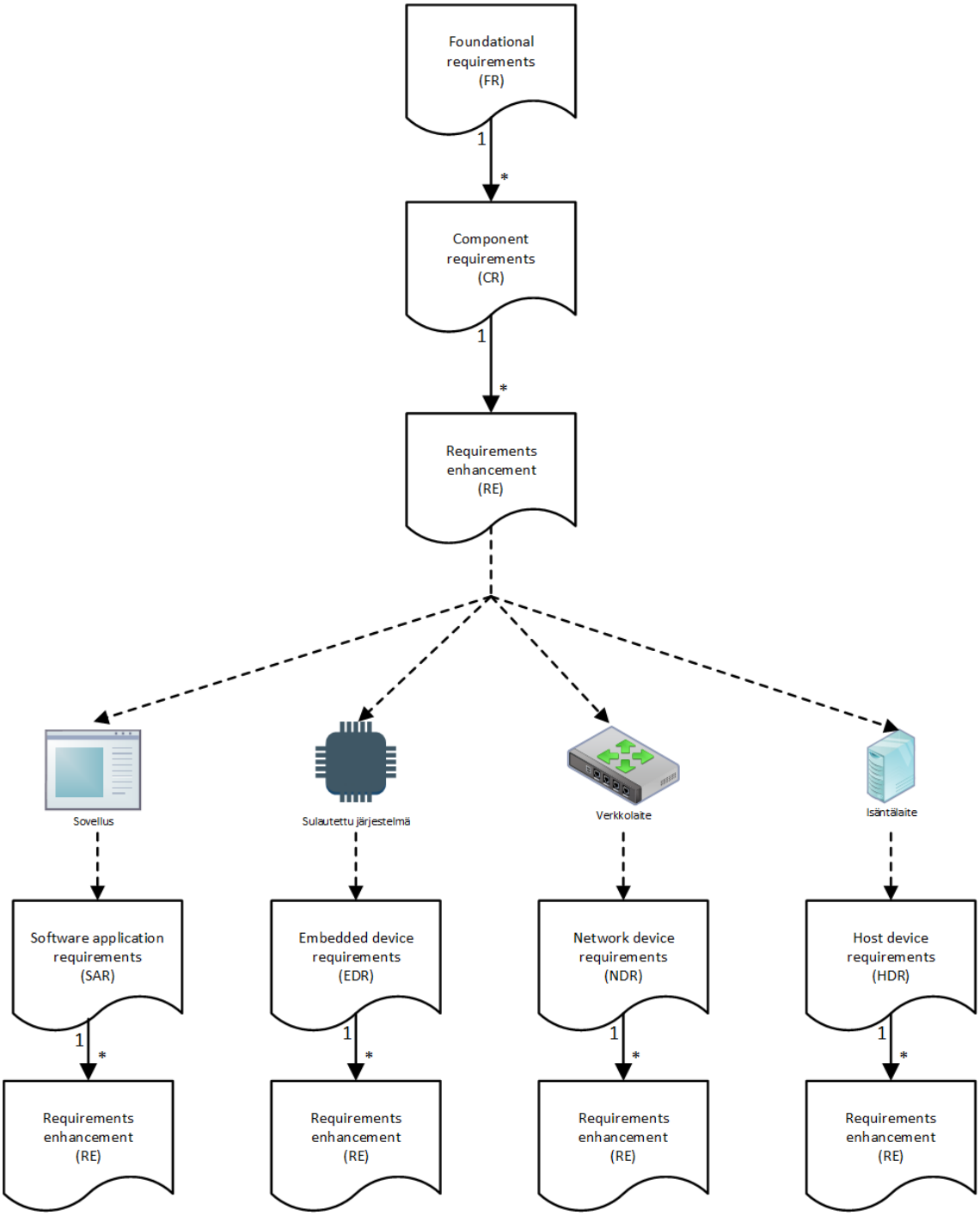
Turvallisuustaso	Tarkoitus	Keino	Resurssi	Taito	Motivaatio
SL1	Satunnainen	-	-	-	-
SL2	Tahallinen	Yksinkertainen	Vähän	Yleiset	Alhainen
SL3	Tahallinen	Kehittynyt	Kohtuullinen	Kohtalaiset	Kohtuullinen
SL4	Tahallinen	Kehittynyt	Laajat	Erityiset	Korkea

Esimerkkinä SL1-tason tekijästä voisi olla teini-ikäinen, joka sattumalta löytää haavoittuvuuden järjestelmästä. Kyberrikolliset voivat edustaa SL3-tason tekijöitä, sillä he saattavat olla kiinnostuneita kohteista, joissa on valmiita heikkouksia. Mikäli haavoittuvuutta ei löydy, he siirtyvät seuraavaan mahdolliseen kohteeseen. Valtiolliset toimijat puolestaan voisivat olla SL4-tason tekijöitä, jotka keskittyvät yhteen kohteeseen ja käyttävät valtavasti aikaa ja resursseja löytääkseen haavoittuvuuden kyseisen kohteen järjestelmästä.

5.17 Komponenttien vaatimukset

IEC 62443-standardisarjassa kaikille komponenteille määritellään kolmen tason vaatimukset. Ensimmäisen tason vaatimuksia kutsutaan perustaviksi vaatimuksiksi (FR). Perustavien vaatimusten alla ovat komponenttivaatimukset (CR), ja näiden alapuolella ovat vaatimusten parannukset (RE).

Jokaiselle komponentille on erikseen määritelty omat vaatimuksensa. Ohjelmistosovellukselle on asetettu ohjelmistosovelluksen vaatimukset (SAR), sulautetulle laitteelle on määritelty sulautetun laitteen vaatimukset (EDR), verkkolaitteelle on määritelty verkkolaitteen vaatimukset (NDR) ja isäntälaitteelle on määritelty isäntälaitteen vaatimukset (HDR). Kuva 8 on esitelty standardinsarjan komponenttien vaatimusrakenne.



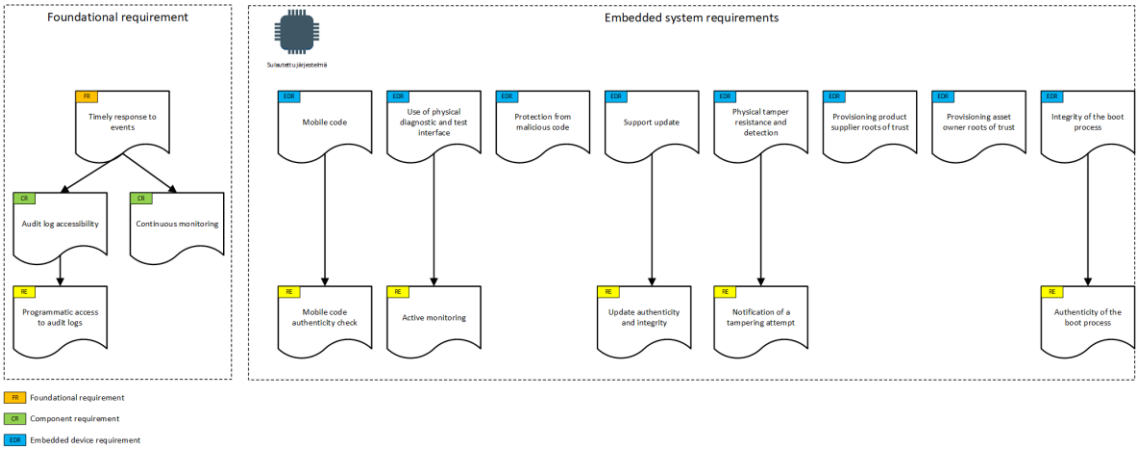
Kuva 8. IEC 62443-4-2 -standardin asettama komponenttien vaatimusrakenne.

Standardissa on tunnistettu seitsemän perusvaatimusta (FR) komponenteille.

Perusvaatimukset ovat:

- Tunnistus- ja todennusvalvonta (Identification and authentication control): Käyttäjien tunnistaminen ja oikeutetun pääsyn varmistaminen määriteltyihin järjestelmiin tai resursseihin.
- Käyttöhallinta (Use Control): Laitteiden tai tietojen suojaaminen luvattomalta käytöltä.
- Järjestelmän eheys (System Integrity): Viestintäkanavien tietojen eheyden varmistaminen suojaamalla niitä luvattomilta muutoksilta.
- Tietojen luottamuksellisuus (Data Confidentiality): Viestintäkanavien tietojen luottamuksellisuuden varmistaminen suojaamalla kanavat salakuuntelulta.
- Tietovirran rajoittaminen (Restrict Data Flow): Tietovirran liikkumisen rajoittaminen viestintäkanavilla estämään tiedon luvattoman julkaisemisen.
- Ajoissa tapahtuva vaste tapahtumaan (Timely Response to Event): Turvallisuusrikkomuksiin reagoidaan ilmoittamalla niistä mahdollisimman nopeasti oikealle taholle, raportoimalla tarvittavasta teknisestä näytöstä ja toteuttamalla ajoissa automaattisesti korjaavia toimenpiteitä toiminnallisesti kriittisissä tai turvallisuuskriittisissä tilanteissa.
- Resurssien saatavuus (Resource Availability): Kaikkien verkkoresurssien saatavuuden varmistaminen suojaamalla resursseja palvelunestohyökkäyksiä vastaan.

Kuva 9 esitetään esimerkki yhdestä perustavanlaatuisesta vaatimushaarasta sekä laitteen erityisvaatimuksista sulautetun laitteen osalta.



Kuva 9. Sulatetun laitteen yhden perusvaatimuksen alavaatimukset sekä komponenttivaatimukset.

Standardisarja edellyttää, että komponentin on täytettävä tietty määrä vaatimuksia, jotta voidaan väittää sen omaavan määritellyn turvallisuustason (SL1, SL2, SL3 tai SL4) kyvykkyyden.

5.18 Käsitteiden suhteet

Seuraavissa alaluvuissa käsitellään lyhyesti malleja ja seuraussuhteen käsitteitä. Näiden avulla voidaan kehittää prosesseja ja soveltaa menetelmiä uhka-arvioiden, haavoittuvuuksien ja eri ominaisuuksien riskiperusteiseen tarkasteluun. Ilman käsitteellistä ymmärrystä näistä suhteista ei voida kehittää malleja ja menetelmiä, jotka mahdollistavat riittävien vaatimustasojen saavuttamisen eri turvallisuustasoilla.

5.18.1 Uhkaketju

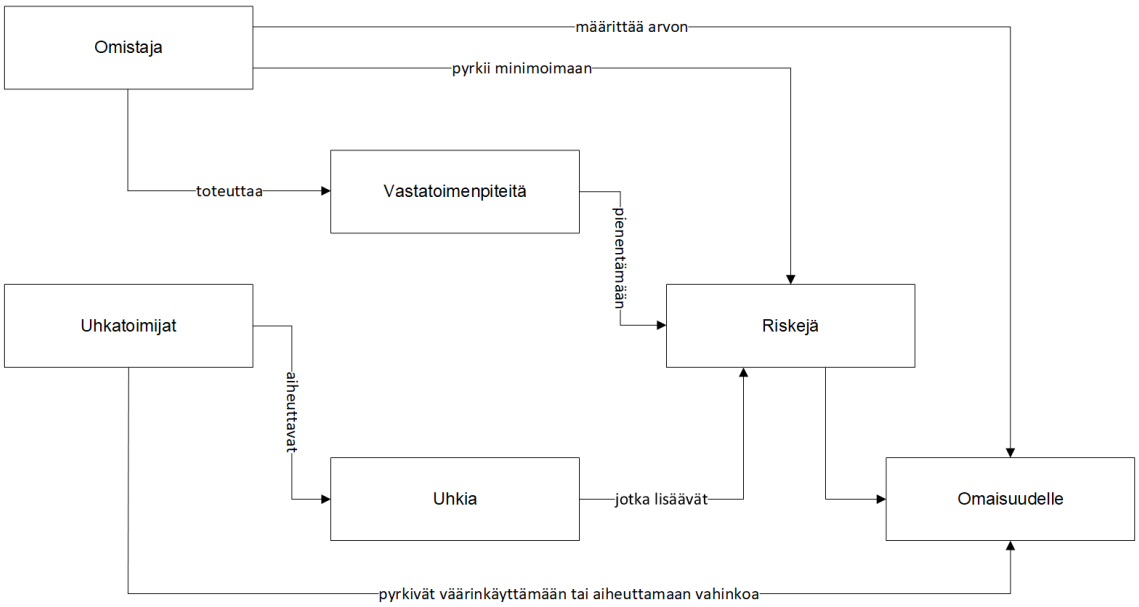
Uhka käyttää hyväkseen yhtä tai useampaa haavoittuvuutta mahdollistaen loukkauksen. Haavoittuvuus on ominaisuus, joka voi olla alttiina hyödyntämiselle,

kun taas uhka on mahdollinen tilaisuus hyödyntää kyseistä haavoittuvuutta hyväksi. Kuva 10 havainnollistetaan uhkaketjua.

Kuva 10. Uhkaketju koostuu uhasta, haavoittuvuudesta ja omaisuudesta.

5.18.2 Kontekstin elementtisuhteet

Kyberturvan kehittämisessä on välttämätöntä ymmärtää eri elementtien väliset suhteet, sillä tämä vuorovaikutus muodostaa perustan tehokkaille tietoturvastrategioille ja -toimenpiteille. Suojattavien kohteiden omistaja arvioi omaisuutensa arvon ja pyrkii minimoimaan riskit asianmukaisia vastatoimia toteuttamalla. Uhkatoimijat (kuten kyberrikolliset) luovat uhkia, jotka lisäävät riskiä pyrkiä väärinkäyttämään omaisuutta tai aiheuttamaan mahdollista vahinkoa omaisuudelle. Kuva 11 havainnollistetaan kontekstin elementtien viittaussuhteita.

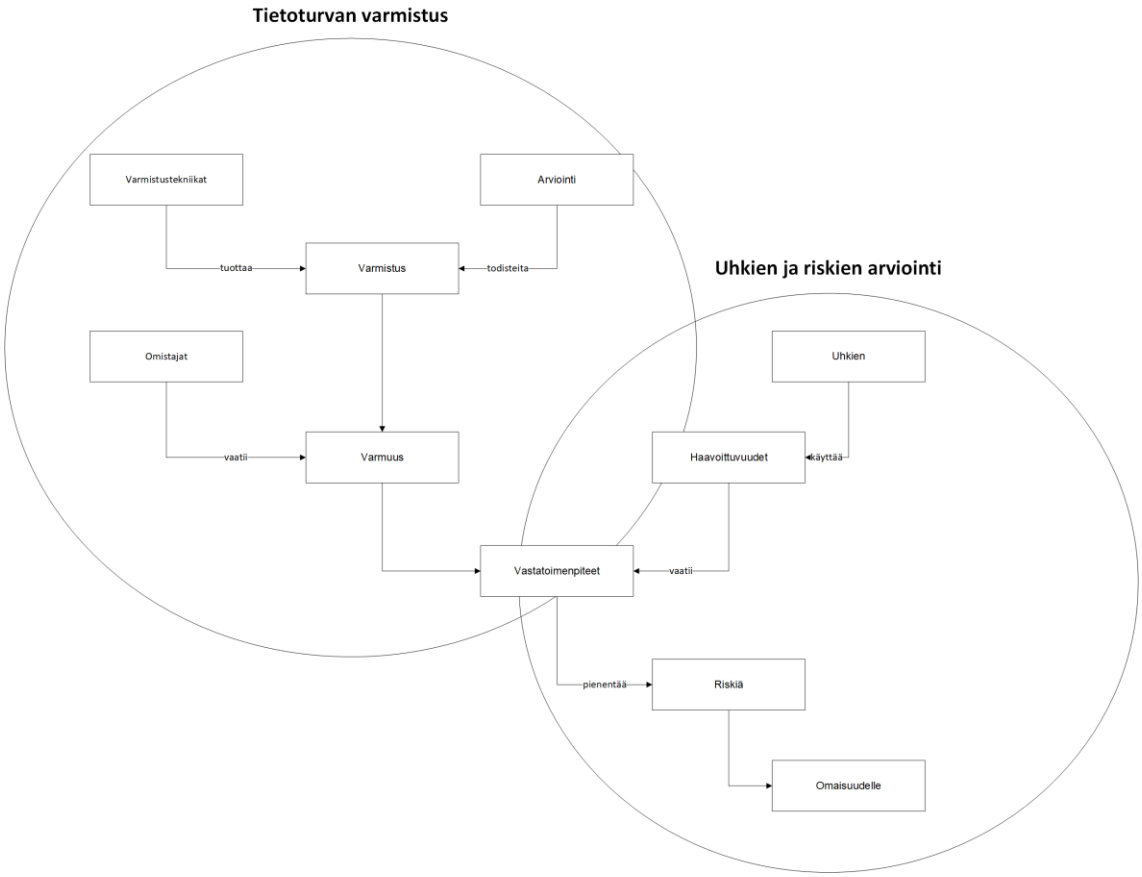


Kuva 11. Kontekstin elementtien viittaussuhteet toisiinsa (6, s. 31).

5.18.3 Kontekstimalli

Varmistustekniikat ovat olennainen osa tietoturvan varmistamista, ja niiden avulla tuotetaan vakuuttavaa näyttöä vastatoimenpiteiden tehokkuudesta. Arviointiprosessi tarjoaa arvokasta tietoa ja todisteita, joiden avulla varmistetaan vastatoimenpiteiden varmuus ja samalla pienennetään riskejä omaisuudelle. Suojattavien kohteiden omistajat asettavat vaatimuksen varmuudelle vastatoimenpiteiden toimivuudesta.

Kontekstimalli integroi tietoturvan varmistustekniikat sekä uhkien ja riskien arvioinnin yhtenäiseksi kokonaisuudeksi, jotka yhdistyvät vastatoimenpiteissä. Tietoturvauhkat käyttävät hyväkseen haavoittuvuuksia ja on tärkeää toteuttaa vastatoimenpiteitä minimoimaan haavoittuvuuksien aiheuttamaa riskiä omaisuudelle. Uhkien ja riskien arvioinnit ovat keskeinen osa tietoturvastrategiaa ja ne auttavat tunnistamaan potentiaaliset uhkat ja varmistamaan, että vastatoimenpiteet ovat kattavia ja tehokkaita. Kuva 12 havainnollistetaan kontekstimallin elementtien viittaussuhteet. Kontekstimalli korostaa tietoturvan varmistuksen ja uhkien ja riskien arvioinnin tärkeyttä.



Kuva 12. Kontekstimallin elementtien viittaussuhteet toisiinsa (6, s. 31).

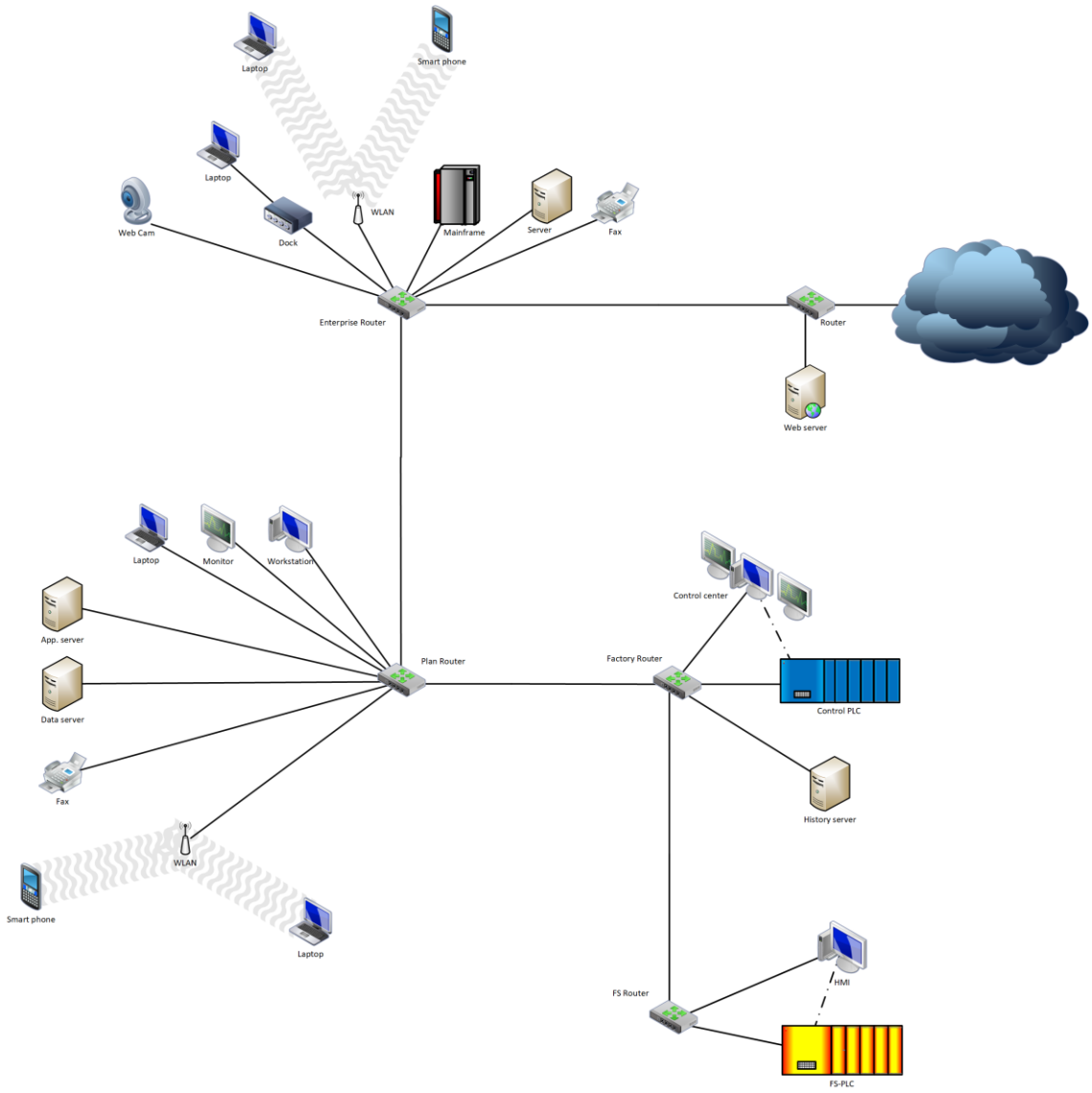
5.18.4 Teknisen ympäristön kontekstualisointi

Tässä alaluvussa käsitellään uudelleen verkkoarkkitehtuurin vyöhykkeitä, turvallisuustasoja ja käytäviä yksinkertaisessa verkkoarkkitehtuurissa Lähtökohtana on aiemmin esitetty arkkitehtuurikuva, joka kuvaa ainoastaan laitteiden välisiä tietoliikenneyhteyksiä. Tämän jälkeen laajennamme kuvaa lisäämällä siihen vyöhykkeet, väylät ja palomuurit vaiheittain. Tämä kumulatiivinen lähestymistapa auttaa lukijaa hahmottamaan, miten arkkitehtuurin ominaisuudet kehittyvät tiedon lisääntyessä.

Jotta suojattavien kohteiden omistaja pystyy määrittämään tarvittavat turvallisuustasot, on olennaista hankkia ymmärrys siitä, millaisesta ympäristöstä ja millaisista laitteista koko järjestelmä koostuu, esimerkiksi yhtiö ja sen tehtaat kokonaisuutena. On tärkeää hahmottaa yhtiön fyysinen ja looginen rakenne

kokonaisuutena. Fyysisen ympäristön arvioinnin perusteella voidaan laatia toimistojen ja tehtaiden turvallisuuspolitiikat ja niihin liittyvät käytännöt. On myös otettava huomioon, että rakennuksen fyysisellä turvallisuudella ja kyberturvallisuudella on yhteys, eikä niitä voida käsitellä erillisinä asioina. Tietoturva kattaa sekä fyysisen tietoturvan että kyberturvan. Toisinaan fyysisellä turvallisuudella voidaan myös luoda vastatoimenpiteitä kyberturvahaasteisiin, kuten esimerkiksi eristämällä laitteisto suljettuun tilaan. Näin ollen näitä käsitteitä on tarkasteltava kokonaisuutena.

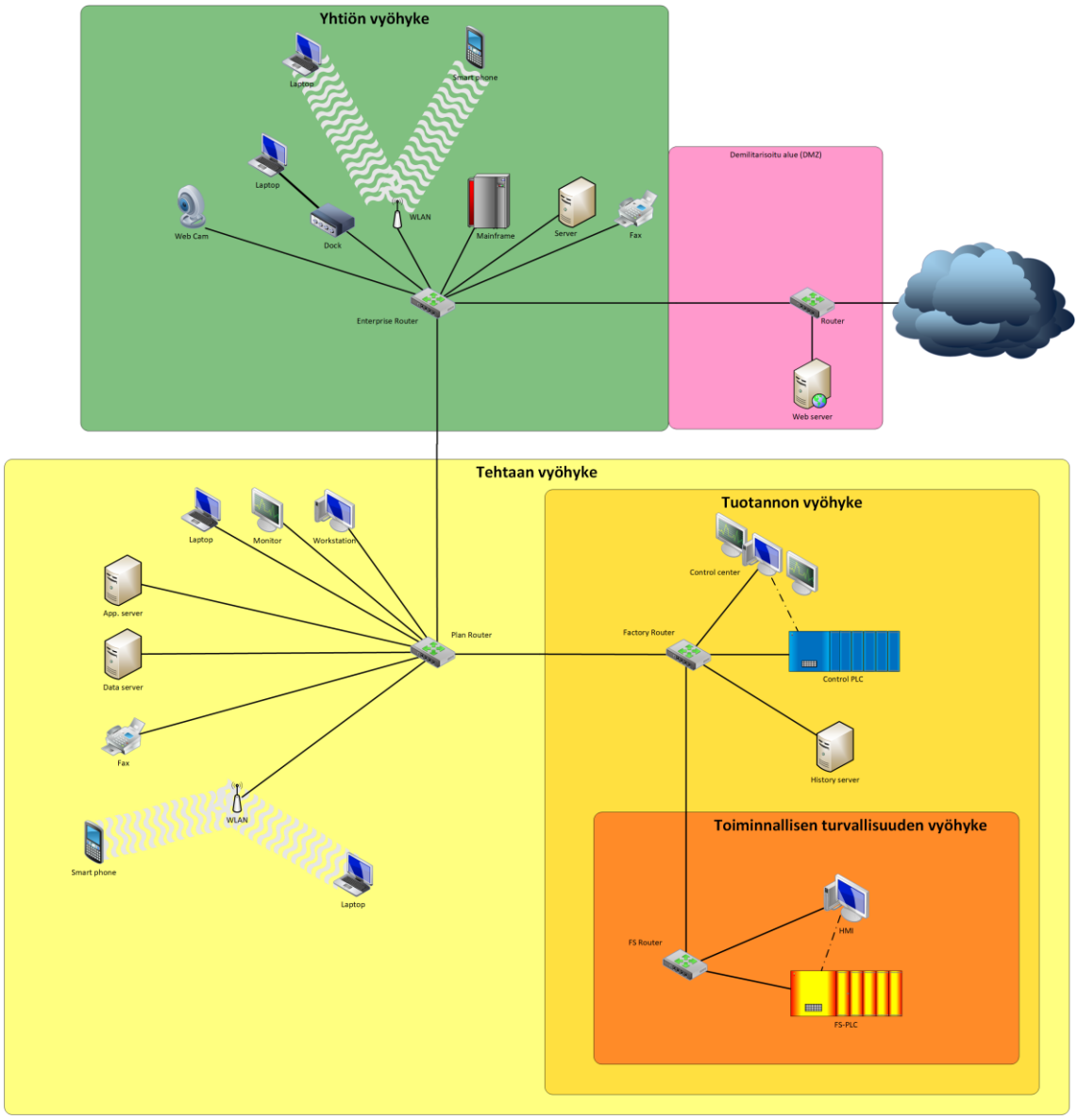
Looginen sijainti viittaa tehtaan ja yhtiön yhteiseen tietoliikenneinfrastruktuuriin. On tärkeää suunnitella tarkkaan, miten tietoliikennearkkitehtuuri rakennetaan tehtaan sisäverkon ja yhtiön sisäverkon välillä, sekä missä kohdassa on kytkentäpiste internetiin. Tämän lisäksi on tunnistettava, onko toimistojen tai tehtaan sisällä vielä erillisiä alueita, joilta vaaditaan korkeampaa turvatasoa. Kuva 13 on hahmoteltu esimerkinomaisesti yhtiön ja tehtaan verkkoarkkitehtuuri.



Kuva 13. Esimerkkiyrityksen toimiston ja tehtaan välinen verkkoarkkitehtuuri, jossa ei ole vielä tunnistettu vyöhykkeitä.

Eri loogiset kokonaisuudet määritetään turvallisuusarviointien perusteella. Turvallisuusarvioinnissa vaikuttaa riskien arvioinnissa löydettyjen tapahtumien haittavaikutus yrityksen toimintaan. Usein haittavaikutuksen mittarina käytetään hintaa, mutta varsinkin tuotannossa tehtaan työturvallisuus ja ympäristölle mahdollisesti aiheutuvat haitat ovat tärkeitä vaikuttimia. Näissä tapauksissa haittavaikutukset muunnetaan myös hinnaksi, jotta ne voidaan yhdistää esimerkiksi tuotannon pysähtymisen kanssa samaan laskentakaavaan. Kun kustannukset eri tapahtumille on määritelty, arvioidaan näiden tapahtumien todennäköisyyksiä.

Tämän analyysin pohjalta määritellään riskitasot. Kuva 14 on havainnollistettu viisi eri vyöhykettä kuvitteellisessa tapauksessa. Nämä ovat: demilitarisoitu vyöhyke, yhtiön vyöhyke, tehtaan vyöhyke, josta on tunnistettu tuotannon vyöhyke, josta on vielä erityisesti tunnistettu toiminnallisen turvallisuuden vyöhyke.



Kuva 14. Esimerkkiyrityksen verkkoarkkitehtuurista, jossa on tunnistettu vyöhykkeet.

Näille vyöhykkeille on määritelty tavoiteltava turvallisuustaso (SL-T). Tämän tiedon pohjalta järjestelmäintegraattori voi suunnitella ja rakentaa tehtaan niin, että saavutettu turvallisuustaso (SL-A) vastaa asetettua tavoitetta. Turvallisuustason

perusteella voidaan määrittää ja asettaa vyöhykkeiden sisällä olevien kanavien turvallisuustaso.

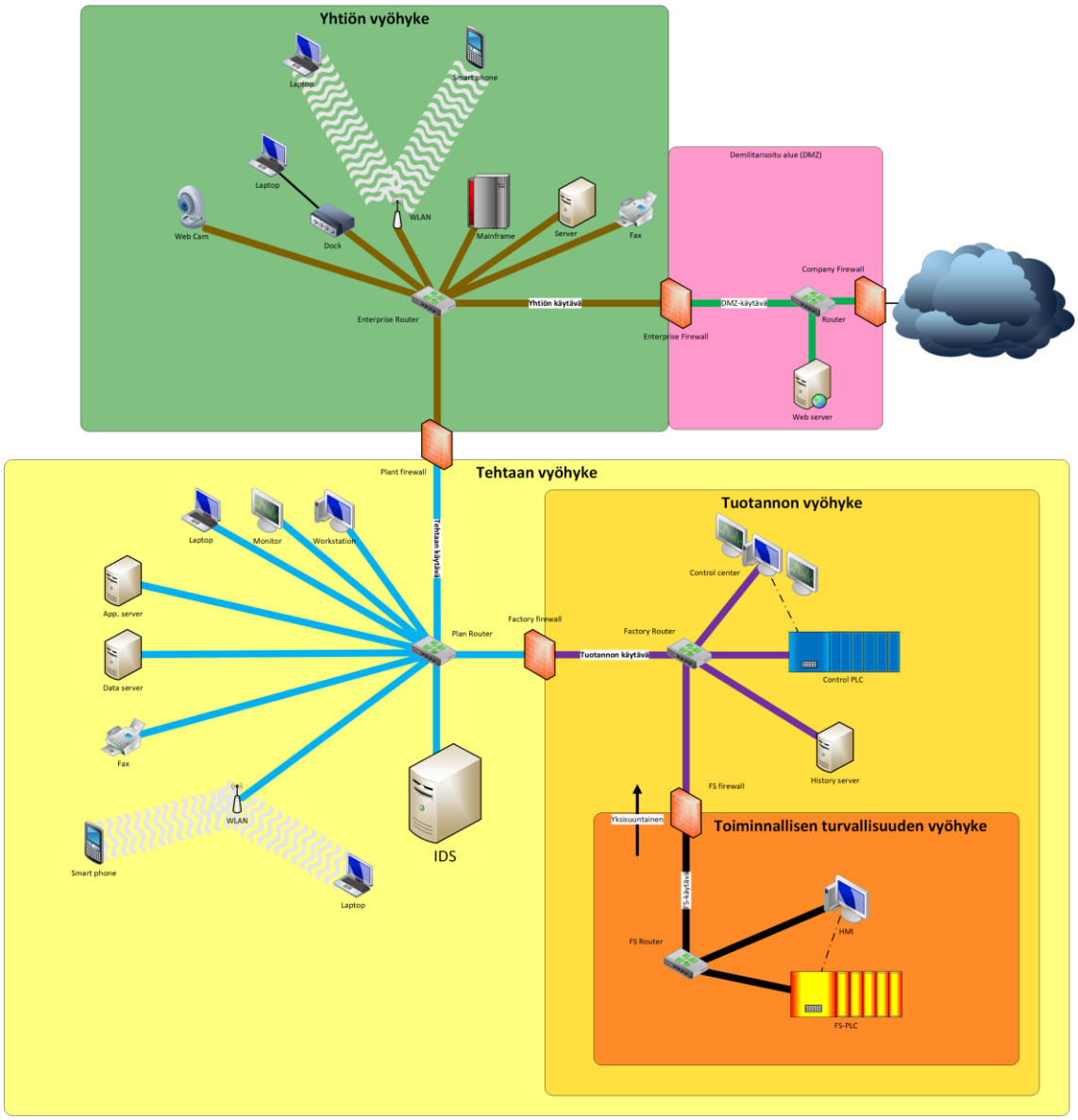
Tarkastellaan tehtaan vyöhykkeen mahdollisia uhkia. Kuva 14 nähdään, että tehtaalla on yksi tietoliikenneyhteys yhtiön vyöhykkeelle. Mahdollinen uhka on, että haittaohjelma tai toimija voi päästä yhtiön sisäverkkoon ja pyrkiä sieltä edelleen tehtaan vyöhykkeelle. Riskin pienentämiseksi yhtiön vyöhykkeen ja tehtaan vyöhykkeen tietoliikenneyhteyteen on asennettava palomuuri, joka sallii vain hyväksytyt yhteydet vyöhykkeiden välillä. Tehtaan sisäverkossa on myös langaton tiedonsiirtoyhteys, mikä luo avoimen rajapinnan mahdollisille hyökkääjille. Verkon radiopeiton suunnittelu tulee tehdä huolellisesti, jotta se ei kantaudu tehtaan alueen ulkopuolelle. Lisäksi laitteiden liittämiseen tukiasemaan tulee asettaa rajoituksia ja suojauksia.

Tehtaassa toimii myös aliurakoitsijoita, joten heidän laitteidensa liittämiseen tulee luoda toimintaohjeet ja vaatimukset, joiden mukaisesti laitteet voidaan kytkeä verkkoon. Koska tehtaan sisäverkossa on suurempi mahdollisuus eri haavoittuvuuksien esiintymiseen, on päätetty asentaa tunkeilijan havaitsemisjärjestelmä (IDS) tehtaan sisäverkkoon, jotta epätavallinen liikenne ja toiminta verkossa tulisi mahdollisimman aikaisessa vaiheessa tietoon.

Tehtaassa on selkeästi erillinen tuotantolaitos, johon kohdistuvien loukkausten on arvioitu aiheuttavan vakavia seurauksia. Tämä johtuu siitä, että tuotantolaitoksen prosessilaitteistoon kohdistuu erityisiä kustannuksia, jos prosessi keskeytyy tai vikaantuu. Tämän takia tehtaan vyöhykkeen ja tuotantolaitoksen vyöhykkeen välille on päätetty asentaa palomuuri, joka sallii vain hyväksytyt yhteydet vyöhykkeiden välillä.

Prosessiohjauksesta erillisenä toimivat prosessin turvatoiminnot, jotka ohjaavat laitoksen turvalliseen tilaan, mikäli prosessissa esiintyy tiloja, jotka eivät ole sallittuja ja jotka voivat aiheuttaa vaaraa prosessille, henkilöille tai ympäristölle. Toiminnallisen turvallisuuden järjestelmälle on päätetty luoda oma vyöhyke, koska sen toiminnot katsotaan äärimmäisen turvakriittisiksi tehtaan

operatiivisen toiminnan kannalta. Mikäli turvatoiminnot olisivat kykenemättömiä toimimaan, tehtaan tuotantolaitokset saattaisivat hajota tai pahimmassa tapauksessa koko tehdas voisi tuhoutua. Tuotantovyöhykkeen ja toiminnallisen turvallisuuden vyöhykkeen välille on päätetty asentaa yksisuuntainen palomuuri, joka sallii liikenteen toiminnallisen turvallisuuden verkosta poispäin. Yksisuuntaisuus on perusteltua, sillä turvatoimintojen tulee olla riippumattomia prosessiohjauksesta, ja ne toimivat vain saamiensa tilatietojen perusteella eivätkä näin ollen tarvitse prosessiohjaukselta tilatietoja. Koska palomuuri välittää tietoliikennettä toiminnallisen turvallisuuden vyöhykkeestä tuotantovyöhykkeelle, prosessiohjaus ja muut teollisuuslaitoksen toimijat voivat saada tietoa turvatoimintojen tiloista. Tämä mahdollistaa sen, että prosessiohjaus tai tehtaan operaattorit voivat reagoida nopeasti mahdolliseen turvatoiminnon aktivoitumiseen. Kuva 15 on havainnollistettu kuvitteellisessa tapauksessa palomuurien paikat sekä vyöhykkeiden väylät.



Kuva 15. Esimerkkiyrityksen vyöhykkeiden väylät ja niiden väliin suunnitellut palomuurit.

Näiden tietojen perusteella järjestelmäintegraattori hankkii tarvittavat komponentit vaadituilla kyvykkyyksillä (SL-C), integroi ne saumattomasti yhteen ja ottaa tehtaan käyttöön niin, että tavoiteltu turvallisuustaso (SL-T) vastaa saavutettua turvallisuustasoa (SL-A).

5.18.5 Teknisen ympäristön kontekstualisointi yhteenveto

Jotta suojattavien kohteiden omistaja voi asettaa tarvittavat turvallisuustasot, on tärkeää ymmärtää järjestelmän kokonaisuus, kuten yhtiö ja sen tehtaat. Fyysisen ympäristön arvioinnin perusteella laaditaan turvallisuuspolitiikat ja käytännöt. Fyysisen turvallisuuden ja kyberturvan yhteys korostuu, eikä niitä tulisi käsitellä erillisinä.

Looginen sijainti viittaa yhteiseen tietoliikenneinfrastruktuuriin. Tietoliikennearkkitehtuurin suunnittelussa on otettava huomioon tehtaan sisäverkon, yhtiön sisäverkon ja internetin kytkentäpisteet. Mahdolliset erilliset alueet tehtaan sisällä, jotka vaativat korkeampaa turvatasoa, on tunnistettava.

Eri loogiset kokonaisuudet määräytyvät turvallisuusarviointien perusteella ja riskien arvioinnissa huomioidaan tapahtumien haittavaikutukset yrityksen toimintaan. Vyöhykkeille määritellään tavoiteltavat turvallisuustasot, ja niiden sisällä olevat käytävät saavuttavat nämä tasot.

Turvallisuustoimenpiteitä, kuten palomuureja, käytetään tehtaan eri vyöhykkeiden suojaamiseen. Mahdollisia uhkia, kuten haittaohjelmia, arvioidaan ja riskiä pienennetään asianmukaisilla toimenpiteillä.

Toiminnallisen turvallisuuden järjestelmälle on luotu oma vyöhyke, ja erilliset palomuurit sallivat vain liikenteen toiminnallisesta turvallisuudesta tuotantovyöhykkeelle. Tämä varmistaa turvatoimintojen riippumattomuuden prosessiohjauksesta.

Järjestelmäintegraattori hankkii tarvittavat komponentit ja integroi ne yhteen saumattomasti. Tämä varmistaa, että saavutettu turvallisuustaso vastaa asetettua tavoitetta.

6 Yhteenveto

Teollisuuslaitokset ja niiden laitteet ovat alttiina verkossa tapahtuville hyökkäyksille, mikä voi vaikuttaa merkittävästi kriittisiin yhteiskunnan toimintoihin. Tietoturvallisuus on monitahoinen haaste, ja se vaatii laajaa yhteistyötä ja asianmukaista sääntelyä. Tarvitaan systemaattinen prosessi jatkuvaan tietoturvallisuuden suunnitteluun ja parantamiseen.

Yritysjohdon arvot, missio ja strategia ovat merkityksellisiä tietoturvan näkökulmasta. Johto osoittaa sitoutumisensa, asettaa selkeät tavoitteet ja vastuut sekä varmistaa, että kyberturva on osa yrityksen strategiaa ja päätöksentekoa. Yritysjohdon tehtävänä on myös luoda kulttuuri, joka tukee tietoturvallista toimintaa, jatkuvaa oppimista ja kehittymistä sekä viestiä kyberturvan merkityksestä kaikille sidosryhmille.

Aiemmin käytössä olleet erikoistuneet tietotekniset laitteet on korvattu suoraan hyllyltä ostettavilla komponenteilla (COTS), mikä parantaa järjestelmien integraatiota mutta tuo mukanaan uusia tietoturvaongelmia. Yhteiset pelisäännöt ovat välttämättömiä, ja kansalliset ja kansainväliset standardit, kuten IEC 62443, tarjoavat viitekehyksen. Vaikka standardit eivät automaattisesti tee laitteistosta täysin tietoturvallista, ne toimivat perustana, kun pyritään hyväksyttävään tietoturvatasoon.

IEC 62443 -standardisarja on laajasti tunnustettu kehys teollisuusyrityksille, laitteistojen ylläpitäjille ja komponenttivalmistajille automaatio- ja ohjausjärjestelmien kyberturvallisuuden suunnittelussa ja toteutuksessa. Standardi tarjoaa joustavan kehyksen tietoturvan hallintaan, sovittaen yhteen liiketoiminnan IT-järjestelmät ja teollisuuden automaatio- ja ohjausjärjestelmän erityispiirteet. IEC 62443 -standardisarja kattaa laajan joukon järjestelmiä, kuten teollisuuden ohjausjärjestelmät, hajautetut ohjausjärjestelmät ja SCADA-järjestelmät. Sarja edellyttää turvallisuuskäytäntöjen laajentamista ja jatkuvaa valvontaa turvallisuustason varmistamiseksi.

Tämä insinöörityö tarjoaa mahdollisuuden syventää osaamista ja ymmärrystä standardisarjasta ja yrityksen johdon sitoutumisen tärkeydestä laadukkaan tietoturvan saavuttamisessa. Lukijalle tarjotaan vahva perusta standardiperheen käytännön soveltamiseen, joka mahdollistaen oman tietoturvallisuuskäytännön parantamisen ja IEC 62443 -standardin tehokkaan noudattamisen.

Lähteet

1 Hyppönen, M. (2021). Internet. E-kirja. Helsinki: WSOY.

2 Enqvist, K. (1998). Olemisen porteilla. E-kirja. Helsinki: WSOY.

3 Holloway, M. 2015. Slammer Worm and Davis-Besse Nuclear Plant. Verkkoaineisto. Stanford University. <http://large.stanford.edu/courses/2015/ph241/holloway2/>. Luettu 3.1.2024.

4 Tyler, W. 2023. Throwback Attack: The slammer worm hits Davis-Besse nuclear plant. Verkkoaineisto. Industrial Cybersecurity Pulse Threats & Vulnerabilities. <https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-the-slammer-worm-hits-davis-besse-nuclear-plant/>. Luettu 14.1.2024.

5 IEC 62443-2-1. 2010. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program. Geneve: IEC.

6 IEC/TS 62443-1-1. 2009. Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. Geneve: IEC.

7 IEC 62443-2-4. 2017. Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers. Geneve: IEC.

8 IEC 62443-4-1. 2018. Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements. Geneve: IEC.

9 IEC/TS 62443-1-1. 2009. Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. Geneve: IEC.

10 IEC 62443-2-1. 2010. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program. Geneve: IEC.

11 IEC TR 62443-2-3. 2015. Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment. Geneve: IEC.

12 IEC 62443-2-4. 2017. Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers. Geneve: IEC.

13 IEC 62443-3-1. 2009. Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems. Geneve: IEC.

14 IEC 62443-3-2. 2020. Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design. Geneve: IEC.

15 IEC 62443-3-3. 2013. Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels. Geneve: IEC.

16 IEC 62443-4-2. 2019. Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components. Geneve: IEC.