SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Samuli Heinula

Automatisoitujen aurinkopaneelijärjestelmien kybertur-vallisuusriskien vähentäminen

Opinnäytetyö
Syksy 2024
Insinööri (AMK), Automaatiotekniikka

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Tutkinto-ohjelma: Insinööri (AMK), Automaatiotekniikka

Suuntautumisvaihtoehto: Sähköautomaatio

Tekijä: Samuli Heinula

Työn nimi: Automatisoitujen aurinkopaneelijärjestelmien kyberturvallisuusriskien vähentäminen

Ohjaaja: Marko Hietamäki

Vuosi: 2024 Sivumäärä: 30

Tässä opinnäytetyössä tutkittiin automatisoitujen aurinkopaneelijärjestelmien kyberturvallisuusriskejä ja keinoja niiden ennaltaehkäisemiseksi. Aurinkopaneelijärjestelmät ovat keskeisiä komponentteja nykyaikaisessa energiainfrastruktuurissa ja ne ovat alttiita mahdollisille kyberhyökkäyksille.

Työssä analysoitiin hyökkäysvektoreita, järjestelmien haavoittuvuuksia ja tapaustutkimuksia aiheesta, samalla tuotiin esiin, mihin riittämättömät turvatoimet johtavat. Tutkimus korostaa monivaiheisen tunnistautumisen, suojatun verkkorakenteen ja jatkuvien riskinarviointien kaltaisten turvallisuusstrategioiden tärkeyttä. Säännöllisten ohjelmistopäivitysten, kohdennetun työntekijäkoulutuksen ja alan standardien noudattamisen tärkeys korostuu entisestään, kun teknologia kehittyy vauhdilla ja kyberuhka mahdollisuudet kasvavat.

Lisäksi työssä arvioitiin lohkoketjuteknologian ja tekoälyn kaltaisten uusien teknologioiden mahdollisuuksia turvatoimien vahvistamisessa. Työ korostaa ennakoivan kyberturvallisuuden merkitystä verkkouhkien torjunnassa.

Tutkimuksen tavoitteena on tarjota selkeitä neuvoja automatisoitujen aurinkopaneelien kyberturvallisuusriskien hallintaan.

[1] Asiasanat: kyberturvallisuus, automaatio, aurinkopaneelit, tekoäly

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Degree program: Bachelor of Engineering, Automation Engineering

Specialization: Electric Automation

Author/s: Samuli Heinula

Title of thesis: Mitigating cybersecurity risks in automated solar panel systems

Supervisor(s): Marko Hietamäki

Year: 2024 Number of pages: 30

The thesis examined the cybersecurity vulnerabilities of automated solar panel systems. These systems, integral to modern energy infrastructure, are alarmingly susceptible to potential cyberattacks.

The research analysed attack vectors, system vulnerabilities, and real case studies to highlight the consequences of inadequate security measures. It also focused on the importance of security strategies, such as multi-factor authentication, secure network architecture, and continuous risk assessments. Regular software updates, targeted employee training, and adherence to industry standards were noted to be more important than ever as technology evolves rapidly and the potential for cyber threats increases.

The aim of the research was to offer clear solutions for managing the cybersecurity risks of automated solar panels. To strengthen security measures, the potential of new technologies, such as blockchain and artificial intelligence, were also assessed. The thesis highlighted the importance of proactive cybersecurity in combating cyber threats.

[1] Keywords: cybersecurity, automation, solar panels, artificial intelligence

SISÄLTÖ

Käytetyt termit ja lyhenteet

AI	Artificial Inteligence eli tekoäly
DREAD	Dread (Damage, Reproducibility, Exploitability, Affected users, Discoverability) on arviointimenetelmä, jolla lasketaan uhkien toteutumisen todennäköisyyttä.
DL	DL (deep learning) eli syväoppiminen
IDPS	IDPS (intrusion detection and prevention system) eli tunkeutumisen havaitsemis- ja estojärjestelmä
IEC	IEC (international Electrotechnical Commission) on sähköalan standardointiorganisaatio
IoT	IoT (Internet of Things) eli esineiden internet.
ISA	International Society of Automation on kansainvälinen automaatioyhdistys
IT	Information Technology Tietotekniikka
MFA	Multi-factor authentication eli monivaiheinen tunnistautuminen
ML	Machine learning eli koneoppiminen
PV	A photovoltaic system eli aurinkosähköjärjestelmä
STRIDE	STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) on identifiointimenetelmä, jota käytetään kyberturvallisuusuhkien tunnistamiseen ja luokitteluun.

1 JOHDANTO

1.1 Tausta

Automatisoidut aurinkopaneelijärjestelmät ovat yhä yleisempiä nykyaikaisessa energiainfrastruktuurissa. Samalla niiden kyberturvallisuusriskit kasvavat. IoT-laitteita sisältävät järjestelmät ovat alttiita kyberuhille, kuten laitteiston hallinnan kaappauksille tai energiantuotannon häirinnälle. Nämä riskit tulee huomioida energia-alalla.

1.2 Tavoite

Tämän työn tavoitteena on aurinkopaneelijärjestelmien kyberturvallisuuden analysointi, jossa keskitytään potentiaalisiin hyökkäysvektoreihin ja järjestelmähaavoittuvuuksiin. Hyökkäysvektorilla tarkoitetaan tapaa tai reittiä, jota pitkin hyökkääjä voi päästä käsiksi järjestelmään ja aiheuttaa vahinkoa. Lisäksi tarkoituksena on tuoda ilmi tehokkaita strategioita näiden riskien hallitsemiseksi. Työn tarkoituksena on luoda kattava opas kyberturvallisuuden parantamiseksi ja tarjota konkreettisia suosituksia järjestelmien turvallisuuden ylläpitämiseksi ja parantamiseksi.

1.3 Rakenne

Opinnäytetyön rakenne etenee johdannosta kirjallisuuskatsaukseen, jossa analysoidaan aiheeseen liittyvää aikaisempaa tutkimusta ja nykyisiä turvallisuuskäytäntöjä. Tulokset ja niiden analyysi esitetään omassa luvussaan ja tutkimus päättyy yhteenvetoon. Luvussa on yhteenveto tärkeimmistä havainnoista ja suosituksia tehokkaista kyberturvallisuutta parantavista toimista.

2 AUTOMAATIO AURINKOENERGIASSA

2.1 Käytettävät teknologiat

Auringonseurantajärjestelmä on järjestelmä, joka säätää automaattisesti aurinkopaneelin asentoa auringon liikkeen seuraamiseksi ja tehon maksimoimiseksi (Mehar ym., 2022, s. 343). Aurinkoseurantalaitteita on kahta päätyyppiä: yksi- ja kaksiakselisia seurantalaitteita.

Automaattiset valvontajärjestelmät on suunniteltu havaitsemaan aurinkosähkömoduulien usein huomaamatta jääneet viat (Joseph ym., 2023). Näiden järjestelmien tavoitteena on varmistaa aurinkosähköjärjestelmän tehokas ja luotettava toiminta.

2.2 Hyötysuhteen nostaminen

Aurinkokennojen seurantajärjestelmien integroiminen aurinkopaneelien asennuksiin parantaa merkittävästi energian talteenottoa, mikä lisää paneelien hyötysuhdetta ja alentaa niiden kustannuksia (Mehar ym., 2022, s. 343). Nämä järjestelmät säätävät aurinkopaneelien suuntausta dynaamisesti, jotta varmistetaan paras mahdollinen altistus auringonvalolle. Tämä on tärkeä tekijä aurinkopaneelien sähköntuoton maksimoimiseksi. Tällaisten automatisoitujen mekanismien käyttöönotto voi lisätä energiantuotantoa noin 40 prosenttia verrattuna kiinteisiin kokoonpanoihin.

2.3 Huoltokustannukset

Josephin, ym. (2023) tutkimuksessa korostetaan aurinkosähköjärjestelmien huoltokustannusten hallintaa erityisesti diagnostiikka-algoritmien ja reaaliaikaisen valvonnan avulla. Aurinkosähköjärjestelmät käyttävät diagnostiikka-algoritmia, joka mahdollistaa vikojen varhaisen havaitsemisen, kuten kapseloinnin epäonnistumisen ja moduulien korroosion. Tämän avulla huolto voidaan tehdä ajoissa, mikä vähentää seisokkiaikoja ja pidentää laitteiden käyttöikää, mikä puolestaan tuo merkittäviä kustannussäästöjä ja parantaa energiatehokkuutta. Reaaliaikainen valvonta mahdollistaa myös virheilmoitusten antamisen käyttäjille, mikä varmistaa, että viat voidaan korjata oikea-aikaisesti.

Näin ollen voidaan nähdä selvä yhteys huoltokustannusten ja kyberturvallisuuden välillä, erityisesti automatisoitujen aurinkopaneelijärjestelmien tapauksessa. Diagnostiikka- ja etävalvontajärjestelmien tehokkuus riippuu kyberturvallisuudesta; jos ne joutuvat kyberhyökkäyksen kohteeksi, vikojen oikea-aikainen havaitseminen voi estyä tai järjestelmä voi tuottaa virheellisiä hälytyksiä. Tämä johtaa huoltojen viivästymiseen, laitteiden käyttöiän lyhenemiseen ja lopulta korkeampiin huoltokustannuksiin. Näin ollen hyvin suojatut järjestelmät ovat keskeisessä asemassa huoltokustannusten hallinnassa, sillä ne varmistavat, että huolto suoritetaan ajallaan, mikä vähentää kustannuksia ja parantaa energiatehokkuutta.

3 KYBERTURVALLISUUSRISKIT: STRIDE- JA DREAD MALLIT

3.1 STRIDE-MALLIT

STRIDE-mallia voidaan käyttää, kyberturvallisuusuhkien tunnistamiseen ja luokitteluun (Rahim ym., 2023, s. 214). Se on erityisen hyödyllinen monimutkaisten järjestelmien, kuten älykkäiden sähköverkkojen, turvallisuustarpeiden arvioinnissa. Mallin avulla uhkia voidaan ryhmitellä kuuteen eri luokkaan: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service ja Elevation of Privilege.

Spoofing (Huijaaminen): Spoofing viittaa identiteetin tai tiedon väärentämiseen, jossa hyökkääjä esiintyy luotettavana käyttäjänä tai laitteena (Rahim ym., 2023, s.214) Esimerkiksi aurinkopaneelilaitteen identiteetti voidaan väärentää, jolloin ohjauskeskukseen toimitetaan virheellistä tietoa.

Tampering (Manipulointi): Tampering käsittää tietojen tai laitteiden luvattoman muokkauksen (Rahim ym., 2023, s.214) Tämä voi tapahtua fyysisesti, kuten laitteiston manipulointi, tai ohjelmallisesti, esimerkiksi konfiguraatiotiedostojen tai ohjelmistojen muuttaminen.

Repudiation (Kieltämys): Repudiation tarkoittaa toimintojen tai tapahtumien kiistämistä (Rahim ym., 2023, s.214) Hyökkääjä voi muokata lokitietoja tai auditointijälkiä piilottaakseen omat toimensa tai syyttääkseen muita käyttäjiä haitallisista toimista.

Information Disclosure (Tiedon paljastuminen): Information Disclosure viittaa luvattomaan pääsyyn tai tiedon vuotamiseen (Rahim ym., 2023, s.214) Tämä voi sisältää arkaluontoisten asiakastietojen paljastumisen tai järjestelmän haavoittuvuuksien ilmitulon.

Denial of Service (Palvelunestohyökkäys): Denial of Service -hyökkäykset pyrkivät häiritsemään järjestelmän tai palvelun saatavuutta (Rahim ym., 2023, s.214) Tämä voidaan saavuttaa esimerkiksi kuormittamalla verkkoa tai ohjauskeskusta liiallisilla pyyntöillä, mikä johtaa palvelun heikkenemiseen tai sen käyttökelvottomuuteen.

Elevation of Privilege (Oikeuksien laajentaminen): Elevation of Privilege tarkoittaa käyttäjän oikeuksien luvatonta laajentamista (Rahim ym., 2023, s.214) Hyökkääjä voi hyödyntää järjestelmän haavoittuvuuksia saadakseen korkeammat käyttöoikeudet, mikä mahdollistaa laajempien resurssien käytön ja suuremman vahingon aiheuttamisen.

3.2 DREAD-MALLIT

DREAD-malli on kyberturvallisuusuhkien arviointimenetelmä, joka auttaa määrittämään uhkien vakavuuden ja niiden mahdolliset vaikutukset järjestelmään (Rahim ym., 2023, s. 214-215). Mallin nimi muodostuu viidestä arviointikriteeristä: Damage Potential, Reproducibility, Exploitability, Affected Users ja Discoverability. Nämä kriteerit tarjoavat kattavan viitekehyksen uhkien analysointiin ja priorisointiin.

Damage Potential (Vahingon potentiaali): Tämä kriteeri arvioi, kuinka suuri vahinko uhan toteutumisesta voi aiheutua (Rahim ym., 2023, s. 214-215). Se ottaa huomioon vaikutuksen järjestelmään, tietoihin ja toimintoihin. Esimerkiksi kriittisen datan menettäminen tai järjestelmän toimintojen halvaantuminen voisi saada korkean arvosanan tässä kategoriassa.

Reproducibility (Toistettavuus): Tämä kriteeri mittaa, kuinka helposti hyökkääjä voi toistaa uhan (Rahim ym., 2023, s. 214–215). Jos hyökkäys voidaan helposti toistaa useita kertoja, se saa korkean arvosanan. Tämä kriteeri auttaa ymmärtämään, onko uhka kertaluonteinen vai jatkuva riski.

Exploitability (Hyödynnettävyys): Tämä kriteeri arvioi, kuinka paljon vaivannäköä tai taitoa hyökkääjältä vaaditaan uhan hyödyntämiseksi (Rahim ym., 2023, s. 214–215). Helposti hyödynnettävä uhka, joka ei vaadi suuria resursseja, saa korkean arvosanan. Tämä auttaa tunnistamaan ne uhat, jotka on helposti toteutettavissa.

Affected Users (Vaikutuksen kohteena olevat käyttäjät): Tämä kriteeri arvioi, kuinka moni käyttäjä tai järjestelmän osa joutuu uhan kohteeksi (Rahim ym., 2023, s. 214–215). Laajoja käyttäjäryhmiä tai kriittisiä järjestelmän osia koskettava uhka saa korkean arvosanan, koska sen vaikutukset ovat laaja-alaiset.

Discoverability (Havaittavuus): Tämä kriteeri mittaa, kuinka helposti uhka voidaan havaita joko hyökkääjien tai puolustajien toimesta (Rahim ym., 2023, s. 214–215). Jos uhka on vaikeasti havaittavissa, se saa korkean arvosanan. Tämä kriteeri auttaa ymmärtämään, kuinka nopeasti uhkaan voidaan reagoida ja sen toteutumista estää.

Jokainen näistä kriteereistä arvioidaan asteikolla 0–10, missä 10 merkitsee korkeinta vakavuutta tai vaikutusta (Rahim ym., 2023, s. 214–215). Kriteerien yhteenlasketut pisteet antavat kokonaisarvosanan uhalle, mikä auttaa priorisoimaan ja kohdentamaan resursseja eri uhkien hallintaan.

3.3 Haavoittuvuudet

Automatisoidut aurinkopaneelijärjestelmät, jotka ovat olennainen osa älykästä sähköverkkoa, voivat kärsiä haavoittuvuuksista, jotka ovat ominaisia toisiinsa liitetyille ja verkkoon kytketyille laitteille (Rahim ym., 2023, s. 210). Aurinkosähköjärjestelmiä sisältävien älykkäiden verkkojen käyttöönotto on edellyttänyt vahvaa uhkien mallintamista ja riskinarviointia koskevaa lähestymistapaa. Nämä haavoittuvuudet johtuvat digitaalisten liitäntöjen, toimilaitteiden, anturimittausten ja langattoman viestinnän laajasta käytöstä automaattisissa järjestelmissä. Tällaiset haavoittuvuudet edellyttävät kattavaa analyysia, jossa hyödynnetään STRIDE- ja DREAD-mallien kaltaisia malleja, jotta riskejä voidaan arvioida ja vähentää merkittävästi.

3.4 Mahdolliset kyberturvallisuusuhat

Nämä järjestelmät ovat alttiita kyberhyökkäyksille sillä ne ovat riippuvaisia IT- ja verkkoinfrastruktuurista. Niiden keskeinen rooli sähköverkossa tekee niistä houkuttelevan kohteen hyökkäyksille, jotka pyrkivät häiritsemään energiantuotantoa. Tätä riskiä lisää entisestään järjestelmien kriittinen rooli laajemmassa sähköverkossa (Harrou ym., 2023, s. 1).

Viimeaikaiset tapahtumat korostavat aurinkosähköjärjestelmien alttiutta kyberuhkille esimerkkinä Ukrainan sähköverkkoon vuonna 2015 ja yhdysvaltalaiseen sähkölaitokseen vuonna 2019 tehty kyberhyökkäys (Harrou ym., 2023, s. 2). Molemmissa tapauksissa aurinkosähkö- ja tuulivoimalaitoksiin kohdistui merkittäviä seurauksia. Molemmissa

tapauksissa digitaalisessa puolustuksessa oli haavoittuvuuksia. Näin ollen nämä tapaukset korostavat tiukkojen kyberturvallisuusprotokollien tarpeellisuutta.

Kun otetaan huomioon näiden haasteiden laajuus, on ehdottoman tärkeää toteuttaa kattava kyberturvallisuusstrategia (Rahim ym., 2023, s.210). Tähän lähestymistapaan kuuluu luoda uhkamalleja, jotka on räätälöity aurinkosähköjärjestelmiä sisältäville älykkäille sähköverkoille ja joissa käytetään menetelmiä, kuten STRIDE-menetelmää uhkien luokitteluun ja DREAD-mallia uhkien ja riskien priorisointiin. Nämä toimenpiteet on suunniteltu suojaamaan aurinkosähköjärjestelmiä uusilta kyberuhkilta ja varmistamaan näin energiainfrastruktuurimme kestävyys.

Kybertoimintaympäristöön voi kohdistua monenlaisia fyysisiä uhkia, jotka häiritsevät järjestelmien toimintaa (Kyberturvallisuusstrategia 2024, s. 13). Esimerkiksi sähkökatkot, tulvat, maanjäristykset ja auringon aktiivisuuden lisääntyminen voivat kaikki vaikuttaa suoraan tietoliikenneyhteyksiin ja tietojärjestelmiin. Myös muut luonnonkatastrofit ja inhimilliset virheet voivat aiheuttaa häiriöitä, jotka heikentävät kyberturvallisuutta.

4 TIETOTURVALOUKKAUSTEN SEURAUKSET

4.1 Vaikutukset energian tuotantoon ja jakeluun

Aurinkosähköjärjestelmien (solar PV) integrointi älykkäisiin sähköverkkoihin tuo mukanaan uusia haasteita erityisesti kyberturvallisuuden osalta (Rahim ym. 2023, s. 211). On tärkeää ymmärtää näiden monimutkaisten järjestelmien potentiaaliset kyberturvallisuushaavoittuvuudet, sillä ne ovat yhteydessä toisiinsa. Haitalliset toimijat voivat hyödyntää näitä haavoittuvuuksia henkilökohtaiseen hyötyyn, palvelukatkoksiin tai sabotointiin. Onnistuneet kyberhyökkäykset voivat johtaa vakaviin seurauksiin, kuten sähköntuotannon häiriöihin, verkon epävakauteen, luvattomaan pääsyyn yksityisiin tietoihin ja yksityisyyden loukkauksiin. Aurinkosähköjärjestelmät voivat myös toimia ponnahduslautana laajemmille hyökkäyksille sähköverkkoon sen vuoksi.

Useat tutkimukset ovat tarkastelleet älykkäiden sähköverkkojen aurinkosähköjärjestelmien kyberturvallisuushaasteita. Esimerkiksi Hasan ym., (2023) korostivat autentikointimekanismien, salaustekniikoiden ja tunkeutumisen havaitsemisjärjestelmien merkitystä. Chehri & Fofana (2021) ehdottivat laadullisia riskinarviointimenetelmiä, ja Teymouri ym., (2018) tarkastelivat kyberhyökkäysten vaikutuksia jännitteen säätelyyn jakeluverkoissa. Islam ym. (2019) keskittyivät fyysisen tason tietoturvaan.

4.2 Taloudelliset vaikutukset

Tietoturvaloukkausten taloudelliset vaikutukset älykkäisiin sähköverkkoihin, jotka sisältävät aurinkosähköjärjestelmiä, voivat olla merkittäviä. Rahim ym. (2023, s. 217) mukaan korkean riskin uhkia, kuten tietojen paljastumista, oikeuksien laajentamista ja tietojen väärentämistä, pidetään erityisen merkittävinä. Ne vaativat välitöntä huomiota ja suurempia investointeja lieventämistoimenpiteisiin. Näiden uhkien seurauksena voi olla sähkön tuotannon vaarantuminen, verkon epävakaus sekä luvattoman pääsyn ja yksityisyydensuojan loukkausten riski. Lisäksi tietoturvaloukkaukset voivat aiheuttaa huomattavia taloudellisia menetyksiä, koska ne saattavat johtaa palvelun keskeytyksiin ja merkittäviin toiminnallisiin ongelmiin energianjakeluverkossa.

4.3 Mainevahingot

Tietoturvaloukkauksista aiheutuvat mainevahingot voivat olla huomattavan suuria ja pitkäaikaisia, ja niiden vaikutukset ulottuvat laajalle organisaation toimintaan (Perera ym., 2022). Kun asiakkaat ja sidosryhmät kokevat, että heidän henkilökohtaiset tai taloudelliset tietonsa eivät ole turvassa, tämä heikentää heidän luottamustaan yritykseen ja sen kykyyn suojata tietojaan. Tämä luottamuspula voi johtaa asiakas- ja kumppanisuhteiden heikkenemiseen, jolloin uusien asiakkuuksien ja yhteistyökumppaneiden hankkiminen vaikeutuu (Infosec, 2020). Lisäksi tällaiset tapaukset voivat vaikuttaa suoraan yrityksen liiketoimintaan, sillä mainehaitta voi vähentää brändin arvoa ja heijastua suoraan myyntiin ja asiakasmääriin.

Julkisuuteen noussut tietoturvaloukkaus voi myös heikentää organisaation uskottavuutta laajemmassa mittakaavassa, mikä voi johtaa siihen, että esimerkiksi sähköpostiviestinnän perillemeno vaikeutuu ja yhteistyö kolmansien osapuolten kanssa hankaloituu (Perera ym., 2022). Organisaation voi olla tarpeen investoida huomattavasti resursseja maineen palauttamiseen ja vahinkojen korjaamiseen, mikä puolestaan kasvattaa taloudellisia kustannuksia ja hidastaa liiketoiminnan kasvua (Infosec, 2020).

5 SRATEGIAT KYBERTURVALLISUUSRISKIEN VÄHENTÄMISEKSI

5.1 Turvallinen verkkoarkkitehtuuri

Vahva verkkoarkkitehtuuri on olennainen kyberturvallisuusriskien vähentämiseksi automatisoiduissa aurinkopaneelijärjestelmissä. Gongin ja Leen (2021) mukaan tehokas reaaliaikaisen uhkien havaitsemisen, analysoinnin ja niihin vastaamisen kehys koostuu useista kriittisistä vaiheista, kuten uhkatiedon keräämisestä, uhkien analysoinnista ja priorisoinnista, tapahtumiin vastaamisen suunnittelusta ja toteutuksesta. Heidän tutkimuksensa osoitti, että tällainen kehys pystyy havaitsemaan ja reagoimaan kyberuhkiin reaaliajassa, mikä lyhentää merkittävästi aikaa, joka kuluu kyberhyökkäysten lieventämiseen energiaympäristössä. Kehyksen kattava lähestymistapa sisältää edistyneiden työkalujen ja tekniikoiden käytön verkon infrastruktuurin turvallisuuden ja resilienssin varmistamiseksi.

5.2 Pääsyvalvonta

Pääsyvalvonta varmistaa, että vain valtuutetut henkilöt tai järjestelmät pääsevät käsiksi suojattuihin resursseihin. Tämä saavutetaan käyttämällä vahvoja salasanoja, kaksivaiheista todennusta ja digitaalisia sertifikaatteja (Pochmara & Świetlicka, 2024, s. 3). Lisäksi teollisuusstandardien, kuten ISA/IEC 62443, noudattaminen varmistaa, että pääsyvalvontaprosessit ovat kattavia ja perustuvat parhaisiin käytäntöihin (mts.1). Erityisesti teollisuusautomaation järjestelmissä, kuten automaattisissa aurinkopaneelijärjestelmissä, verkkojen segmentointi ja pääsyn hallinta eri verkon osiin ovat keskeisiä toimenpiteitä, joilla pyritään rajoittamaan tietomurtojen vaikutuksia.

6 Parhaat käytännöt automatisoitujen aurinkopaneelijärjestelmien turvaamiseksi

6.1 Säännölliset ohjelmistopäivitykset ja korjausten hallinta

Automatisoitujen aurinkopaneelijärjestelmien turvallisuuden ja toiminnallisuuden varmistaminen edellyttää säännöllisiä ohjelmistopäivityksiä (Pochmara & Świet-licka, 2024, s. 10). Lisäksi tarvitaan tehokasta korjausten hallintaa, jossa pyritään nopeaan ja järjestelmälliseen vikojen korjaamiseen. Nämä päivitykset ovat olennaisia suojaamaan järjestelmiä uusilta haavoittuvuuksilta.

Korjausten hallintaan kuuluu korjausten nopea käyttöönotto turvallisuusvirheiden korjaamiseksi ja järjestelmän suorituskyvyn parantamiseksi (Safitra ym., 2023, s. 7). Automaattiset työkalut voivat auttaa korjausten tehokkaassa jakelussa, mikä minimoi päivitysten julkaisun ja soveltamisen välisen viiveen (Pochmara & Świetlicka, 2024, s. 12). Lisäksi ennen täyttä käyttöönottoa on tärkeää testata korjaukset hallitussa ympäristössä, jotta estetään uusien ongelmien syntyminen.

Jatkuvaa vaatimustenmukaisuuden seurantaa tulisi myös suorittaa säännöllisesti, jotta voidaan varmistaa, että kaikki korjaukset on sovellettu vaaditulla tavalla ja että organisaatio noudattaa omia turvallisuuskäytäntöjään (Safitra ym., 2023, s. 10).

6.2 Työntekijöiden koulutus ja tietoisuusohjelmat

Organisaatioiden tulisi tarjota säännöllistä turvallisuuskoulutusta työntekijöilleen tietoisuuden ja ymmärryksen lisäämiseksi turvallisuusriskeistä (Safitra ym., 2023, s. 14-15). Koulutusohjelmien tulisi sisältää ajankohtaista tietoa siitä, miten tunnistaa ja reagoida mahdollisiin uhkiin. Näin varmistetaan, että henkilöstö osaa toimia oikein kyberuhkien kohdatessa ja pystyy minimoimaan mahdolliset vahingot.

Turvallisuustietoisuuden kulttuurin kehittäminen jatkuvan koulutuksen ja opetuksen avulla auttaa organisaatioita vähentämään ihmistekijöistä johtuvia riskejä, näitä usein pidetään kyberturvallisuuden heikoimpana lenkkinä (Safitra ym., 2023, s. 18). Tämä kulttuuri edistää

työntekijöiden proaktiivisuutta ja parantaa heidän valmiuksiaan suojautua erilaisilta kyberuhkilta. Säännölliset päivitykset ja harjoitukset auttavat pitämään tiedot ja taidot ajan tasalla.

6.3 Fyysiset turvatoimet

Fyysiset turvatoimet ovat keskeinen osa organisaation tietoturvaa, sillä ne estävät fyysisiä hyökkäyksiä ja suojaavat kriittisiä resursseja, kuten laitteita ja tietojärjestelmiä (Knuutila, 2022). Tärkeitä fyysisen turvallisuuden keinoja ovat esimerkiksi Red Team -testaus, kulunvalvonta, kameravalvonta ja murtohälyttimet.

Knuutilan (2022,) mukaan Jelen (2021) kertoo Red Team -testauksen menetelmästä, jossa asiantuntijat pyrkivät tunkeutumaan organisaation tiloihin hyökkääjän näkökulmasta, mikä auttaa tunnistamaan fyysisiä haavoittuvuuksia ja kehittämään suojauksia. Lisäksi henkilöstön koulutus ja käytännöt, kuten puhtaan pöydän politiikka, auttavat estämään sosiaalista manipulointia ja varmistamaan turvallisuuskäytäntöjen noudattamisen.

Fyysisten turvatoimien ylläpito vaatii jatkuvaa arviointia ja päivityksiä, jotta ne pysyvät tehokkaina ja vastaavat organisaation tarpeita. (Knuutila, 2022).

6.4 Kolmannen osapuolen toimittajien hallinta

Organisaatioiden on tärkeää luoda vahvoja kumppanuuksia kyberturvallisuuden ekosysteemissä. Tämä tarkoittaa, että eri tahojen, kuten yritysten, viranomaisten ja toimittajien tulee tehdä yhteistyötä. Yhteistyön avulla parannetaan tietoturvaa kaikkien osapuolten välillä. (Safitra ym., 2023). Yhteistyö liikekumppaneiden, toimittajien ja aktiivisten loppukäyttäjien kanssa voi tarjota merkittävää tukea monimutkaisten haasteiden ratkaisemisessa. Tällainen yhteistyö edistää kokonaisvaltaisten ja tehokkaiden ratkaisujen kehittämistä erilaisiin kyberuhkiin.

Tehokas kolmannen osapuolen toimittajien hallinta edellyttää, että kaikki toimittajat noudattavat organisaation määrittelemiä tietoturvapoliittisia menettelyjä (Safitra ym., 2023). Tämä voidaan varmistaa säännöllisten auditointien ja arviointien avulla, jotka takaavat, että toimittajat ylläpitävät vaadittuja turvallisuusstandardeja. Näin voidaan varmistaa, että kaikki osapuolet toimivat yhtenäisesti turvallisuuskäytäntöjen mukaisesti, mikä vähentää merkittävästi riskiä, että toimittajien kautta syntyy haavoittuvuuksia ja muita turvallisuusuhkia.

6.5 Alan standardien ja määräysten noudattaminen

Teollisuusautomaation järjestelmien suojaaminen kyberhyökkäyksiltä vaatii monenlaisten tietoturvatoimien käyttöönottoa (International Society of Automation, 2023, viitattu Pochmara & Świetlicka, 2024, s.1–2). Näihin toimiin kuuluvat muun muassa verkkoturvallisuuden parantaminen, ohjelmistojen säännölliset päivitykset, verkkoliikenteen seuranta, pääsynvalvonta sekä henkilöstön kouluttaminen kyberturvallisuusasioissa. On myös erittäin tärkeää noudattaa alan vakiintuneita turvallisuusstandardeja, kuten ISA/IEC 62443 -standardeja.

ISA/IEC 62443 -standardit ovat kansainvälisesti hyväksyttyjä ohjeita, jotka on kehitetty Kansainvälisen automaatioyhdistyksen (ISA) ja Kansainvälisen sähkötekniikan komission (IEC) toimesta (International Society of Automation, 2023, viitattu Pochmara & Świetlicka, 2024, s.1–2). Näiden standardien noudattaminen auttaa yrityksiä vähentämään hyökkäysriskejä ja parantamaan teollisuusautomaation järjestelmien kestävyyttä kyberuhkia vastaan.

7 Esimerkkitapaukset: Tietoturvatapahtumista saadut kokemukset.

7.1 Tapahtuma 1: Kuvaus ja vaikutukset

Vuonna 2022 suomalainen aurinkoenergian tarjoaja joutui merkittävän palvelunestohyökkäyksen (DoS) kohteeksi (Kyberturvallisuuskeskus, 2022). Hyökkäys ohjasi valtavia määriä liikennettä yrityksen palvelimille, jolloin ne eivät enää vastanneet ja johtivat valvonta- ja ohjausjärjestelmien tilapäiseen pysäyttämiseen. Tapaus toi esiin yrityksen verkkoinfrastruktuurin haavoittuvuudet, erityisesti sen, ettei siinä ollut riittävää liikenteen suodatusta ja kapasiteettia käsitellä odottamattomia äkillisiä virtauksia. Hyökkäys ei vaikuttanut ainoastaan palveluntarjoajan toimintaan vaan myös sen asiakkaisiin, jotka kokivat viivästyksiä ja häiriöitä energianhallintapalveluissa.

7.2 Tapahtuma 2: Kuvaus ja vaikutukset

Vuonna 2023 Energy One, australialainen energia-alan ohjelmistoyritys, kärsi merkittävästä tietoverkkohyökkäyksestä, joka vaikutti sen yritysjärjestelmiin Australiassa ja Yhdistyneessä kuningaskunnassa. (SecurityWeek, 2023). Hyökkäyksessä käytettiin hyväksi haavoittuvuuksia yrityksen internetiin kytketyissä aurinkopaneelien valvontajärjestelmissä. Tapaus osoitti, että uusiutuvan energian järjestelmät ovat alttiita kyberuhkille, erityisesti niihin liitettyjen komponenttien, kuten invertterien ja valvontajärjestelmien, kautta. Tietomurto johti siihen, että osa yrityksen ja asiakkaiden järjestelmien välisistä yhteyksistä katkaistiin väliaikaisesti vaikutusten lieventämiseksi. Tapahtuma korosti vahvojen kyberturvatoimien merkitystä kriittisen infrastruktuurin suojaamisessa.

7.3 Tapahtuma 3: kuvaus ja vaikutukset

Vuonna 2014 Home Depot koki merkittävän tietomurron (Keskin ym., 2021, s. 6). Hyökkääjät onnistuivat varastamaan yli 50 miljoonan asiakkaan luottokorttinumerot ja 53 miljoonaa sähköpostiosoitetta. Tämä tietomurto johti siihen, että Home Depot joutui maksamaan vähintään 134,5 miljoonaa dollaria korvauksia Visalle, MasterCardille ja eri pankeille.

Lisäksi yli 50 oikeusjuttua yhdistettiin kahteen ryhmäkanteeseen, mikä johti 19 miljoonan dollarin korvauksiin, joista 13 miljoonaa oli vahinkojen korvaamiseksi ja 6,5 miljoonaa henkilöllisyyden suojelupalveluihin. Lisäksi Home Depot maksoi vaikutuksen kohteeksi joutuneille rahoituslaitoksille 27 miljoonaa dollaria, mikä nosti kokonaiskustannukset 179 miljoonaan dollariin.

Hakkerit käyttivät varastettuja tunnistetietoja yhdeltä Home Depotin toimittajalta päästäkseen yrityksen verkkoon (Keskin ym., 2021, s. 6). Näiden tunnistetietojen avulla hakkerit pystyivät hyödyntämään Windowsin nollapäivähaavoittuvuutta ja asentamaan räätälöidyn haittaohjelman itsepalvelukassoihin Yhdysvalloissa ja Kanadassa. Haittaohjelma jäi havaitsematta viideksi kuukaudeksi huhtikuusta syyskuuhun 2014. Tapaus korosti puutteellista verkon segmentointia ja tarpeen parantaa kolmannen osapuolen toimittajien pääsyn valvontaa ja hallintaa.

7.4 Esimerkkitapausten yhteisten piirteiden analysointi

Tapaukset korostavat energia-alan, myös aurinkoenergiajärjestelmien, merkittäviä kyberturvallisuusriskejä. Yhteisiä piirteitä ovat heikkojen todennusmekanismien, oletustunnusten ja riittämättömien turvaprotokollien hyödyntäminen. Nämä esimerkkitapaukset korostavat seuraavien seikkojen merkitystä:

-Säännölliset ohjelmistopäivitykset: Varmistetaan, että laiteohjelmistot ja ohjelmistot ovat ajan tasalla tunnettujen haavoittuvuuksien torjumiseksi.

-Vahva todennus: Monitekijätodennuksen käyttöönotto ja oletustunnusten välttäminen.

-Jatkuva seuranta: Järjestelmien säännöllinen seuranta epäilyttävän toiminnan ja mahdollisten rikkomusten varalta.

-Kattavat riskinarvioinnit: Perusteellisten arviointien tekeminen mahdollisten turvallisuusriskien tunnistamiseksi.

8 Kyberturvallisuuden tulevat trendit ja uudet teknologiat

8.1 Tekoäly uhkien havaitsemisessa

Aurinkopaneelijärjestelmät ovat yhä useammin yhteydessä verkkoon IoT-laitteiden kautta, mikä altistaa ne monenlaisille kyberuhille. Tekoäly (AI) tarjoaa kehittyneitä ratkaisuja näiden uhkien havaitsemiseen ja torjuntaan, mikä on erityisen tärkeää aurinkosähköjärjestelmien toiminnan ja luotettavuuden kannalta.

Tekoäly (AI) on noussut keskeiseksi työkaluksi kyberturvallisuustoimenpiteiden parantamisessa, erityisesti automatisoiduissa aurinkopaneelijärjestelmissä. Eri AI-tekniikat ja -menetelmät parantavat merkittävästi kyberuhkien havaitsemista ja torjuntaa, mikä johtaa turvallisempiin ja kestävämpiin järjestelmiin.

Yksi tärkeimmistä edistysaskeleista tällä alalla on syväoppimismenetelmien (DL) käyttö haittaohjelmien tunnistuksessa ja analyysissä (Djenna ym., 2023, s. 9–11). Syväoppimistekniikat ovat ylittäneet perinteiset koneoppimismenetelmät (ML) kyvyllään käsitellä suuria tietomääriä, tunnistaa monimutkaisia kuvioita ja vähentää tunnistusaikaa. Lisäksi dynaamisen syväoppimisen ja heuristisen menetelmien yhdistäminen on merkittävästi parantanut haittaohjelmien tunnistusasteita, tarkkuutta ja kykyä käsitellä uusia ja tuntemattomia haittaohjelmaversioita, mukaan lukien zero-day-uhat. Aurinkopaneelijärjestelmien osalta tämä tarkoittaa parempaa suojaa kehittyneitä kyberuhkia vastaan, jotka voivat kohdistua järjestelmän ohjaus- ja valvontakomponentteihin

Keskittymällä ohjelmiston käyttäytymiseen allekirjoituspohjaisten menetelmien sijaan voidaan tehokkaasti torjua nykyaikaisten haittaohjelmien hämäystekniikat (Djenna ym., 2023, s. 3–11). Allekirjoituspohjaiset menetelmät tarkoittavat haittaohjelmien tunnistamista sisältävien tunnettujen koodisekvenssien eli "allekirjoitusten" perusteella. Tämä menetelmä on nopea ja tehokas tunnetuille haittaohjelmille, mutta tehoton uusille, tuntemattomille hyökkäyksille (Djenna ym., 2023, s. 9).

8.2 Lohkoketjuteknologia aurinkoenergian turvallisuudessa

Lohkoketjuteknologia on osoittautunut lupaavaksi vaihtoehdoksi, erityisesti energiasektorilla (Khezami ym., 2022 s. 1–6). Lohkoketju on hajautettu digitaalinen pääkirja, joka ylläpitää historian kaikista liiketoimintaverkoston tapahtumista varmistaen, että näitä tietueita ei voida muokata tai poistaa kerran syötettynä. Jokainen tapahtuma on kryptografisesti linkitetty edelliseen, muodostaen turvallisen ja läpinäkyvän ketjun. Näiden tapahtumien vahvistus saavutetaan konsensusmekanismin kautta, johon osallistuvat ennalta määritellyt osapuolet. Nämä lohkoketjuteknologian ominaisuudet tekevät siitä houkuttelevan ratkaisun energiaverkkojen ja resurssien älykkääseen hallintaan, mikä helpottaa siirtymistä kestävämpään ja turvallisempaan energiajärjestelmään.

Kun tarkastellaan lohkoketjuja energianhallinnassa, on tärkeää tunnistaa energialähteet, jotka ovat parhaiten yhteensopivia tämän teknologian kanssa ja jotka edustavat tulevaisuuden tutkimustrendejä. Kolme päätyyppiä ovat fossiilinen energia (eniten käytetty maailmanlaajuisesti), fissioenergia (korkein kapasiteettikerroin) ja uusiutuva energia (lupaavin).

Tutkimukset ovat osoittaneet, että uusiutuva energia on yleisimmin käytetty lohkoketjuteknologian kanssa, muodostaen 91,28 % asiaan liittyvistä artikkeleista (Khezami ym., 2022, s.24–25). Tämä keskittyminen uusiutuviin energialähteisiin vastaa odotusta, että niiden osuus maailmanlaajuisessa sähköntuotannossa kasvaa nykyisestä alle 10 prosentista 90 prosenttiin vuoteen 2050 mennessä, osana IEA: n "netto nollapäästöt" -suunnitelmaa. Ennakoitu 2 biljoonan dollarin vuotuinen investointi vihreään energiaan vuoteen 2030 mennessä lisää myös tutkimusintoa. Uusiutuvista energialähteistä aurinkoenergia on eniten mainittu (82 %), seuraavina tuulivoima (11,29 %), geoterminen energia (2,87 %), vesivoima ja biomassa (molemmat 1,92 %). Aurinkoenergian etusija tuulivoimaan nähden johtuu aurinkopaneelien laskevista kustannuksista ja niiden soveltuvuudesta asuinkäyttöön, mikä mahdollistaa tehokkaan vertaiskaupan lohkoketjuteknologian avulla.

Lohkoketjuteknologian ensisijaiset sovellukset energiasektorilla ovat turvallisuus (29,92 %), energiakauppa (25,12 %), energian varastointi (14,44 %), sähköajoneuvot (14,01 %), älyverkot (7,85 %), energianhallinta (7,85 %) ja hiilidioksidipäästöjen seuranta (0,82 %) (Khezami ym., 2022, s.27). Turvallisuus on tärkein sovellus, ja lähes 550 artikkelia 769

käsittelee tätä aihetta. Vuodesta 2016 lähtien kiinnostus on kasvanut lohkoketjuteknologian käyttöön erityisesti turvallisten ja yksityisten transaktioiden varmistamiseksi sekä perinteisissä että vertaisenergiaverkoissa.

Tämän analyysin perusteella lohkoketjuteknologia voi merkittävästi parantaa järjestelmien kyberturvallisuutta. Hajautettu rakenne estää yksittäisiä haavoittuvuuspisteitä, mikä tekee järjestelmistä vastustuskykyisempiä kyberhyökkäyksille. Lisäksi lohkoketjun muuttumattomuus takaa, että aurinkoenergian tuotanto- ja kulutustiedot ovat luotettavia ja tarkkoja, mikä estää tietojen manipuloinnin. Tarkastelujen perusteella älykkäät sopimukset (smart contracts) mahdollistavat automaattiset ja turvalliset transaktiot energian myynnissä ja ostossa, vähentäen inhimillisten virheiden ja petosten riskiä.

Lohkoketjuteknologian ominaisuudet, kuten hajauttaminen, muuttumattomuus ja konsensuspohjainen validointi, tekevät siitä ihanteellisen ratkaisun aurinkoenergiajärjestelmien turvaamiseen. Näiden ominaisuuksien avulla voidaan luoda turvallinen ja läpinäkyvä alusta aurinkoenergian tuotannon, jakelun ja kulutuksen hallintaan. Havaintojen perusteella lohkoketjuteknologian käyttö energianhallinnassa edellyttää energialähteiden yhteensopivuuden tunnistamista. Fossiilinen energia, fissioenergia ja uusiutuva energia ovat kolme päätyyppiä, jotka edustavat tulevaisuuden tutkimustrendejä. Uusiutuva energia, erityisesti aurinkoenergia, on lupaava vaihtoehto kestävään energiantuotantoon ja sopii hyvin lohkoketjun kanssa käytettäväksi.

9 YHTEENVETO

Tässä opinnäytetyössä on tutkittu automatisoitujen aurinkopaneelijärjestelmien kyberturvallisuusriskejä ja ehdotettu strategioita näiden riskien lieventämiseksi. Keskeiset havainnot osoittavat, että nämä järjestelmät ovat alttiita erilaisille uhkille, koska ne ovat riippuvaisia verkkoyhteyksistä ja digitaalisesta teknologiasta. Haavoittuvuuksia ovat muun muassa heikot todennusmekanismit, vanhentuneet ohjelmistot ja riittämättömät verkkoturvatoimenpiteet.

Tässä työssä esitettiin miten verkkohyökkäyksillä voi olla vakavia seurauksia energiantuotannolle ja -jakelulle, taloudelliselle vakaudelle ja yrityksen maineelle. Kolme esimerkkitapausta osoittivat, miten hyökkäykset voivat häiritä merkittävästi energiantuotantoa ja paljastaa puutteita yritysten turvallisuusstrategioissa.

Tässä työssä tutkittiin uusien teknologioiden, kuten tekoälyn ja lohkoketjuteknologian, mahdollisuuksia parantaa aurinkopaneelijärjestelmien kyberturvallisuutta. Näillä teknologioilla voidaan parantaa uhkien havaitsemista ja hallintaa sekä suojata tärkeitä tietoja tehokkaammin.

9.1 Suositukset tehokkaiden kyberturvallisuustoimenpiteiden toteuttamiseksi.

Automaattisten aurinkopaneelijärjestelmien turvallisuuden varmistaminen edellyttää useita käytännön toimia, jotta järjestelmät pysyvät suojattuina kyberuhkia vastaan ja niiden haavoittuvuudet saadaan minimoitua. On tärkeää varmistaa järjestelmien keskeytyksetön toiminta. Lisäksi on tärkeää minimoida riskit, jotka voivat häiritä energiantuotantoa ja -jakelua. Alla esitetyt suositukset sisältävät käytännön keinoja kyberturvallisuuden parantamiseen ja järjestelmien turvallisuuden ylläpitämiseen:

- Säännölliset ohjelmistopäivitykset: Varmista, että kaikki komponentit, myös laiteohjelmisto ja sovellukset, pidetään ajan tasalla haavoittuvuuksien minimoimiseksi.
- Monitekijätodennus: Käytä useita eri todentamismenetelmiä, kuten salasanaa ja biometrisiä tunnisteita, estääksesi luvattoman käytön.

- Turvallisuuskoulutus: Kouluta työntekijöitä säännöllisesti. Luo jatkuva oppimisympäristö.
- Lohkoketjuteknologia: Hyödynnä lohkoketjuteknologiaa tietojen eheyden varmistamiseksi ja turvallisen energiakaupan mahdollistamiseksi.
- Jatkuva seuranta: Käytä jatkuvaa seurantaa ja häiriötilanteisiin reagoimista koskevia suunnitelmia, jotta poikkeamat voidaan havaita ja niihin voidaan reagoida nopeasti.

9.2 Jatkuvan arvioinnin ja parantamisen merkitys

Kyberturvallisuus on jatkuvasti kehittyvä ala, jossa uhat ovat yhä kehittyneempiä. Siksi on tärkeää, että yritykset sitoutuvat jatkuvaan kyberturvallisuuden arviointiin ja parantamiseen. Säännölliset riskinarvioinnit, ajantasaiset uhkatiedot ja mukautuvat turvallisuusstrategiat ovat olennaisen tärkeitä kyberuhkien torjunnassa. Jatkuva parantaminen edellyttää myös sitä, että pysytään ajan tasalla teknologian kehityksestä ja sisällytetään uusia ratkaisuja, kuten tekoälyä ja lohkoketjuja, turvallisuusstrategioihin.

Organisaatioiden olisi myös ylläpidettävä työntekijöiden tietoja kyberturvallisuudesta ja varmistettava, että työntekijät ovat aina valmiita tunnistamaan uudet uhat ja vastaamaan niihin. Kyberturvallisuuden parantaminen ei ole kertaluonteinen hanke, vaan jatkuva prosessi, joka edellyttää jatkuvaa sitoutumista.

LÄHTEET

Alajlan, R., Alhumam, N., & Frikha, M. (2023). Cybersecurity for blockchain-based IoT systems: A review. *Applied Sciences*, 13(13), 1-26. https://doi.org/10.3390/app13137432

AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023). Cybersecurity risk analysis in the IoT: A systematic review. *Electronics*, 12(18), 1-19. https://doi.org/10.3390/electronics12183958

Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review. *Electronics*, 11(2), 1-27. https://doi.org/10.3390/electronics11020198.

Chandra, R., Bhaumik, T., & Banerjee, D. (2023). Arduino based solar tracking system as a step towards efficient utilization of clean energy: A review. *International Journal for Research in Applied Science and Engineering Technology*, 11(2), 1511-1514. https://doi.org/10.22214/ijraset.2023.49306

Chehri, A.; Fofana, I.; Yang, X. Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. *Sustainability* 2021, 13, 3196. https://doi.org/10.3390/su13063196

Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. *Symmetry*, 15(3), artikkeli 677. https://doi.org/10.3390/sym15030677

Gong, S., & Lee, C. (2021). Cyber threat intelligence framework for incident response in an energy cloud platform. *Electronics*, 10(3), artikkeli 239. https://doi.org/10.3390/electronics10030239

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems*, 12(5), 165. https://doi.org/10.3390/systems12050165

Harrou, F., Taghezouit, B., Bouyeddou, B., & Sun, Y. (2023). Cybersecurity of photovoltaic systems: Challenges, threats, and mitigation strategies: A short survey. Frontiers in *Energy Research*, 11, artikkeli 1274451. https://doi.org/10.3389/fenrg.2023.1274451

Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network andComputer Applications*, 209(August 2022), 103540. https://doi.org/10.1016/j.jnca.2022.103540

Infosec. (2020). *Phishing: Reputational damages*. https://www.infosecinstitute.com/resources/phishing/reputational-damages/

International Society of Automation. (2023). *ISA/IEC 62443 series of standards*. Saatavilla osoitteessa https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Islam, S. N., Baig, Z., & Zeadally, S. (2019). Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures. IEEE Transactions on Industrial Informatics, 15(12), 6522–6530. https://doi.org/10.1109/TII.2019.2931436

Joseph, E., Kumar, P. M. V., Singh, B. S. M., & Ching, D. L. C. (2023). Performance monitoring algorithm for detection of encapsulation failures and cell corrosion in PV modules. *Energies*, *16*(8), artikkeli 3391. https://doi.org/10.3390/en16083391

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics, 10*(10), artikkeli 1168. https://doi.org/10.3390/electronics10101168

Khezami, N., Gharbi, N., Neji, B., & Benhadj Braiek, N. (2022). Blockchain technology implementation in the energy sector: Comprehensive literature review and mapping. *Sustainability, 14*(23), artikkeli 15826. https://doi.org/10.3390/su142315826

Knuutila, O. (2022). Fyysinen tietoturva: testausmetodit ja hallintakeinot. Turun ammattikorkeakoulu. Saatavilla osoitteessa https://www.theseus.fi/handle/10024/745101

Kovacs, E. (2023, August 22). Australian energy software firm Energy One hit by cyberattack. *SecurityWeek*. https://www.securityweek.com/australian-energy-software-firm-energy-one-hit-by-cyberattack/

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, 8(6), artikkeli 898. https://doi.org/10.3390/app8060898

Kyberturvallisuuskeskus. (2022). *Palvelunestohyökkäykset ovat arkipäivää Suomessa*. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-ovat-arkipaivaa-suomessa

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. *Encyclopedia, 1*(3), 602-617. https://doi.org/10.3390/encyclopedia1030050

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet, 12*(9), artikkeli 157. https://doi.org/10.3390/fi12090157

Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks, 11*(6), artikkeli 101. https://doi.org/10.3390/risks11060101

Mehar, K. H., Anudeepak, K., Teja, K. R., Murali, K., Abbaye, Ch. A., & Ramu, R. R. (2022). Self-powered dual axis solar tracking system. Teoksessa S. Anban & A. Pandey (toim.), *Proceedings of the 2nd Indian International Conference on Industrial Engineering and Operations Management* (pp. 343-348). IEOM Society. https://ieomsociety.org/proceedings/2022india/143.pdf

Mubeen, S., Lisova, E., & Vulgarakis Feljan, A. (2020). Timing predictability and security in safety-critical industrial cyber-physical systems: A position paper. *Applied Sciences, 10*(9), artikkeli 3125. https://doi.org/10.3390/app10093125

Nankya, M., Chataut, R., & Akl, R. (2023). Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies. *Sensors, 23*(21), artikkeli 8840. https://doi.org/10.3390/s23218840

Perera, S.; Jin, X.; Maurushat, A.; Opoku, D.-G.J. Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. Informatics 2022, 9, 28. https://doi.org/10.3390/informatics9010028

Pochmara, J., & Świetlicka, A. (2023). Cybersecurity of industrial systems A 2023 report. *Electronics, 13*(7), artikkeli 1191. https://doi.org/10.3390/electronics13071191

Rahim, F. A., Ahmad, N. A., Magalingam, P., Jamil, N., Che Cob, Z., & Salahudin, L. (2023). Cybersecurity vulnerabilities in smart grids with solar photovoltaic: A threat modelling and risk assessment approach. *International Journal of Sustainable Construction Engineering and Technology*, 14(3), 210-220. https://doi.org/10.30880/ijscet.2023.14.03.018

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), artikkeli 7273. https://doi.org/10.3390/s23167273

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), artikkeli 13369. https://doi.org/10.3390/su151813369

Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2023). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences, 13*(1), artikkeli 395. https://doi.org/10.3390/app13010395

Teymouri, A., Mehrizi-Sani, A., & Liu, C. C. (2018). Cyber security risk assessment of solar PV units with reactivepower capability. *Proceedings: IECON 2018 -44th Annual*

Conference of the IEEE Industrial Electronics Society, 1(October), 2872–2877. https://doi.org/10.1109/IECON.2018.8591583