VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Nico Sinimäki

DATADIODI

Meriteollisuuden tietoturvaratkaisut

Tekniikka
2022

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Nico Sinimäki
Opinnäytetyön nimi	Datadiodi
Vuosi	2022
Kieli	suomi
Sivumäärä	24
Ohjaaja	Kalevi Ylinen

Tämän opinnäytetyön tavoitteena on esitellä meriteollisuudessa esiintyvien ongelmien ratkaisua datadiodin ja tietoturvallisuuden näkökulmasta. Opinnäytetyön päätavoitteena on löytää vastaus siihen, minkälaisia ongelmia datadiodin implementointi laivan järjestelmään tuottaa. Tietoturvaa käsiteltiin laajasti yleisellä tasolla ja meriliikenteen näkökulmasta. Selvittämisen jälkeen saadaan tietoa siitä, kannattaako datadiodin lisääminen ja minkälaisia ongelmia se tuottaa.

Työ toteutettiin pääosin käyttämällä internetistä löytyvää tietoa, joka sisältää ammattilaisten saamaa tietoa. Työtä tehdessä kerättyjä tietoja ja laitevalmistajien antamia dokumentteja käytettiin tukena.

Lopuksi havaittiin datadiodin olevan erittäin hyödyllinen ja tehokas laite tietoturvan lisäämiseksi. Huomattiin myös, että datadiodin käyttömahdollisuudet ovat laajemmat kuin aluksi luultiin. Datadiodin huomattiin olevan helpoimmin lisättävissä uusiin järjestelmäkokonaisuuksiin.

Avainsanat Tietoturva, meriteollisuus, data, meriliikenne

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Nico Sinimäki
Title	Data Diode
Year	2022
Language	Finnish
Pages	24
Name of Supervisor	Kalevi Ylinen

The aim of this thesis was to present a solution to the problems of the marine industry from the perspective of data diode and information security. The main goal of the thesis was to find an answer to what kind of problems that the implementation of a data diode in a ship's system produces.

The thesis was carried out mainly by using information found on the internet, which includes information that was researched by professionals. The information collected during work and the documents provided by manufacturers were used as support.

Finally, the data diode was discovered to be a very useful and efficient device to increase information security. It was also noted that the intended use of the data diode was wider than initially thought. It was found out that the implementation for the data diode was easier in new systems.

Keywords Information security, marine industry, data, and marine traffic

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

KUVALUETTELO

1 JOHDANTO 7

1.1 Tavoitteet 7

1.2 Asiakas 7

2 TIETOTURVA 9

2.1 Tietoturvan määritelmä 9

2.2 Tietoturva laitteistona 9

2.3 Tietoturva laivaverkossa 10

2.4 Tietoturvan merkitys meriteollisuudessa 10

3 DATA MERITEOLLISUUDESSA 12

3.1 Data yleisesti 12

3.2 Kommunikointiprotokollat 12

3.2.1 Modbus TCP 12

3.2.2 UDP 13

3.2.3 ATM-teknologia 13

3.3 Datan suojaaminen 14

3.4 Tietoturvaratkaisut 15

3.4.1 Virustorjuntaohjelmat 15

3.4.2 Vakoiluohjelmien torjunta 16

3.4.3 Palomuurit 16

4 DATADIODI LAIVAVERKOSSA 17

4.1 Datadiodi yleisesti 17

4.2 Datadiodi rautatasolla 18

4.3 Datadiodin käyttötarkoitus 18

5 YHTEENVETO 19

5.1 Datadiodi tietoturvavälineenä 19
5.2 Datadiodin käyttäminen laivaverkossa 19
6 JOHTOPÄÄTÖKSET 20
6.1 Tietoturva ja meriliikenne 20
6.2 Ongelmat 20
LÄHTEET 21

KUVALUETTELO

Kuva 1. Laivan verkon layout 10

Kuva 2. Esimerkki Modbus-verkon rakenteesta (Modbus, 2012, 3) 13

Kuva 3. Verkon segmentointi (Owlcyberdefence, What is datadiode?, 2021) 17

1 JOHDANTO

1.1 Tavoitteet

Tämän opinnäytetyön tarkoituksena on tutkia meriteollisuuden tietoturvaratkaisuja julkisen sektorin vientiyrityksen näkökulmasta. Projekti toteutetaan Arnon Oy:n nimissä. Työn on tarkoitus selventää yksityiskohtia asiakkaalle tarjottavan kokonaisuuden toimivuudesta sekä toteutettavuudesta. Työn päätavoitteena on selvittää, miten datadiodin kaltainen laite soveltuu asiakkaan haluamaan toimintaympäristöön. Datadiodi määritelmältään on yksinkertaisimmillaan laite, jonka avulla siirretään tietoa vain yhteen suuntaa. Tällaisen laitteen avulla voidaan rajoittaa ja eliminoida täysin toiseen suuntaan kulkevan tietoliikenteen kohtaamat vaarat. Datadiodin turvallisuus perustuu siihen, että sen avulla voidaan fyysisesti kytkeä pois toiseen suuntaan kulkeva liikenne. Tämä takaa sen, että ulkopuolelta vaikuttavat uhkatekijät eivät voi käyttää hyväkseen erilaisia haavoittuvaisuuksia. Näihin haavoittuvaisuuksiin kuuluu erityisesti virtuaalisesti kytkettävissä olevat laitteet, johon on mahdollista päästä käsiksi internet yhteyden avulla. Työn ymmärrettävyyden helpottamiseksi käydään myös läpi eri näkökulmia yleisen tietoturvan, sekä tarkemmin meriteollisuuden tietoturvan perustietoja. Näitä tietoja voidaan siten peilata työn lopputulokseen, jotta saadaan käsitys käytettävän kokonaisuuden toimivuudesta ja käytännöllisyydestä.

1.2 Asiakas

Asiakas kertoo omilla nettisivuillaan olevansa ”kansainvälisesti johtava ja kokonaiselinkaariratkaisujen toimittaja merenkulku- ja energiamarkkinoilla.”, jonka toiminnasta löytyy vahvaa osaamista jo yli kahdensadan vuoden ajalta. Yrityksen vaikutus ulottuu erityisesti meriteollisuuteen, kuten laivan moottoreihin ja niiden lisälaitteisiin, sekä erilaisiin voimalaitoksiin.

Maailman vauhdikas kehitys lisää ongelmia, joihin kansainvälisesti toimiva kestävään kehitykseen tähtäävä liiketoiminta pyrkii tuomaan uusia innovaatioita. Yrityksen halu ”maksimoida asiakkaiden alusten ja voimalaitosten ympäristötehokkuuden ja taloudellisuuden keskittymällä kestäviin innovaatioihin” on erittäin kriittinen arvo nopeasti kasvavalla ja kehittyvällä työkentällä. Yritys kertoo myös työllistäneensä noin 18 000 henkilöä ympäri maailmaa ja sen liikevaihto oli 4,6 miljardia euroa vuonna 2020.

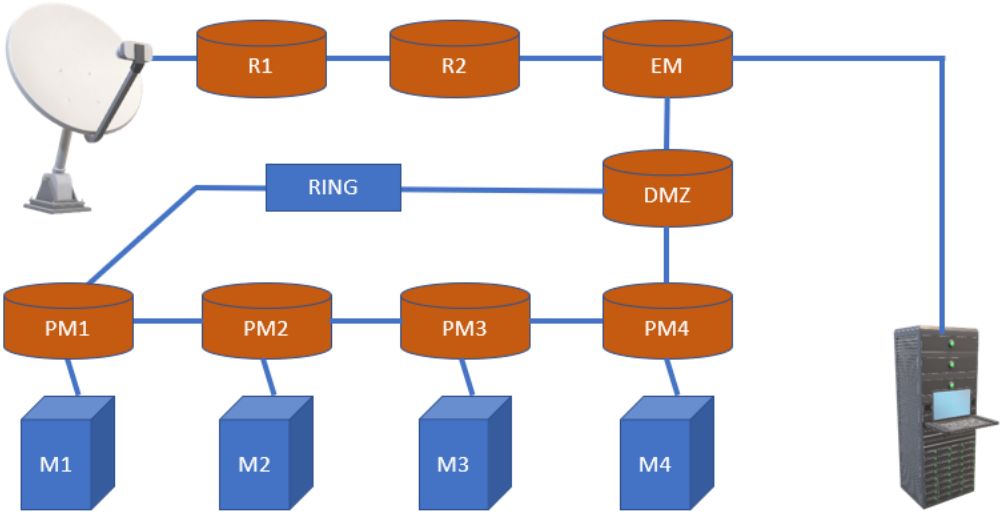
2 TIETOTURVA

2.1 Tietoturvan määritelmä

Datadiodin merkitys tietoturvassa on erityinen, sillä sen käyttötarkoitus on varmistaa tietyissä tilanteissa turvallinen tiedonsiirto. Sen käyttö on kuitenkin hyvin suppeaa, sillä monesti tiedonsiirtojärjestelmät etenkin meriteollisuudessa on vaikea mukauttaa sen toimintaan. Tietoturva on nykypäivänä keskeisimpiä käsitteitä teknologiateollisuuden parissa, sillä jatkuvasti kehittyvä maailma tuo mukanaan monia uusia haasteita. Näihin haasteisiin tulee vastata jatkuvalla sykkeellä, sillä varaa pysähdyksiin ja katkoksiin sähköntuotannossa tai vientiteollisuudessa ei ole. Yksikin katkos väärään aikaan väärässä paikassa voi maksaa useita ihmishenkiä. Kyberturvallisuuskeskuksen mukaan ”tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys sekä käytettävyys”. (Kyberturvallisuuskeskus, Tietoturva, 2020) Tällä tarkoitetaan sitä, että kaikki järjestelmän sisällä oleva tieto on käytettävissä vain siihen oikeutetuilla tahoilla.

2.2 Tietoturva laitteistona

Tietoturvalaitteita on lähes yhtä useita kuin niiden käyttöympäristöjä, mutta niistä käytetyimpiä ovat palomuurit. Yleensä palomuurikäsite yhdistetään kotikoneessa toimivaan ohjelmaan. Tämä ei kuitenkaan ole täysin väärä käsitys, sillä sen toimintaperiaate on hyvin samankaltainen. Tietoja turvaava laitteisto täytyy olla suunniteltu niin, että sen ohjattavuus on minimoitu aina konfiguraatiotasolta mekaanisiin käyttövipuihin. **(Kuva 1.)** Minimointi täytyy kuitenkin tapahtua muiden vaikuttavien laitekokonaisuuksien käytön mukaan, sillä myös liiallisesta toimintojen estämisestä voi tulla järjestelmää suuresti rajoittava pullonkaula.



Kuva 1. Laivan verkon layout

2.3 Tietoturva laivaverkossa

Laivaverkon turvaaminen toteutetaan käyttämällä useita palomuureja sekä Cisco -reitittimiä. Reitittimien tehtävä on varmistaa laivan sisällä, sekä sieltä ulos kulkevan datan turvallisuus yhdessä muun turvallisuuslaitteiston kanssa. Palomuurit suojaavat laivan moottoreista saatavaa tietoa siten, että luodaan suojaus DMZ- ja EDGE-tyyppisten palomuurien avulla. DMZ-palomuurin avulla luodaan aliverkko, joka on julkisen ja yksityisen verkon välissä. Toisin sanoin tämän avulla lisätään suojakerrointa paikallisen verkon ja epäluotettavan verkon väliin. EDGE on nimensä mukaisesti verkon reunalla oleva palomuuri, joka kontrolloi ulos- ja sisäänpäin kulkevaa tietoa. (Fortinet, What is DMZ Network?, 2022)

2.4 Tietoturvan merkitys meriteollisuudessa

Meriteollisuus on yksi maailman kriittisimmistä tietoturvakohteista, sillä meriteitse kulkee suurin osa maailman rahdista. ”Lähes 90 % Suomen viennistä ja tuonnista kulkee meriteitse”, kertoo Suomen Varustamot. (Suomen Varustamot, Merenkulun avainluvut, 2020) Parhaimmassakin tapauksessa meriviennistä liikaa

riippuvaiset maat joutuisivat kokemaan suuria menetyksiä vähintäänkin rahallisesti, mikäli merivienti keskeytyy tai lakkaa huomattavaksi ajaksi.

Todennäköisimpiä hakkereiden kiristyskohteita voisivat olla esimerkiksi suuret öljytankkerit, joiden kariuduttua on mahdollisuudet suurelle ympäristökatastrofille. Tämä tietenkin riippuu siitä mikä on hyökkääjän motiivi ja päämäärä. Meriteollisuus on selvä kohde monille tahoille, on sitten kyseessä poliittista tai rahallista hyötyä havitteleva tietoturvarikollinen. Poliittiseen lopputulokseen tähtäävä hyökkääjä ei välitä siitä, miten päämäärä saadaan toteutettua, kunhan oman poliittisen maaliviivan yli päästään. Tällaisessa niin sanotussa ”loppu oikeuttaa keinot” tyyppisessä hyökkäyksessä halutaan vain kiristämällä pakottaa yritystoimija tekemään tiettyjä päätöksiä. Usein yritykset kuitenkin taipuvat poliittisena uhrina rikollisten tahtoon, sillä toivovat näin minimoivansa aiheutuvat haitat. Toinen mahdollinen hyökkäys voi tapahtua esimerkiksi kilpailevan yrityksen toimesta, jolloin pyrkimyksenä on tehdä mahdollisimman suurta rahallista tai esineellistä haittaa.

Etteplanin sivuilla julkaistussa ”Tietoturva on teollisuuden uusi normaali” artikkelissa on hyvin kuvailtu tietoturvaan vaikuttavat tekijät, joista ilmeisin on tietenkin ihminen. Meriteollisuudessa työskentelevät ihmiset eivät ole yleisesti ottaen tietoturva-alan ammattilaisia, josta voimme päätellä moniakin asioita. Artikkelissa sanotaan, että ”Jos tietokonetta käyttävä työntekijä surffaa kahvitauollaan netissä, voi hän pahaa aavistamattaan saastuttaa tietokoneen ja sen operoiman laitteen”. (Etteplan, Tietoturva on teollisuuden uusi normaali, 2021) Tämä ei korreloidu suoraan meriteollisuuteen, sillä useimmilla laivoilla internetin käyttäminen on hyvin rajoitettua. Kuitenkin laivalle töihin menevän asentajan yksi työtehtävistä voi olla laitteen uudelleenkonfigurointi. Tällaisessa tilanteessa asentajalla kuuluisi tietenkin olla vain työkäyttöön soveltuva tietokone, jolla konfigurointi suoritetaan. Näistä turvallisuuskäytännöistä huolimatta kyseessä oleva tietokone saattaa olla saastunut jo ennen laivaan astumista, eikä sen omistaja tiedä siitä mitään.

3 DATA MERITEOLLISUUDESSA

3.1 Data yleisesti

Dataa voidaan saada mistä tahansa yhteiskunnassa olevasta asiasta. Se on kerättävää tai siirrettävää tietoa, joka määritellään yleensä jonkinlaisena tietoa sisältävänä merkkijonona. Tällainen merkkijono voidaan lähettää laitteesta sitä vastaanottavalle päätelaitteelle. Data on tietoa, jonka ei tarvitse olla ymmärrettävässä muodossa ollakseen dataa. Useimmiten se kuitenkin esiintyy ymmärrettävässä muodossa olevana tietona, kuten sähköpostina tai ihmisen käyttäytymismallina.

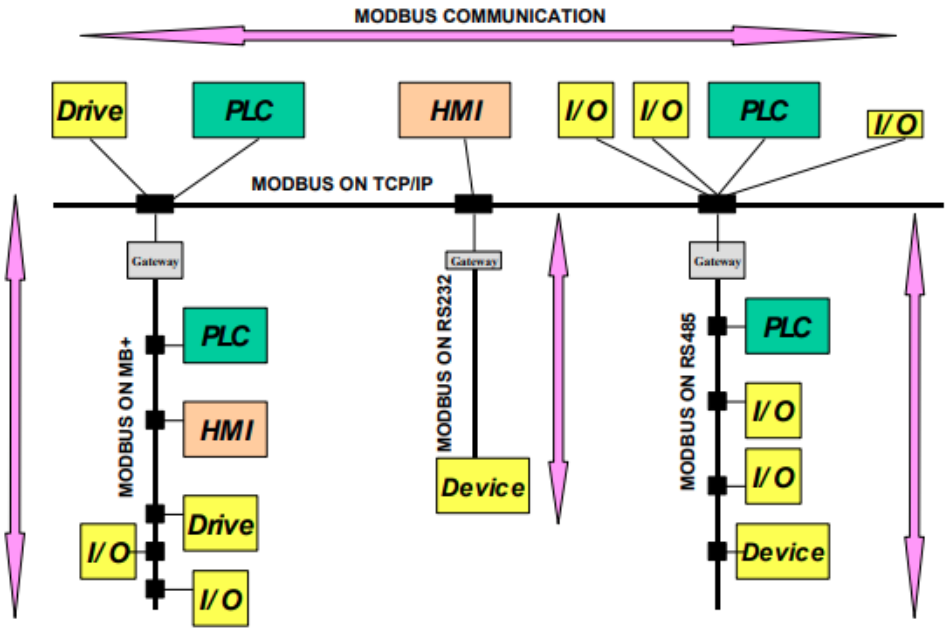
3.2 Kommunikointiprotokollat

Tässä kappaleessa käsitellään erilaisten kommunikointiprotokollien käyttömahdollisuuksia. Tarkoituksena on käsitellä kaikki työhön liittyvä protokollat pääpiirteittäin.

3.2.1 Modbus TCP

Meriteollisuudessa yleisesti käytettävänä sarjaliikenneprotokollana toimii Modiconin kehittämä Modbus-protokolla. Modbus on pyyntö-/vastausprotokolla, joka on toiminut ’de facto’ standardina teollisuudessa jo vuodesta 1979. (Modbus, 2012, 2) Sen avulla erilaisiin väyliin ja verkkoihin kytketyt laitteet, kuten palvelimet ja PLC voivat kommunikoida keskenään.

Modbus-protokollan avulla erilaisten laitekokonaisuuksien yhteys on helppo pitää yllä. Vastaavanlainen yhteys voidaan luoda sekä sarjaliikenne että ethernet TCP/IP-verkoissa. Useat erityyppiset PLC, HMI ja I/O-laitteet voivat käyttää tarvittaessa Modbus-protokollaa. **(Kuva 2.)**



Kuva 2. Esimerkki Modbus-verkon rakenteesta (Modbus, 2012, 3)

3.2.2 UDP

UDP eli 'User Datagram Protocol' on yksi datansiirtoprotokolleista, jonka tyyli lähettää ja käsitellä dataa erottaa sen muista protokollista. UDP-protokolla siirtää dataa siten, että tapahtuman aikana tietoa voi kadota matkan varrella. Dataa saattaa myös ilmestyä väärässä järjestyksessä tai tuplana, joka tekee siitä erittäin epäluotettavan. Yksinkertaisuus ja nopeus tekee siitä kuitenkin toimivan ratkaisun tilanteisiin missä nopeus on tärkeämpää kuin tarkkuus. (Fox P., Khanacademy, User datagram protocol, 2020)

3.2.3 ATM-teknologia

Asynkroninen tiedonsiirtotapa on toimintamuoto, jonka tarkoituksena on muuntaa ja jakaa tieto pieniin soluihin. Solujen määrä on täysin muuttumaton 53 bittiä toisin kuin muissa kilpailevissa protokollissa. Jokainen näistä soluista koostuu 5 bittiä pitkästä otsikosta ja 48 bittiä pitkästä kuormasta. Kun siirtotapa

on aina vakiomuotoa ja lähetettävä kuorma ei muutu, niin sen toiminta on hyvin ennustettavissa. Nämä asiat takaavat loppukäyttäjälle tasaisen ja laadukkaan palvelun.

Siirtotapa poikkeaa muista siten, että se hakee valmiit reitit ennen tiedonsiirron alkamista. Käytännössä jonkinlainen pysyvä yhteys täytyy olla käytössä, että tiedonsiirto vastaanottimien välillä voi alkaa. ATM-teknologialla ei ole kykyä mukautua nopeaan verkkoliikenteen muutokseen. ”Äänipaketin koolla ei ole väliä, sillä ne kohtaavat aina kokonaisia datapaketteja ja voivat kokea täydet jonotusviiveet.” (Techopedia, Asynchronous Transfer Mode, 2020) Tästä syystä pakettien koon tulisi olla aina sama. Korjattu solun rakenne ATM-teknologiassa tarkoittaa, että se on helposti vaihdettavissa laitteistolla ilman viivettä. ”Tästä syystä jotkut luulevat, että ATM-teknologia on ratkaisu internetyhteyden kohtaamiin ongelmiin.” (Techopedia, Asynchronous Transfer Mode, 2020) ATM-teknologia tarjoaa siirtokerroksen palveluita, jotka toimivat OSI-mallin ensimmäisessä eli fyysisessä kerroksessa. ”Solujen ollessa määrätyn pituisia, verkon liikenne on helposti ennustettavissa.” (Techopedia, Asynchronous Transfer Mode, 2020)

3.3 Datan suojaaminen

Dataa voidaan suojata monilla eri tavoilla. Näistä käytetyimpiä ovat virustorjuntaohjelmat, palomuurit, salaus sekä varmuuskopiointi. Suojaamiseen voidaan käyttää monia tapoja, mutta jokainen tavoista on silti ihmisen luoma ja näin haavoittuvainen hyväksikäytölle. Hyökkäystä ei voida ikinä estää täysin, mutta siitä voidaan tehdä todella hankalaa ja siten myös vähemmän kannattavaa.

Erityisen tärkeä osa datan suojausta on laitteiston päivitysten ylläpitäminen. Valmistajan suosittelemat päivitykset asentamalla on helppo tapa varmistaa, että laitteiston toiminta pysyy ajan tasalla. Laitteiston ja sovellusten päivitykset voidaan useimmiten automatisoida ja kannattaa se myös mahdollisuuksien mukaan tehdä. (Bonta, R., Online privacy, 2021) Kriittisten sovellusten kuten

selainten, sähköpostin, palomuurin ja virustorjuntaohjelmien päivitykset ovat kaiken eturintamassa, sillä ne ovat vastaanottamassa tulevaa hyökkäystä. Nämä kyseessä olevat päivitykset poistavat ohjelmistosta vikoja, joiden avulla hyökkääjät pääsevät käsiksi haluamaansa tietoon.

Perustason suojauksen voi toteuttaa käyttämällä salasanoja, joiden pituus on vähintään 12 kirjainta ja parhaimmillaan 21. Salasanan tulee sisältää kaikenlaisia erikoismerkkejä, numeroita sekä isoja ja pieniä kirjaimia. Myös kaksoisautentikointi on nykyään erittäin käytetty ja toimiva lisä suojaukseen. Kahden vaiheen autentikointi voidaan toteuttaa tekstiviestitse, applikaationa tai fyysisen laitteen kautta, joka syöttää uuden merkkisarjan tietyin väliajoin. Tarkoituksena on siis syöttää ensin henkilökohtainen salasana, jonka käyttö yksittäisenä vahvistustapana on varsin vajavainen. Tämän jälkeen järjestelmä pyytää syöttämään sillä hetkellä näkyvän merkkijonon, jonka tarkoitus on todentaa käyttäjän aitous. (CNET, Two-Factor authentication, 2015)

Kalasteluhyökkäykset ovat edelleen yksi käytetyimmistä hyökkäysmuodoista, joiden tarkoituksena on saada käyttäjä klikkaamaan haluttua linkkiä. (Bonta, R., Online privacy, 2021) Linkin takaa löytyy kuitenkin hyökkääjän pelikenttä, jossa hyökkääjä päättää miten tietoa käsitellään. Kalasteluyritys voi olla lievimmillään tietokyselylomake ja pahimmillaan lataa haittaohjelman kohdekoneeseen avattavan tiedoston muodossa.

3.4 Tietoturvaratkaisut

Tässä kappaleessa käsitellään virustorjuntaohjelmistoja, sekä niiden ominaisuuksia.

3.4.1 Virustorjuntaohjelmat

Virustorjuntaohjelmien on tarkoitus suojata laitetta viruksilta, joiden tarkoitus on rampauttaa, tuhota tai vahingoittaa tietojärjestelmässä olevaa tietoa tai laitetta.

Ohjelma suojaa laitetta käymällä läpi siinä olevia tiedostoja ja poistaa sekä varoittaa käyttäjää mahdollisista vaaranpaikoista. (Bonta, R., Online privacy, 2021)

3.4.2 Vakoiluohjelmien torjunta

Vakoiluohjelmistot keräävät henkilökohtaista tietoa laitteella tapahtuvasta liikenteestä. Tällaisten ohjelmistojen kohteena on useimmiten pankkitiedot ja käyttäjätunnukset. Merkkejä vakoiluohjelman saastuttamasta koneesta on muun muassa laitteen äkillinen hidastuminen. Ohjelmistoja ladattaessa on käytettävä virallisia lähteitä, jolloin mahdollinen saastumisvaara saadaan minimoitua. (Bonta, R., Online privacy, 2021)

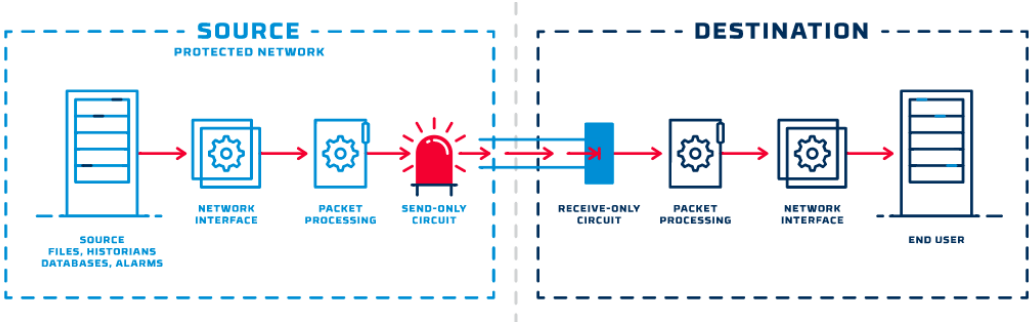
3.4.3 Palomuurit

Palomuurin tarkoituksena on valvoa sisään ja ulos kulkevaa tietoliikennettä sekä ohjata sitä erikseen sallittuihin osoitteisiin. (Bonta, R., Online privacy, 2021) Asetuksista voidaan säätää sääntöjä, jotka kertovat mistä osoitteesta ja portista tiedon halutaan liikkuvan. Palomuuri toimii eräänlaisena suodattimena, jonka avulla voidaan rajoittaa suuri määrä ylimääräisistä osoitteista. (Bonta, R., Online privacy, 2021) Hyökkääjän mahdollisuudet päästä sisään laitteeseen vähenee huomattavasti osoitteiden määrän vähentyessä.

4 DATADIODI LAIVAVERKOSSA

4.1 Datadiodi yleisesti

Datadiodilla suojataan verkkoa ja siirretään tietoa vain yhteen suuntaan. Sen tarkoitus on toimia yksisuuntaisena välikappaleena kaksisuuntaisten ulko- ja sisäverkkojen välillä. Datadiodi toimii lähettävän ja vastaanottavan laitteen avulla, jotka fyysisesti erottavat verkot toisistaan. Näiden laitteiden tarkoitus on muuntaa eri protokollat ATM-paketeiksi ja kohteessa muuntaa ne takaisin halutuksi protokollaksi. **(Kuva 3.)** Hyökkääjien on mahdotonta päästä datadiodin läpi, sillä data ei koskaan kulje kuin yhteen suuntaan. Datadiodi on suunniteltu alun perin estämään kaikenlainen luvaton pääsy ydinasejärjestelmiin. (OWL datadiodes.pdf, 1, 2019)



Kuva 3. Verkon segmentointi (Owlcyberdefence, What is datadiode?, 2021)

Datadiodin etu on, että se ei ole altis zero-day -hyökkäyksille tai ohjelmavioille. Erityisesti zero-day -hyökkäysten poissulkeminen listalta antaa tietoturvan näkökulmasta laitteelle suuren etumatkan muihin vastaaviin kopioihin. Zero-day hyökkäyksen tarkoituksena on hyödyntää vikoja ja hyökätä ennen kuin kukaan ehtii edes reagoida tapahtuneeseen. Yleensä tämänkaltaiset hyökkäykset huomataan vasta siinä vaiheessa, kun suurempi vahinko on jo tapahtunut. (FireEye, What is a Zero-day Exploit?, 2022) Tästä syystä datadiodin toimintamalli on erittäin hyvä juuri tällaisia uhkia vastaan, sillä niiden suojausmetodi perustuu

fyysiseen kytkimeen johon hyökkääjä ei pääse käsiksi. Ne eivät myöskään tarvitse jatkuvaa ylläpitoa pysyäkseen toimintakunnossa ja turvallisina. Datadiodin luoma ”ilmarako” takaa sen, että toisella puolella rakoa oleva verkkosegmentti pysyy toimintakuntoisena toisen puolen saastuttua. (OWL datadiodes.pdf, 2, 2019)

4.2 Datadiodi rautatasolla

Laitetasolla datadiodi on joko räkkiin tai DIN-kiskolle asennettava laite, johon asiakas voi itse valita lisävarusteita, esim. kuituportin. Projektin suunnitteluvaiheessa käytiin ensin keskustelua siitä, että datadiodin tulisi olla Sarlinin tuottama mbXLINK-datadiodi. Sarlinin sivuilla on hyvin kiteytettynä laitteen toiminta yhteen virkkeeseen. ”Datadiodin toiminnallisuus on toteutettu ”rautatasolla”, mikä merkitsee, että kommunikoinnin paluukanava on normaalikäytön aikana fyysisesti erotettu.” (Sarlin mbXLINK datadiodit, 2021) Laitteen asetuksien muuttaminen ei siis ole mahdollista, jos laitteessa olevaa fyysistä kytkintä ei ole käytetty. Tällä menetelmällä voidaan taata, että tietomurtajan verkkoon pääseminen datadiodin kautta on mahdotonta.

4.3 Datadiodin käyttötarkoitus

Datadiodia käytetään kaiken kokoisten verkkojen segmentointiin, puolustamiseen sekä tiedon yksisuuntaiseen siirtämiseen. Niiden avulla datan siirtäminen teollisuusverkosta toiseen on turvallista. ”Se on korkeimmin sertifioitu IT-turvallisuustuote maailmassa.” (Fox it, Fox Datadiode, Video, 2021) Datadiodia käytetään useimmiten erilaisten teollisuusalojen tiedonsiirron suojaamiseen. Sen tarkoitus on luoda reaaliajassa toimiva suojattu yhteys lähettäjän ja vastaanottajan välille. Oikein käytettynä se suojaa verkon täydellisesti, sillä toinen verkkoa käyttävä osapuoli ei voi päästä käsiksi toisessa päässä oleviin järjestelmiin. Tieto kulkee järjestelmässä aina vain toiseen suuntaan ja sulkee takaisin tulevan datan liikenteen. Tällä tavalla vältytään erilaisilta ulkoisilta uhkatekijöiltä, joiden tarkoitus on päästä laivan verkkoon sisäänpäin kulkevan liikenteen mukana.

5 YHTEENVETO

5.1 Datadiodi tietoturvavälineenä

Käytettäessä datadiodin kaltaista teknologiaa yleisen tietoturvan parantamisessa on erittäin suositeltavaa. Kaikki järjestelmät eivät ole välttämättä suunniteltu tämän kaltaisen tiedonsiirron ympärille, joten datadiodin käyttö vaatii usein vanhoissa järjestelmissä paljon suunnittelua. Voi myös olla, että datadiodin kaltaisen teknologian implementointi vanhoihin järjestelmäkokonaisuuksiin ei ole edes kannattavaa. Tämä saattaisi tarkoittaa joissain tapauksissa sitä, että kokonaisen verkon suunnittelu täytyisi tehdä uudestaan. Käytettäessä datadiodia silloin kun se on alkuperäisessä verkon suunnitelmassa, pystytään välttämään erilaiset ongelmat. Voidaan kuitenkin todeta, että datadiodi on erittäin vahva suoja usean eri tason tarpeisiin.

5.2 Datadiodin käyttäminen laivaverkossa

Laivoissa verkko on useimmiten suunniteltu TCP-tyyppisen protokollan ympärille, jolloin sen kääntämisessä ja paketoimisessa voi tulla ongelmia. Laivaverkossa käytettynä datadiodi on silti erittäin varma valinta. Kuitenkin usein täytyy ottaa huomioon millaista tietoliikennettä kyseinen laiva lähettää ulos- ja sisäänpäin. Kun laiva lähettää vain toiseen suuntaan menevää tietoa, niin datadiodin käyttäminen ei tuota ongelmia. Usein kuitenkin joudutaan toteamaan, että myös sisäänpäin kulkevaa tietoliikennettä on paljon. Tällaisessa tapauksessa datadiodin käyttämistä on harkittava uudestaan. Usein datadiodia on mahdollista käyttää myös siten, että sen lävitse kulkee dataa molempiin suuntiin. Tämän lisäksi osa laitteista tukee myös useiden datavirtojen ja protokollien käyttöä samaan aikaan.

6 JOHTOPÄÄTÖKSET

6.1 Tietoturva ja meriliikenne

Meriliikenteessä tietoturvan takaamiseksi käytettävä laitteisto vaihtuu usein, sillä sen on mukauduttava jatkuvasti. Usein tehdään tietoisia ratkaisuja, joiden toiminta nähdään jatkuvan parhaimmassa tilanteessa noin viiden vuoden ajan. Usein tilanteet muuttuvat nopeammin, joten tietoturvan ja sitä ylläpitävien tahojen on reagoitava nopeasti. Normaalissa tilanteessa laivan rakennus saattaa kestää useita vuosia, jolloin laitteiden toimittajalla on aikaa reagoida. Tätä mukavuutta ei kuitenkaan vanhempien laivojen huoltopalveluilla ole vaan tilanteeseen on saatava ratkaisu heti.

Useimmiten laivoissa käytetyt menetelmät kuitenkin toimivat ja ongelmista huolimatta ne ovat täynnä useita mahdollisuuksia. Käytetyissä protokollissa on selkeitä aukkoja, jotka usein tiedostetaan jo ennestään. Kuitenkin niiden tarjoamat laajasti mukautuvat osat helpottavat uusien laitteiden ja käytäntöjen implementointia. Riippuen tilanteesta on myös suositeltavaa miettiä, että mikä on laivan tietoturvan todelliset tarpeet. Vaikka tietoturvan taso täytyy olla korkea, niin usein joudutaan harkitsemaan tietoturvan, toimintavarmuuden ja nopeuden välillä. Kaikkea ei voi saada kerralla, joten joskus tietoturvan taso saattaa kärsiä, mikäli halutaan nopeammin toimivia ratkaisuja.

6.2 Ongelmat

Datadiodin implementoinnissa ongelmakohdiksi saattaa aiheutua laivan omat ominaisuudet. Etenkin vanhoihin laivoihin lisättävän laitteiston kanssa ongelmat lisääntyvät, sillä ongelmat täytyy kiertää lisäämällä ylimääräisiä osia. Lisäksi joissain tapauksissa liikutettavan datan muotoa voidaan joutua muuttamaan useaan kertaan ennen lopullista lähettämistä. Datan siirto tällä tekniikalla on erittäin turvallista, mutta se voi olla pahimmassa tapauksessa hidasta.

LÄHTEET

Bonta R., Attorney General, State of California Department of Justice, Protect your computer from viruses, hackers, and spies, 2021. Viitattu 3.8.2021

https://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer

Etteplan, Artikkeli, Tietoturva on teollisuuden uusi normaali, 2021. Viitattu 25.6.2021

https://www.etteplan.com/fi/artikkelit/tietoturva-teollisuuden-uusi-normaali

FireEye, What is a Zero-day Exploit?, 2022. Viitattu 8.1.2022

https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

Fortinet, What is a DMZ network?, 2022. Viitattu 9.1.2022

https://www.fortinet.com/resources/cyberglossary/what-is-dmz

FOX IT, Datadiode use for ICS, Video, 2021. Viitattu 22.7.2021

https://cybersecurity.fox-it.com/datadiode-ics

Fox P., Khanacademy, User datagram protocol, 2020. Viitattu 27.7.2021

https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/user-datagram-protocol-udp

Kyberturvallisuuskeskus, Tietoturva, 9.7.2020. Viitattu 26.6.2021

https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Modbus, Modbus Application Protocol V1 1b3, 26.3.2012. Viitattu 27.7.2021

https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

Owlcyberdefence, Learn about data diodes, 2021. Viitattu 23.7.2021

https://owlcyberdefense.com/learn-about-data-diodes/

Owlcyberdefense, Securing simultaneous one-way bidirectional transfer, 2021. Viitattu 23.7.2021

https://owlcyberdefense.com/resource/securing-simultaneous-one-way-bidirectional-data-transfers/

Owlcyberdefence, What's the difference between firewalls & data diodes, 19.5.2019 Viitattu 21.7.2021

https://owlcyberdefense.com/wp-content/uploads/2019/05/19-OWL-Data-Diodes-Firewalls.pdf

Rosenblatt S. & Cipriani J., CNET, Two-factor authentication: What you need to know, 15.6.2015. Viitattu 6.10.2021

https://www.cnet.com/tech/services-and-software/two-factor-authentication-what-you-need-to-know-faq/

Sarlin, mbXLINK datadiodit, 2021. Viitattu 26.7.2021

https://www.sarlin.com/tuote/mbxlink-datadiodit/

Suomen Varustamot, Merenkulun avainluvut, 2020. Viitattu 17.7.2021

https://shipowners.fi/kilpailukyky/merenkulun-avainluvut/

Techopedia, Asynchronous transfer mode (ATM), 12.8.2020. Viitattu 28.7.2021

https://www.techopedia.com/definition/5339/asynchronous-transfer-mode-atm