OULUN AMMATTIKORKEAKOULU

Eemeli Kyröläinen

VALAISTUKSEN OHJAUKSEN TIETOTURVALLISUUS

VALAISTUKSEN OHJAUKSEN TIETOTURVALLISUUS

Eemeli Kyröläinen
Opinnäytetyö
Syksy 2015
Tietototekniikan tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma, langattomat laitteet

Tekijä: Eemeli Kyröläinen
Opinnäytetyön nimi: Valaistuksen ohjauksen tietoturvallisuus
Työn ohjaajat: Ensio Sieppi, Ville Moilanen
Työn valmistumislukukausi ja -vuosi: Syksy 2015 Sivumäärä: 55 + 4 liitettä

Opinnäytetyön aiheena oli valaistuksen ohjauksen tietoturvallisuus ja työn tilaajana toimi Greenled Oy. Työn tavoitteina oli tutustua tietoturvallisuuden teoriaan ja valaistuksen ohjausta koskeviin tietoturvallisuuden osa-alueisiin, tehdä tietoturvakartoitus Greenled Oy:n valaistuksen ohjausjärjestelmälle ja luoda ohjausjärjestelmien tietoturvaohje yrityksen sisäiseen käyttöön.

Työn ensimmäisessä vaiheessa koottiin teoriatieto valaistuksen ohjauksesta, tietoturvallisuudesta ja valaistuksen ohjausjärjestelmiä koskevasta tietoturvallisuudesta. Teoriatiedon pohjalta luotiin erillinen tietoturvakartoitusdokumentti, jonka avulla kartoitettiin Greenled Oy:n valaistuksen ohjausjärjestelmän tietoturvallisuuden nykytila, tunnistettiin tietoturvauhkia sekä arvioitiin riskien suuruutta. Kartoituksen tulosten ja teoriatiedon pohjalta valittiin tarvittavat toimenpiteet riittävän tietoturvallisuuden tason saavuttamiseksi. Viimeisenä vaiheena luotiin ohjausjärjestelmien tietoturvaohjeistus.

Tietoturvakartoituksen tulosten avulla yritys sai selkeän kuvan ohjausjärjestelmän tietoturvallisuuden tämän hetkisestä tilanteesta. Työn tuloksiin sisältyi myös koonti tarvittavista toimenpiteistä tietoturvallisuuden kehittämiseksi sekä suunnitelma tietoturvallisuuden ylläpidosta. Ohjausjärjestelmän tietoturvallisuutta tullaan tarkastelemaan jatkossa säännöllisesti ja tietoturvaohjetta päivitetään tarkastelun tulosten perusteella.

Asiasanat: valaistus, ohjauslaitteet, tietoturva, kyberturvallisuus

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Technology, Wireless Devices

Author: Eemeli Kyröläinen
Title of thesis: Information security of lighting control
Supervisors: Ensio Sieppi, Ville Moilanen
Term and year when the thesis was submitted: Autumn 2015 Pages: 55 + 4 appendices

---

The subject of this thesis was information security of lighting control and the work was ordered by Greenled Ltd. The goals of this thesis was get to know theory of information security, explore information security of lighting control, make the information security survey on Greenled Ltd's lighting control system and create information security guideline for control systems on company's internal use.

The first phase of this work was compiled theoretical knowledge of lighting control, information security and information security of lighting control systems. Then information security survey was created on the basis of theoretical knowledge and with that was surveyed current state of Greenled Ltd's lighting control system. After that information security threats were identified and evaluated the risks. The necessary actions were selected on the basis of the survey's results and theoretical knowledge in order to achieve a sufficient level on information security. The last was created to information security guidelines for control systems.

From the results of information security survey the company obtained a clear vision from current state of the control system information security. On the results of this work was also included in the summary of the actions for the development of information security and plan for information security maintenance. The information security of lighting control systems will be reviewed in the future on a regular basis and the security guideline will be updated based on the results of the review.

Keywords: lighting, control systems, information security, cybersecurity

ALKULAUSE

Haluan kiittää Greenled Oy:tä tämän opinnäytetyön mahdollistamisesta. Idea opinnäytetyöni aiheesta syntyi keväällä ja kesällä 2015 yritykselle tekemieni valaistuksen ohjaukseen liittyvien projektien aikana. Tämä työ ei olisi toteutunut ilman Greenled Oy:n tarjoamia projektiaiheita ja tukea idean muuttamisesta opinnäytetyöksi.

Erityisesti haluan kiittää Greenled Oy:n Chief Technology Officer Ville Moilasta ja OAMK:n yliopettaja Ensio Sieppiä opinnäytetyöni ohjauksesta ja työn edetessä saamastani rakentavasta palautteesta.

Iso kiitos myös Juulialle kaikesta tuesta ja kannustuksesta kuluneen syksyn aikana.

Oulussa 28.12.2015

Eemeli Kyröläinen

SISÄLLYS

SANASTO

AES	Advanced Encryption Standard, tietotekniikassa käytettävä lohkosalausmenetelmä.
ANSI	American National Standards Institute, voittoa tavoittelematon yksityinen organisaatio, joka valvoo standardien kehittymistä Yhdysvalloissa.
APN	Access Point Name, mobiiliverkkojen ja julkisen Internetin välisen yhdyskäytävän nimi.
CIA	Confidentiality, Integrity and Availability, tietoturvallisuuden pääperiaatteet ovat luottamuksellisuus, eheys ja saatavuus.
DALI	Digital Addressable Lighting Interface, standardoitu digitaalinen valaistuksen ohjausväylä.
DMX512	Digital MultipleX, valaistustekniikassa käytettävä standardoitu digitaalinen sarjaliikenneprotokolla.
EnOcean	Erittäin vähän energiaa kuluttava langaton tiedonsiirtotekniikka, joka kerää käyttöenergiansa ympäristöstä.
HTTP	Hypertext Transfer Protocol, selaimien ja WWW-palvelimien käyttämä sovellustason tiedonsiirtoprotokolla.
HTTPS	Hypertext Transfer Protocol Secure, tiedon suojattuun siirtämiseen käytettävä HTTP-protokollan ja TLS/SSL-protokollan yhdistelmä
IEC	International Electrotechnical Commission, kansainvälinen sähköalan standardointiorganisaatio.
IEEE	Institute of Electrical and Electronics Engineers, kansainvälinen tekniikanalan järjestö, joka määrittelee monia alan keskeisiä standardeja.

IETF	The Internet Engineering Task Force, organisaatio, joka vastaa Internet protokollien standardoinnista.
IoT	Internet of Things- eli esineiden Internet -käsitteellä tarkoitetaan Internet-verkon laajentumista kaikkiin laitteisiin ja koneisiin.
IPv4	Internet Protocol version 4, RFC 791 -dokumentissa määritelty pakettikytkennäisen Internet-verkon tietoliikenneprotkolla, jonka tehtävänä on huolehtia tietoliikennepakettien toimittamisesta perille.
IPv6	Internet Protocol version 6, uusin RFC 1883 -dokumentissa määritelty versio pakettikytkennäisen Internet-verkon tietoliikenneprotkollasta. Version tärkein uudistus on osoitteiden pidennys.
ISM band	Industrial, Scientific and Medical Radio Bands, lupavapaa ja maailmanlaajuinen radiotaajuuskaista, joka on alun perin tarkoitettu teolliseen, tieteelliseen ja lääketieteelliseen käyttöön.
ISO	International Organization for Standardization, kansainvälinen standardoimisjärjestö.
LAN	Local Area Network, rajoitetulla alueella toimiva paikallinen tietoliikenneverkko.
LED	Light Emitting Diode, valoa säteilevä diodi.
LON	Local Operating Network, automaatiojärjestelmien ohjausprotokolla.
OSI-malli	Open Systems Interconnection Reference Model, seitsemänkerroksinen standardoitu kuvaus tiedonsiirtoprotokollien yhdistelmästä.
PIR	Passive Infrared sensor, infrapunavalon heijastumista mittaava elektroninen sensori, jota käytetään liikkeen ilmaisuun.
PLC	Powerline Communications, tiedonsiirtoprotokolla sähköverkossa tapahtuvaan tiedonsiirtoon.

PoE	Power over Ethernet on tekniikka, joka mahdollistaa käyttöjännitteen syöttämisen laitteille verkkokaapelin kautta.
SSL	Secure Sockets Layer, salausprotokolla tietoliikenteen salamiseen Internetissä. SSL on nykyään korvattu TLS-salauksella.
TLS	Transport Layer Security, salausprotokolla tietoliikenteen salaamiseen Internetissä.
UNB	Ultra Narrow Band, kapealla taajuuskaistalla toimiva tiedonsiirtotekniikka.
VAHTI	Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä, julkisen hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä sekä ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelin.
VPN	Virtual Private Network, virtuaalinen erillisverkko jonka avulla kaksi tai useampi verkko voidaan yhdistää suojatusti julkisen verkon yli.
ZigBee	IEEE 802.15.4 -standardin mukainen lyhyen kantaman langaton tietoliikenneverkko.
6loWPAN	IPv6 over Low Power Wireless Personal Area Networks, matalatehoinen lyhyen kantaman IPv6-protokollaa tukeva langaton tietoliikenneverkko.

1 JOHDANTO

Teknologian parissa eletään parhaillaan aikaa, jolloin käsitteet teollinen Internet ja esineiden ja asioiden Internet sekä lyhenteet IoT, IoE ja M2M ovat alan huomion keskipisteessä. Näille kaikille yhteistä on ajatus siitä että tulevaisuudessa yhä useampi laite on kytketty Internettiin ja että laitteet keskustelevat keskenään luoden älykkäitä kokonaisuuksia. Tällä hetkellä käsitteiden ympärillä käydään keskustelua muun muassa siitä, mitkä kaikki laitteet tulisi yhdistää verkkoon, mitä tietoliikenneprotokollaa tulisi käyttää ja kuinka kaikkea verkkoon kytketyistä laitteista kertyvää dataa voidaan hallita ja hyödyntää. Yhä nopeampi laitteiden verkottuminen tuo mukanaan myös omat tietoturvahaasteensa ja laitteita verkkoon kytkiessä tietoturvallisuuteen ei välttämättä kiinnitetä tarpeeksi huomiota.

Osana tätä laaja-alaista laitteiden verkottumista tietoliikenneverkot ja älykkäät laitteet ovat tulleet myös osaksi valaistuksen ohjausta. Nykyaikaisia valaistuksen ohjausjärjestelmiä voidaan ohjata etänä langattomien tai langallisten verkkoyhteyksien kautta. Langattomissa verkoissa ja julkisessa Internet-verkossa tapahtuva tiedonsiirto mahdollistaa tiedon salakuuntelun, kaappauksen ja väärentämisen. Myös verkon kautta toimivat käyttöliittymät ovat alttiita erilaisille hyökkäyksille ja väärinkäytölle.

Opinnäytetyön tavoitteena oli tutustua valaistuksen ohjauksen tietoturvallisuuteen, tehdä tietoturvakartoitus Greenled Oy:n valaistuksen ohjausjärjestelmälle, valita tarvittavat toimenpiteet ja luoda ohjausjärjestelmien tietoturvaohje yrityksen sisäiseen käyttöön.

Idea tämän opinnäytetyön aiheesta syntyi, kun työskentelin Greenled Oy:n ulkovalaistuksen ohjausjärjestelmän parissa ja huomasin, että valaistuksen ohjauksen tietoturvallisuudesta löytyy verrattain vähän julkaistua tietoa. Eri valmistajien järjestelmien esitteissä ja markkinoinnissa mainitaan usein niissä käytettyjä tietoturvatekniikoita, mutta yleensä kokonaiskuva tietoturvallisuudesta jää epäselväksi.

Tarkoituksena oli aloittaa työ tutustumalla tietoturvallisuuden teoriaan ja sitä määritteleviin lakeihin, standardeihin ja ohjeisiin. Teoriatiedossa oli tarkoitus huomioida tietoturvallisuuden keskeisimpiä käsitteitä sekä tutustua valaistuksen ohjausta koskeviin tietoturvallisuuden osa-alueisiin. Perimmäisenä tavoitteena oli tämän teoriatiedon pohjalta rakentaa tietoturvakartoitus, jonka avulla voitaisiin tarkistaa yrityksen tuotteiden tämänhetkinen tietoturvallisuuden taso. Tietoturvakartoituksen tulosten ja teoriatiedon perusteella tuli tehdä tarvittavat toimenpiteet sisältävä ohjeistus, jonka avulla voidaan saavuttaa riittävä tietoturvallisuuden taso yrityksen tuotevalikoimaan kuuluvissa valaistuksen ohjausjärjestelmissä. Tietoturvakartoituksesta, kartoituksen tuloksista ja tietoturvaohjeistuksesta sovittiin, että ne jätetään pois opinnäytetyön julkisesta osuudesta niiden sisältämien luottamuksellisten tietojen vuoksi. (1.)

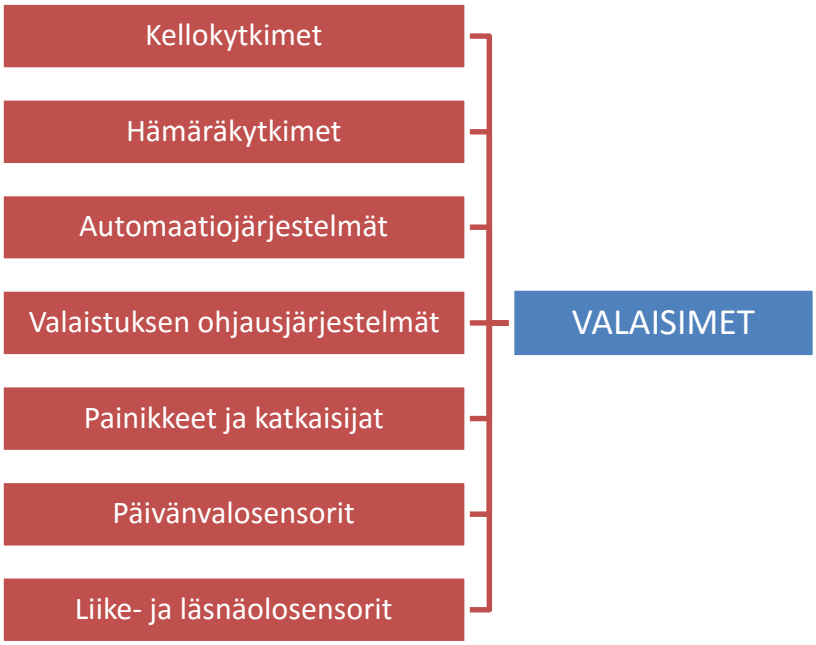
Työn tilaajana toimi Greenled Oy ja työ tehtiin syksyn 2015 aikana. Greenled Oy on kotimainen kokonaisvaltaisten LED-valaistusratkaisujen toimittaja ja valaisinvalmistaja. Yrityksen pääkonttori sekä tuotanto sijaitsevat Kempeleessä ja muut toimipisteet Tampereella ja Vantaalla. Yrityksen asiakkaille suunnittelemat ja toteuttamat kokonaisvaltaiset valaistusratkaisut sisältävät yhä useammin myös valaistuksen ohjauksen. Greenled Oy:n LED-valaisimet ovat Suomessa suunniteltuja ja valmistettuja. Tuotevalikoimasta löytyy valaistusratkaisuja niin toimisto-, varasto-, teollisuus- ja liiketiloihin kuin myös alue-, tie- ja katuvalaistukseen. Yritys työllistää tällä hetkellä noin 36 henkilöä. (2, linkki Yritys.)

2 VALAISTUKSEN OHJAUS

Valaistuksen ohjauksen tavoitteena on saada oikea määrä valoa oikeaan aikaan ja sinne, missä sitä tarvitaan. Näin vähennetään turhaa energian kulutusta ja varmistetaan valaistuksen tehokkuus myös tilanteiden mukaan muuttuvissa käyttöympäristöissä. Ohjauksen avulla halutaan myös parantaa viihtyvyyttä ja näkemisolosuhteita sekä korostaa tilojen ilmettä (3, linkki DALI_teoria_joulu2014, s. 7).

2.1 Määritelmä

Valaistuksen ohjauksella tarkoitetaan valaisimien ohjaamista kellonajan, liikkeen, ympäristön valoisuuden tai tilanteen perusteella. Ohjaus voi olla valaisimien kytkemistä päälle ja pois tai valaisimien valotehon himmentämistä. Valaisimia voidaan ohjata ryhmäkohtaisesti tai valaisinkohtaisesti usealla eri tavalla (kuva 1). Ohjaus voi olla yksinkertaisimmillaan toteutettu valaisimeen liitetyllä liikeilmaisimella tai hämäräkytkimellä, joka ohjaa releen avulla valaisimen käyttöjännitettä päälle ja pois. Vastaavasti valaistuksen ohjaus voi olla myös erilaisia sensoreita sisältävä älykäs kokonaisuus, jota hallinnoidaan tietokoneella toimivan käyttöliittymän kautta. (4, s. 59–61.)



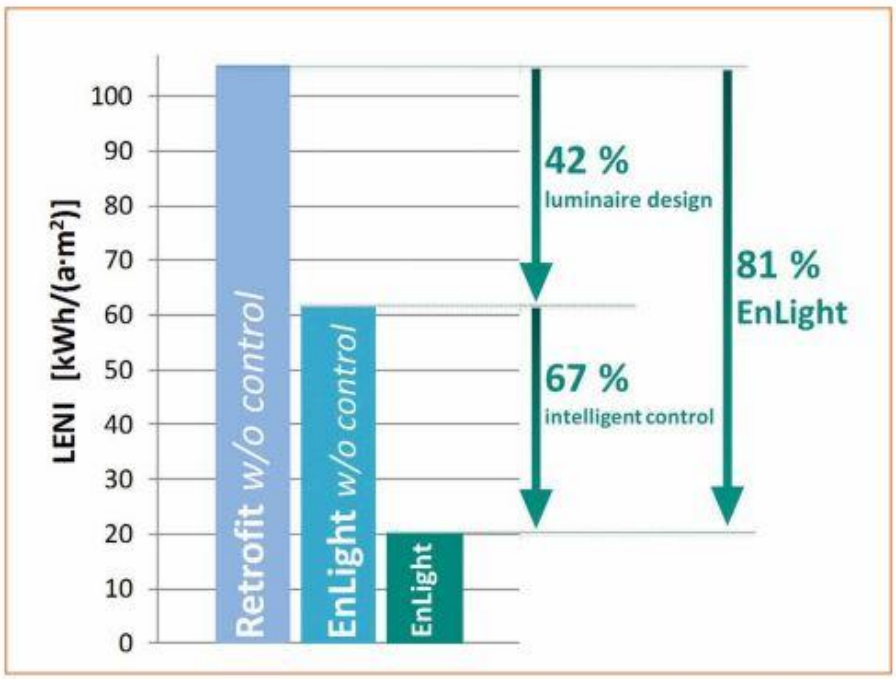
KUVA 1. Valaisimien ohjaustavat

Valaistuksen ohjaus voidaan jakaa käyttöympäristön perusteella kahteen osaan, jotka ovat sisävalaistus sekä ulkovalaistus. Suurin osa markkinoilla olevista järjestelmistä on suunniteltu käytettäväksi vain toisessa näistä käyttöympäristöistä, koska tarvittavat toiminnot ja valaistuksen tekninen rakenne ovat erillaisia.

2.2 Valaistuksen energiankulutus

Valaistuksen osuus maailman kokonaissähkönkulutuksesta on International Energy Agencyn mukaan noin 20 % (5). Tämän ja tiukentuneiden energiamääräysten johdosta valaisimien energian kulutukseen kiinnitetään yhä enemmän huomiota. Nykyaikaisilla LED-valaisimilla pystytään jo saavuttamaan huomattavat energiansäästöt halogeeni-, elohopeahöyry- ja suurpainenatriumlampuilla varustettuisiin valaisimiin nähden. EU-tasolla valaisimien energiankulutusta pyritään kaitsemaan myös direktiivien sekä asetusten kautta. Vuoden 2015 huhtikuun aikana muun muassa elohopeahöyrylamput poistettiin markkinoilta, koska ne eivät täytä vuonna 2009 asetettuja vaatimuksia. (6, s. 2.)

Energiatehokkaiden valaisimien lisäksi valaistuksen kuluttamaan kokonaisenergian määrään voidaan vaikuttaa huomattavasti myös valaistuksen ohjauksella. Esimerkiksi eurooppalaisen EnLight-tutkimusprojektin tuloksissa todettiin, että energiatehokkaiden LED-valaisimien ja älykkään valaistuksen ohjauksen yhdistelmällä voidaan saavuttaa jopa 45–70 %:n energiansäästöt (7). Yhdessä tutkimusprojektin demotiloista saavutettiin älykkäällä valaistuksen ohjauksella 67 %:n säästöt energian kulutuksessa verrattuna valaisimiin ilman ohjausta (kuva 2).



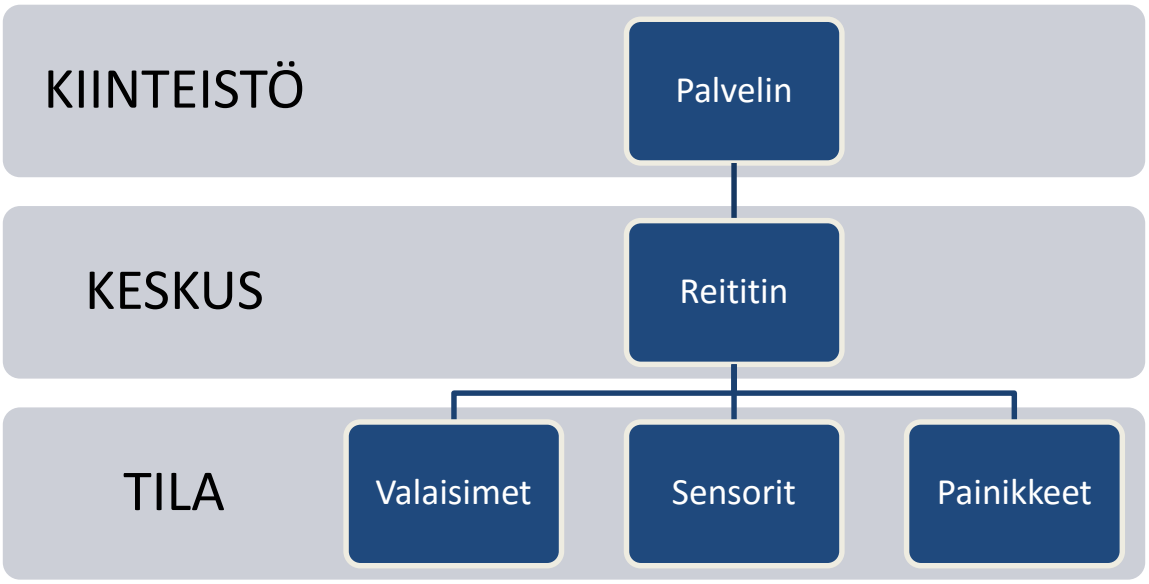
KUVA 2. EnLight-tutkimusprojektin tuloksia (8, s. 39.)

2.3 Sisävalaistuksen ohjaus

Sisävalaistuksen ohjauksella pyritään vähentämään valaistuksen energiankulutusta, mukauttamaan valaistusta tilanteiden mukaan ja parantamaan työtilojen valaistusolosuhteita. Mikäli tilojen käyttötarkoitus muuttuu, voidaan valaistuksen ohjausjärjestelmän avulla muuttaa myös tilan valaistus vastaamaan uutta käyttötarkoitusta. Sisävalaistuksen yhteydessä käytetään usein liike- ja läsnäolotunnistusta sekä valoisuuden mittausta, joiden avulla valaisimien energiankulutusta voidaan pienentää ohjaamalla tarvittava määrä valoa vain niihin tiloihin, joita käytetään, ja muuttamalla valaistuksen tasoa tiloihin sisälle tulevan luonnonvalon määrän perusteella. (9, s. 60–61.)

Sisävalaistuksen ohjausjärjestelmällä tarkoitetaan ohjattavista valaisimista, sensoreista, painikkeista, reitittimistä, palvelimesta ja käyttöliittymästä koostuvaa kokonaisuutta (kuva 3). Ohjausjärjestelmien tekniset rakenteet vaihtelevat valmistajakohtaisesti sekä asiakastarpeiden perusteella. Ohjausjärjestelmän avulla kiinteistön valaisimia voidaan ohjata päälle ja pois sekä himmentää ryhmäkohtaisesti tai valaisinkohtaisesti. Valaisinta voidaan ohjata, mikäli siinä käytetään

elektronista liitäntälaitetta, joka tukee valaisimen ohjausta esimerkiksi DALI- tai 0–10V-ohjausprotokollan avulla. (9, s. 60–61.)



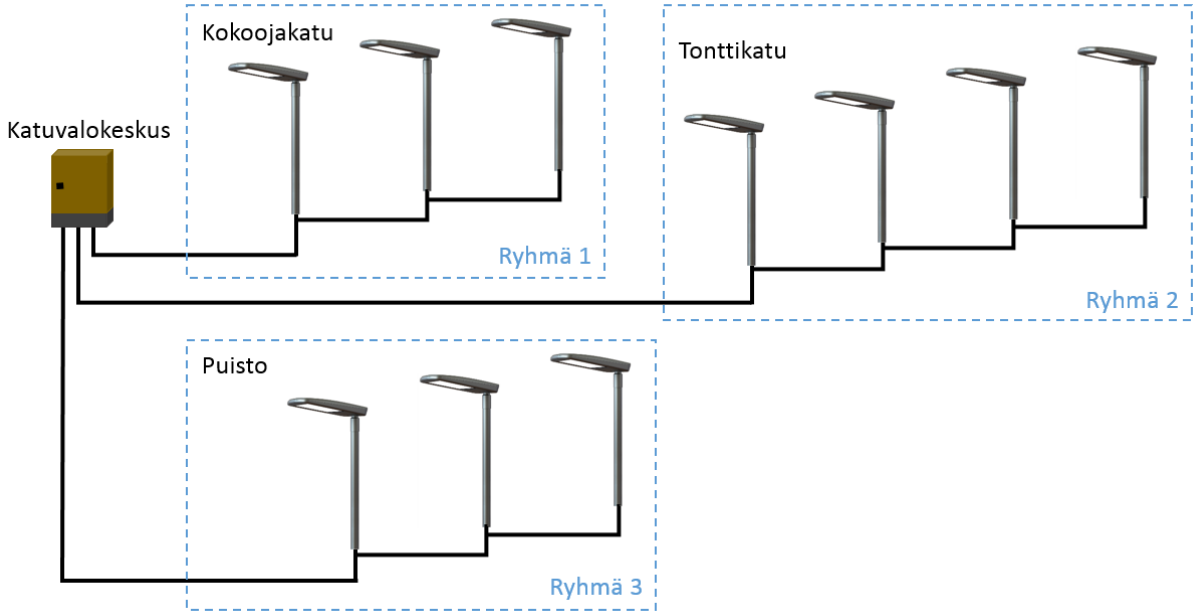
KUVA 3. Sisävalaistuksen ohjausjärjestelmän rakenne

2.4 Ulkovalaistuksen ohjaus

Ulkovalaistuksen ohjauksen yleisenä tavoitteena on pienentää valaistuksen energiankulutusta, lisätä turvallisuutta ja vähentää huolto- ja ylläpitokustannuksia. Viimeisten vuosien aikana valaistuksen ohjauksesta on tullut myös yhä houkuttelevampaa, koska markkinoille saapuneiden LED-valaisimien ohjaaminen on entistä helpompaa niiden elektronisen rakenteen vuoksi. Maailmanlaajuisesti on myös alettu kiinnittämään huomiota valaistuksen energian kulutukseen ja hiilidioksidipäästöihin. Ulkovalaistuksen ohjauksella pyritään vähentämään valaistuksen vianetsintä-, huolto- ja ylläpitokustannuksia keskitetyn hallinnan ja järjestelmistä saatavien raporttien sekä ilmoitusten avulla. Ohjauksella mahdollistetaan myös valaistustason mukauttaminen erilaisiin tilanteisiin ja käyttöolosuhteisiin sopivammaksi. Yhä useammin esille nousee myös tarve ohjata valaistusta ihmisten liikkeiden, liikennemäärien, sääolosuhteiden ja ympäristön valoisuuden perusteella. (10.)

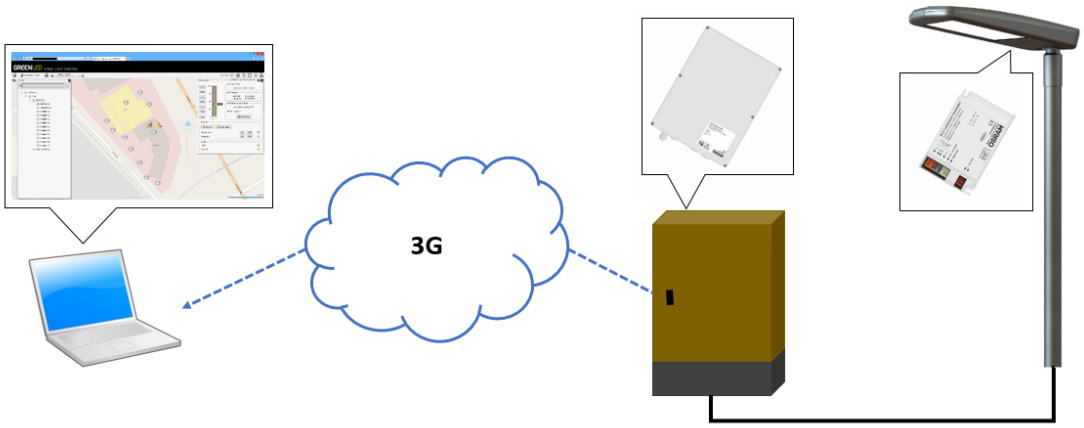
Vähitellen ulko- ja katuvalaistuksen ohjaus on löytänyt paikkansa myös Suomessa käytettävistä suunnitteluohjeista. Tästä hyvänä esimerkkinä toimii keväällä 2015 julkaistu Liikenneviraston Maantie- ja rautatiealueiden valaistuksen suunnittelu -ohje, jossa valaistuksen ohjaukseen kiinnitetään aikaisempaa enemmän huomiota. Ohje sisältää menetelmiä ja keinoja tievalaistuksen ajoittaiseen vähentämiseen. Valaistusta voidaan himmentää valaistusluokkien mukaisesti ja himmennys tulee ajoittaa ajankohtiin, jolloin tuntiliikennemäärät alittavat määritellyt tasot. (11, s. 14–20.)

Ulkovalaistuksen ohjausjärjestelmät voidaan jakaa kahteen ryhmään niiden ohjaustavan perusteella: perinteiset ryhmäkohtaiset ohjausjärjestelmät ja enemmissä määrin yleistyvät valaisinkohtaiset ohjausjärjestelmät. Valaistuksen ryhmäkohtaisella ohjauksella tarkoitetaan järjestelmää, jonka avulla valaisinryhmiä voidaan ohjata ja monitoroida valaisinkeskuksien kautta (kuva 4). Ohjainlaite asennetaan valaisinkeskukseen ja järjestelmän hallinta tapahtuu erillisen ohjelmiston tai käyttöliittymän kautta. Valaisinkeskukseen asennettava ohjainlaite sisältää yleensä omat ohjausreleet eri valaisinryhmien sähkösyötön päälle ja pois ohjaukseen. Ohjainlaite on yhdistetty järjestelmän palvelimeen tai suoraan hallintaohjelmistoon langallisen tai langattoman verkkoyhteyden kautta. Ohjainlaitteeseen voidaan usein myös yhdistää energiamittari, jonka avulla valaisinryhmien energiankulutusta voidaan seurata järjestelmän etäkäyttöliittymän kautta. (10, s. 41–42.)



KUVA 4. Valaisimien ryhmäkohtainen ohjaus

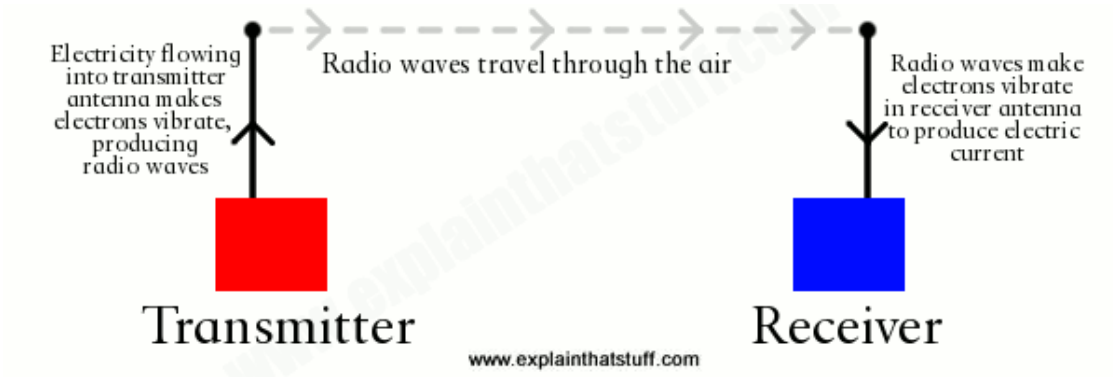
Valaisinkohtaisella ohjauksella tarkoitetaan järjestelmää, jossa yksittäisiä valaisimia voidaan ohjata ja monitoroida jokaista erikseen (kuva 5). Jokainen valaisin sisältää ohjattavan liitäntälaitteen ja ohjainyksikön. Ohjainyksikkö liikennöi langattoman tai langallisen tietoliikenneyhteyden kautta valaisinkeskukseen sijoitetun keskittimen kanssa. Keskitin taas liikennöi järjestelmän palvelimen tai suoraan hallintaohjelmiston kanssa langattoman tai langallisen verkkoyhteyden kautta. Kaikissa järjestelmissä ei välttämättä ole keskitintä ollenkaan, vaan valaisimien ohjainyksiköt keskustelevat suoraan järjestelmän palvelimen tai hallintaohjelmiston kanssa langattoman verkkoyhteyden kautta. (10, s. 41–42.)



KUVA 5. Valaisinkohtainen ohjaus

2.5 Langattomat ohjaustekniikat

Langattomassa tiedonsiirrossa signaali kulkee radioaaltojen välityksellä ilmateitse lähettäjältä vastaanottajalle (kuva 6). Valaistuksen ohjausjärjestelmien langattomassa tiedonsiirrossa käytetään useita erilaisia tiedonsiirtotekniikoita ja -protokollia. Useimmiten käytetty tekniikka on ZigBee, mutta eri valmistajien kesken ei ole yhtenäistä linjaa käytettävästä tekniikasta. Tästä johtuen onkin usein vaikea valita ohjausjärjestelmää, jonka hankkiminen ei sido asiakasta vain yhden valmistajan tuotteisiin.



KUVA 6. Langaton tiedonsiirto (12.)

ZigBee

ZigBeellä tarkoitetaan avoimen ja ei-kaupallisen ZigBee-allianssin luomaa tietoliikennestandardia, joka on tarkoitettu vähävirtaisten ja lyhyen kantaman tietoliikenneverkkojen luomiseen. Pohjan ZigBeelle rakentaa IEEE 802.15.4 -standardi, joka määrittelee tietoliikenneverkolle OSI-mallin fyysisen kerroksen ja siirtoyhteyskerroksen. ZigBee-allianssin standardi määrittelee yhteyden verkkoyhteys- ja kuljetuskerrokset. (13.) Tästä ylemmät OSI-mallin kerrokset jäävät ZigBee-standardissa teknologiaa käyttävien yritysten määriteltäviksi. Tämä on johtanut tilanteeseen, jossa suurimmalla osalla valmistajista on omat sovelluskerroksensa ZigBee-standardin päällä ja tästä johtuen eri valmistajien laitteet eivät ole yhteensopivia keskenään.

6LoWPAN

6LoWPAN on vähävirtainen MESH-tietoliikenneverkko, jossa jokaisella laitteella on oma IPv6-osoitteensa ja ne voivat keskustella suoraan Internettiin perinteisten tietoliikenneprotokollien välityksellä. 6LoWPAN-tietoliikenneverkko pohjautuu IEEE 802.15.4 -standardiin OSI-mallin fyysisien kerroksen ja siirtoyhteyskerroksen osalta (14). Loppuosa verkosta perustuu avoimiin standardeihin, jotka on määritelty IETF:n RFC 6282 -dokumentissa (15).

EnOcean

EnOcean on teknologia, joka mahdollistaa erittäin vähän energiaa kuluttavien langatonta tiedonsiirtoa käyttävien tuotteiden luomisen. Teknologiassa käytettävä tiedonsiirto rakentuu ISO/IEC 14543-3-10 -standardin ja EnOcean-allianssin luoman sovelluskerroksen pohjalle. ISO/IEC 14543-3-10 -standardi kattaa OSI-mallin fyysisen, siirto- ja verkkokerroksen. Teknologialla toteutetuissa laitteissa käytetään hyväksi ympäristöstä ja liikkeestä kerättävää energiaa. Tarkoituksena on, että järjestelmän laitteet tuottavat itse tiedonsiirtoon tarvittavan energian, ja näin ollen erillisille virtalähteille tai akuille ei ole tarvetta. (16; 17.)

Ultra Narrow Band

UNB on langaton tiedonsiirtotekniikka, joka mahdollistaa tiedonsiirrolle pitkän kantaman pienellä energian kulutuksella (19). Tekniikassa käytetään alle 1 GHz:n taajuusalueella kapeaa taajuuskaistaa. Käytettävät taajuudet ovat yleensä

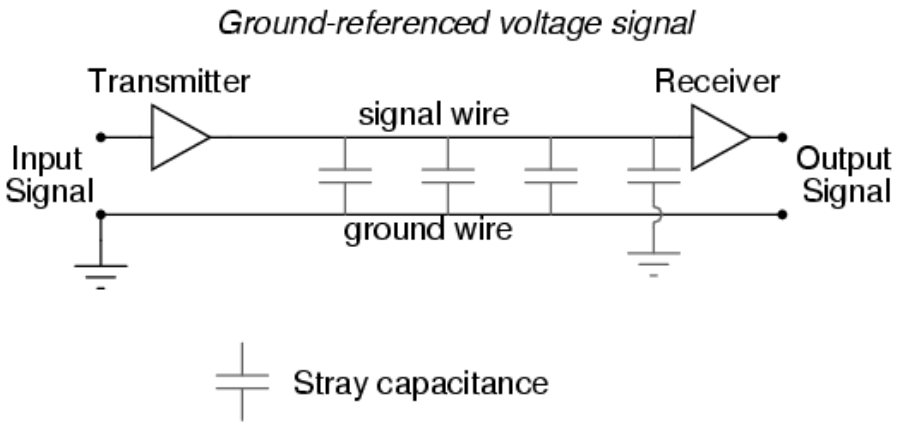
lisenssivapaita taajuuskaistoja eli niin sanottuja ISM-taajuuksia. Euroopassa suosituin ISM-taajuuskaista on 868 MHz ja Yhdysvalloissa vastaavasti 902 MHz (18). Tekniikan etuja ovat pitkät kantomatkat, edulliset komponentit ja pieni energiankulutus. Heikkouksiin kuuluu pieni tiedonsiirtonopeus. (18; 19.)

Mobiiliverkot

Valaistuksen ohjausjärjestelmien tiedonsiirrossa voidaan käyttää olemassa olevia 2G-, 3G- ja 4G-matkapuhelinverkkoja. Tiedonsiirrossa käytettävä taajuusalue ja tiedonsiirtonopeus vaihtelevat käytettävän tekniikan mukaan. Esimerkiksi 2G-verkoissa voidaan käyttää GPRS- ja EDGE-tekniikkaa, joilla tiedonsiirron nopeus liikkuu teoriassa 114 kbit/s:n ja 473,6 kbit/s:n välillä. 3G-verkossa tiedonsiirron nopeus vaihtelee 384 kbit/s:n ja 41 Mbit/s:n välillä. Käyttämällä tiedonsiirrossa matkapuhelinverkkoja on mahdollista rakentaa valaistuksen ohjausjärjestelmä ilman erillisiä keskittimiä. Tällaisessa tapauksessa valaisinkohtaiset ohjaimet keskustelevat suoraan matkapuhelinverkkojen datayhteydellä järjestelmän palvelimen kanssa. (20.)

2.6 Langalliset ohjaustekniikat

Langallisessa tiedonsiirrossa signaali kulkee fyysistä siirtotietä pitkin lähettäjältä vastaanottajalle (kuva 7). Valaistuksen ohjausjärjestelmien langallisessa tiedonsiirrossa voidaan käyttää useita erilaisia tiedonsiirtotekniikoita ja -protokollia. Käytettävä tekniikka tai protokolla voidaan valita esimerkiksi käyttökohteen, laitteiden ominaisuuksien tai kustannusten perusteella.



KUVA 7. Langallinen tiedonsiirto (21.)

DALI

Digital Addressable Lighting Interface on maailmanlaajuinen standardi, joka on luotu valaistuksen ohjausta varten. DALI-protokolla määritellään IEC 62386 -standardissa. DALI-järjestelmä voi koostua liitäntä- ja ohjauslaitteista, tuloista sekä virtalähteistä. Yhteen DALI-väylään voi kuulua maksimissaan 64 laitetta, väylä voi olla maksimissaan 300 m pitkä ja väylän maksimi virrankulutus on 250 mA. Tiedonsiirto tapahtuu 2-johtimisella kaapelille, jossa kulkee noin 16 V:n polariteettivapaa signaali. (22.)

PLC

Power Line Communication tekniikka mahdollistaa tiedonsiirron olemassa olevien sähkökaapeleiden kautta. Tiedonsiirto voidaan toteuttaa usean erilaisen protokollan avulla. Tunnetuimpia käyttökohteita tekniikalle ovat etäluettavat sähkömittarit. Euroopassa PLC-tiedonsiirtoon on varattu neljä eri taajuusaluetta, joilla jokaisella on määritelty omat vaatimuksensa. Energiayhtiöiden käyttöön on varattu taajuusalue 3–95 kHz ja kaupalliseen käyttöön taajuusalueet 95–125 kHz, 125–140 kHz ja 140–148,5 kHz. (23.)

KNX

KNX-standardi on luotu kiinteistöautomaatiota varten ja sen tekniset ominaisuudet on määritelty EN 50090- ja ISO/IEC 14543-3 -standardeissa. KNX on luotu European Home Systems Protocol- , BatiBUS- ja European Installation Bus-standardien pohjalta ja se määrittelee tiedonsiirrolle kaikki OSI-mallin kerrokset. Tiedonsiirto KNX-standardissa perustuu väylätekniikkaan, jossa väylään liitetyt laitteet ja anturit kommunikoivat keskenään. (24.)

DMX

DMX512-valaistuksenohjausstandardi on luotu pääsääntöisesti efekti-, lavaste- ja esitysvalaistuksen ohjaukseen. Ohjaustavan tekniset ominaisuudet ovat määritelty alun perin USITT DMX512/1990 -standardissa ja myöhemmin ANSI E1.11 - 2008 (R2013) -standardissa. DMX512 on sarjaliikennemuotoinen digitaalinen tiedonsiirtoprotokolla. Protokollassa laitteiden ohjaus tapahtuu 8-bittisten kanavien kautta, joita voi olla yhteensä 512 kappaletta. (25.)

LON

LonWorks on avoin tiedonsiirtotekniikka, joka on luotu erilaisten laitteiden ohjaamista varten. Alkuperäisen protokollan on luonut amerikkalainen Echelon Corporation automaatiolaitteita varten. Ohjaustekniikan tiedonsiirtoprotokolla, signalointi parikaapelissa, Power line communication -signalointi ja IP-yhteensopivuus on standardoitu vuonna 2008 standardeissa ISO/IEC 14908-1, -2, -3, and -4. LonWorks-standardi ottaa huomioon tiedonsiirron kaikki seitsemän OSI-mallin mukaista kerrosta. (26; 27.)

PoE

Power over Ethernet -tekniikan avulla voidaan tarjota verkotetuille laitteille tasajännitettä normaalia tietoliikennekaapelointia pitkin. PoE-tekniikka on määritelty IEEE 802.3 -standardissa, jossa kuvataan, kuinka tasajännitettä voidaan kuljettaa verkkokytkimeltä verkkokaapelia pitkin laitteille. Alkuperäinen IEEE 802.3af-2003 -standardi määritteli laitteiden maksimi tehonkulutukseksi 15,4 W. Standardin tuorein, vielä julkaisematon, IEEE 802.3bt -versio mahdollistaa jopa 90 W:n tehoa tarvitsevien laitteiden käyttämisen 50-57 V:n tasajännitteellä. (28.)

0/1–10V

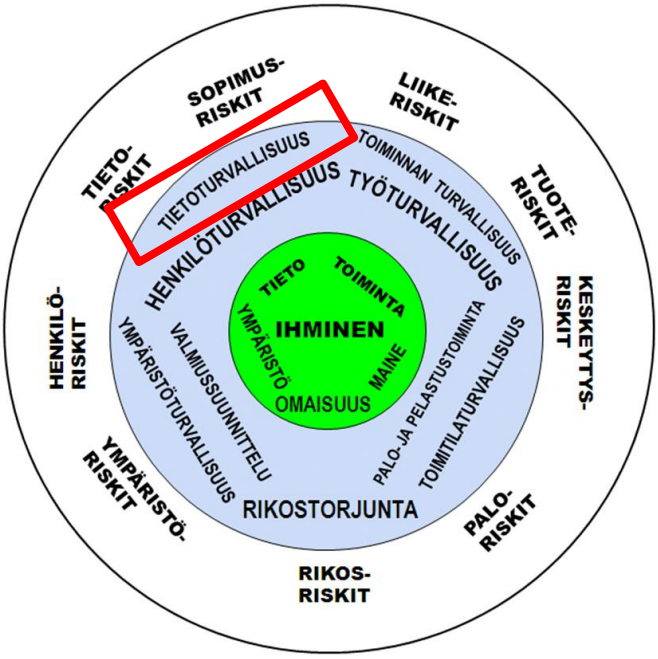
0/1–10V -tekniikka perustuu analogiseen jännitesignaaliin, jonka jännitetasoa muuttamalla voidaan ohjata laitteita tai ilmoittaa esimerkiksi sensorin antama arvo. Ohjaussignaalilla voidaan esimerkiksi ohjata valaisimien liitäntälaitteita valaistutason himmentämiseksi. Ohjaustekniikassa ohjattavalle laitteelle syötetään kahden johtimen kautta tasajännitettä, jonka jännitetaso kertoo esimerkiksi himmennyksen asteen. Jännitetaso 0/1 V vastaa yleensä minimivalotehotasoa ja jännitetaso 10 V maksimivalotehotasoa. (29.)

3 TIETOTURVALLISUUS

”Tietoturva ei ole projekti vaan prosessi” (30, s. 241).

Kyseinen ajatuslause toistuu hyvin usein tietoturvallisuutta käsittelevissä kirjoissa ja artikkeleissa. Lause kuvaa ytimekkäästi sen, mistä tietoturvassa pohjimmiltaan on kyse. Tietoturvallisuuden huomioimisesta on todellista hyötyä vain, kun sitä ajatellaan yhtäjaksoisena prosessina, jota ajetaan ja kehitetään koko ajan eteenpäin. Mikäli tietoturvallisuus ajatellaan vain projektina, joka alkaa ja loppuu, menettävät tehdyt toimenpiteet merkityksensä, kun yhä uusia tietoturvahaavoittuvuuksia ja -uhkia ilmenee.

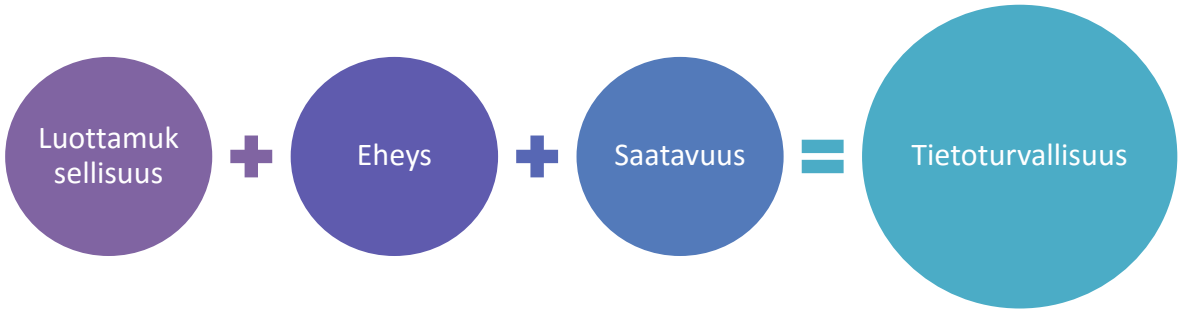
Tietoturvallisuudesta puhuttaessa usein esille nousevat termit hakkeri, tietokonevirus, salasanat ja varmuuskopiointi. Kaikki nämä asiat liittyvät kyllä tietoturvallisuuteen, mutta käsite tietoturva on todellisuudessa paljon laajempi. Tietoturva käsitetään usein myös omaksi erilliseksi aihekokonaisuudeksi, mutta todellisuudessa tietoturvallisuus on vain yksi osa-alue turvallisuuden kokonaiskuvasta (kuva 8). Tämä kokonaiskuva sisältää hyvin laaja-alaisesti yrityksessä tai organisaatiossa huomioon otettavat turvallisuuden osa-alueet.



KUVA 8. Tietoturvallisuus on yksi osa-alue turvallisuudesta (31, s. 7)

3.1 Tietoturvallisuuden määritelmä

Tietoturvallisuudella tarkoitetaan tietojärjestelmissä käsiteltävien tietojen suojaamista siten, että voidaan varmistaa tiedon luottamuksellisuus, eheys ja saatavuus (kuva 9). Näiden termien yhteydessä käytetään lyhennettä CIA, jolla tarkoitetaan englannin kielen sanoja confidentiality, integrity ja availability. Nämä kolme asiaa toimivat tietoturvallisuuden keskeisimpinä tavoitteina, mutta näiden lisäksi tulee huomioida kiistämättömyys, käyttäjän tunnistus ja todennus. (32, s. 22.)



KUVA 9. Tietoturvallisuuden osatekijät

Luottamuksellisuus

Luottamuksellisuudella (confidentiality) tarkoitetaan tietoturvallisuudessa sitä, että tietoa pääsevät katselemaan ja käsittelemään vain ne henkilöt, joilla on siihen oikeus. Keinoja tiedon luottamuksellisuuden ylläpitämiseen ovat käyttäjän todennus ja tiedon salaus. (32, s. 22.)

Eheys

Tietoturvallisuudessa eheydellä (integrity) tarkoitetaan sitä, että tiedon muuttuminen vahingossa tai tahallaan ei saa jäädä huomaamatta. Tietojen eheyden säilyminen voidaan varmistaa esimerkiksi käyttämällä tarkistussummia, keräämällä lokitiedostoja ja ajamalla sisäisiä tarkistuksia. (32, s. 22–23.)

Saatavuus

Tietoturvallisuudessa saatavuudella (availability) tarkoitetaan sitä, että tarvittava tieto on käyttäjän saatavilla silloin, kun hän sitä tarvitsee. Käytännössä termillä

tarkoitetaan sitä, että verkkoyhteyksien, tietokoneiden ja tietojärjestelmien toiminta täytyy turvata kaikissa tilanteissa. Yksi saatavuuden osa-alueista on tiedostojen varmuuskopiointi, jolla taataan, että tieto on saatavilla tai palautettavissa myös laiterikkojen ja muiden ongelmien jälkeen. (32, s. 24.)

Kiistämättömyys, tunnistus ja todennus

Saatavuuden, luottamuksellisuuden ja eheyden lisäksi tietoturvallisuudessa tulee kiinnittää huomiota tiedon kiistämättömyyteen sekä käyttäjän tunnistukseen ja todennukseen.

Kiistämättömyydellä tarkoitetaan sitä, että tiedon käyttäjät ja heidän tekemänsä muutokset pystytään todistamaan esimerkiksi erilisten lokitiedostojen avulla. Tapahtumien kiistämättömyys voidaan varmistaa tietojen eheyden ja käyttäjän todennuksen avulla sekä varustamalla tapahtumat aikaleimalla. (32, s. 27–28.)

Käyttäjän tunnistuksella tarkoitetaan sitä, että tietojärjestelmän käyttäjä voidaan tunnistaa esimerkiksi käyttäjätunnuksen perusteella. Tietojärjestelmän käyttäjä voi olla henkilö, organisaatio tai laite. (32, s. 24–27.)

Käyttäjän todennuksella tarkoitetaan menetelmää, jonka avulla tietojärjestelmän käyttäjä voidaan todentaa luotettavasti käyttöoikeuden omaavaksi käyttäjäksi. Käyttäjän todennus voidaan tehdä esimerkiksi salasanan, sirukortin tai biotunnisteen avulla. (32, s. 24–27).

3.2 Tietoturvaohjeet ja -käytännöt

Tietoturvallisuus mielletään hyvin usein vahvasti tekniikkaan liittyväksi asiaksi, mutta todellisuudessa tietoturvallisuus liittyy suurimmilta osin ihmisten käyttäytymiseen. Tästä johtuen usein yritysten todelliset käytännöt ovat ristiriidassa tietoturvaohjeiden kanssa. Yrityksen tietoturvaohjeiden ja käytäntöjen tulisi ennen kaikkea olla sellaisia, että työntekijät noudattaisivat niitä, koska muuten parhaimmalla mahdollisellakaan menetelmällä ei ole mitään merkitystä. Ohjeiden ja käytäntöjen tulisi olla tavoiteltavaan turvallisuuden tasoon riittäviä, mutta ei ylimitoitettuja. Yksi ohjeiden ja käytäntöjen noudattamiseen vaikuttava tekijä on luottamuksen ilmapiiri, sillä mikäli yrityksen ilmapiiri on pahoin tulehtunut, houkuttelee se helposti rikkomaan yhteisiä sääntöjä. Myös vain ulkoisiin uhkiin keskittyminen

voi aiheuttaa sen, että kokonaiskuva huomioon otettavista asioista jää näkemättä. Hankkimalla palomuureja ja torjuntaohjelmia voidaan hyvin ehkäistä ulkoisia uhkia, mutta mikäli näitä laitteita ja ohjelmistoja ei tunneta tarpeeksi hyvin, voidaan niillä aiheuttaa myös uusia uhkia. Työntekijät tuntevat usein todella hyvin käytössä olevat turvajärjestelmät ja osaavatkin näin ollen myös parhaiten kiertää ne. (32, s. 122–125.)

3.3 Kyberturvallisuus

Termillä kyberturvallisuus tarkoitetaan kyberympäristön suojaamista sitä koskevilta uhkilta ja sen toiminnan varmistamista. Kyberympäristöllä tarkoitetaan eri tietojärjestelmistä koostuvaa sähköisessä muodossa olevaa tiedon käsittelyyn tarkoitettua ympäristöä. (33.)

Kyberturvallisuus nousee yhä useammin esille keskusteltaessa tietoturvallisuudesta yritysmaailmassa, koska nykyään yritysten käyttämät tietojärjestelmät ja alustat eivät ole enää vain yritysten omissa verkoissa ja omien työntekijöiden hallinnassa. ICT-palveluita ja tietojärjestelmiä pyritään yhä useammin ulkoistamaan, sekä siirtämään erilaisiin pilvipalveluihin. Samanaikaisesti myös laitteiden verkottuminen tuo mukanaan uusia haasteita yritysten toimintaympäristöön.

3.4 Tietoturvallisuuden osa-alueet

Tietoturvallisuus koskettaa hyvin laaja-alaisesti monia osa-alueita yrityksestä tai organisaatiosta. Tämän vuoksi tietoturvallisuus jaotellaan usein yhdestä kokonaisuudesta erikseen tarkasteltaviin osa-alueisiin. Perinteisesti käytetään jaottelua kahdeksaan osa-alueeseen, jotka ovat

1. hallinnollinen turvallisuus
2. fyysinen turvallisuus
3. henkilöstöturvalisuus
4. tietoliikenneturvallisuus
5. ohjelmistoturvallisuus
6. tietoaineistoturvallisuus
7. käyttöturvallisuus
8. laitteistoturvallisuus (30, s. 52).

Näistä osa-alueista valaistuksen ohjauksen tietoturvallisuuden tarkastelun kannalta tärkeimmät ovat tietoliikenneturvallisuus, tietoaineistoturvallisuus, laitteistoturvallisuus ja käyttöturvallisuus.

3.4.1 Tietoliikenneturvallisuus

Tietoliikenne on erittäin kriittinen osa nykyaikaisten tietojärjestelmien sekä verkkopalvelujen toimintaa ja tämän vuoksi tietoliikenneturvallisuuden tavoitteita ovat tiedonsiirron turvaaminen ja toimivuuden sekä luotettavuuden varmistaminen kaikissa tilanteissa. Tietoliikenneturvallisuuteen liittyviä osa-alueita ovat tiedonsiirtoyhteyksien käytettävyys, tiedonsiirron turvaaminen, käyttäjien tunnistaminen, tietoliikenteen suojaaminen ja salaaminen. (30, s. 69–76; 34.)

3.4.2 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuden tarkoituksena on turvata asiakirjojen, tiedostojen ja tietokantojen luottamuksellisuus ja estää näissä olevien tietojen tahallinen ja vahingossa tapahtuva tuhoaminen tai muokkaaminen. Olennainen osa tietoaineistoturvallisuutta on tiedon jatkuva varmistaminen, tallenteiden asianmukainen säilyttäminen ja aineiston tietoturvallinen hävittäminen. Yksi esimerkki tietoaineiston turvaamisesta on tietojen luokittelu turvaluokkiin niiden tärkeyden perusteella. Käytettävät turvaluokat voivat olla esimerkiksi julkiset, salaiset ja erittäin salaiset tiedot. (35.)

3.4.3 Laitteistoturvallisuus

Laitteistoturvallisuuden avulla pyritään suojaamaan tekniset laitteet ja laitteistot koko niiden elinkaaren ajan. Suojaaminen kattaa kaikki eri vaiheet aina asennuksesta ylläpitoon ja poistamiseen asti, sekä näihin vaiheisiin kuuluvan hallinnoinnin. Huomioon otettavia asioita laitteistoturvallisuudessa ovat muun muassa laitteiden takuut, ylläpitosopimukset, tukipalvelut, varaosien saatavuus, täydelliset varmuuskopiot, laitteiden valvonta, järjestelmien tietoturvapäivitykset ja ohjeet. (36.)

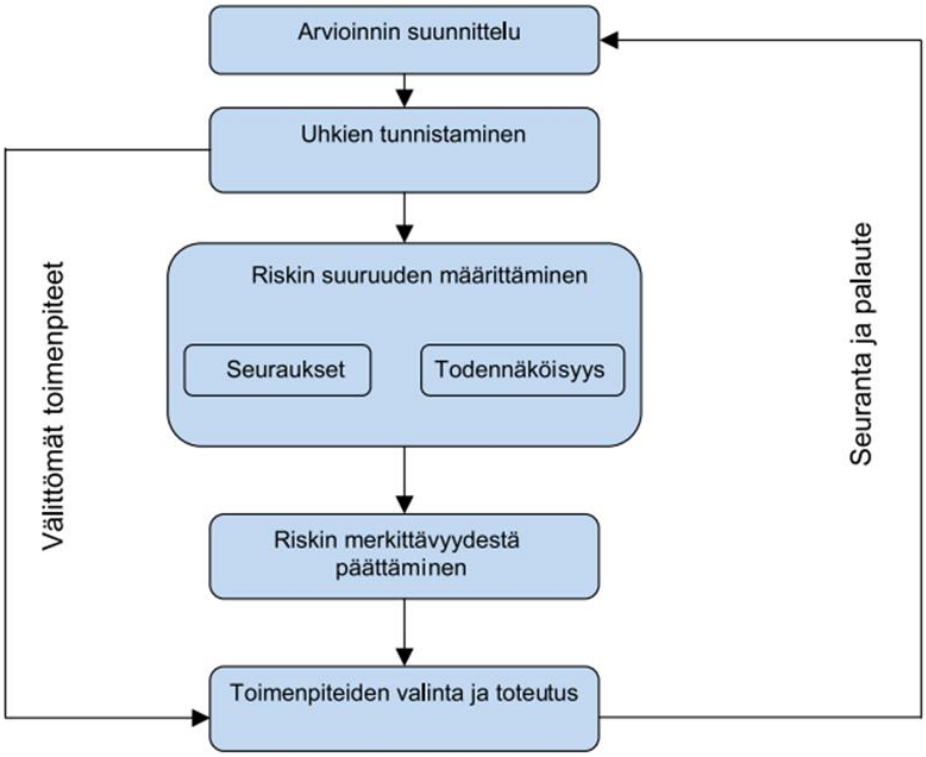
3.4.4 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan muun muassa salasanojen hallintaa ja järjestelmien valvontaa. Käyttöturvallisuudessa tulee ottaa huomioon myös IT-palveluiden ulkoistaminen, etätyö ja -käyttö, muutosten hallinta ja varautuminen poikkeusoloihin. Tavoitteena on pitää tietoturvallisuuden taso riittävänä päivittäisessä toiminnassa. Tärkeä osa käyttöturvallisuutta on myös suojata tietojärjestelmät haittaohjelmilta esimerkiksi virustorjuntaohjelmistolla. (37.)

3.5 Riskien arviointi

Riskien arviointi on tärkeä osa tietoturvallisuutta edistävien ratkaisujen ja toimenpiteiden valintaa. Arvioinnin avulla voidaan varmistaa että käyttöönotettavat ratkaisut ja toimenpiteet ovat yritykselle tai organisaatiolle tarkoituksenmukaisia ja taloudellisesti järkeviä. (38, s. 10.)

Riskien arvioinnilla tarkoitetaan jatkuvaa prosessia (kuva 10), jossa yrityksen tai organisaation toimintaan liittyvät uhkat pyritään tunnistamaan ja arvioimaan uhkien todennäköisyyttä sekä niistä mahdollisesti aiheutuvien seurauksien suuruutta. Tämän arvioinnin perusteella määritetään riskien suuruus ja päätetään niiden merkittävyys. Prosessin viimeisessä vaiheessa riskien arvioinnin tulosten perusteella valitaan tarvittavat toimenpiteet ja toteutetaan ne. (38, s. 15–18.)



KUVA 10. Riskien arvioinnin vaiheet (38, s. 16)

Riskien arvioinnin prosessissa käytetyllä termillä uhka tarkoitetaan mahdollisesti toteutuvaa haitallista tapahtumaa. Uhan aiheuttaja voi olla esimerkiksi rikollinen, työntekijä, alihankkija, tavarantoimittaja, vierailija tai luonnonilmiö. Termillä riski tarkoitetaan kokonaisuutta, joka rakentuu uhan todennäköisyydestä ja siihen liittyvän vahingon taloudellisesta arvosta. Uhkien tunnistamisen kannalta oleellista on ymmärtää mitkä ovat yrityksen tai organisaation suojattavia kohteita. Suojattaviin kohteisiin voidaan lukea kaikki ne kohteet, joita täytyy suojata uhkilta. Suojattavat kohteet jaotellaan yleensä kolmeen luokkaan:

- fyysiset kohteet
- loogiset kohteet
- ihmisiin liittyvät kohteet (39, s. 40).

3.6 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan yrityksen tai organisaation moniosaista prosessia, jonka avulla pyritään jatkuvasti parantamaan tietoturvallisuuden tasoa. Hallintajärjestelmää käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan yhä uudelleen ja uudelleen. Yleisesti järjestelmän katsotaan sisältävän organisaatiorakenteen, organisaation politiikat, suunnittelutoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit ja resurssit. (31; 40, s. 8.)

3.7 Sertifiointi ja auditointi

Yritysten ja organisaatioiden on mahdollista sertifioida ISO/IEC 27001-standardin vaatimusten perusteella käyttämänsä tietoturvallisuuden hallintajärjestelmä. Tämän sertifioinnin avulla yritys voi osoittaa, että pystyy hallitsemaan tietoturvallisuuteen liittyviä riskejä ja kykenee tunnistamaan tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat uhkat. (41.)

Tietoturva-auditoinnilla tarkoitetaan yrityksen tai organisaation tietoturvallisuuteen liittyvien järjestelmien ja käytäntöjen arviointia ja mittaamista. Tämän tarkastelun tarkoituksena on selvittää kuinka hyvin yrityksessä tai organisaatiossa on varmistettu tiedon luottamuksellisuus, saatavuus ja eheys. Auditointi voi olla organisaation sisäinen auditointi tai kolmannen osapuolen suorittama ulkoinen auditointi. Tietoturva-auditoija on yleensä ulkopuolinen yritys tai toimija, mutta hänellä täytyy olla hyvä kokonaiskuva organisaation toiminnasta ja käytössä olevasta sisäisestä tiedosta. (42.)

3.8 Lait ja standardit

Tietoturvallisuuteen liittyviä asioita määritellään Suomen laissa, asetuksissa ja standardeissa. Lainsäädännöllä ja standardeilla pyritään yleisesti siihen, että tietoturvallisuus huomioidaan ja hoidetaan asianmukaisesti niin yrityksissä kuin julkisella puolella. (30, s. 52–53.)

Tietoturvallisuutta käsitellään muun muassa seuraavissa laissa:

- Rikoslaki (39/1889)

- Tietoyhteiskuntakaari (917/2014)
- Työturvallisuuslaki (738/2002)
- Pelastuslaki (379/2011)
- Arkistolaki (831/1994)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Henkilötietolaki (523/1999).

Tietoturvallisuutta määritellään myös useissa standardeissa:

- ISO/IEC 27001 Tietoturvallisuuden hallintajärjestelmät. Vaatimukset
- ISO/IEC 27002 Tietoturvallisuuden hallintaa koskeva menettelyohje
- SFS-ISO/IEC 27003 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita
- SFS-ISO/IEC 27004 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallinta. Mittaaminen
- SFS-ISO/IEC 27005 Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta
- IEC/TS 62443-1-1 Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 1-1: Terminologia, käsitteet ja mallit
- SFS-IEC 62443-2-1 Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 2-1: Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten
- IEC/TR 62443-3-1:fi Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille.

3.9 Julkaisut ja ohjeet

Internetistä löytyy useita kattavia ja vapaasti saatavissa olevia julkaisuja, ohjeita ja oppaita, joissa käsitellään tietoturvallisuutta, kyberturvallisuutta tai niiden osa-alueita. Osa julkaisuista ja ohjeista on suunnattu julkishallinnon tai viranomaisten käyttöön, mutta niiden hyödyntäminen yritysten ja organisaatioiden tietoturvallisuuden tarkastelussa on helppoa. Kattavia ja hyödyllisiä julkaisuja, oppaita ja ohjeita löytyy muun muassa seuraavista lähteistä:

- Puolustusministeriön verkkosivut - Katakri 2015, Tietoturvallisuuden auditointityökalu viranomaisille
- Valtiovarainministeriön verkkosivut - VAHTI-tietoturvaohjeisto
- Viestintäviraston verkkosivut - Julkaisut ja tietoturvaohjeet
- Nixu Oyj:n verkkosivut - Julkaisut

3.9.1 Katakri

Katakri on tietoturvallisuuden auditointityökalu viranomaisille. Työkalun uusin versio on julkaistu vuonna 2015 ja aiemmat versiot vuosina 2011 sekä 2009. Katakri on jaettu kolmeen osaan, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen tietoturvallisuus. Työkalun ensisijainen tarkoitus on auttaa viranomaisia arvioimaan yritysten turvallisuusjärjestelyjen toteutumista ja heidän omien tietojärjestelmiensä tietoturvallisuuden arviointia. Katakri on todella kattava tietopaketti ja hyvä työkalu myös yritysten tietoturvallisuuden tarkasteluun. (43; 44.)

3.9.2 VAHTI-ohjeet

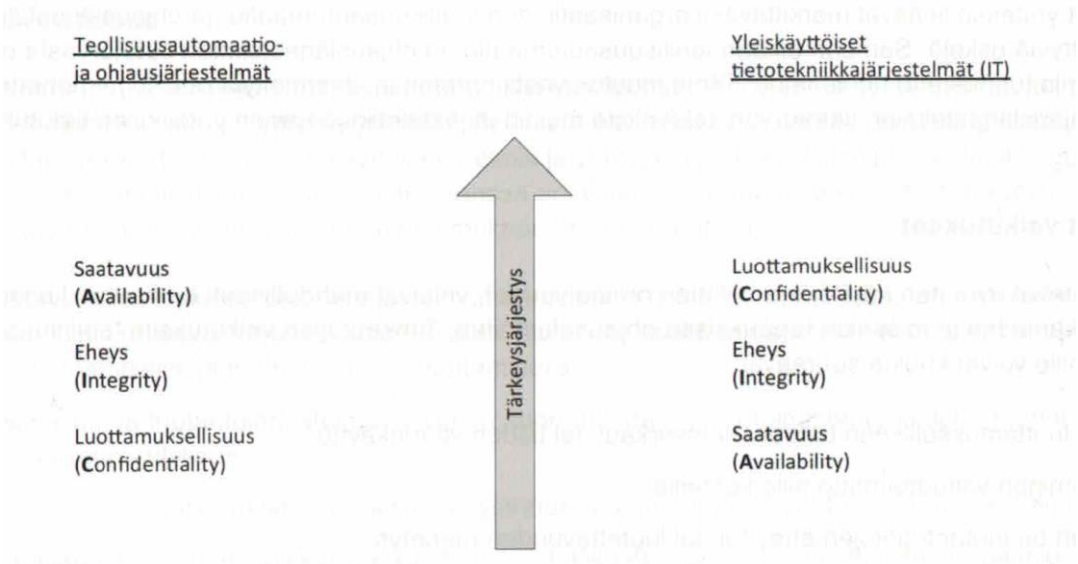
VAHTI-ohjeet ovat Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmän ylläpitämä tietoturvallisuutta koskeva ohjeisto. Ohjeiston tavoitteena on kehittää julkishallinnon ja erityisesti valtionhallinnon tieto- ja kyberturvallisuutta. Koko ohjeisto on saatavilla vapaasti ja kattavasti www.vahtiohje.fi-verkkosivuston kautta. (45.)

4 VALAISTUKSEN OHJAUKSEN TIETOTURVALLISUUS

Tulevaisuudessa yhä useamman kiinteistön valaistuksen ohjausjärjestelmää käytetään julkisen Internet-verkon yli ja yhä useampi ulkovalaisimen ohjainyksikkö liikennöi muun muassa matkapuhelinverkkojen kautta ohjausjärjestelmän palvelimen kanssa. Tämä muutos tuo mukanaan uusia uhkakuvia valaistuksen ohjausjärjestelmien tietoturvallisuudelle. Laitteiden verkottumisen ja pilvipalveluratkaisujen yleistymisen vuoksi myös valaistuksen ohjausjärjestelmien tietoturvallisuuteen tulee kiinnittää enemmän huomiota tulevaisuudessa.

4.1 Tietoturvallisuuden tavoitteet

Valaistuksen ohjausjärjestelmät voidaan rinnastaa teknisesti osittain tietotekniikkaan, mutta osittain myös automaatio- ja ohjausjärjestelmiin. Automaatio- ja ohjausjärjestelmien tietoturvallisuuden ydintavoitteita ovat saatavuus, eheys ja luottamuksellisuus, mutta näiden tavoitteiden tärkeysjärjestys voi olla hyvin erilainen verrattuna yleiskäyttöiseen tietotekniikkaan (kuva 11). Esimerkiksi yrityksen tuotannon kannalta kriittisen ohjausjärjestelmän kohdalla saatavuus voi olla paljon tärkeämpää kuin järjestelmässä käsiteltävän tiedon luottamuksellisuus tai eheys. Tämän takia valaistuksen ohjausjärjestelmien tietoturvallisuuden tavoitteiden tärkeysjärjestys on syytä määritellä aina kohdekohtaisesti.



KUVA 11. Tietoturvallisuuden tavoitteiden vertailu (39, s. 30.)

4.2 Tuotteiden tietoturvallisuus

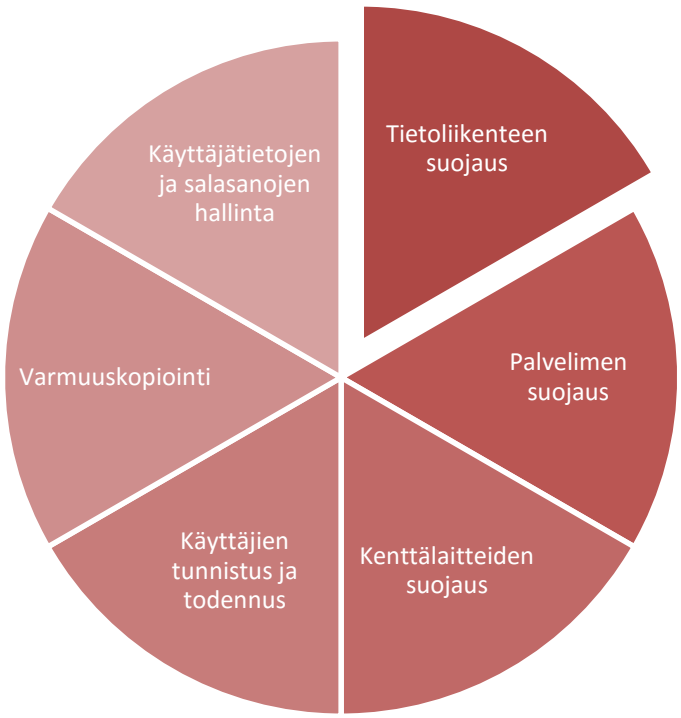
Tällä hetkellä markkinoilla on laaja kattaus erilaisia valaistuksen ohjausjärjestelmiä, niin ulkovalaistukseen kuin sisävalaistukseen. Järjestelmien rakenteet, tietoliikenneprotokollat ja ohjelmistot vaihtelevat suuresti eri valmistajien välillä. Tuotteiden esitteissä ja markkinoinnissa käytetään vielä hyvin vähän tietoturvallisuuteen liittyviä mainintoja. Usein mainitaan vain että järjestelmän langaton tiedonsiirto on suojattu salauksella ja järjestelmän hallintaohjelmisto on suojattu salasanalla. On toki ymmärrettävää, että kaikkia tietoturvallisuuteen vaikuttavia ratkaisuja ei voi julkaista tai kertoa esitteissä, jotta ne eivät menetä merkitystään.

4.3 Standardit ja ohjeet

Valaistuksen ohjausjärjestelmien tietoturvallisuuden tarkasteluun ja suunnitteluun ei ole olemassa vielä valmiita standardeja tai ohjeita. Tämä johtuu osittain siitä, että suurin osa tietoturvallisuutta koskevista standardeista ja ohjeista on tehty siten, että niitä voidaan soveltaa laaja-alaisesti erilaisiin järjestelmiin. Valaistuksen ohjauksen tietoturvallisuutta onkin mahdollista lähestyä yleisten ohjeiden ja kiinteistöautomaatiojärjestelmille sekä teollisuusjärjestelmille tehtyjen standardien ja ohjeiden kautta. Tietoturvallisuuden laajasta materiaalista täytyy rajata juuri kyseistä järjestelmää, sen rakenteita ja uhkien kartoituksesta saatuja tuloksia vastaavat osat.

4.4 Osa-alueet

Valaistuksen ohjausjärjestelmän tietoturvallisuutta ei voi ajatella vain yhtenä kokonaisuutena. Huomioon tulee ottaa järjestelmän eri osien, käytettävien tekniikoiden ja käyttäjien mukanaan tuomat uhkakuvat. On tärkeää myös huomioida järjestelmän suunnittelijoiden, asentajien ja ylläpitäjien toiminnasta johtuvat tietoturvauhkat. Esimerkiksi järjestelmän kaikki muut suojausmenetelmät menettävät merkityksensä, mikäli asentaja ei vaihda käyttöönoton yhteydessä laitteiden oletussalasanoja ohjeiden mukaisesti. Tämä altistaa laitteet verkkoon kytkettyinä tunkeutujille ja väärinkäytöksille. Valaistuksen ohjausjärjestelmän tietoturvallisuutta tarkastellessa ja mahdollisia uhkia kartoittaessa on suotavaa jaotella kokonaisuus pienempiin osa-alueisiin ja suojattaviin osiin (kuva 12).



KUVA 12. Esimerkki valaistuksen ohjausjärjestelmän suojattavista osa-alueista

4.5 Tietoturvatekniikat

Valaistuksen ohjausjärjestelmän suojauksessa on mahdollista käyttää useita tietoturvatekniikoita ja -menetelmiä. Käytettävissä olevat suojauskeinot riippuvat usein järjestelmän rakenteesta, ominaisuuksista ja käytettävistä tiedonsiirtomenetelmistä. Tässä osiossa käydään lyhyesti läpi yleisimpiä menetelmiä järjestelmien eri osien suojaamiseksi.

4.5.1 Laitteiden suojaus

Internettiin kytketyt laitteet tulisi suojata mahdollisimman hyvin, jotta ulkopuoliset tahot eivät pääse käsiksi laitteiden tietoihin tai vaikuttamaan niiden kautta järjestelmän muihin osiin. Verkkoon kytketty laite tulisi olla palomuurin takana tai suojattu jollain muulla tavalla siten, että kaikki ylimääräiset tietoliikenneportit verkosta laitteelle päin on suljettu. Myös laitteiden ylimääräiset ominaisuudet kannattaa kytkeä pois päältä, koska jokainen ominaisuus tuo mukanaan mahdollisuuden uudesta haavoittuvuudesta ja tietoturva-aukosta. Laitteiden ohjelmistojen tulisi

olla tietoturvallisuuden kannalta aina päivitetty viimeisimpään versioon, jotta ohjelmistoissa olevia tietoturva-aukkoja ei ole mahdollista hyödyntää. Mikäli laitteita päivitetään julkisen tietoliikenneverkon yli, tulisi huolehtia, että myös päivitykset ovat suojattu, jotta kukaan ulkopuolinen ei pääse sisällyttämään päivitystiedostoihin haittakoodia. (46.)

Laitteiden suojauksessa tulee myös huomioida onko fyysinen pääsy laitteiden luo estetty luvattomilta henkilöiltä. Mikäli laitteet sijaitsevat esimerkiksi maastossa tai julkisissa tiloissa ja niitä ei ole sijoitettu lukittuihin laitekaappeihin, tulee huolehtia, että laitteiden asetuksia ei pääse muokkaamaan fyysisten liitäntöjen tai käyttöpaneelien kautta ilman salasanaa.

4.5.2 Tiedonsiirron suojaus

Olennainen asia laitteiden välisen tiedonsiirron luottamuksellisuuden ja eheyden ylläpitämisen kannalta on tiedonsiirron suojaaminen. Tiedonsiirron suojamiseen on olemassa useita keinoja. Yleisimmät keinot ovat tiedon salaaminen ennen siirtoa, ulkopuolisilta suljetun tiedonsiirtoyhteyden käyttäminen tai tiedon siirtäminen salatun yhteyskäytävän kautta.

Salaus

Salauksella tarkoitetaan tiedon koodaamista sellaiseen muotoon, että voidaan varmistaa tiedon olevan käytettävissä vain niille käyttäjille, joilla on siihen oikeus. Koodauksessa digitaalinen viesti muutetaan salausavaimen avulla muotoon, josta sen sisällön ymmärtäminen on mahdotonta. Vastakohtana koodaukselle toimii tiedon purkaminen oikealla salausavaimella takaisin alkuperäiseen muotoon, jotta vain käyttäjä jolla on oikeus siihen, voi hyödyntää tietoa. Salausmenetelmät voidaan jaotella yleisesti kahteen osaan:

- symmetrinen salaus (salaiseen avaimeen perustuva salaus)
- epäsymmetrinen salaus (julkiseen avaimeen perustuva salaus).

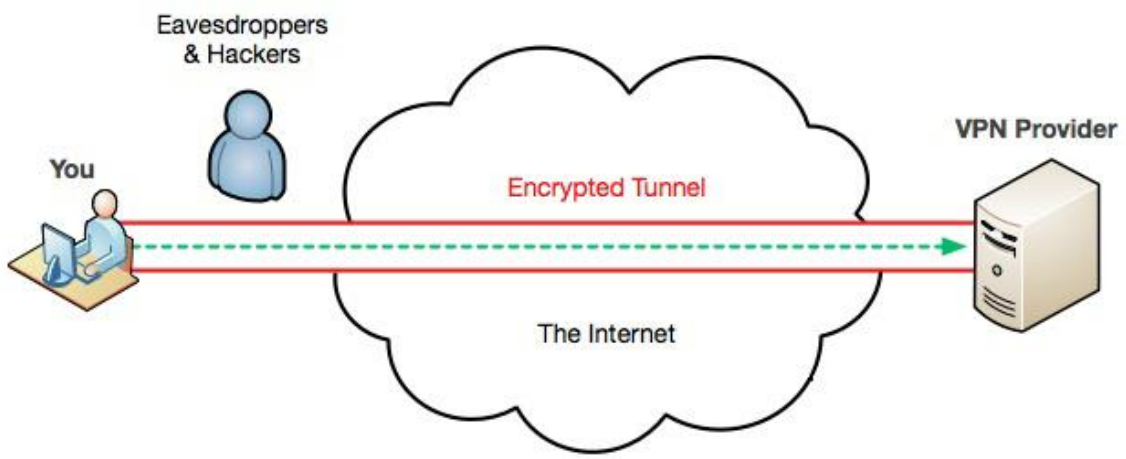
Symmetrisessä salauksessa tieto koodataan ja puretaan samalla salaisella avaimella. Menetelmän luotettavuus perustuu siihen olettamukseen, että vain tiedon koodaaja ja purkaja tietävät salaisen avaimen ja pitävät sen salassa muilta. Epäsymmetrisessä salauksessa tieto koodataan julkisella avaimella ja puretaan

yksityisellä avaimella. Avainten välillä on ainoastaan matemaattinen yhteys siten, että julkisella avaimella salatun tiedon voi purkaa ainoastaan siihen kytköksissä olevalla yksityisellä avaimella. (47, s. 47–53.)

Valaistuksen ohjausjärjestelmissä salausta tulee käyttää tiedonsiirtoyhteyksissä, jotka ovat alttiina väärinkäytöksille ja häirinnälle. Tällaisia yhteyksiä ovat useimmiten julkisessa tietoliikenneverkossa tapahtuva tiedonsiirto tai langattomat yhteydet. Tiedonsiirron salauksella aina valaisimelta palvelimelle asti varmistetaan tiedon luottamuksellisuus ja eheys.

VPN

VPN eli Virtual Private Network on menetelmä jossa suojataan julkisessa tietoliikenneverkossa tapahtuva tiedonsiirto salauksella suojatun tunnelin avulla. Ohjelman avulla luodaan salattu yksityinen yhteys julkisen verkon yli ja näin ollen suojataan siirrettävä tieto julkisen verkon aiheuttamilta uhkilta (kuva 13). VPN-tunnelin avulla voidaan yhdistää esimerkiksi kaksi palomuurilla suojattua verkkoa julkisen Internet-verkon kautta. (40, s. 53–54.)



KUVA 13. VPN-tiedonsiirto (48.)

Valaistuksen ohjausjärjestelmässä VPN-yhteyttä voidaan hyödyntää keskitinlaitteiden ja palvelimen sekä palvelimen ja käyttäjän välisissä yhteyksissä. Käyttämällä VPN-tunnelointia voidaan tiedonsiirto tehdä turvallisesti julkisen verkon yhteyksiä käyttäen ja varmistaen samalla, että tiedonsiirtoa ei voi salakuunnella.

APN

APN:n tehtävänä on toimia yhdyskäytävänä matkapuhelinverkon ja julkisen Internet-verkon välillä. Matkapuhelinverkkojen operaattoreilla on jokaisella omat APN-osoitteensa, joiden avulla verkon käyttäjät tunnistetaan. Osa operaattoreista tarjoaa yrityksille mahdollisuutta luoda oman APN-osoitteen, jonka avulla yrityksen käyttäjien yhteyttä suojataan. Menetelmää käytetään muun muassa M2M-yhteyksissä ja kun laitteiden tai käyttäjien tunnistus on tarve tehdä vain liittymän numeron avulla. (49; 50.)

Yrityskohtaista APN-yhdyskäytävää voidaan hyödyntää valaistuksen ohjausjärjestelmissä tietoliikenteen rajaamiseen. Käytettäessä yksityistä APN-yhdyskäytävää ohjausjärjestelmän laitteiden ja palvelimen välinen tietoliikenne kulkee omassa verkossa ja ulkopuoliset eivät pääse puuttumaan siihen. Laitteiden tunnistus tapahtuu liittymän numeron ja APN-osoitteen avulla.

4.5.3 Palvelimen suojaus

Palvelimen tietoturva itsessään on hyvin laaja käsite ja huomioon otettavat asiat riippuvat suuresti palvelimen rakenteesta, ohjelmistosta ja käyttötarkoituksesta. Seuraavassa on kuvattu yleisimpiä palvelimen suojausmenetelmiä ja -tekniikoita.

Palomuuri ja haittaohjelmien torjunta

Palomuurin tehtävänä on toimia nimensä mukaisesti liikennettä rajoittavana muurina palvelimen ja julkisen verkon välissä. Rajoittamalla ja estämällä julkisesta verkosta tulevaa liikennettä ennalta määriteltyjen sääntöjen mukaisesti turvataan palvelin tunkeilijoilta ja haittaohjelmilta. Palomuuri tarkistaa siihen määriteltyjen sääntöjen mukaisesti sen läpi kulkevien tietoliikennepakettien sisällön ja estää pääsy paketeilta, joita säännöt eivät hyväksy. Rakenteellisesti palomuuri voi olla esimerkiksi palvelimelle asennettava ohjelma tai fyysinen laite, joka on suunniteltu ja valmistettu nimenomaan palomuuriksi. (51, s. 328–332.)

Tärkeä osa palvelimen suojausta on haittaohjelmien eli erilaisten tietokonevirusten, matojen ja troijalaisten torjunta. Palvelin altistuu haittaohjelmille siihen ladattavien ja siirrettävien ohjelmien, tiedostojen sekä tietoliikenneyhteyksien kautta. Haittaohjelmia voidaan torjua asentamalla palvelimelle ohjelmisto, joka tarkkailee

palvelimelle asennettuja ohjelmia ja palveluita sekä skannaa muistissa olevia tiedostoja ja tarkistaa ladattavia tiedostoja. Myös palvelimen käyttöjärjestelmä ja ohjelmat tulee pitää päivitettynä uusimpiin versioihin, jotta haittaohjelmat eivät pääse hyödyntämään niiden mahdollisia haavoittuvuuksia. (32, s. 275–281.)

Todennus ja valtuutus

Todennuksen tavoitteena on varmuudella tunnistaa järjestelmän tai verkon käyttäjät, laitteet, sovellukset, palvelut ja resurssit. Näiden käyttäjien tunnistus tehdään perinteisesti käyttäjätunnukseen ja salasanaan perustuvan kirjautumisen avulla. Todennus voidaan tehdä myös omistamisen, fyysiseen ominaisuuden, sijainnin tai ajankohdan perusteella. Käytettäviä tekijöitä lisäämällä saadaan todennuksesta yhä varmempaa. Kahden tekijän todennusmenetelmää käytetään nykyään hyvin usein erilaisissa verkkopalveluissa. Käyttäjä tunnistetaan ensi salasanalla ja tämän jälkeen ennalta määriteltyyn puhelinnumeroon tai sähköpostiosoitteeseen lähetettävän vahvistuskoodin perusteella. Valtuutuksella määritellään mihin järjestelmän tietoihin tai osiin käyttäjällä on oikeus. (47, s. 21–22.)

Päivitykset

Käyttöjärjestelmät ja ohjelmistot ovat useimmiten rakenteeltaan monimutkaisia ja laajoja kokonaisuuksia, joten on todennäköistä että niistä löytyy virheitä ja puutteita. Tästä johtuen käyttöjärjestelmiä ja ohjelmistoja ylläpidetään sekä päivitetään jatkuvasti. Tämän lisäksi käyttöjärjestelmien ja ohjelmistojen päivitykset sisältävät hyvin usein myös erilaisten haavoittuvuuksien korjauksia sekä muita tietoturvallisuuteen liittyviä parannuksia. Päivittämällä palvelimen käyttöjärjestelmän ja siihen asennetut ohjelmat aina uusimpiin ohjelmistoversioihin voidaan varmistaa niistä löytyvien haavoittuvuuksien korjaantuminen mahdollisimman nopeasti. (32, s. 74–77.)

Varmuuskopiointi

Tarpeellisten ja tärkeiden tiedostojen säännöllisellä varmuuskopioinnilla estetään tiedon katoaminen vahingon sattuessa. Palvelimeen ja sen tiedostoihin voi kohdistua monenlaisia uhkia. Palvelimeen saattaa ujuttautua esimerkiksi haittaohjelma, joka tuhoaa tai tekee sen sisältämät tiedostot käyttökelvottomiksi. Myös palvelimen komponentit saattavat hajota tai palvelinsali vahingoittua tulipalon

vuoksi aiheuttaen tiedostojen tuhoutumisen. Varmuuskopiointi voidaan tehdä erillisten tiedostojen, tiedostokansioiden, levyjen tai koko tallennustilan tasolla. Pelkkien tiedostojen varmuuskopioinnin lisäksi palvelimesta voidaan myös ottaa täydellinen levynkuva, joka sisältää identtisen kopion palvelimen käyttöjärjestelmästä, ohjelmista ja tiedostoista. Palvelimen kovalevyn rikkoutuessa tämä levynkuva siirretään uudelle kovalevylle ja palvelimen toiminta voi jatkua normaalisti. (32, s. 56–60.)

Fyysinen suojaus ja tietoliikenneyhteyden varmistus

Palvelimen suojauksessa oleellinen puoli on sen fyysinen suojaus mahdollisilta vahingoilta. Fyysiseen turvallisuuteen katsotaan kuuluvan palvelintilan kulunvalvonta, vartiointi sekä palo-, vesi-, sähkö- ja murtovahinkojen torjunta. Esimerkiksi pääsyn palvelimelle tulee olla rajattu, jotta voidaan estää haittaohjelmien tartuttaminen palvelimeen fyysisten liitäntöjen kautta. Palo- ja vesivahingot voivat vaurioittaa palvelinta siten, että sen käyttäminen ei ole enää mahdollista tai osa sen sisältämistä tiedoista tuhoutuu. (30, s. 52–65.)

Verkottuneessa järjestelmässä pelkkä palvelimen suojaus ei takaa järjestelmän toimivuutta häiriötilanteissa, vaan tärkeää on suojata ja varmistaa palvelimen verkkoyhteyden toiminta myös poikkeusoloissa. Verkkoyhteyden tulisi olla kahdennettu siten, että sen toiminta ei ole riippuvainen yksittäisen laitteen tai yhteyden rikkoutumisesta. Kahdennetussa verkossa pääyhteyden tueksi on rakennettu varayhteys, jonka avulla tarpeellinen tietoliikenne voidaan hoitaa, kun pääyhteys ei ole käytettävissä. Varautuminen tulee kuitenkin aina suhteuttaa tietoliikenteen kriittisyyteen. Mikäli tietoliikenteen hetkellisestä katkoksesta ei ole järjestelmän toimivuudelle suurta vaikutusta, ei varayhteydelle välttämättä ole tarvetta. Varayhteyden lisäksi häiriöihin ja poikkeustilanteisiin voidaan varautua toimintasuunnitelmilla, jotka mahdollistavat verkkoyhteyden nopean korjauksen tarpeen vaatiessa. (30, s. 72–73.)

4.5.4 Käyttöliittymän suojaus

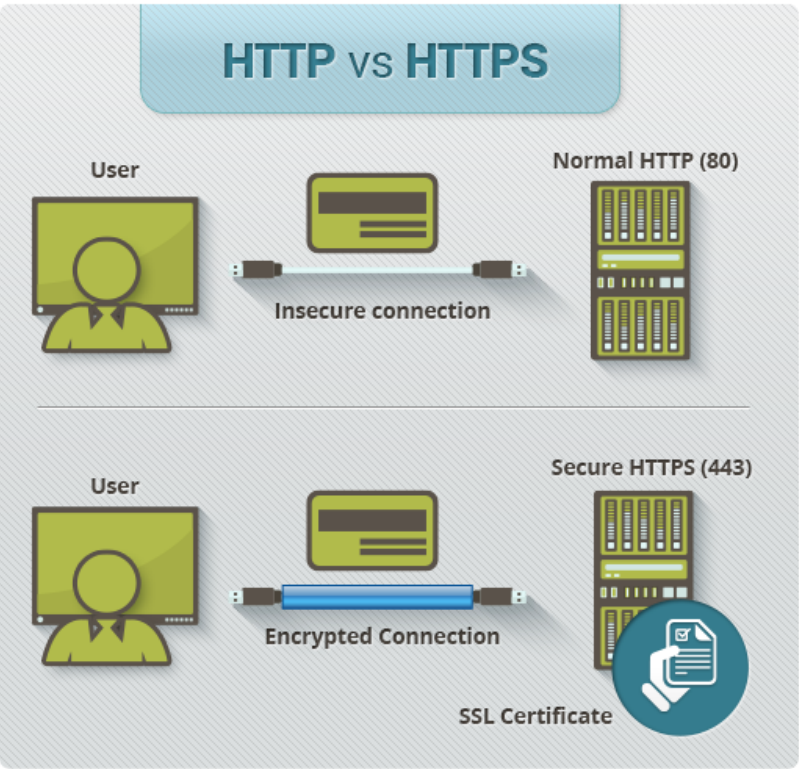
Järjestelmän käyttöliittymän suojauksen menetelmissä ratkaisevaa on millaisen käyttöliittymän kautta järjestelmää käytetään ja hallitaan. Valaistuksen ohjausjär-

jestelmää käytetään yleensä joko erilliseltä tietokoneelle asennettavalta ohjelmistolta tai verkkoselaimessa toimivan käyttöliittymän kautta. Joissakin tapauksissa myös älypuhelimille on luotu omia sovelluksia, joiden kautta järjestelmän käyttö ja hallinta tapahtuu. Toinen ratkaiseva tekijä on se, mitä kautta tiedonsiirto tapahtuu käyttöliittymän ja palvelimen välillä. Turvallisin vaihtoehto on jos hallinta- ja käyttöliittymää käytetään suoraan järjestelmän palvelimella tai esimerkiksi yrityksen sisäverkon kautta. Yhä useammin palvelimen ja käyttöliittymän välinen tiedonsiirto tapahtuu ainakin osittain julkisen verkon kautta. Tällaisessa tapauksessa tulee huomioida julkisen verkon mukanaan tuomat uhkat. Käyttöliittymän ja palvelimen välistä tietoliikennettä voidaan suojata esimerkiksi tietokoneelle asennettavan ohjelmiston tapauksessa VPN-yhteydellä ja verkkoselaimessa toimivan käyttöliittymän yhteydessä HTTPS-protokollalla. (30, s. 202–203.)

Käyttöliittymien ohjelmistojen rakenteet ovat yleensä aina monimutkaisia ja laajoja. Tämän vuoksi ohjelmista ja niissä käytetyistä ohjelmointikielistä voi aina löytyä virheitä ja haavoittuvuuksia. Näiden korjaamiseksi ja paikkaamiseksi tulee muistaa huolehtia ohjelman ja sen liitännäisten ajantasaisuudesta. Uusimmat päivitykset kannattaa ottaa käyttöön ajallaan.

HTTPS ja varmenteet

HTTPS-protokolla on HTTP-tiedonsiirtoprotokollan ja TLS/SSL-salausprotokollan yhdistelmä, jota käytetään Internetissä tapahtuvan tiedonsiirron suojaamiseen (kuva 14). Protokolla määrittelee käytännön, jossa kaikki HTTP-tietoliikenne salataan TLS-protokollalla ennen sen lähettämistä ja vastaanottamista käyttäjän ja palvelimen välillä. Näin estetään tiedon luvaton käyttö ja muuttaminen tiedonsiirron aikana. TLS-protokollan edeltäjä oli SSL-protokolla, mutta sitä ei tulisi enää käyttää siitä löytyneiden heikkouksien ja haavoittuvuuksien takia. TLS/SSL-salauksen parhaan mahdollisen toiminnan kannalta on myös oleellista käyttää riittävän pitkää salausavainta. Avaimen pituuden tulisi olla vähintään 128 bittiä. (51, s. 310–313; 52.)



KUVA 14. HTTP- ja HTTPS-protokollan vertailu (53.)

Tietoliikenneyhteyden salaamiseksi HTTPS-protokollan avulla täytyy palvelimen jakaa käyttäjälle varmenne. Varmenne sisältää muun muassa palvelimen julkisen avaimen ja tunnistukseen tarvittavat tiedot. Varmenteelle voidaan hankkia erillinen kolmannen osapuolen todentaja, jonka tehtävänä on todentaa käyttäjälle, että kyseisen varmenteen jakaja on todella se kuka väittää olevansa. (51, s. 288–289.)

Käyttäjän todennus

Järjestelmän tai sen osien luvaton käyttö voidaan estää käyttäjän todennuksen avulla. Käyttö- ja hallintaohjelmissa käyttäjän todennus tehdään hyvin usein käyttäjätunnuksen ja salasanan avulla. Tässä tapauksessa luotetaan siihen, että oikean salasanan tietää vain luotettu käyttäjä. Salasanaan perustuvan käyttäjän todennuksen heikkoudet liittyvät salasanan vahvuuteen ja salakuuntelun helppouteen. Käytettävien salasanojen tulisikin olla riittävän pitkiä ja monimutkaisia. Salasanojen salakuuntelua voidaan estää käyttämällä tiivistefunktioita käyttöliittymän ja palvelimen välisessä tiedonsiirrossa ja opastamalla käyttäjiä olemaan valppaina mahdollisen fyysisen urkinnan varalta. (47, s. 24–27.)

5 TIETOTURVAKARTOITUS

5.1 Tavoite

Yksi opinnäytetyön tavoitteista oli toteuttaa tietoturvakartoitus Greenled Oy:n valaistuksen ohjausjärjestelmätuotteille. Kartoituksen avulla haluttiin selvittää nykyisten tuotteiden tietoturvallisuuden taso, tunnistaa järjestelmien tietoturvallisuuteen liittyvät uhkat ja riskit sekä luoda ohjeistus toimenpiteistä, joilla taataan riittävä tietoturvan taso. Järjestelmien kartoituksessa tuli huomioida järjestelmien erilainen rakenne ja niiden käytön sekä hallinnan toteuttaminen verkkopalveluina. (1.)

5.2 Lähtötilanne

Opinnäytetyön tekeminen alkoi siitä lähtötilanteesta, että Greenled Oy:n tuotevalikoimassa oli kaksi valaistuksen ohjausratkaisua, joista toinen oli tarkoitettu sisävalaistuksen ohjaukseen ja toinen ulkovalaistuksen ohjaukseen. Syksyn 2015 aikana yritys laajensi tarjontaansa myös yhdellä uudella kiinteistöjen sisävalaistuksen ohjaukseen tarkoitetulla järjestelmällä.

Työn aloitushetkellä tietoturvallisuus oli huomioitu yrityksen tuotteissa niiden valmistajien ohjeiden mukaisesti ja yleisellä tasolla, mutta varsinaista yhtenäistä ohjeistusta järjestelmien tietoturvallisuuden huomioimiseksi ei ollut. Yrityksen myymät tuotteet kuitenkin kytketään yhä useammin myös julkiseen verkkoon ja niitä käytetään sekä hallitaan koko ajan enemmän Internet-yhteyden kautta. Tämän vuoksi yrityksessä haluttiin tutustua järjestelmien tietoturvallisuuteen ja luoda ohjeistus tarvittavista toimenpiteistä.

Greenled Oy tuottaa asiakkaille LED-valaistusta kokonaisratkaisuna siten, että kokonaisuudessa on huomioitu tarpeenmukainen valaistus ja valaistuksen ohjaus. Yrityksen tuotevalikoimaan kuuluu kiinteistöjen sisävalaistuksen ohjaukseen tarkoitetut Osramin Encelium-ohjausjärjestelmä ja Helvarin Digidim-ohjausjärjestelmä, sekä ulkovalaistuksen ohjaukseen tarkoitettu Sirius!-palvelu. (2, linkki Yritys.)

Sirius!-palvelu

Greenled Oy:n Sirius!-palvelu on alue-, tie- ja katuvalaistuksen kokonaishallintapalvelu, joka rakentuu Osramin Street Light Control -komponenttien ympärille. Palvelu mahdollistaa ulkovalaisimien hallinnan verkon yli paikasta ja ajasta riippumatta.

Järjestelmä rakentuu valaisinkohtaisista ohjaimista, keskittimistä, virtuaalipalvelimesta ja web-käyttöliittymästä. Valaisinkohtaiset ohjaimet keskustelevat katuvalaisinkeskuksessa sijaitsevan keskittimen kanssa normaalia sähkökaapelia pitkin LON-protokollalla. Keskittimen tehtävänä on ohjata valaisimia asetettujen aikataulujen mukaan ja välittää tietoa 3G-yhteyden kautta järjestelmän palvelimelle. Palvelimen tehtävänä on luoda käyttöliittymä palvelulle ja tallentaa valaisimilta kerätyt tiedot tietokantaan. (2, linkki Sirius!-palvelu; 54.)

Encelium

Greenled Oy:n tuotevalikoimaan kuuluva Osramin Encelium-valaistuksen ohjausjärjestelmä on tarkoitettu kiinteistöjen sisävalaistuksen ohjaukseen. Järjestelmä koostuu Polaris 3D -ohjelmistosta, SSU-palvelimesta, DALI ECU -reitittimistä ja DALI-yhteensopivista valaisimista, käyttöliittymistä ja sensoreista. Encelium-valaistuksen ohjausjärjestelmän avulla on mahdollista hallita koko kiinteistön valaistusta helppokäyttöisen ja visuaalisen käyttöliittymän kautta. Järjestelmän avulla on mahdollista saavuttaa energiansäästöä usealla eri tavalla, aina läsnäolotunnistuksesta valoisuusmittauksen kautta käyttäjäkohtaiseen ohjaukseen asti. (55.)

Helvar Digidim

Toinen Greenled Oy:n tuotevalikoimaan kuuluva sisävalaistuksen ohjausjärjestelmä on Helvarin Digidim. Helvarin valaistuksenohjausjärjestelmä rakentuu Digidim 920, 910 ja 905 -reitittimien ympärille. Reitittimiä voidaan yhdistää suuremmiksi valaistuksenohjausjärjestelmäksi Ethernet-liitännän kautta ja myös integroida muihin järjestelmiin kuten kiinteistöautomaatiojärjestelmiin. Digidim-reitittimeen voidaan kytkeä mallista riippuen 64–128 DALI-laitetta ja Digidim 920 -reitittimeen myös DMX- ja S-DIM-ohjattavia laitteita. Digidim-reititinjärjestelmään

voidaan yhdistää myös Helvarin uSee-käyttöliittymä, joka mahdollistaa valaistuksen ohjausjärjestelmän etäkäytön verkon yli. Käyttöliittymä on verkkoselainpohjainen, joten sitä voidaan käyttää niin tietokoneen kuin taulutietokoneenkin kautta. (56; 57; 58.)

5.3 Suunnittelu

Työn aikataulutuksen ja kokonaisuuden hallinnan vuoksi tietoturvakartoitus täytyi ensimmäisenä suunnitella vastaamaan asetettuja tavoitteita. Työ alkoi jaottelemalla tietoturvakartoitus osiin tavoitteiden ja riskien arvioinnin toimintamallin perusteella. Jaottelun tuloksena tietoturvakartoitusdokumentin rakenteeksi muodostui seuraava kokonaisuus:

1. Johdanto
2. Ohjausjärjestelmän rakenne
3. Nykytilan kartoitus
4. Tietoturvariskien arviointi
5. Toimenpiteet
6. Tietoturvallisuuden ylläpito

5.4 Toteutus ja tulokset

Varsinainen tietoturvakartoitus toteutettiin opinnäytetyöstä erillisenä dokumenttina sen sisältämien luottamuksellisten tietojen takia. Dokumentti sisältää kartoituksen tulokset, tietoturvariskien arvioinnin tulokset, koonnin tarvittavista toimenpiteistä ja suunnitelman tietoturvallisuuden ylläpitämisestä. Kartoituksen tulosten pohjalta luotiin myös ohjausjärjestelmiä koskeva tietoturvaohje Greenled Oy:n sisäiseen käyttöön. Tietoturvakartoitus on merkitty opinnäytetyön liitteeksi 2, nykytilan kartoituksen tulokset liitteeksi 3 ja tietoturvaohje liitteeksi 4.

6 POHDINTA

Työn tavoitteena oli tutustua tietoturvallisuuden teoriaan ja valaistuksen ohjausta koskeviin tieturvallisuuden osa-alueisiin, tehdä tietoturvakartoitus Greenled Oy:n valaistuksen ohjausjärjestelmälle ja luoda ohjausjärjestelmien tietoturvaohje yrityksen sisäiseen käyttöön. Aikataulun osalta tavoitteena oli saada opinnäytetyö valmiiksi jouluksi 2015.

Vaikka tietoturvallisuus on käsitteenä todella laaja, onnistuin mielestäni kokoamaan työn teoriaosaan selkeän kokonaisuuden tietoturvallisuudesta työn aiheen näkökulmasta. Teoriaosuutta varten perehdyin useisiin tietoturvallisuutta käsitteleviin kirjoihin, standardeihin, verkosta löytyviin julkaisuihin ja ohjeisiin sekä valaistusalan lehtien artikkeleihin. Työn kannalta erityisen hyödyllinen lähde oli SFS-käsikirja 631-3, joka sisältää automaation tietoturvallisuutta koskevat standardit.

Tutustuessani lähteisiin ja seuratessani valaistusalalla käytävää keskustelua sain mielikuvalleni vahvistuksen siitä, että valaistuksen ohjauksen tietoturvallisuuteen kiinnitetään vielä todella vähän huomiota. Omalta osaltaan laitteiden tai ohjelmistojen valmistajat kiinnittävät huomiota tuotteidensa tietoturvallisuuteen, mutta valmiiden ohjausjärjestelmäkokonaisuuksien tietoturvallisuus jää hyvin usein järjestelmän asentajan, ylläpitäjän tai asiakkaan huolehdittavaksi. Mikäli järjestelmän asentaja, ylläpitäjä tai asiakas ei osaa kiinnittää tarpeeksi huomiota ohjausjärjestelmän tietoturvallisuuteen, altistetaan järjestelmä, tiedot ja käyttäjät tietoturvauhkille.

Valaistuksen ohjausjärjestelmien tietoturvallisuutta heikentää muun muassa laitteiden pitkiksi venyvät eliniät, julkisen verkon yli tapahtuva tiedonsiirto ja alan toimijoiden vähäinen tietotaito. Tietoturvallisuuden kannalta valaistuksen ohjausjärjestelmissä on syytä kiinnittää huomiota reitittimien tai keskittimien ja palvelimen välisen tietoliikenteen suojaamiseen, käyttäjän ja palvelimen välisen tietoliikenteen suojaamiseen, käyttäjien tunnistukseen, salasanojen hallinnointiin, varmuuskopiointiin ja laiterikkoihin sekä toimintahäiriöihin varautumiseen.

Greenled Oy:n valaistuksen ohjausjärjestelmälle tehty tietoturvakartoitus onnistui mielestäni todella hyvin ja kartoituksen tulosten perusteella tarvittavien toimenpiteiden valinta oli helppoa. Tietoturvakartoitusta varten tehtyä dokumenttia voidaan myös tulevaisuudessa hyödyntää uusien järjestelmien kartoittamiseen tai olemassa olevien järjestelmien uudelleenkartoitukseen. Työn teoriaosuuden ja tietoturvakartoituksen tulosten pohjalta kokoamastani ohjausjärjestelmien tietoturvaohjeesta syntyi selkeä ja käytännöllinen dokumentti yrityksen sisäiseen käyttöön.

Valaistuksen ohjauksen tietoturvallisuus oli mielestäni erittäin mielenkiintoinen, mutta myös todella haasteellinen aihe. Haasteelliseksi aiheen teki se, että en onnistunut löytämään suoraan valaistuksen ohjauksen tietoturvallisuuteen liittyviä lähteitä, vaan lähteet käsittelivät joko erikseen tietoturvallisuutta tai valaistuksen ohjausta. Tämä kertoo osaltaan sen, että aiheesta ei ole käyty vielä kovin paljon keskustelua eikä kirjoitettu julkaisuja. Haasteellisuutta lisäsi myös tietoturvallisuutta käsittelevän lähdemateriaalin laajuus ja monimuotoisuus. Keskeisimpien ja työn aiheen kannalta tärkeimpien asioiden poimiminen tuntui välillä todella työläältä.

Kiinnostukseni tietoturvallisuudesta ja työn aiheen ainutlaatuisuus auttoivat pitämään mielenkiintoa yllä ja saavuttamaan asetetut tavoitteen. Kokonaisuutena olen erittäin tyytyväinen työn lopputuloksiin ja kuluneen syksyn aikana olen päässyt oppimaan paljon uutta tietoturvallisuudesta sekä valaistuksen ohjauksesta.

LÄHTEET

1. Moilanen, Ville 2015. Chief Technology Officer, Greenled Oy. Opinnäytetyön aloituspalaveri 14.8.2015.

2. Greenled Oy. Saatavissa: http://www.greenled.fi. Hakupäivä 3.10.2015.

3. Kallioharju, Kari 2012. DALI-koulutus, teoriaosio. Tampere: Tampereen ammattikorkeakoulu. Saatavissa: http://www.oamk.fi/~kurki/Valaistustekniikka/. Hakupäivä 15.10.2015.

4. Chemel, Brian 2010. Intelligent lighting systems drive radical energy-efficiency gains. LEDsmagazine, nro november/december 2010. Saatavissa: http://www.ledsmagazine.com/articles/print/volume-7/issue-12.html. Hakupäivä 9.10.2015.

5. About lighting. 2015. International Energy Agency. Saatavissa: https://www.iea.org/topics/energyefficiency/subtopics/lighting/. Hakupäivä 20.9.2015.

6. Elohopealamput poistuvat markkinoilta 2015 – mitä tilalle katuvalaistukseen? 2014. Motiva Oy. Saatavissa: http://www.motiva.fi/files/8729/Katuvalaisuesite_10032014.pdf. Hakupäivä 20.9.2015.

7. Results. 2015. EnLight-project. Saatavissa: http://www.enlight-project.eu/en/results/. Hakupäivä 30.11.2015.

8. Juntunen, Eveliina - van Tujil, Frank - Weib, Herbert - Talen, Ambali 2015. Granular Lighting Control Enables Significant Energy Savings with Optimized User Comfort. Enlight project. Saatavissa: http://www.enlight-project.eu/user/files/enlight-06granularlightingcontrolenablessignificantenergysavingswithoptimizedusercomfort.pdf. Hakupäivä 30.11.2015.

9. Chemel, Brian 2010. Intelligent lighting systems drive radical energy-efficiency gains. LEDsmagazine, nro November/December 2010. Saatavissa:

http://www.ledsmagazine.com/articles/print/volume-7/issue-12.html. Hakupäivä: 3.10.2015.

10. Lokhoff, Gerard 2015. Standards will futureproof intelligent outdoor SSL deployments. LEDsmagazine, nro july/august 2015. Saatavissa: http://www.ledsmagazine.com/articles/print/volume-12/issue-7.html. Hakupäivä 16.9.2015.

11. Maantie- ja rautatiealueiden valaistuksen suunnittelu. 2015. Liikennevirasto. Saatavissa: http://www2.liikennevirasto.fi/julkaisut/pdf8/lo_2015-16_maantie_rautatiealueiden_web.pdf. Hakupäivä 8.12.2015.

12. ZigBee PRO with Green Power. ZigBee Alliance. Saatavissa: http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeepro/. Hakupäivä 29.9.2015.

13. Woodford, Chris 2007. Wireless Internet. Explain that Stuff. Saatavissa: http://www.explainthatstuff.com/wirelessinternet.html. Hakupäivä 21.11.2015.

14. Olsson, Jonas 2014. 6LoWPAN demystified. Texas Instruments. Saatavissa: http://www.ti.com/lit/wp/swry013/swry013.pdf. Hakupäivä 29.9.2015.

15. Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks. 2015. The Internet Engineering Task Force. Saatavissa: http://datatracker.ietf.org/doc/rfc6282/. Hakupäivä 29.9.2015.

16. EnOcean Wireless Standard ISO/IEC 14543-3-10. 2015. EnOcean Alliance Inc. Saatavissa: https://www.enocean-alliance.org/en/enocean_standard/. Hakupäivä 29.9.2015.

17. Energy Harvesting Wireless Technology. 2015. EnOcean GmbH. Saatavissa: https://www.enocean.com/en/energy-harvesting-wireless/. Hakupäivä 29.9.2015.

18. Sigfox technology. 2014. Sigfox. Saatavissa: http://www.sigfox.com/en/#!/technology. Hakupäivä 30.9.2015.

19. Ultra Narrow Band. 2015. Telensa. Saatavissa: http://www.telensa.com/technology/ultra-narrow-band/. Hakupäivä 30.9.2015.

20. Rontu, Riitta 2011. Matkapuhelinverkot osa 1. T762506 Langattomat laajakaistatekniikat. Opintojakson materiaali. Oulu: Oulun ammattikorkeakoulu Oy.

21. Kuphaldt, Tony 2000. Lessons In Electric Circuits -- Volume IV. Chapter 14. Digital communication. Saatavissa: http://www.ibiblio.org/kuphaldt/electricCircuits/Digital/DIGI_14.html. Hakupäivä 21.11.2015.

22. Technical Overview. DALI - a working group of ZVEI. Saatavissa: http://www.dali-ag.org/discover-dali/technical-overview.html. Hakupäivä 30.9.2015.

23. What is Power Line Communication? 2011. Cypress Semiconductor. Saatavissa: http://www.eetimes.com/document.asp?doc_id=1279014. Hakupäivä 30.9.2015.

24. What is KNX? 2014. KNX Association cvba. Saatavissa: http://www.knx.org/knx-en/knx/association/what-is-knx/index.php. Hakupäivä 3.10.2015.

25. DMX 101: A DMX 512 handbook. 2008. Elation Professional. Saatavissa: http://elationlighting.com/pdffiles/dmx-101-handbook.pdf. Hakupäivä 8.10.2015.

26. What is the LonWorks Platform? 2015. LonMark International. Saatavissa: http://www.lonmark.org/connection/what_is_lon. Hakupäivä 9.10.2015.

27. Introduction to the LonWorks Platform. Echelon Corporation. Saatavissa: http://downloads.echelon.com/support/documentation/manuals/general/078-0183-01B_Intro_to_LonWorks_Rev_2.pdf. Hakupäivä 9.10.2015.

28. Makdessian, Alec 2015. PoE technology for LED lighting delivers benefits beyond efficiency. LEDsmagazine, nro September 2015. Saatavissa:

http://www.ledsmagazine.com/articles/print/volume-12/issue-8.html. Hakupäivä 2.10.2015.

29. Lighting Control Protocols. 2011. Illuminating Engineering Society. Saatavissa: http://www.ies.org/PDF/Store/TM-23-11_FINAL.pdf. Hakupäivä 8.10.2015.

30. Andreasson, Ari – Koivisto, Juha 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma Oy.

31. Tietoturvallisuuden hallintajärjestelmä: ISO/IEC 27000. 2015. Suomen Standardisoimisliitto SFS ry. Saatavissa: http://www.sfsedu.fi/files/121/ISO-27000_2015.ppt. Hakupäivä 15.9.2015.

32. Järvinen, Petteri 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo Finland Oy.

33. Kyberympäristö ja kyberturvallisuus. FiCom ry. Saatavissa: http://www.ficom.fi/linked/fi/ohjeita/Kyber_esite_WEB.pdf. Hakupäivä 15.9.2015.

34. Tietoturva. Suomen Kuntaliitto. 2015. Saatavissa: http://www.kunnat.net/fi/asiantuntijapalvelut/tyk/tietohallinto/tietoturva/Sivut/default.aspx. Hakupäivä 10.10.2015.

35. Tietoaineistoturvallisuus. 2009. Valtionhallinnon tietoturvallisuuden johtoryhmä. Saatavissa: https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus. Hakupäivä 10.10.2015.

36. Laitteistoturvallisuus. 2009. Valtionhallinnon tietoturvallisuuden johtoryhmä. Saatavissa: https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus. Hakupäivä 11.10.2015.

37. Käyttöturvallisuus. 2009. Valtionhallinnon tietoturvallisuuden johtoryhmä. Saatavissa: https://www.vahtiohje.fi/web/guest/kayttoturvallisuus1. Hakupäivä 10.10.2015.

38. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003. Valtiovarainministeriö. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10128&groupId=10229. Hakupäivä 10.10.2015.

39. IEC/TS 62443-1-1:fi. 2013. Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 1-1: Terminologia, käsitteet ja mallit. Helsinki: Suomen Standardisoimisliitto SFS.

40. ISO/IEC 27001:fi.2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS.

41. ISO 27001 -sertifiointi. Bureau Veritas Certification. Saatavissa: http://www.bureauveritas.fi/e3af93004db0c46a9b5fdf10c0640809/BureService_ISO27001_FI_web.pdf?MOD=AJPERES&CACHEID=e3af93004db0c46a9b5fdf10c0640809. Hakupäivä 14.10.2015.

42. Hayes, Bill 2003. Conducting a Security Audit: An Introductory Overview. Symantec Corporation. Saatavissa: http://www.symantec.com/connect/articles/conducting-security-audit-introductory-overview. Hakupäivä 12.10.2015.

43. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Puolustusministeriö. Saatavissa: http://www.defmin.fi/katakri. Hakupäivä 11.10.2015.

44. Tietoturvallisuuden auditointityökalun (Katakri) uudistus on valmis. 2015. Valtioneuvosto. Saatavissa: http://valtioneuvosto.fi/artikkeli/-/asset_publisher/tietoturvallisuuden-auditointityokalun-katakri-uudistus-on-valmis. Hakupäivä 11.10.2015.

45. Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmän (VAHTI) ohjesivusto. Valtionhallinnon tietoturvallisuuden johtoryhmän. Saatavissa: https://www.vahtiohje.fi/web/guest/home. Hakupäivä 18.12.2015.

46. Verkkoon kytkeytyvien laitteiden tietoturvassa on usein puutteita. 2014. Viestintävirasto. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/03/ttn201403101402.html. Hakupäivä 20.10.2015.

47. IEC/TS 62443-3-1:fi. 2013. Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille. Helsinki: Suomen Standardisoimisliitto SFS.

48. Rashid, Fahmida 2013. How to Set Up a VPN in Windows 7. PCMag. Saatavissa: http://www.pcmag.com/article2/0,2817,2419611,00.asp. Hakupäivä 2.12.2015.

49. Sonera Mobile Gate. 2015. TeliaSonera Finland Oyj. Saatavissa: https://www.sonera.fi/yrityksille/tuotteet+ja+palvelut/verkkoratkaisut/mobile+gate. Hakupäivä 19.10.2015.

50. Frequently asked questions. 2015. Wireless Logic. Saatavissa: http://www.wirelesslogic.com/faqs/. Hakupäivä 20.10.2015.

51. Gollmann, Dieter 2011. Computer security. Chichester: John Wiley & Sons Ltd.

52. Tarkista ylläpitämäsi verkkopalvelun suojaustaso. 2012. Viestintävirasto. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2012/05/ttn201205141441.html. Hakupäivä 25.10.2015.

53. What is HTTPS? 2015. Comodo CA Limited. Saatavissa: https://www.instantssl.com/ssl-certificate-products/https.html. Hakupäivä 21.11.2015.

54. OSRAM Street Light Control – innovatiivinen ulkoalueiden valonsäätöjärjestelmä. 2015. OSRAM GmbH. Saatavissa: http://www.osram.fi/osram_fi/uutiset--tiedot/valonsaeaetoejaerjestelmae/tuotetiedot/street-light-control/index.jsp. Hakupäivä 3.10.2015.

55. ENCELIUM - seuraavan sukupolven valonohjausta. 2015. OSRAM GmbH. Saatavissa: http://www.osram.fi/osram_fi/uutiset--tiedot/valonsaeaetoejaerjestelmae/tuotetiedot/encelium/index.jsp. Hakupäivä 3.10.2015.

56. Helvar reititinjärjestelmät. 2011. Helvar Oy Ab. Saatavissa: http://www.helvar.fi/sites/default/files/RouterSystems_web_FI.pdf. Hakupäivä 10.10.2015.

57. uSee Selainpohjainen Käyttöliittymä. 2013. Helvar Oy Ab. Saatavissa: http://www.helvar.fi/sites/default/files/uSeeBrochure_Finn.pdf. Hakupäivä 10.10.2015.

58. Valaistusjärjestelmien sovellukset. 2014. Helvar Oy Ab. Saatavissa: http://www.helvar.fi/sites/default/files/application_brochure_2014_FI_WEB.pdf. Hakupäivä 10.10.2015.

LÄHTÖTIETOMUISTIO

Työn tiedot	Tekijä[1] Eemeli Kyröläinen	Tilaaja[2] Greenled Oy
	Tilaajan yhdyshenkilö ja yhteystiedot[3] Ville Moilanen, [redacted]	
	Työn nimi[4] **Valaistuksen ohjausjärjestelmien tietoturvallisuus**	
	Työn kuvaus[5] Opinnäytetyön aiheena on valittujen valaistuksenohjausjärjestelmien tietoturvallisuus. Työssä käydään läpi ohjausjärjestelmien tietoturvallisuutta ja kartoitetaan kahden järjestelmän tilanne viestintäviraston yms. ohjeiden perusteella. Kartoituksen pohjalta tehdään Greenled Oy:lle sisäinen ohjeistus miten riittävä tietoturvallisuuden taso saavutetaan ja miten sitä voidaan parantaa.	
	Työn tavoitteet[6] - Nykytilan kartoitus valaistuksen ohjausjärjestelmien tietoturvallisuudesta. - Tutustutaan kilpailijoiden tuotteisiin. - Tutustutaan viranomaismääräyksiin ja standardeihin. - Selvitetään tulevaisuuden näkymät tietoturvallisuus osalta. - Kartoitetaan Greenled Oy:n valaistuksen ohjauspalveluiden tietoturvallisuus. - Luodaan valaistuksen ohjauspalveluiden tietoturvakäytänteet ja -ohjeistus Greenled Oy:n sisäiseen käyttöön.	
	Tavoiteaikataulut[7] - Opinnäytetyö on valmis 31.12.2015.	
	Päiväys ja allekirjoitukset[8] 14/8/2015 Tekijän allekirjoitus Eemeli Kyröläinen	14/8/2015 Tilaajan allekirjoitus Ville Moilanen

1. Tekijän nimi, puhelinnumero ja sähköpostiosoite.
2. Työn teettävän yrityksen virallinen nimi.
3. Sen henkilön nimi ja yhteystiedot, joka yrityksessä valvoo työn suoritusta.
4. Työn nimi voi olla tässä vaiheessa työnimi, jota myöhemmin tarkennetaan.
5. Työ kuvataan lyhyesti. Siinä esitetään muun muassa työn tausta, lähtötilanne ja työssä ratkaistavat ongelmat.
6. Esitetään lyhyesti ja selvästi työn tavoitteet.
7. Esitetään projektin tavoiteaikataulu. Silloin, kun työllä on välitavoitteita, myös ne merkitään aikatauluun. Tavoiteaikataulun ja oppilaitoksen yleisaikataulun perusteella tekijä laatii oman aikataulunsa.
8. Lähtötietomuistio päivätään ja sen allekirjoittavat tekijä ja tilaajan yhdyshenkilö