Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Timo Laakso ja Pasi Savolainen

Kyberturvallisuuden huomioiminen älyrakennuksen suunnitteluvaiheessa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

13.5.2019

Tekijät Otsikko Sivumäärä Aika	Timo Laakso, Pasi Savolainen Kyberturvallisuuden huomioiminen älyrakennuksen suunnitteluvaiheessa 66 sivua 13.5.2019
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	Tietoverkot ja sovellukset
Ohjaaja	Lehtori Erik Pätynen

Insinöörityön tarkoituksena oli tutkia älyrakennuksiin ja sen tietojärjestelmiin kohdistuvia uhkakuvia sekä suunnitella kattavat yleistason ohjeet sille, mitä ja minkälaisia kontrolleja älyrakennuksen toteuttamishankkeessa suunnitteluvaiheessa tulisi määrittää, jotta riskit ja uhkakuvat huomioiden varmistetaan kyberturvallinen ja älykäs rakennusympäristö.

Työ toteutettiin parityönä, jossa työnjako ja vastuut jaettiin tasaisesti molempien tekijöiden kesken. Insinöörityön kohderyhmänä ovat tieto- ja viestintätekniikan sekä kiinteistö- ja rakennusalan ammattilaiset, kuten suunnittelijat, toteuttajat ja rakennusten ylläpitäjät. Myös muut tahot, kuten rakennusten omistajat hyötyvät insinöörityöstä ja sen tuloksista.

Insinöörityö rajattiin koskemaan älyrakennuksiin kohdistuvien uhkakuvien tutkintaa sekä sitä, kuinka kyberturvallisuus tulee suunnitteluvaiheessa huomioida, jotta älyrakennuksen toteuttamis- ja ylläpitovaiheessa vältytään mahdollisilta uhkakuvien aiheuttamilta vahingoilta. Työn laadinnassa ei otettu konkreettisella tasolla kantaa siihen, kuinka älyrakennus toteutetaan tai kuinka sitä ylläpidetään.

Työn alussa tutkittiin ja selvitettiin, mitä ja minkä tyylisiä mahdollisia älyrakennuksiin kohdistuvia kyberhyökkäysskenaarioita on mahdollista toteuttaa ja mihin niitä on mahdollista kohdistaa. Tutkimustulosten pohjalta saatiin tarkka käsitys siitä, miten haavoittuvaisia rakennusten älykkäät ratkaisut ovat ja kuinka laajaa tuhoa kyberhyökkäyksillä on mahdollista aiheuttaa. Näiden tutkimustulosten pohjalta suunniteltiin yleistason ohjeet niille kontrolleille, joita sovelletaan älyrakennuksen toteutus- ja ylläpitovaiheissa.

Insinöörityön edetessä todettiin, että kyberturvallisuutta käsittelevää sekä älyrakennuksia käsittelevää materiaalia tuotetaan, mutta älyrakennusten kyberturvallisuutta käsittelevää materiaalia ei ole suomen kielellä tuotettu lähes laisinkaan.

Useimpien älylaitteiden suunnittelussa jätetään kyberturvallisuus huomioimatta kokonaan, jonka seurauksena uhkakuvat kyberhyökkäyksille lisääntyvät. Tulosten perusteella voitiin päätellä, että tämän kaltaiselle työlle on kysyntää.

Avainsanat	älyrakennus, älykäs, rakennus, kyberturvallisuus, kyber, IoT

Authors Title Number of Pages Date	Timo Laakso, Pasi Savolainen Cybersecurity in the Planning Phase of a Smart Building 66 pages 13 May 2019
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Professional Major	Communication Networks and Applications
Instructor	Erik Pätynen, Senior Lecturer

The purpose of this thesis was to research and identify potential risks and threats facing smart buildings and smart systems, and then plan comprehensive, general and cybersecure guidelines for smart building implementation and building phases.

The information and guidelines provided in this thesis are directed to professionals who work in the field of real estate, building, construction or information and communication technology. The thesis can also be useful for other people, such as building owners.

At the beginning of this project, the thesis was defined to concern the research of potential risks and threats, and then plan how to manage these risks and threats when implementing and designing smart building solutions. The implementation and administration phases were not part of this thesis.

The research results revealed how vulnerable the embedded systems in smart buildings are and how severe damage can be caused in case the smart systems are accessed without permission or if attempted cyberattacks are successful. The research results also showed that there is nearly no information in Finnish where cybersecurity and smart buildings are covered together as one solution. It can be concluded that there is a huge need for this kind of work.

Keywords	smart, building, cybersecurity, cyber, security, IoT

Sisällys

Lyhenteet ja käsitteet

1 Johdanto 1

2 Älyrakennukset 5

2.1 Mikä on älyrakennus? 5
2.2 Älyrakennuksen ekosysteemi 7
2.2.1 Rakennusautomaatio ja kiinteistönhallintajärjestelmä 9
2.2.2 Anturit ja aktuaattorit 10
2.2.3 Tietoverkot ja tiedonsiirto 12
2.2.4 Integraatiot 15
2.2.5 Big data ja data-analytiikka 15
2.3 Älyrakennuksen ominaisuudet ja käyttäjän vuorovaikutus 17
2.4 Älyrakennus ja älykäs kaupunkiympäristö 19

3 Kyberturvallisuus 20

4 Älyrakennuksen uhkaympäristö 23

5 Älyrakennuksen suunnittelu- ja rakennusprosessi 31

5.1 Tarveselvitys 34
5.2 Hankesuunnittelu 34
5.3 Hankinta-aineistojen laatiminen 35
5.4 Toteutussuunnittelu 35
5.5 Rakentaminen, valvonta ja laadun varmistus 36
5.6 Käyttö ja ylläpito 37
5.7 Purku ja poisto 37

6 Älyrakennuksen kyberturvallisuus 38

6.1 Vaatimustenmukaisuus 38
6.2 Sisäänrakennettu kyberturvallisuus ja tietosuoja 38
6.3 Omaisuuden hallinta ja ympäristön kuvaaminen 39
6.4 Laiteturvallisuus 40

6.5 Vikaturvallisuus ja vikasietoisuus 42
6.6 Päivitysten hallinta 43
6.7 Pääsynhallinta 44
6.8 Salaus 46
6.9 Tietoverkko 47
6.10 Sovellusten turvallisuus 49
6.11 Syötteen- ja ulostulonhallinta 51
6.12 Valvonta ja havainnointikyky 52
6.13 Testaus ja katselmoinnit 53
6.14 Elinkaaren päättymiseen varautuminen 54
6.15 Haavoittuvuuksien hallinta 55
6.16 Jatkuvuudenhallinta 55
6.17 Kolmansien osapuolien hallinta 58
6.18 Fyysinen turvallisuus 58
7 Yhteenveto 60
Lähteet 62

Lyhenteet ja käsitteet

ACEEE	American Council for an Energy-Efficient Economy. Yhdysvaltalainen energiatehokkuutta edistävä järjestö.
Alexa	Yhdysvaltalaisyritys Amazonin kehittämä tekoälyä hyödyntävä puheentunnistus-, puhehaku- ja puheohjausratkaisu.
API	Application Programming Interface. Ohjelmointirajapinta, joka sallii useiden eri sovellusten keskinäisen kommunikoinnin.
BIA	Business Impact Analysis. Toiminnanvaikutusanalyysi, jolla arvioidaan riskien vaikutusta yrityksen tai rakennuksen käyttäjien ydin- ja liiketoimintaan.
Big Data	Massiivinen määrä tietojärjestelmien tuottamaa analysoitavaa ja hyödynnettävää tietoa.
Bluetooth	Radiotekniikkaa hyödyntävä lyhyen kantaman langaton tiedonsiirtotekniikka.
BMS	Building Management System. Kiinteistönhallintajärjestelmä, jonka kautta hallinnoidaan älyrakennuksen rakennusautomaatiota.
Bottiverkko	Haittaohjelmien avustuksella haltuun otettu useista haavoittuvista tietojärjestelmistä koostuva toisiinsa kytkeytynyt tietojärjestelmien joukko.
Brute-force	Väsytyshyökkäys. Hyökkäystekniikka, jonka tarkoituksena on manuaalisesti tai tietojärjestelmien avulla löytää tietojärjestelmän oikea salasana.
CIA	Confidentiality, Integrity, Availability. Tiedon luottamuksellisuutta, eheyttä ja saatavuutta kuvaava tietoturvakolmio.
CPU	Central Processing Unit. Tietokoneohjelmiston konekielisiä käskyjä suorittava tietojärjestelmän prosessori.

DBIR	Data Breach Investigation Report. Vuosittain julkaistava tietomurtotutkimus.
DDoS	Distributed Denial of Service. Hajautettu palvelunestohyökkäys, jossa yritetään lamaannuttaa kohdejärjestelmä useasta eri lähteestä toimitettavan tietoliikenteen avulla.
Domain	Verkkotunnus. Tietojärjestelmän helposti luettava osoite Internetissä.
DoS	Denial of Service. Palvelunestohyökkäys, jolla pyritään vaikuttamaan tiedon saatavuuteen.
DR	Disaster Recovery. Toipumissuunnitelma, jolla varmistetaan tietojärjestelmän normaali toiminta häiriötilanteen jälkeen.
EOL	End-of-life. Tietojärjestelmän tai muun fyysisen objektin elinkaaren päättyminen.
Firmware	Laiteohjelmisto. Tietoteknisen laitteen perustoiminnoista huolehtiva, kiinteästi laitteeseen asennettu sovellus tai osa.
HA	High Availability. Korkea käytettävyys, jonka tarkoituksena on mahdollistaa tietojärjestelmän jatkuva ja häiriötön käyttö.
I/O	Input/Output. Siirräntä, jolla tarkoitetaan tietojärjestelmien välistä tiedon siirtämistä.
IAM	Identity and Access Management. Identiteetin ja pääsynhallinta.
IDS	Intrusion Detection System. Tunkeilijan havaitsemisjärjestelmä, joka havaitsee tietojärjestelmiin kohdistuvat hyökkäysyritykset.
IoT	Internet of Things. Esineiden Internet käsittää laitteet, joiden tietoja voidaan lukea tai ohjata tietoverkkojen välityksellä.

IP	Internet Protocol. Verkkokerroksella toimiva protokolla, joka huolehtii tietoliikennepakettien välittämisestä vastaanottajalle.
IPS	Intrusion Prevention System. Murron estämisjärjestelmä, joka estää tietojärjestelmiin kohdistuvat hyökkäysyritykset.
IPsec	Internet Protocol Security. Verkkokerroksella toimiva protokolla, joka huolehtii salauksesta, osapuolten autentikoinnista ja tiedon eheydestä.
JEA	Just Enough Administration. Menetelmä, joka sallii vain juuri toimenpiteisiin tarvittavan määrän oikeuksia hallintatunnusten käytölle.
JIT	Just in Time Administration. Menetelmä, jolla pyritään myöntämään hallintaoikeuksia vain silloin, kun niitä tarvitaan ja vain hetkellisesti.
Kapselointi	Toiminto, jossa kootaan tietoa tai eri toimintoja yhdeksi kokonaisuudeksi.
Konsoli	Komentoliittymä, jonka kautta syötetään tekstipohjaisia komentoja tietojärjestelmään.
LVI	Lämpö, Vesi, Ilma. LVI-järjestelmät ovat osa talotekniikkaa.
Malware	Haittaohjelma, tietokoneohjelma, jonka tarkoituksen on tahallisesti aiheuttaa vahinkoa kohteensa tietojärjestelmiin.
MITM	Man-In-The-Middle. Hyökkäystapa, jossa ohjataan tai kuunnellaan kahden tai useamman osapuolen välistä tietoliikennettä.
OSI-malli	Open System Interconnection model. Tietoliikenteen arkkitehtuurin kuvaamiseen kehitetty viitemalli.
OWASP	Open Web Application Security Project. Avoin verkkoyhteisö, joka julkaisee artikkeleita, ohjeita ja työkaluja tietojärjestelmien suojaamista varten.
Pino	Tietojenkäsittelykäsite, joka toimii periaatteella viimeiseksi sisään, ensimmäisenä ulos.

Puskuri	Muisti, jota tietojärjestelmä tarvitsee aloittaessaan toimintansa.
RFID	Radio Frequency Identification. Radiotaajuinen tunnistus.
Root	Juuri, korkeimman mahdollisen käyttäjätason käyttöoikeudet.
Rootkit	Piilohallintaohjelma, joka asentuu onnistuneen hyökkäyksen yhteydessä kohdetietojärjestelmään.
RPO	Recovery Point Objective. Tavoiteltu tietojärjestelmän toipumispiste.
RS232	Recommended Standard 232. Tietoliikenneportti kahden tietokoneen väliseen tietoliikenteeseen.
RTO	Recovery Time Objective. Tavoiteltu tietojärjestelmän toipumisaika.
SE	Security Element. Turvaelementti, jonka avulla pystytään suojaamaan ja säilömään arkaluontoista tietoa.
SIEM	Security Information and Event Management. Tietoturvatietojen ja -tapahtumienhallinta. Kerää, tallentaa ja hyödyntää jonkin järjestelmän tapahtumatietoja.
SQL-injektio	Structured Query Language -injektio. Hyökkäystapa, jossa SQL-komentojen avulla hyödynnetään tietojärjestelmien haavoittuvuuksia.
Takaportti	Hyökkäystapa, jossa kohdetietojärjestelmään päästään käsiksi ohittamalla normaali todennusprosessi.
TCB	Trusted Computing Base. Turvallisen ja luotettavan tietojenkäsittelyn varmistava rakenne. Laitteisto ja käyttöjärjestelmä muodostavat TCB-pohjan.
TCP/IP	Transmission Control Protocol / Internet Protocol. Tietoverkkoliikenteessä käytettävä tietoliikenneprotokolla.
TEE	Trusted Execution Environment. Luotettu ohjelmistokoodien ajoympäristö.

TLS	Transport Layer Security. Salausprotokolla, joka varmistaa turvallisen tietoliikenteen tietoa siirrettäessä.
UEBA	User and Entity Behavioral Analytics. Käytönvalvontaan ja havainnointiin tarkoitettu koneoppimisjärjestelmä.
Varjo-IT	Shadow IT. Organisaatiossa käytössä tai kehitteillä olevat hyväksymättömät ja keskitetyn hallinnan ulkopuolella olevat tietojärjestelmät ja laitteet.
Web	World Wide Web. Käytetään nimitystä Web, tietoverkoissa toimiva hypertekstijärjestelmä.
WLAN	Wireless Local Area Network. Langaton lähiverkko on tietoverkkotekniikka, jossa tietojärjestelmät kommunikoivat toistensa kanssa langattomasti.
VLAN	Virtual Local Area Network. Virtuaalilähiverkko on tietoverkkotekniikka, jossa tietoverkko voidaan segmentoida useisiin osiin.
Volatile	Haihtuva muisti on tietokoneiden hyödyntämää muista, joka menetetään, mikäli tietokone menettää käyttövirtansa.
VPN	Virtual Private Network. Virtuaalinen erillisverkko, jossa tietoverkkoliikenne on salattu ja suojattu.

1 Johdanto

Digitalisaatio on yksi tämän hetken megatrendeistä ja vaikuttaa kaikkiin toimialoihin. Se on myös tulevaisuuden elinehto toimialasta riippumatta. Tämä kehitys näkyy myös kiinteistö- ja rakennustoimialalla, missä älyrakennukset ja älyrakentaminen kehittyvät jatkuvasti ja tulevat yhä enemmän osaksi päivittäistä arkea.

Älyrakennuksissa tavoitteena on tunnistaa rakennusten käyttäjien tarpeet paremmin sekä luoda tehokkaammin ja ennustettavimmin toteutettava rakennusten ylläpito ja hallinta. Pelkän teknologian ja suuren datamäärän avulla rakennuksesta ei tule vielä älykästä, vaan siihen tarvitsee kehittää oikeat toiminnallisuudet, jotka tuottavat tavoitellun hyödyn. Hyötynä ovat muun muassa paremmat ja yksilöllisemmät käyttäjäkokemukset, automatisoitu ja ennustettavaempi ylläpito sekä ekologisuus ja kustannustehokkuus.

Uusien teknologioiden ja ratkaisujen käyttö muodostaa myös uudenlaisia riskejä, joihin täytyy varautua asianmukaisin suojauskeinoin. Käyttäjälähtöisemmän ja paremmin hallittavan älykkään rakennuksen suunnittelussa ja toteutuksessa on siis myös kyettävä tunnistamaan ja ymmärtämään muuttuvasta toimintaympäristöstä syntyvät riskit ja määrittää, kuinka niitä tulee hallita.

Toimialalla on suuri potentiaali kehitykselle, ja se on muodostumassa myös välttämättömyydeksi. Teknologian tuomiin valtaviin mahdollisuuksiin liittyy kuitenkin myös merkittäviä riskejä, jotka ovat monessa tapauksessa myös realisoituneet maailmalla ja Suomessa, kun älyrakennuksiin liittyviä riskejä ei ole hallittu eikä niiden kyberturvallisuus ole ollut asianmukaisella tasolla. Tähän liittyville periaatteille ja ohjeille on välitön tarve, jotta älyrakennusten tuomat hyödyt saadaan tuotua turvallisesti osaksi yhteiskunnan, kaupunkien ja rakennusten kehittymistä osana toimialan digitalisoitumista.

Älyrakennusten kyberturvallisuus on aihe, joka on noussut esiin, mutta siitä ei vielä ole laadittu kattavia periaatteita ja ohjeita tai insinööritöitä. Nykytilanteessa älyrakennuksia koskevaa kirjallisuutta ja yleisohjeita on syntynyt hieman, mutta niissä vain sivutaan kyberturvallisuutta. Vastaavasti kyberturvallisuuteen tai fyysiseen turvallisuuteen liittyvissä ohjeissa ei oteta suoraan kantaa älyrakennusten kontekstiin.

Insinöörityö on tutkimus- ja suunnittelutyö, joka toteutetaan parityönä. Työnjako ja vastuut on jaettu tasan molempien kirjoittajien kesken. Insinöörityössä tutkitaan älyrakennuksiin kohdistuvia riskejä sekä mahdollisia uhkakuvia sekä selvitetään, minkälaisia ja minkä tyylisiä mahdollisia hyökkäysskenaarioita älyrakennuksiin ja sen tietojärjestelmiin on mahdollista toteuttaa. Näiden tutkimustulosten pohjalta suunnitellaan ja luodaan selvä prosessi ja yleistason ohjeet sille, miten kyberturvallisuus huomioidaan osana älyrakennusten suunnittelu- ja toteutusprojekteja.

Tutkimukselle luodaan hyvä pohja, kun tutkijan tekemät valinnat ovat yhteensopivia neljällä tasolla: ongelmanasettelun tasolla, tieteenfilosofian tasolla, tutkimusstrategisella tasolla ja teoreettisen ymmärtämisen tasolla. Seuraavassa käydään läpi tämän insinöörityön osalta näitä valintoja kyseisillä neljällä tasolla. [Hirsjärvi ym. 2003: 111-112.]

Ongelman asettelun taso

Ongelman asettelun tasolla pohditaan, kuinka täsmällisesti tutkimusongelma voidaan nimetä ja miten jäsentää sekä muotoilla selvästi ja ymmärrettävästi. Tutkimuksen ongelmien tulisi olla tarkkaan harkittuja ja muotoiltuja jo ennen aineiston keruuseen ryhtymistä. Kvalitatiivisessa tutkimuksessa on kuitenkin huomioitava, että ennakkohypoteesit tai tutkimukselliset kysymykset saattavat muuttua tutkimuksen edetessä. Joka tapauksessa tulee kuitenkin olla aina jonkinlainen käsitys tutkimuksen ongelman tai tutkimuskysymyksen asettelusta ohjaamassa tutkimuksen toteuttamista. Pääongelmalle voidaan myös asettaa osa- tai alaongelmia. Näistä pääongelma on usein yleisluontoinen kysymys, jolla hahmotetaan koko tutkittavaa kokonaisuutta, kun alaongelmien vastauksilla mahdollistetaan vastaamista pääongelmaan. [Hirsjärvi ym. 2003: 113-116.]

Tämän insinöörityön tehtävänä on tunnistaa älyrakennuksiin liittyviä kyberuhkia ja määrittää älyrakennusten suunnitteluvaiheessa huomioitavia suojauskeinoja, joiden avulla keskeisiin uhkiin voidaan varautua. Työn keskeisenä tavoitteena ja tutkimusongelmana on ”*Miten älyrakennuksiin liittyvät kyberturvallisuusriskit huomioidaan osana rakennusten suunnittelua ja toteutusta?”* Kyseiselle tutkimusongelmalle tai tutkimuskysymykselle voidaan muodostaa seuraavat alakysymykset:

- Miten määritetään älyrakennus?
- Millaisia kyberuhkia älyrakennuksiin kohdistuu?
- Millaisia suojauskeinoja älyrakennuksen suunnitteluvaiheessa tulee huomioida, jotta se toteutetaan kyberturvalliseksi?

Tieteenfilosofinen taso

Tieteenfilosofia toimii tutkimusstrategian ja aineistonhankinnan taustana ja on keskeisenä osana tutkimuksen tekemistä. Tieteenfilosofian tasolla määritetään ontologinen kysymys eli miten tutkittava kohde ja todellisuus ymmärretään sekä epistemologinen kysymys eli miten ajatellaan saatavan tietoa. Näitä suuntauksia voidaan pitää tieteellisen ajattelun lähtökohtina ja niissä käsitys tiedon ja todellisuuden luonteesta eroaa toisistaan. [Hirsjärvi ym. 2003: 112, 117-119; Lähdesmäki ym.]

Tämän insinöörityön ontologia pohjaa subjektiivisen tiedontulkinnan käsitykseen, jossa tutkittava kohde sekä siihen liittyvät tekijät mielletään muodostuvaksi ihmisten subjektiivisista käsityksistä. Insinöörityön tekijät myös tulkitsevat kohdetta ja siihen liittyvää teoriaa muodostaen ratkaisuja omasta subjektiivisesta näkökulmastaan. Tieto-opillisesti insinöörityötä lähestytään interpretivismin kautta. Interpretivismi korostaa tulkinnallisuutta ja tulkintoja tiedon tuottamisessa. Tutkimuksessa tuotetaan siis tuloksia tulkitsemalla hankittua tietoa ja muodostamalla siitä uusia malleja. [Lähdesmäki ym.]

Tutkimusstrategian taso

Tutkimusstrategialla tarkoitetaan tutkimuksessa käytettyjen menetelmällisten ratkaisujen kokonaisuutta, ja sen alakäsitteinä ovat tutkimusmetodit. Tutkimuksen strategia ja siihen kuuluvien yksittäisten metodien valinta riippuu tutkimuksen tavoitteesta ja sille asetetusta tutkimusongelmasta. Strategia ohjaa menetelmien valintaa ja siinä on kyse niistä periaatteista, joilla tutkimus on tarkoitus toteuttaa. [Hirsjärvi ym. 2003: 112, 117-119; Lähdesmäki ym.]

Tämä insinöörityöprosessi pohjaa teoreettiseen tutkimusotteeseen, jossa pyritään hahmottamaan ja muodostamaan malleja, selityksiä ja rakenteita aiemman tutkimuskirjallisuuden ja tiedon pohjalta. Olemassa olevaa kyberturvallisuuteen ja uusiin teknologioihin liittyvää tutkimusta ja tietoa hyödynnetään älyrakennusta koskevien kyberturvallisuuteen liittyvien mallien muodostamisessa.

Teoreettisen ymmärtämisen taso ja teoreettinen viitekehys

Teoreettisen ymmärtämisen tasolla pohditaan tutkimuksen aiheeseen liittyviä teorioita sekä niiden ja tutkimuksen suhdetta, käsitellään tutkimuksen avainkäsitteitä ja niiden määrittelyä sekä pohditaan mahdollisten hypoteesien asettamisen tarpeellisuutta ja tarvittaessa asetetaan niitä. [Hirsjärvi ym. 2003: 112.]

Tämän insinöörityön keskeisimpiä käsitteitä ovat älyrakennukset ja niiden suunnittelu, kyberturvallisuus, riskienhallinta sekä tekniset ja hallinnolliset suojakeinot. Keskeisinä lähteinä hyödynnetään tunnettuja ja vakiintuneita kontrolliviitekehyksiä ja ohjeita sekä muita keskeisiä kyberturvallisuuteen liittyviä malleja, jotka ovat sovellettavissa älyrakennusten kontekstiin.

Insinöörityön tarkoituksena on tarjota rakennuksia suunnitteleville ja toteuttaville sekä myös käyttäville ja ylläpitäville tahoille periaatteita ja ohjeita, joiden avulla uusia teknologioita voidaan ottaa käyttöön riskit huomioiden, jotta näiden teknologioiden tuomat hyödyt saadaan käyttöön mahdollisimman tehokkaasti ja turvallisesti. Insinöörityö on älyrakennusten kyberturvallisuutta ilmiönä kuvaileva ja tähän liittyviä ratkaisuja kartoittava työ. Sen tavoitteena on kuvata älyrakennuksia ilmiönä sekä nostaa esiin periaatteita ja keinoja, joiden avulla älyrakennusten kanssa toimivat organisaatiot voivat osaltaan hallita niihin liittyviä kyberturvallisuusriskejä hyväksyttävälle tasolle.

2 Älyrakennukset

2.1 Mikä on älyrakennus?

Kaupungistuminen on ollut viime vuosina nopeaa. Vuonna 2018 jo noin 55 % maailman väestöstä asui kaupunkialueilla ja Yhdistyneiden kansakuntien tekemän arvion mukaan 68 % maailman väestöstä asuu kaupunkialueilla vuoteen 2050 mennessä. [68% of the world population projected to live in urban areas by 2050, says UN 2018.] Tämä tarkoittaa sitä, että rakennusten on nyt ja jatkossa pystyttävä toimimaan entistä tehokkaammin, jotta pystytään täyttämään rakennusten nykyisten ja tulevien käyttäjien tarpeet.

Rakentaminen on enenevissä määrin muuttunut kohti älykkäämpää suuntaa. Sille, mikä tekee rakennuksesta älykkään, ei ole mitään tarkkaa määrittelyä tai sääntöä. Jokainen rakennus on erilainen ja palvelee käyttäjiään eri tavalla, minkä vuoksi myös älykkyyden määrittely vaihtelee. Älyrakennuksen yhtenä määritelmänä voidaan pitää rakennusta, jonka tietojärjestelmät ja toiminnot on integroitu toiminaan yhtenä kokonaisuutena palvellen rakennuksen käyttäjiä mahdollisimman käyttäjälähtöisesti ja kustannustehokkaasti heidän tarpeidensa mukaisesti. [Improving Performance with Integrated Smart Buildings 2012: 2.]

Rakennusten omistajien, hallinnoijien ja käyttäjien vaatimukset ovat viime vuosina lisääntyneet. Omistajat vaativat rakennuksilta kustannustehokkuutta, jotta kulut saadaan minimoitua ja tuotto maksimoitua. Rakennuksia hallinnoivat tahot kuten esimerkiksi isännöitsijät vaativat rakennuksilta mahdollisimman keskitettyä ja automaattista toimintaa, jotta rakennusten hallinnoinnista saadaan tehokasta. Rakennusten käyttäjät kuten esimerkiksi työntekijät haluavat mahdollisimman paljon tietoa työskentelytiloistaan, esimerkiksi mistä löytää vapaa työskentelypiste, millä työskentelypisteellä on paras ilmanlaatu tai mistä löytää mahdollisimman rauhallinen tila tehdä työtä. Nämä kaikki lisääntyneet vaatimukset ovat lisänneet tarvetta uusille antureille ja IoT-laitteille (*IoT, Internet of Things*). [Talon & Goldstein 2015: 3-4.]

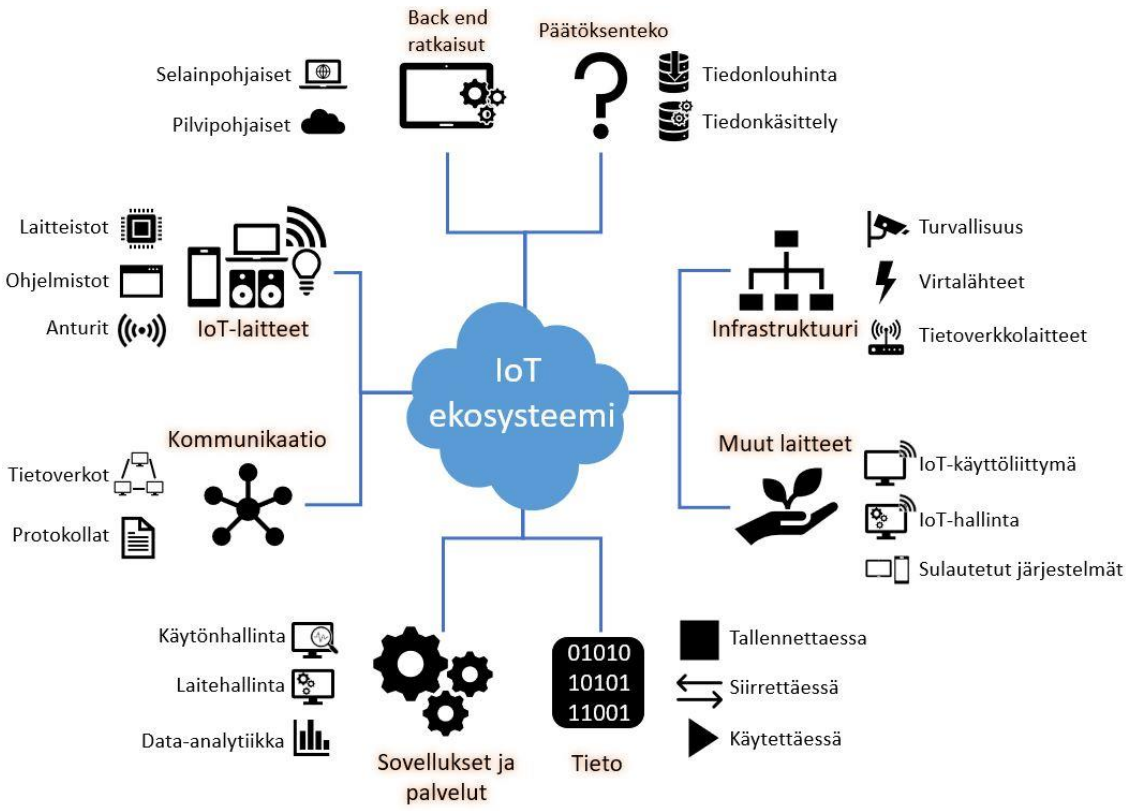
Yhdysvalloissa on älyrakentamisessa hyödynnetty jo useamman vuoden ajan puheohjauksen tuomia mahdollisuuksia. Sitä on käytetty lähinnä älykoteihin liittyvissä toteutuksissa, mutta viime aikoina puheohjauksen tuomia mahdollisuuksia on alettu hyödyntämään laajemminkin älyrakennuksissa toteuttaen isompia kokonaisuuksia interaktiivisemmiksi esimerkiksi Amazonin Alexa -puheohjauksella. [Amazon Partner with Marriott Hotels to Launch Alexa for Hospitality 2018.] Puheohjattavissa älyrakennuksissa rakennuksen tietojärjestelmiä ja toimintoja ohjataan pelkän puheen avulla. Käyttäjä voi esimerkiksi pyytää Alexaa ohjaamaan älyrakennuksen valaistusta tai lämpötilaa. Myös mahdollisten huoltotoimenpiteiden tilaukset onnistuvat puheohjauksen kautta. Puheohjattavien älyrakennusten pääasiallisena tarkoituksena on tehostaa käyttäjien toimintaa ja parantaa älyrakennuksen kustannustehokkuutta. [Verma 2019.]

Antureiden sekä muiden IoT-laitteiden lisääntyminen on viime vuosina ollut nopeaa. Kansainvälisen tieto- ja viestintätekniikan alan tutkimusyhtiö Gartnerin arvion mukaan IoT-laitteiden lukumäärä tulee vuonna 2020 ylittämään 20 miljardin rajapyykin, joka on yli kolme kertaa enemmän kuin vuonna 2016. Huomionarvoista on myös se, että tässä arviossa ei ole huomioituna tietokoneita, älypuhelimia tai tabletteja. [What makes a building ”smart” and why does it matter? 2018: 3.]

Älyrakennuksen tulisi kokonaisuutena olla sellainen, että se palvelee rakennuksen käyttäjiä ja omistajia mahdollisimman kustannustehokkaasti ja käyttäjälähtöisesti. Käyttäjälähtöinen älyrakennus toimii reaktiivisesti, eli se on vuorovaikutuksessa rakennuksen käyttäjän kanssa ja se pystyy reagoimaan käyttäjiinsä yksilöllisesti. Älyrakennuksella on kyky reagoida käyttäjien yleisiin ja toistuviin käyttäytymismalleihin ja toimia näiden käyttäytymismallien mukaisesti esimerkiksi säätämällä valaistusta ja lämpötilaa huoneeseen saapuvan henkilön preferenssien mukaiseksi automaattisesti. Älykkäässä rakennuksessa on otettu käyttäjien kasvavat tarpeet huomioon, jotta esimerkiksi mukavuus, turvallisuus, taloudellisuus ja energiatehokkuus on saatu toteutettua mahdollisimman tehokkaasti. [Rantala ym. 2015: 20.]

2.2 Älyrakennuksen ekosysteemi

Tavallisen rakennuksen ekosysteemillä tarkoitetaan koko sitä kokonaisuutta, joka muodostuu rakennuksen talotekniikasta, tietojärjestelmistä ja palveluista. Rakennuksen taloteknisiä järjestelmiä ovat esimerkiksi lämmitys- ja jäähdytysjärjestelmät, ilmastointijärjestelmät, valaistusratkaisut ja energian tuottojärjestelmät. Digitalisaation vahvan yleistymisen myötä myös IoT-ratkaisut ovat tulleet osaksi rakennuksen ekosysteemiä. IoT-ratkaisut mahdollistavat osaltaan älykkäämpien rakennusten toteuttamista. IoT-laitteiden ja osajärjestelmien integraatioilla mahdollistetaan muun muassa pienemmät energiankulutukset ja -kustannukset, pienemmät hiilidioksidipäästöt sekä osajärjestelmien itsenäiset ja älykkäät toiminnat. [Rantala ym. 2015: 37; Baseline Security Recommendations for IoT 2017: 18.]



Kuva 1. IoT:n ekosysteemi [Baseline Security Recommendations for IoT 2017: 26].

Kuvassa 1 on esitettynä IoT:n ekosysteemi, joka on osa koko älyrakennuksen ekosysteemiä. Kuva 1 havainnollistaa, kuinka IoT käsitteenä koostuu useista kriittisistä sekä

vähemmän kriittisistä kokonaisuuksista. Seuraavassa käydään lävitse IoT:n ekosysteemin tärkeimpiä elementtejä. [Baseline Security Recommendations for IoT 2017: 18.]

- Esineiden Internetin esineet (*Things in the IoT*). IoT:n ympäristössä esine on fyysinen tai virtuaalinen objekti, joka pystytään tunnistamaan tai integroimaan osaksi tietoverkkoja. Tämä on välttämätöntä, jotta esineet pystyvät vaihtamaan tietoja keskenään tietoverkkojen ja pilvipalveluiden ylitse. Esineillä voi olla myös muita vaihtoehtoisia toimintoja. Ne voivat esimerkiksi aistia, tallentaa, käsitellä ja siirtää tietoa. IoT:n esineitä pystytään hallitsemaan ja tarkkailemaan jonkin älykkään tietojärjestelmän kautta. [Baseline Security Recommendations for IoT 2017: 19.]

- Älykäs päätöksenteko on ominaisuus, jossa tehdyt päätökset riippuvat ensisijaisesti siitä, mitä ja minkälaista tietoa on saatavilla. Nämä päätökset voivat yksinkertaisimmillaan olla vain raja-arvopoikkeamiin reagoivia valmiiksi määritettyjä reaktioita tai hyvin edistyneitä kone- ja syväoppimiseen perustuvia järjestelmiä. Päätösten tulokset johtavat lopulta toimenpiteisiin, jotka tarjoavat uutta tietoa IoT:n ekosysteemin eri elementeille. [Baseline Security Recommendations for IoT 2017: 19.]

- Anturit ja aktuaattorit ovat avainasemassa IoT:n ekosysteemissä. Anturit ovat integroituja elementtejä, joiden avulla IoT-laitteet pystyvät tarkkailemaan ja aistimaan ympäristössä tapahtuvia muutoksia. Ne voivat kooltaan olla vain muutamia millimetrejä, minkä ansiosta niitä on helppo sulauttaa osaksi fyysisiä objekteja. Fyysisellä tasolla anturit voivat mitata määriteltyjä fyysisiä, kemiallisia tai biologisia indikaattoreita. Digitaalisella tasolla anturit pystyvät keräämään tietoja tietoverkoista ja sovelluksista. Aktuaattorit eli toimilaitteet toimivat käänteisesti. Ne keräävät tietoa antureilta ja muuttavat tämän digitaalisen tiedon joksikin fyysiseksi toimenpiteeksi. [Baseline Security Recommendations for IoT 2017: 19-20.]

- Antureiden ja aktuaattoreiden lisäksi IoT-laitteet voivat olla sulautettuna myös älyrakennuksen tietojärjestelmiin. Tällaisia sulautettuja ratkaisua ovat esimerkiksi

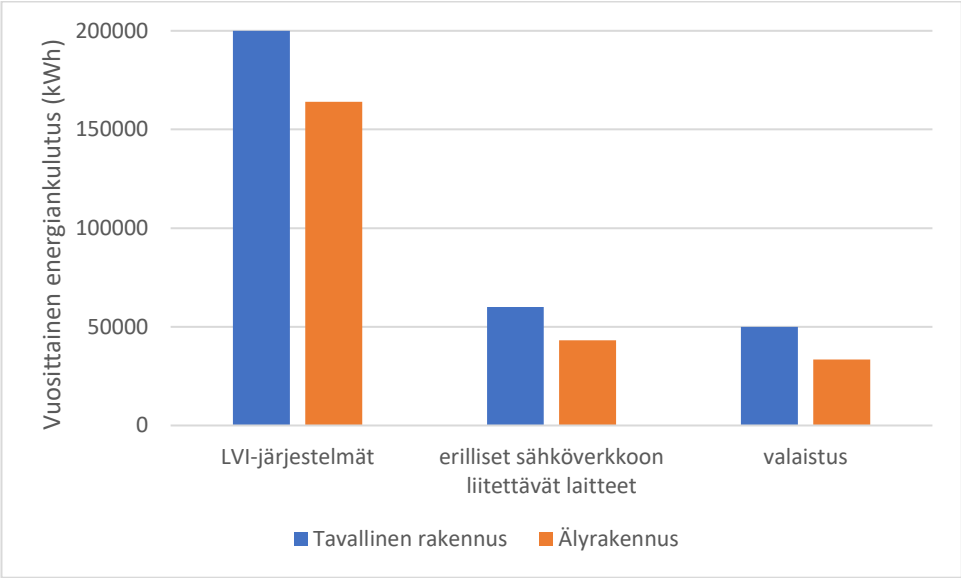
sulautetut anturit ja aktuaattorit. Sulautettu ratkaisu voi myös olla jokin ominaisuus, jonka avulla tietojärjestelmät pystyvät automaattisesti yhdistymään älyrakennuksen lähiverkkoon, tai ne pystyvät automaattisesti suorittamaan jonkin ohjelmiston. [Baseline Security Recommendations for IoT 2017: 20.]

IoT vaikuttaa nykypäivänä lähes kaikessa. Sen tarkoituksena on sulauttaa älykkyys osaksi esineitä ja laitteita, mikä tekee näistä entistä hyödyllisempiä kaikilla elämän osa-alueilla. [Baseline Security Recommendations for IoT 2017: 18.]

2.2.1 Rakennusautomaatio ja kiinteistönhallintajärjestelmä

Jotta rakennuksesta saadaan turvallinen sekä funktionaalisesti ja tehokkaasti toimiva, tarvitaan rakennukseen talotekniikkaa. Taloteknisillä laitteilla pystytään tuottamaan rakennukseen elintärkeitä toimintoja kuten esimerkiksi lämpöä, ilmaa, vettä, valoa sekä turvallisuutta. Rakennuksen talotekniikkaa ohjataan rakennusautomaation avustuksella. Rakennusautomaatio mahdollistaa rakennusten taloteknisten laitteiden tarkkailun, hallinnoinnin ja automatisoinnin. Sen avulla pystytään esimerkiksi pitämään huoneiden lämpötila aina optimaalisena ja valaisemaan rakennuksen tiloja vain silloin, kun se on tarpeellista. Myös turvallisuutta pystytään parantamaan esimerkiksi hallinnoimalla rakennuksen ovia tai tarkkailemalla kameravalvontaa. [Building management and integrated/intelligent building management systems.]

Rakennusautomaation hallinta tapahtuu yleensä jonkin rakennukseen integroidun kiinteistönhallintajärjestelmän (*BMS, Building Management System*) kautta. Kiinteistönhallintajärjestelmä on rakennukseen asennettu ratkaisu, joka mahdollistaa rakennuksen osajärjestelmien hallinnoin erillisen tietokoneeseen asennetun graafisen hallinnointiliittymän kautta. Tietokone tai palvelin, johon hallinnointiliittymä on asennettu, sijaitsee fyysisesti itse rakennuksessa tai maantieteellisesti aivan muualla, jolloin rakennuksen hallinnointi tapahtuu tietoverkon ylitse salatun VPN-yhteyden (*VPN, Virtual Private Network*) kautta. Kiinteistönhallintajärjestelmän kautta on mahdollista tarkkailla rakennuksen laitteiden toimintaa ja reagoida rakennuksessa tapahtuviin muutoksiin ja hälytyksiin nopeasti. [Building management and integrated/intelligent building management systems.]



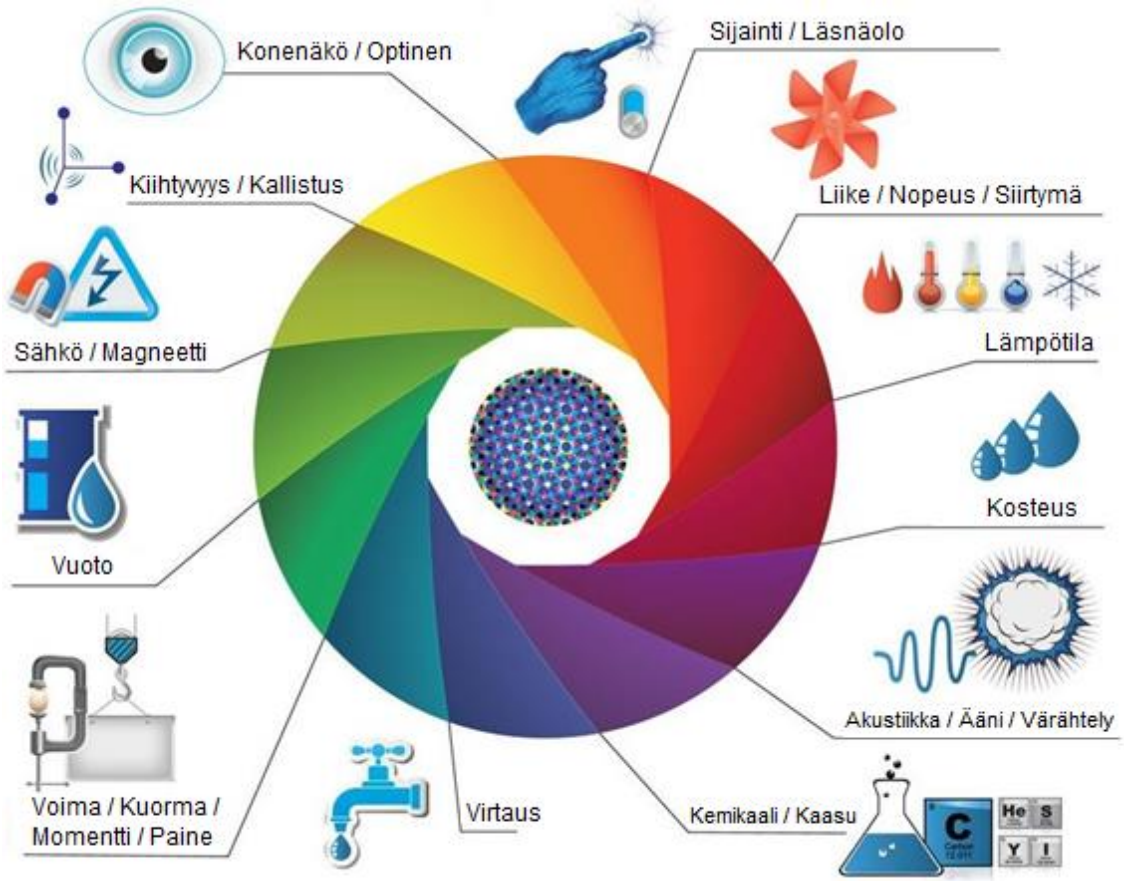
Kuva 2. Älykkäiden teknologioiden vaikutus energiankulutukseen [Perry 2017: 9].

Rakennusautomaatio ja älykkäät järjestelmät mahdollistavat pienillä investoineilla isoja säästöjä. Esimerkiksi energiankulutusta on mahdollista vähentää huomattavasti. Kuvassa 2 on energiatehokkuutta edistävän yhdysvaltalaisjärjestö ACEEE:n (*ACEEE, American Council for an Energy-Efficient Economy*) laatima arvio siitä, kuinka paljon enemmän älykkäillä teknologioilla varustettu älyrakennus pystyy toimistoympäristössä säästämään energiaa verrattuna tavalliseen rakennukseen. ACEEE:n arvion mukaan älyrakennus pystyy keskimäärin säästämään noin 18 % LVI-järjestelmien (*LVI, Lämpö, vesi ja ilma*) energiakuluissa, noin 28 % erillisten sähköverkkoon liitettävien laitteiden, kuten tietokoneiden energiakuluissa sekä noin 33 % valaistuksen energiakuluissa. [Perry 2017: 9.]

2.2.2 Anturit ja aktuaattorit

Anturit ovat laitteita, jotka pystyvät havaitsemaan ympäristössään tapahtuvia muutoksia ja tapahtumia. Anturit voivat tarkkailla esimerkiksi liikettä, ääntä, lämpötilaa ja ilmanlaatua. Kun puhutaan älyrakennuksista ja sen tietojärjestelmistä, anturit ovat todella merkittävässä roolissa. Antureita voidaan ohjelmoida siten, että ne havaitsevat niiltä vaaditut parametrit ympäristössään ja muuttavat havaitsemansa tiedon helposti luettavaan muotoon. [Balani 2015: 3.]

Antureissa ei itsessään ole ominaisuutta, jonka avulla niiden keräämää tietoa pystyttäisi suoraan lukemaan. Havaittua tietoa pystytään tarkkailemaan ja hallinnoimaan hyödyntäen erillistä aktuaattoria tai järjestelmää, joka on yhdistetty anturiin joko suoraan kaapeloimalla tai langattoman tietoverkon kautta. [Balani 2015: 3.]



Kuva 3. Älyrakennuksen antureita [What Is The ”Internet of Things”?].

Kuvassa 3 on kuvattuna erilaisia älyrakennuksessa käytettäviä antureita, kuten olosuhteita tarkkailevia lämpötila- ja kosteusantureita sekä liikettä, sijaintia ja ääntä tarkkailevia antureita. Läsnäoloanturi on yksi monista älyrakennuksessa toimivista antureista, joka aistii esimerkiksi ihmisen läsnäolon toimistohuoneessa. Monesti läsnäoloanturi sekoitetaan liikeanturin kanssa. Nämä kaksi anturia toimivat samalla periaatteella, mutta niillä on silti yksi pieni olennainen ero. Liikeanturi tunnistaa esimerkiksi kävelyliikkeen alueellaan ja reagoi siihen sytyttämällä huoneeseen valot. Kun liikeanturi ei enää havaitse kävelyliikettä, se sammuttaa huoneesta valot. Läsnäoloanturi on huomattavasti liikeanturia

tarkempi havaitsemaan liikettä. Se pystyy havaitsemaan pienenkin sormen liikahduksen, ja näin ollen huone pysyy valaistuna, vaikka ihminen työskentelisi pitkiäkin aikoja paikallaan toimistossa. [What is the difference between a presence and motion sensor?.]

Älyrakennusten käyttäjien tarpeet määrittävät sen, minkälaisia ja kuinka tarkkoja antureita ja aktuaattoreita rakennuksessa tarvitaan. Kaikilla tällaisilla liikkeeseen reagoivilla antureilla on kuitenkin yksi ja sama perimmäinen tarkoitus: energiatehokkuus. Kun ihmisen ei enää tarvitse huolehtia valaistuksesta, energiaa käytetään automaattisesti tehokkaammin. [What is the difference between a presence and motion sensor?.]

2.2.3 Tietoverkot ja tiedonsiirto

Tänä päivänä tietoverkot ovat osa meidän jokapäiväistä elämäämme. Tietoverkot ovat usein näkymättömiä, mutta niitä on kaikkialla, ympäri maailman. Tietoverkko yhdistää tietokoneet ja laitteet, jotta ne voivat kommunikoida keskenään maantieteellisestä sijainnistaan riippumatta. Tietokoneiden ja laitteiden välinen kommunikointi tietoverkkojen ylitse on mahdollista tiedonsiirtoprotokollien avulla. Protokolla on sarja sääntöjä ja rajoituksia, jotka määrittävät sen, kuinka tieto kulkee tietoverkoissa. Laitteiden välinen kommunikointi on mahdollista vain, mikäli ne noudettavat samaa protokollaa. [Odom 2016: 19-20.]

Riippuen älyrakennuksessa käytettävästä tiedonsiirtomediasta, älyrakennuksien hyödyntämä tietoverkkoteknologia voidaan jakaa kolmeen eri tyyppiin: datasähkö, väylä ja langaton tiedonsiirto. [Qolomany ym: 9.]

Datasähkö (*PLC, Powerline Communications*) käyttää hyödykseen rakennuksen olemassa olevia sähköjohtoja eli tiedonsiirto tapahtuu sähköverkossa. Datasähkö on historiallisesti vanhin käytössä oleva tiedonsiirtoteknologia. Se on yleisesti ottaen halpa ratkaisu, koska se pystyy hyödyntämään olemassa olevaa kaapelointia ja uutta kaapelointia ei näin ollen tarvita. Datasähkö on kuitenkin epäluotettava, eikä se skaalaudu kovinkaan hyvin. Alun perin datasähkön tarkoituksena oli turvata rakennusten päävirtalähteiden virrantuotto mahdollisten häiriöiden varalta. Jotkin datasähköä hyödyntävät proto-

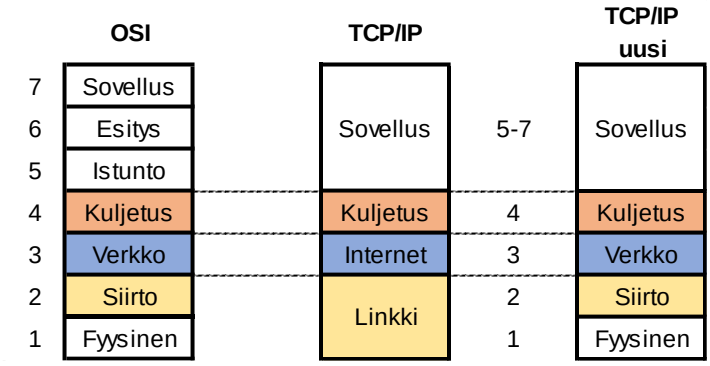
kollat tukevat vain yhdensuuntaista kommunikaatiota, eli laitteet saavat tietoa, mutta eivät pysty kommunikoimaan takaisin. Datasähköä hyödyntäviä protokollia ovat esimerkiksi X-10 ja INSTEON. [Qolomany ym: 9.]

Väyläratkaisussa älyrakennuksen tietoverkot hyödyntävät erillistä fyysistä mediaa, yleensä kierrettyä parikaapelia. Väyläteknologian konfigurointi on monimutkaista, ja se vaatii vankkaa osaamista tietoverkoista. Koska väylä hyödyntää erillistä kaapelointia, mahdollistaa se nopeat tiedonsiirtonopeudet sekä korkean luotettavuuden. Useat väyläteknologiaa hyödyntävät protokollat mahdollistavat kaksisuuntaisen kommunikaation laitteiden välillä. Yleisimmät väyläteknologiaa hyödyntävät protokollat ovat KNX, LON ja BACnet. [Qolomany ym: 9-10.]

Monet uudet älyrakennusten laitteet ja sovellukset hyödyntävät langatonta tiedonsiirtoteknologiaa. Langatonta tiedonsiirtoa hyödyntäviä tekniikoita ovat muun muassa infrapuna ja radioliikenne. Langaton tiedonsiirto on älyrakennuksen käyttäjille miellyttävä vaihtoehto sen vapauden ja langattomuutensa vuoksi. Älyrakennuksen laitteet ja anturit pystyvät kommunikoimaan keskenään langattomasti, sillä radioliikenne pystyy läpäisemään seinät, katot ja lattiat. Langattoman tiedonsiirtoteknologian etuna langattomuutensa lisäksi on kustannustehokkuus ja luotettavuus. Langatonta tiedonsiirtoteknologiaa hyödyntäviä protokollia ovat esimerkiksi RFID, WLAN ja Bluetooth. [Qolomany ym: 10.]

Edellä mainitut tietoverkkoteknologiat ovat osa älyrakennuksen sisäistä tietoverkkoa, jossa laitteet yhdistetään toisiinsa rakennuksen sisällä. Älyrakennuksesta puhuttaessa rakennuksella ja sen laitteilla on usein tarpeellista olla yhteydessä myös ulkomaailmaan eli Internetiin. Älyrakennus pystyy kommunikoimaan ulkomaailman kanssa hyödyntämällä TCP/IP-protokollaa (*TCP/IP, Transmission Control Protocol / Internet Protocol*). [Qolomany ym: 9.]

TCP/IP-protokollan pohjalta on kehitetty TCP/IP-viitemalli, jonka tarkoituksen on kuvata tietoliikenteen arkkitehtuuria. Tietoliikenteen arkkitehtuurin kuvaamiseen on kehitetty myös toinen malli nimeltä OSI-malli (*OSI model, Open System Interconnection Model*), jota käytetään terminologiansa takia etenkin opetustarkoituksessa enemmän kuin TCP/IP-viitemallia. [Odom 2016: 20, 32.]



Kuva 4. OSI-malli ja TCP/IP-mallit kerroksineen [Odom 2016: 33].

Kuvassa 4 on esitettynä OSI-malli, alkuperäinen TCP/IP-malli sekä uudistettu versio TCP/IP-mallista. Kyseisillä malleilla kuvataan sitä, kuinka tieto liikkuu laitteesta toiseen tietoverkon ylitse. OSI-mallissa tietoverkon funktiot ja protokollat on jaettu seitsemään eri kerrokseen. TCP/IP-mallissa tietoverkko on jaettu neljään kerrokseen ja päivitetyssä versiossa siirtokerros on jaettu kahteen osaan sekä terminologiaa on muutettu OSI-mallin mukaisesti. [Odom 2016: 32-33.] Seuraavassa on lyhyesti selitettynä jokaisen eri kerroksen tehtävät.

Jokaisella kerroksella on omat tehtävänsä ja vastuut kuljetettaessa tietoa laitteesta toiseen tietoverkon ylitse. Tieto lähtee liikkeelle sovelluskerroksesta ja etenee kerros kerrokselta alaspäin, kunnes saavuttaa fyysisen kerroksen. Sovelluskerros luo lähetettävän tiedon, kapseloi sen ja välittää tiedon eteenpäin esityskerrokselle. Esityskerros yhteensovittaa ja huolehtii tietorakenteiden oikeasta esittämistavasta, jonka jälkeen tieto siirtyy istuntokerrokselle. Istuntokerros pitää huolen siitä, että yhteys kahden laitteen välille muodostuu ja pysyy yllä koko tiedonsiirron ajan. Kuljetuskerros huolehtii tiedon kuljettamisesta kahden laitteen välillä sekä vastaa tiedon pilkkomisesta sopivan kokoisiin segmentteihin. Verkkokerros kapseloi saamansa tiedon paketeiksi ja huolehtii pakettien reitittämisestä tietoverkkojen ylitse. Siirtokerros luo tiedolle kehyksen ja kapseloi verkkokerrokselta saamansa tiedon. Fyysinen kerros määrittää tiedonsiirtoon käytettävän fyysisen median, muuntaa tiedon biteiksi ja huolehtii bittien siirtämisestä. Tämän jälkeen tieto siirtyy tietoverkkoa pitkin vastaanottajalle ja tieto puretaan kerros kerrokselta käänteisessä järjestyksessä. [Odom 2016: 30-36.]

2.2.4 Integraatiot

Tietoverkkojen ja tiedonsiirtoprotokollien avulla on mahdollista yhdistää useampi rakennuksen laite ja järjestelmä toimimaan yhtenä kokonaisuutena. Tätä kutsutaan integraatioksi. Integraatioita pidetään älyrakennusten määritelmän perustana. Älyrakennuksien integraatiot lähtevät siitä, että yhdistetään rakennuksen ydintoiminnot kuten valaistus, sähkömittarit, vesimittarit, pumput, lämmitys ja viilennys antureihin ja hallintajärjestelmiin. Tämä mahdollistaa rakennusten toimintojen automatisoinnin, pienemmät hallinnointikulut, tehokkaamman käytön, tehokkaamman suunnittelun sekä se tukee myös liiketoiminnan kehittymistä ja kasvua. [The benefits of integrating enterprise-wide systems: 2-3.]

Mikäli järjestelmät ja ohjelmistot eivät integroidu keskenään, tekee se niiden käyttämisestä haastavaa. Useiden eri järjestelmien käyttäminen vie aikaa ja tekee työntekijöiden työstä tehottomampaa. Integroimalla olemassa olevat järjestelmät ja laitteet yhdeksi kokonaisuudeksi on mahdollista säästää rahaa ja aikaa. Integraatiot mahdollistavat yrityksien työntekijöille tehokkaamman ja nopeamman tavan työskennellä, mikä kasvattaa tuottavuutta. Ilman keskenään kommunikoivia järjestelmiä työntekijä joutuu manuaalisesti keräämään ja siirtämään tietoa eri järjestelmien välillä. Tämä lisää riskiä myös virheiden tekemiselle. [Chignell 2017.]

Integraatioiden hyötynä on myös tiedon yhtenäisyys, ajantasaisuus ja päivitettävyys. Mikäli samaa tietoa säilytetään useassa eri järjestelmässä, lisää se riskiä sille, että tieto ei pysy ajan tasalla tai se vääristyy ajan saatossa. Tiedon ajantasaisuuden lisäksi integraatiot mahdollistavat sen, että tieto on helposti ja reaaliaikaisesti saatavilla. Mitä nopeammin yritykset pystyvät reagoimaan järjestelmissä tapahtuviin asioihin ja muutoksiin, niin sen parempi. Kun tieto on reaaliaikaista, pystytään mahdollisiin ongelmakohtiinkin puuttumaan nopeasti ja ajoissa. [Chignell 2017.]

2.2.5 Big data ja data-analytiikka

IoT-laitteiden määrä rakennuksissa on viime vuosina kasvanut räjähdysmäisesti, mikä on tehnyt rakennuksista entistä monimutkaisempia kokonaisuuksia. Lisääntyneet laitteet ovat myös aiheuttaneet sen, että rakennukset ja sen laitteet tuottavat entistä enemmän

analysoitavaa tietoa. Kun IoT-laitteet tuottavat massiivisen määrän analysoitavaa ja hyödynnettävää tietoa puhutaan Big Datasta. Useimpien älyrakennuksien kiinteistönhallintajärjestelmät eivät kuitenkaan hyödynnä tätä valtavaa tietomäärää tarpeeksi tehokkaasti ja näin ollen menettävät hyödyllisiin päätöksiin tarvittavaa tietoa. Tämä asettaa nyt ja tulevaisuudessa haasteita rakennusten omistajille ja hallinnoijille, jotta kiinteistönhallinnasta saadaan mahdollisimman tehokasta ja ympäristöä säästävää. [Cooper 2017.]

Markkinoille on viimeisen vuosikymmenen aikana ilmaantunut useita erilaisia teknisiä työkaluja ja sovelluksia, jotka on suunniteltu avustamaan kiinteistönhoitajia heidän päivittäisissä rakennuksen ylläpito- ja suunnittelutehtävissä. Mutta aivan kuten kiinteistönhallintajärjestelmätkin, myös nämä työkalut ovat monimutkaisia ja vaativat investointeja, jotta kiinteistönhoitajat osaavat käyttää ja hyödyntää näiden työkalujen tarjoamia mahdollisuuksia. Kiinteistönhoitoalalla on lisäksi myös korkea vaihtuvuus, jonka takia monien rakennusten hallinnointi on puutteellista, sillä työkaluja ja järjestelmiä ei osata käyttää tehokkaasti. On arvioitu, että vain noin 20 % kiinteistönhoitajista hyödyntää kiinteistönhallintajärjestelmiensä täyttä potentiaalia ja loput 80 % kiinteistönhoitajista hyödyntävät vain 20 % siitä potentiaalista, johon kiinteistönhallintajärjestelmillä olisi mahdollisuus. [Cooper 2017.]

Kiinteistönhallintajärjestelmien ja teknisten työkalujen monimutkaisuuksien takia kiinteistönhallinnassa on ryhdytty hyödyntämään dataa analysoivia ohjelmistoja, jotta laitteiden tuottamaa valtavaa tietomäärää pystytään tulkitsemaan mahdollisimman tehokkaasti. Ihanteellinen data-analyyttinen ohjelmisto on sellainen, joka tulkitsee automaattisesti esimerkiksi energiankulutuksen kehityssuunnan, havaitsee mahdolliset häiriöt ja tunnistaa häiriöiden aiheuttajat sekä asettaa ratkaisutoimenpiteet tärkeysjärjestykseen kustannuksiin, viihtyvyyteen ja ylläpitoon liittyvien vaikutusten perusteella. Data-analytiikka täydentää kiinteistönhallintajärjestelmän toimintoja ja sen avulla pystytään tulkitsemaan tietoa paremmin. Se auttaa ymmärtämään miksi älyrakennus eivätkä sen palvelut toimi tehokkaasti ja näin ollen pysyvästi korjaaviin toimenpiteisiin on helppo ryhtyä. Data-analytiikan avulla voidaan esimerkiksi havaita ongelmat laitteistossa ennen kuin niitä tarvitsee korjata tai vaihtaa. Näin ollen korjaavat toimenpiteet voidaan ajoittaa tehtäväksi ennen laitteiston rikkoutumista, joka puolestaan vähentää korjauskustannuksia ja tarjoaa rakennuksen käyttäjille optimaalisen viihtyvyyden. [Cooper 2017.]

2.3 Älyrakennuksen ominaisuudet ja käyttäjän vuorovaikutus

Käyttäjälähtöisessä älyrakennuksessa rakennus auttaa sen käyttäjiä muun muassa turvallisuuden ja mukavuuden kasvattamisessa, kustannusten pienentämisessä ja ekologisuuden saavuttamisessa. Älyrakennus on vuorovaikutussuhteessa käyttäjiensä kanssa reaaliaikaisesti reagoivien järjestelmien avulla. [Rantala ym. 2015: 14-15.]

Älyrakennuksen tulisi vastata sen käyttäjien tarpeisiin mahdollisimman tehokkaasti. Älyrakennuksen käyttäjillä tarkoitetaan esimerkiksi rakennuksen omistajaa, asukasta, työntekijää, vuokralaista tai huolto- ja kunnossapitohenkilöä. Kaikilla näillä henkilöillä on erilaisia rooleja liittyen rakennuksessa oleiluun tai toimimiseen ja kaikkiin näihin rooleihin liittyy erilaisia tarpeita. Roolit määrittävät sen, mitkä palvelut tai tekniset ratkaisut ovat käyttäjille merkityksellisiä. Taulukossa 1 on kuvattuna älyrakennuksen eri ominaisuuksia sekä niiden merkityksiä rakennuksen eri käyttäjille. Käyttäjien kokemat ominaisuudet ovat kuvassa pisteytettynä 0-3, jossa 0 = ei merkitystä, 1 = pieni merkitys, 2 = keskisuuri merkitys ja 3 = suuri merkitys. [Rantala ym. 2015: 19-21.]

Taulukko 1. Älyrakennusten ominaisuudet käyttäjien näkökulmasta [Rantala ym. 2015: 21].

Käyttäjän kokema ominaisuus	Asukas	Toimisto-työntekijä	Kunnossa-pito-työntekijä	Omistaja / isännöitsijä
Toiminnalliset ominaisuudet				
käytön ja toimintojen helppo ymmärrettävyys ja käytettävyys	3	3	3	3
käyttäjän ei tarvitse puuttua rakennuksen toimintoihin	3	3	2	1
taloudelliseen ja energiatehokkaaseen käyttäytymiseen kannustaminen	2	2	3	3
tilojen toimivuus, turvallisuus ja terveellisyys	3	3	1	2
järjestelmien varmatoimisuus	3	3	2	3
Tekniset ominaisuudet				
helppo käytettävyys	3	3	3	2
vuorovaikutteisuus	1	2	2	2

säädettävyys (itsenäisesti, yksilöllisesti, yhdessä ja yhteisellä käyttöliittymällä	3	2	3	2
huollettavuus ja kunnossapidettävyys	1	1	3	3
liitettävyys vieraisiin taloihin, kortteliin, kaupunginosaan, kaupunkiin, sekä valtakunnallisiin järjestelmiin	3	1	2	2
järjestelmien muunneltavuus, vaihdettavuus, laajennettavuus, ja päivitettävyys	0	0	2	3
eri järjestelmien keskinäinen yhteensopivuus	0	0	2	2
kyberturvallisuus	3	3	3	3
avoin mittausdatan käyttö	0	0	3	3
digitaalinen joustavuus ja muunneltavuus	2	1	3	3
rakennustekninen terveellisyys ja turvallisuus	2	2	3	3
rakenteellinen muunneltavuus	0	0	1	3
energiatehokkuus ja vähäpäästöisyys	1	1	1	3
ekotehokkuus	2	1	2	3
kiinteistön ylläpitotietojen hallittavuus	0	0	3	3
Taloudelliset ominaisuudet				
kustannustehokkuus	1	1	3	3
kustannusten reaaliaikainen raportointi	3	3	3	3
arvon säilyminen elinkaaren aikana	2	2	2	3
elinkaariedullisuus	0	0	2	3
arvon tuottaminen käyttäjilleen	1	2	0	2

Kuten taulukosta 1 nähdään, kaikki käyttäjäryhmät haluavat älyrakennuksen ja sen toimintojen olevan helppoja ymmärtää ja käyttää. Teknisiltä ominaisuuksilta kaikki käyttäjäryhmät myös näkevät kyberturvallisuuden merkityksen olevan suuri. Tämä siis vahvistaa sen, että myös rakennusten käyttäjien mielestä kyberturvallisuus tulee nyt ja jatkossa huomioida älyrakennusten suunnittelussa ja toteutuksessa.

2.4 Älyrakennus ja älykäs kaupunkiympäristö

Älykäs kaupunkiympäristö eli Smart City on käsitteenä maailmanlaajuisesti tunnettu ja kuvaa sitä, kuinka alueita, kaupunkeja, kuntia ja kyliä tulisi kehittää kohti ekologisempaa ja modernimpaa yhteiskuntaa. Useimpien älykaupunkien yleisenä päämääränä on selvittää, miten informaatioteknologia, IoT, digitalisaatio, Big Data ja integroidut tietojärjestelmät voivat myötävaikuttaa modernimman ja kestävämmän kaupungistumisen kehittymistä. Älykkäiden kaupunkien perimmäinen päämäärä on ihmisten elämänlaadun parantaminen mahdollisimman taloudellisella ja ympäristöystävällisellä tavalla. [Karlsen 2017: 4.]

Älykäs kaupunki hyödyntää antureita, IoT-laitteita ja Big Dataa, joiden avulla saadaan yhdistettyä olemassa olevat järjestelmät, infrastruktuuri, rakennukset, kulkuneuvot, tieverkostot, tietoverkot, liikennevalot, katuvalot ja julkinen liikenne yhdeksi valtavaksi ja moderniksi kokonaisuudeksi. Älykkäässä kaupungissa esimerkiksi katuvalot toimivat siten että ne menevät päälle havaitessaan pimeään aikaan ihmisen tai ajoneuvon, ja vastaavasti sammuvat, mikäli tiellä ei havaita liikennettä. Tämä lisää turvallisuutta ja samalla säästää valtavat määrät energiaa. Älykaupungit toimivat siis täysin samalla periaatteella kuin älyrakennuksetkin mutta vain isommassa mittakaavassa. Älyrakennukset ovat yksi osa älykaupunkia. [Karlsen 2017: 5.]

Älykkäässä kaupunkiympäristössä älyrakennusten tietojärjestelmät ovat yhteydessä sekä toisten rakennusten järjestelmiin, kuten myös globaaleihin ja alueellisiin tietojärjestelmiin. On suositeltavaa, että jokaisella älyrakennuksella olisi oma ja paikallisesti toimiva hallinnollinen tietojärjestelmä, joka voi tarvittaessa olla kahdennettu esimerkiksi pilvipalveluun. Tämä lisää kyberturvallisuutta rakennuksissa. Olennaista kyberturvallisuuden osalta on se, että rakennuksen perustoiminnot kuten sähkön- ja vedenjakelu toimisivat autonomisesti, ja tarvittaessa niiden tilatietoja voidaan tarkkailla palvelimen kautta. [Rantala ym. 2015: 31.]

3 Kyberturvallisuus

Viimeisten vuosien aikana tapahtuneen nopean digitalisaation yleistymisen myötä ympärillemme on muodostunut kaksi eri todellisuutta, fyysinen maailma sekä ihmisen keinotekoisesti luoma digitaalinen maailma. Fyysisellä maailmalla tarkoitetaan kaikkea sitä konkreettista, jonka pystymme käsillämme tuntemaan ja silmillämme havaitsemaan. Digitaalinen maailma on ihmisen luoma digitaalinen ympäristö, johon kuuluvat muun muassa Internet, tietoverkot ja tietojärjestelmät. Älyrakennus on hyvä malliesimerkki tilanteesta, jossa fyysisen ja digitaalisen maailman rajat hämärtyvät. Digitaalisesta maailmasta käytetään myös nimitystä kybermaailma tai kybertoimintaympäristö. [Limnéll ym. 2014.]

Kyber-sanaa harvoin käytetään sellaisenaan, vaan siihen lisätään yleensä jokin loppuliite, kuten esimerkiksi kyberturvallisuus [Limnéll ym. 2014]. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa organisaatiot ja ihmiset voivat luottaa kybertoimintaympäristöön ja jossa sen riskit ovat pienennetty hyväksyttävään minimiin. Kybertoimintaympäristö taas on toimintaympäristö, joka muodostuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä. [Kyberturvallisuuden Sanasto 2018: 21-22.] Tietojärjestelmät koostuvat tiedoista, tietoa käsittelevistä ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista, tietoja käsittelevistä ohjelmista ja tietojen käsittelysäännöistä tarkoituksenaan tehostaa sekä helpottaa jotakin toimintaa, tai mahdollistaa tällainen toiminta. Kybertoimintaympäristöön liittyy keskeisesti myös tiedon käsittelyyn liittyvät fyysiset rakenteet. [Finto.]

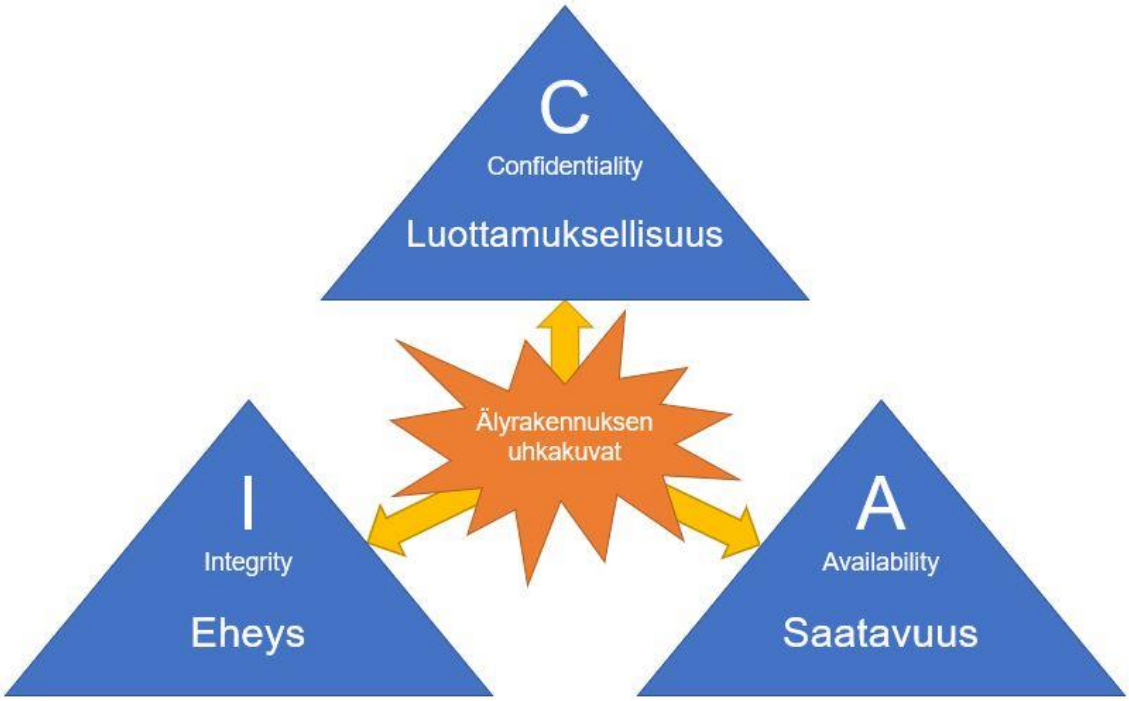
Tietoturvallisuus ja kyberturvallisuus sekoitetaan useasti toisiinsa. Tietoturvallisuus on turvallisuuden osa-alue, jossa keskitytään yksinomaan suojaamaan tietoa taaten tiedon luottamuksellisuus, eheys ja saatavuus. Kuten edellä on mainittu, kyberturvallisuus on käsitteenä laajempi, jolla pyritään tiedon lisäksi turvaamaan koko digitaalinen maailma kaikkine tietojärjestelmineen ja toimintoineen. Kyberturvallisuus pitää sisällään useita turvallisuuden osa-alueita, kuten muun muassa tietoverkkoturvallisuuden, sovellusturvallisuuden, tietoturvallisuuden, operatiivisen turvallisuuden, jatkuvuudenhallinnan ja toipumissuunnittelun. On kuitenkin huomioitava, että kyberturvallisuus ei käsitä aivan kaikkea sitä, mitä edellä mainitut turvallisuuden osa-alueet sisältävät. Esimerkiksi puhtaasti fyysisessä muodossa säilytettävä ja turvattava tieto, kuten papereiden kassakaappisäi-

lytys, on tietoturvallisuutta, mutta ei kuitenkaan kyberturvallisuutta. Käsitteet siis leikkaavat toisiaan ja ovat osin päällekkäisiä, mutta niihin liittyy myös omia, toisistaan erillisiä, kokonaisuuksia. [What is Cyber-Security?; Limnéll ym. 2014.]

Tietoa tuotetaan nykyään enemmän kuin koskaan aiemmin ja sen tuottaminen kasvaa päivä päivältä entistä suurempiin määriin. Maailmassa otetaan päivittäin käyttöön lukuisia uusia järjestelmiä ja laitteita, jotka tuottavat uutta tietoa saataville. Teknologian räjähdysmäinen kehitys onkin edesauttanut myös tiedon tuottamisen suurta kasvua. Tieto saattaa olla myös arkaluontoista tai salassa pidettävää, jolloin tiedon joutuminen vääriin käsiin voi aiheuttaa mittavia vahinkoja yrityksille, yksilöille kuten myös älyrakennuksillekin. [Limnéll ym. 2014.]

Suojattavan tiedon osalta keskeiseen rooliin nousee tietoturvallisuus eli ne järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Tiedon saatavuudella turvataan se, että tieto on siihen oikeutettujen saatavilla haluttuna aikana. Eheyden avulla varmistetaan tiedon muuttumattomuus ja oikeudettomien muutosten havaitseminen. Luottamuksellisuus varmistaa, että tieto on vain siihen oikeutettujen saatavilla. [Kyberturvallisuuden Sanasto 2018: 15.]

Kyberhyökkäyksillä on mahdollista vahingoittaa haavoittuvaa tietoa kolmella tapaa. Varastamalla tietoa saadaan tiedon luottamuksellisuus murrettua, muuttamalla tietoa saadaan tiedon eheys vaarannettua sekä estämällä pääsy tiedolle tai järjestelmille saadaan tiedon saatavuus vaarannettua. [Donaldson ym. 2015: 10.]



Kuva 5. CIA-kolmio [Donaldson ym. 2015: 11].

Kuvassa 5 on esitettynä tietoturvakolmio, jota kutsutaan myös nimellä CIA-kolmio (*CIA, Condifentiality, Integrity, Availability*). Kolmio kuvaa sitä, kuinka kyberhyökkäyksien aiheuttamilla vahingoilla tieto menettää luottamuksellisuutensa, eheytensä ja saatavuutensa. Älyrakentamisessa onkin keskityttävä tarkasti siihen, että rakennuksen laitteiden ja järjestelmien luoma ja hallinnoima tieto pysyy mahdollisimman tarkasti suojattuna. Seuraavassa käydään lävitse CIA-kolmion osia tarkemmin. [Donaldson ym. 2015: 11.]

Tiedon luottamuksellisuuteen kohdistetut hyökkäykset ovat yleisimpiä tietomurtoja. Potilastietojen, järjestelmätietojen, sosiaaliturvatunnusten tai pankkitietojen vuotaminen tietomurtojen yhteydessä ovat esimerkkejä siitä, minkälaisia tietoja yritysten ja rakennusten järjestelmistä on mahdollista saada kyberhyökkäysten yhteydessä varastettua. Luottamuksellisuuteen kohdistetut tietomurrot keskittyvät yleensä saamaan pääsyn sinne, jossa yritysten ja rakennusten tietoja säilytetään. Yleisimpiä kohteita ovat tietokannat, tietokantojen varmuuskopiot, palvelimet sekä järjestelmien ylläpitäjät. [Donaldson ym. 2015: 11.]

Tiedon eheyteen kohdistettujen hyökkäysten tavoitteena on saada muokattua haavoittuvaa tietoa. Tämän tyyppisillä tietomurroilla pystytään vaikuttamaan muun muassa yritysten julkisuuskuvaan. Kohteena voivat esimerkiksi olla yrityksen internetsivut, jossa hyökkäyksen tarkoituksena on saada muokattua internetsivuilta löytyvää tietoa tarkoituksella virheelliseksi. Eheyteen liittyvien tietomurtojen päämääränä voi olla myös internetsivujen tai domain-tunnusten kaappaaminen. [Donaldson ym. 2015: 12.]

Tiedon saatavuuteen kohdistettujen tietomurtojen tarkoituksena on vaikuttaa rakennusten järjestelmien käytettävyyteen ja pyrkiä estämään käyttäjien pääsy tietojärjestelmiin. Tämän tyylisiä tietomurtoja voi olla vaikea havaita, sillä hyökkäystilanteessa järjestelmät yleensä kyllä toimivat mutta erittäin hitaasti. Yksi tunnetuimmista isojen palvelimien tai rakennusten tietojen saatavuuteen kohdistetuista hyökkäystavoista ovat hajautetut palvelunestohyökkäykset (*DDoS, Distrubuted Denial of Service).* Näissä hyökkäyksissä pyritään usean eri tietojärjestelmän avulla aiheuttamaan rakennuksen järjestelmiin ja palvelimiin suuri määrä tietoliikennettä, jolloin rakennuksen tietojärjestelmät ylikuormittuvat ja lopulta lakkaavat toimimasta. [Donaldson ym. 2015: 12.]

4 Älyrakennuksen uhkaympäristö

Älyrakennuksen tietojärjestelmien ja IoT-laitteiden integraatioiden tuloksena syntyy monimutkaisia kokonaisuuksia, jotka tuovat esiin uusia älyrakennuksen turvallisuuteen ja jatkuvuuteen liittyviä haasteita. Kuten aiemmin mainittu, tietoa tuotetaan jatkuvasti lisää IoT-laitteiden ja tietojärjestelmien välityksellä, mikä lisää huolta yksityisyydestä ja turvallisuudesta. Käyttäjien halukkuus jakaa henkilökohtaisia tietojaan tietojärjestelmille riippuu siitä, voivatko he luottaa tietoa käsittelevien tietojärjestelmien kykyyn hallita ja suojata tietoa laillisella ja vastuullisella tavalla. [Smart Buildings: people and performance 2013: 17.]

Älyrakennuksiin kohdistuvilla kyberhyökkäyksillä voidaan aiheuttaa vakavia maineellisia vahinkoja. Tietojärjestelmien jatkuvalla kehittämisellä voidaan parantaa niiden luotettavuutta. Tekemällä tiiviimpää yhteistyötä viranomaisten kanssa, pystytään kyberhyökkäyksiä ehkäisemään tehokkaammin. Myös sääntelyiden, sopimusten ja standardien

avulla pystytään suojamaan älyrakennuksia, organisaatioita kuin myös kansalaisiakin. [Smart Buildings: people and performance 2013: 17.]

Yhdysvaltalaisen tietoliikenneyritys Verizonin vuosittain julkaistavan DBIR-raportin (*DBIR, Data Breach Investigation Report*) mukaan vuonna 2018 tapahtui 155 vahvistettua tietomurtoa, joissa arkaluontoista tietoa päätyi hyökkääjien käsiin. Noin joka neljäs näistä tapahtumista (25 %) johtui yritysten työntekijöiden tekemistä virheistä. Luku pitää sisällään väärin konfiguroidut tietojärjestelmät, sekä julkaisuvaiheessa tapahtuneet virheet. Vaikka näiden ongelmien torjuntaa voidaan jatkuvalla ja säännöllisellä käyttäjien kouluttamisella ja tietoisuuden lisäämisellä parantaa, tarvitaan tulevaisuudessa myös entistä vastustuskykyisempiä tietojärjestelmiä. [Data Breach Investigations Report 2019: 46-47; Smart Buildings: people and performance 2013: 17.]

Taulukko 2. OWASP, kymmenen yleisintä uhkaa IoT-laitteille. [OWASP Internet of Things Project 2018.]

	IoT-laitteisiin kohdistuva kyberuhka	**Kuvaus**
1	Heikot, arvattavat tai kovakoodatut salasanat	Julkisesti saatavien, helposti väsytyshyökättävien (*brute-force*) tai muuttumattomien pääsytietojen käyttäminen, sisältäen myös takaportit laiteohjelmistossa/tietokoneohjelmistossa, jotka myöntävät luvattoman tietojärjestelmien käytön.
2	Turvattomat tietoverkkolaitteet ja -palvelut	Tarpeettomien ja turvattomien aktiivisten palveluiden käyttö tietoverkkolaitteistossa, etenkin suoraan Internetiin alttiit palvelut, jotka vaarantavat tiedon luottamuksellisuuden, eheyden ja saatavuuden ja mahdollistivat tietojärjestelmien luvattoman etäkäytön.

3	Turvattomat ekosysteemin rajapinnat	Turvattomat ekosysteemin tietojärjestelmien ulkopuolella sijaitsevat Web-, pilvi- tai mobiilirajapinnat, jotka sallivat murtautumisen ekosysteemin tietojärjestelmiin. Yleiset ongelmat käsittävät heikon todentamisen, heikon salaamisen ja puutteellisen I/O (*I/O, Input/Output*) suodatuksen.
4	Turvapäivitysten puute	Puutteellinen kyvykkyys tietojärjestelmien turvapäivityksille, kuten puutteellinen laitteiston validointi, puutteellinen suojattu tiedonsiirto ja puutteellinen tulevien turvapäivitysten ilmoittaminen.
5	Turvattomien ja vanhentuneiden komponenttien käyttäminen	Vanhentuneiden tai turvattomien komponenttien käyttö, joilla vaarannetaan tietojärjestelmät. Esimerkiksi turvattomien kustomoitujen käyttöjärjestelmien käyttö tai murretusta toimituksetjusta peräisin olevan kolmannen osapuolen ohjelmiston tai komponentin käyttö.
6	Puutteellinen yksityisyydensuoja	Ekosysteemin tietojärjestelmiin tallennettujen käyttäjien henkilökohtaisten tietojen turvaton, sopimaton tai luvaton käyttö.
7	Turvattomat tietoliikenneyhteydet ja tallennustilat	Puutteellinen pääsynhallinta tai salaus arkaluontoista tietoa tallennettaessa, siirrettäessä tai käsiteltäessä.
8	Puutteellinen laitehallinta	Puutteellinen tuki tuotantokäytössä oleville tietojärjestelmille. Käsittää omaisuuden hallinnan,

		päivitystenhallinnan, turvallisen tietojärjestelmien poiston ja tietojärjestelmien tarkkailun.
9	Turvattomat oletusasetukset	Turvattomilla oletusasetuksilla konfiguroidut tietojärjestelmät, tai puutteellinen kyvykkyys tehdä tietojärjestelmistä turvallisempia rajoittamalla ylläpitäjien muutosoikeuksia tietojärjestelmien asetuksiin.
10	Puutteellinen tietojärjestelmien kovennus	Puutteellinen kyvykkyys tietojärjestelmien koventamistoimenpiteisiin, joka antaa mahdollisille hyökkääjille mahdollisuuden saada käsiinsä arkaluontoista tietoa, jolla voidaan tehostaa hyökkäystä tai saada jokin tietojärjestelmä hallintaan.

Taulukossa 2 on kuvattuna OWASP-yhteisön (*OWASP, Open Web Application Security Project)* vuonna 2018 päivitetty IoT-projektiin liittyvä listaus, jossa listataan kymmenen yleisintä IoT-laitteisiin kohdistuvaa kyberuhkaa. Esimerkiksi vuonna 2016 tapahtuneet Mirai-bottiverkon hyökkäykset kohdistettiin tietojärjestelmiin, joissa kaikista löytyi yksi tai useampi taulukossa 1 kuvattu puute. OWASP-projektin tarkoituksena on tarjota tietoa kaikista IoT-laitteiden haavoittuvuuksista, hyökkäyspinta-aloista ja tietojärjestelmien heikkouksista. Samalla se antaa tietoa siitä, kuinka älyrakennuksesta ja sen tietojärjestelmistä saadaan suunniteltua ja toteutettua mahdollisimman kyberturvallinen. [OWASP Internet of Things Project 2018; Baseline Security Recommendations for IoT 2017: 31.]

Älyrakennukseen ja sen tietojärjestelmiin kohdistuvat uhkakuvat ovat IoT-laitteiden yleistymisen myötä lisääntyneet viimeisten vuosien aikana merkittävästi. Uhkakuvat voidaan luokitella pahantahtoisiin toimiin, katkoksiin, fyysisiin hyökkäyksiin, onnettomuuksiin, salakuunteluihin, vaurioihin ja käyttöhäiriöihin.

- Pahantahtoisilla toimilla tarkoitetaan muun muassa palvelunestohyökkäyksiä (*DoS*), haittaohjelmia (*Malware*), piilohallintaohjelmia (*Rootkit*), väärennettyjä tietojärjestelmiä tai tiedon yksityisyyteen kohdistettuja hyökkäyksiä [Baseline Security Recommendations for IoT 2017: 34].

- Katkoksilla tarkoitetaan tietojärjestelmien häiriöitä, tieto- tai sähköverkon katkoksia tai tukipalveluiden menettämistä [Baseline Security Recommendations for IoT 2017: 35].

- Fyysisillä hyökkäyksillä tarkoitetaan tietojärjestelmien pahantahtoisia modifiointeja, sabotaaseja tai tuhoamisia [Baseline Security Recommendations for IoT 2017: 35].

- Onnettomuuksilla tarkoitetaan luonnonuhkia, kuten esimerkiksi tulvia, maanvyöryjä ja lumimyrskyjä tai ympäristöön liittyviä uhkia, kuten esimerkiksi tulipaloja ja räjähdyksiä [Baseline Security Recommendations for IoT 2017: 35].

- Salakuunteluilla tarkoitetaan esimerkiksi MITM-hyökkäyksiä (*MITM, Man-in-the-middle*), IoT-kommunikaatioprotokollien kaappauksia, tietoverkkotiedusteluja ja istuntojen kaappauksia [Baseline Security Recommendations for IoT 2017: 34].

- Vaurioilla tarkoitetaan tilanteita, joissa yllättävien tietojärjestelmien rikkoutumisten seurauksena menetetään arkaluontoista tietoa [Baseline Security Recommendations for IoT 2017: 35].

- Käyttöhäiriöillä tarkoitetaan tietojärjestelmien haavoittuvuuksia tai kolmannen osapuolen tarjoamien palveluiden häiriöitä [Baseline Security Recommendations for IoT 2017: 34-35].

Edellä mainituilla uhkakuvilla ja riskeillä voidaan aiheuttaa älyrakennukseen ja sen tietojärjestelmiin mittavia vahinkoja. Uhkakuvia voidaan hyökkäystilanteessa käyttää myös tapahtumasarjana, jolloin älyrakennuksen infrastruktuuria pystytään vahingoittamaan monelta eri tasolta. . [Baseline Security Recommendations for IoT 2017: 35.]

Taulukossa 3 käydään läpi mahdollisia älyrakennuksiin kohdistuvia erilaisia hyökkäysskenaarioita. Hyökkäysskenaarion tärkeysaste kuvaa sitä, kuinka negatiivinen vaikutus hyökkäyksellä olisi, mikäli se tapahtuisi oikeassa elämässä. Käytettävät tärkeysasteet ovat matala, keskisuuri, suuri ja kriittinen. [Baseline Security Recommendations for IoT 2017: 35.]

Taulukko 3. Mahdolliset älyrakennukseen kohdistuvat hyökkäysskenaariot [Baseline Security Recommendations for IoT 2017: 36].

Mahdollinen älyrakennukseen kohdistuva hyökkäysskenaario	**Tärkeysaste**
1. Hyökkäys antureiden ja aktuaattoreiden väliseen tietoverkkoyhteyteen.	Suuri – Kriittinen
2. Hyökkäys antureihin, jossa modifioidaan antureiden lukemia ja havainnoimia arvoja.	Suuri – Kriittinen
3. Hyökkäys aktuaattoreihin, jossa modifioidaan tai sabotoidaan aktuaattoreiden normaaleja asetuksia.	Suuri – Kriittinen
4. Hyökkäys IoT-laitteita ylläpitävään hallintajärjestelmään.	Suuri - Kriittinen
5. Protokollien haavoittuvuuksien hyödyntäminen.	Suuri
6. Hyökkäys, jossa syötetään komentoja tietojärjestelmien konsoliin.	Suuri - Kriittinen
7. DDoS-hyökkäykset IoT-bottiverkkoa hyödyntäen.	Kriittinen

8. Virtalähteiden manipuloinnit.	Keskisuuri – Suuri
9. Kiristyshaittaohjelmat.	Keskisuuri - Kriittinen

Jotta mahdolliset älyrakennuksiin kohdistuvat hyökkäysskenaariot ymmärretään paremmin, on niitä hyvä käsitellä tarkemmin lävitse. Älyrakennuksen antureiden ja aktuaattoreiden väliseen tietoverkkoyhteyteen kohdistuvien hyökkäysten pääasiallisena tarkoituksena on salakuunnella tai päästä käsiksi arkaluontoiseen tietoon, jota voidaan hyödyntää useissa ilkeämielisissä toiminnossa, kuten myöhemmissä hyökkäyksissä älyrakennuksen tietojärjestelmiin. Riippuen älyrakennuksen ympäristöstä, hyökkäyksen negatiivinen vaikutus voi olla joko matala tai korkea. Kyseessä voi kuitenkin olla myös merkki suuremmasta käynnissä olevasta hyökkäyksestä. [Baseline Security Recommendations for IoT 2017: 36.]

Älyrakennuksen antureihin kohdistuvissa hyökkäyksissä tavoitellaan mahdollisuutta päästä manipuloimaan älyrakennuksen antureiden asetuksia. Muuttamalla antureiden raja-arvoja saadaan anturit havainnoimaan ympäristöstään sellaista tietoa, jota niiden ei kuuluisi. Tämä muodostaa vakavan uhkan älyrakennuksen tietojärjestelmille. Suuremmissa älyrakennuksissa tilakohtaisia antureita on useampia, joten hyökkääjän on pystyttävä murtautumaan useampaan eri anturiin, jotta hyökkäys olisi tehokas. [Baseline Security Recommendations for IoT 2017: 36.]

Älyrakennuksen aktuaattoreihin kohdistuvien hyökkäysten tavoitteena on aktuaattoreiden konfiguraatioiden manipulointi, mikä saa ne käyttämään vääriä tietoja, konfiguraatioita ja raja-arvoja. Tällä vaikutetaan aktuaattoreiden normaaliin toimintaan sabotoimalla niiden normaalit toiminta-asetukset. Hyökkäyksen vakavuus riippuu hyökkäyksen kohteena olevasta aktuaattorista. [Baseline Security Recommendations for IoT 2017: 37.]

Älyrakennuksen IoT-laitteita ylläpitävään hallintajärjestelmään kohdistuvassa hyökkäyksessä pyritään saamaan hallintajärjestelmä hyökkääjien täyteen hallintaan, joka mahdollistaa koko älyrakennuksen ekosysteemin vaarantamisen. Esimerkiksi asuinkäytössä

olevan älyrakennuksen tietojärjestelmistä saattaa onnistuneen hyökkäyksen yhteydessä vuotaa arkaluontoista asukkaita yksilöivää tietoa, kuten asukastietoja, kamerasyötteitä tai tietoja asukkaiden asumiskäyttäytymistä. Älyrakennuksen tietojärjestelmiä voidaan onnistuneessa hyökkäyksessä hyödyntää myös esimerkiksi kryptovaluutan louhinnassa. Mikäli hallintajärjestelmissä käytetään heikkoja oletussalasanoja, on hyökkäyksen onnistuminen todennäköistä. On huomioitava, että tämäntyyppinen hyökkäys on mahdollista toteuttaa koko älyrakennuksen elinkaaren aikana. [Baseline Security Recommendations for IoT 2017: 37; Wueest 2019: 8.]

Protokollien haavoittuvuuksia hyödyntävät hyökkäykset ovat useasti osa suurempaa hyökkäystä ja apukeino suuremman hyökkäyksen toteuttamista varten. Näissä hyökkäyksissä pyritään hankkimaan korkeimman tason (*Root*) luvattomat käyttöoikeudet älyrakennuksen tietojärjestelmiin, joiden avulla tietojärjestelmiin pystytään asentamaan vahingollista sisältöä tai avaamaan uusia takaportteja. Protokollien haavoittuvuuksia hyödyntäviä hyökkäyksiä on vaikea havaita ja useasti tilanne havaitaan vasta, kun hyökkäys on jo saatu toteutettua. [Baseline Security Recommendations for IoT 2017: 37.]

Älyrakennuksen tietojärjestelmiin kohdistuvissa konsolihyökkäyksissä pyritään luvattomien ja korkeamman tason käyttöoikeuksien avulla suorittamaan komentoja tietojärjestelmien konsoliin. Mikäli konsolihyökkäys toteutetaan onnistuneesti, hyökkääjä saattaa päästä käsiksi myös muihin älyrakennuksen tietojärjestelmiin. [Baseline Security Recommendations for IoT 2017: 37.]

Bottiverkkoa hyödyntävien hyökkäysten kohteena ei välttämättä ole oman älyrakennuksen tietojärjestelmät, mutta niitä hyödynnetään hyökkäyksessä, jossa kohteena ovat esimerkiksi toisen älyrakennuksen tietojärjestelmät. Bottiverkko muodostuu, kun haittaohjelmat automaattisesti löytävät haavoittuvia ja helposti tartutettavia tietojärjestelmiä, ja ottaa ne haltuun osaksi laajaa tartutettujen tietojärjestelmien armeijaa. Bottiverkkohyökkäyksissä hyödynnetään hajautettua palvelunestohyökkäystä (*DDoS*), jossa lähetetään samanaikaisesti suuri määrä tietoliikennettä kohteena olevaan tietojärjestelmään, jonka lopputuloksena kohde saadaan lamaannutettua. [Baseline Security Recommendations for IoT 2017: 38.]

Virtalähteisiin kohdistuvissa hyökkäyksissä pyritään vaikuttamaan älyrakennuksen virtalähteisiin peukaloimalla älyrakennuksen virtalähteitä tai virtakaapeleita joko fyysisesti tai haittaohjelman avulla. Haittaohjelmien avulla saadaan esimerkiksi älyrakennuksen tietojärjestelmät luulemaan, että laitteiston akuston virtataso on joko liian korkea tai matala, jolloin tietojärjestelmät joko sulkeutuvat kokonaan tai asettuvat virransäästötilaan heikentäen tietojärjestelmien suorituskykyä. [Baseline Security Recommendations for IoT 2017: 38.]

Kiristyshaittaohjelmilla on mahdollista saada lukittua älyrakennuksen tietojärjestelmät, jotka ovat mahdollista saada auki vain lunnaita vastaan. Kiristyshaittaohjelmia pystytään torjumaan pitämällä huolta siitä, että älyrakennuksen tietojärjestelmiä päivitetään säännöllisesti ajantasaisilla turvapäivityksillä. Älyrakennuksissa haastavaa on se, että useita tietojärjestelmiä, kuten IoT-laitteita on hankala päivittää tai niitä ei mahdollisesti pysty päivittämään laisinkaan. [Baseline Security Recommendations for IoT 2017: 38.]

5 Älyrakennuksen suunnittelu- ja rakennusprosessi

Älyrakennuksen suunnittelussa tulee ottaa rakennuksen käyttäjälähtöisyys, ekologisuus ja kustannustehokkuus mahdollisimman tarkasti huomioon. Älykkäiden rakennusten tulisi olla sellaisia, että ne pystyvät parantamaan ja tehostamaan rakennuksen omistajan ja käyttäjien tarpeita sekä toimintoja. Rakennuksen suunnittelun alkuvaiheessa onkin tärkeää päättää ja valita haluttu rakennuksen älykkyystaso. [Rantala ym. 2015: 103.]

Rakennuksen älykkyystason luokittelu määräytyy sillä perusteella, onko kyseessä uudisrakennus vai jo olemassa oleva rakennus. Taulukossa 4 on esitetty sekä uudisrakennuksen että olemassa olevan rakennuksen älykkyyden luokittelut.

Taulukko 4. Älyrakennuksen luokittelutavat [Rantala ym. 2015: 23-26].

Älyrakennuksen luokitus	Uudisrakennus	Vanha rakennus

Luokka E	---	Rakennusta ei paranneta millään tavalla, ei investointeja. Rakennuksen arvo laskee.
Luokka D	Normaali osajärjestelmien toteutus. Järjestelmät toimivat itsenäisesti ja automaattisesti, eivät integroidu toisten järjestelmien kanssa. Energiatehokkuusluokka C.	Rakennusta peruskorjataan vastaamaan nykyhetken vaatimuksia ja tasoja. Tekninen ja älyllinen taso pysyy ennallaan. Rakennusautomaatio otetaan käyttöön, toimii itsenäisenä järjestelmänä. Energiatehokkuutta parannetaan.
Luokka C	Rakennuksen järjestelmät toteutettu optimaalisesti, toiminta automaattista ja itsenäistä. Osa järjestelmistä integroituu toimimaan yhdessä toisten järjestelmien kanssa. Energiatehokkuusluokka B.	Rakennusta parannetaan, osajärjestelmät tukevat ja optimoivat älyrakennuksen ominaisuuksia. Tietomallinnetaan koko rakennus. Energiatehokkuutta parannetaan tehokkaammin kuin luokassa D.

Luokka B	Rakennuksen järjestelmät toimivat yhdessä ja niiden hallinta tapahtuu yhteisen käyttöliittymän kautta. Energiatehokkuusluokka A.	Rakennuksen järjestelmät toimivat yhdessä ja niiden hallinta tapahtuu yhteisen käyttöliittymän kautta. Tekninen ja älyllinen taso paranee. Energiatehokkuutta parannetaan tehokkaammin kuin luokassa C.
Luokka A	Yhteydet älykkääseen kaupunkiympäristöön tietoverkkojen kautta. Kyberturvallinen yhteys ympäristöön ja muuhun maailmaan. Energiatehokkuusluokka A.	Yhteydet älykkääseen kaupunkiympäristöön tietoverkkojen kautta. Kyberturvallinen yhteys ympäristöön ja muuhun maailmaan. Energiatehokkuutta parannetaan tehokkaammin kuin luokassa B.

Älyrakennuksen älykkyysluokittelun valinnassa tulisi ottaa kaikkien rakennusten käyttäjien tarpeet huomioon. Valitettavasti varsinkin asuisrankentamisessa asukkaiden vaikutusmahdollisuus jää yleensä pieneksi, sillä usein rakennuksen älykkyyteen liittyvät investointipäätökset on ehditty tekemään jo ennen kuin asukkaiden älykkyyteen liittyviä toiveita päästään huomiomaan. Älyrakentamisessa tulisi kiinnittää huomioita siihen, että rakennuksen tulevat käyttäjät, hallinnoijat ja omistajat pääsisivät mukaan hankesuunnitteluun mahdollisimman aikaisessa vaiheessa. [Rantala ym. 2015: 104.]

Älyrakennuksen suunnittelussa valittava älykkyystaso ja käyttöön tulevat ratkaisut sekä teknologiat vaikuttavat myös kyberturvallisuuden ja suojauskeinojen suunnitteluun. Jokainen tehty valinta tuo mukanaan uusia uhkia ja mahdollisuuksia, jotka täytyy huomioida myös älyrakennuksen kyberturvallisuuden suunnittelussa.

Älyrakennuksen suunnittelun ja toteutusvaiheen suurin ja tärkein päämäärä on saada rakennuksesta käyttäjälähtöinen, ekologinen ja kustannustehokas älyrakennus. Käyttäjälähtöisen älyrakennuksen vastakohtina voidaan pitää järjestelmäkeskeistä älyrakennusta tai asiantuntijakeskeistä älyrakennusta. Järjestelmäkeskeisen älyrakennuksen hankesuunnitteluvaiheessa teknologia valitaan jo ennen kuin käyttäjien tarpeita on päästy huomioimaan. Asiantuntijakeskeisessä älyrakennuksessa älykkyyteen liittyvät ratkaisut valitaan älypalveluita tuottavien asiantuntijoiden olettamuksien perusteella, joissa asiantuntijat olettavat tietävänsä älyrakennuksen tulevien käyttäjien tarpeet. On siis erittäin tärkeää, että rakennuksen tulevien ja pääasiallisten käyttäjien tarpeet otetaan huomioon mahdollisimman aikaisessa vaiheessa, jotta älyrakennuksen tarjoamat älypalvelut ovat mahdollisimman käyttäjälähtöisiä, helppokäyttöisiä sekä hyödyllisiä. [Rantala ym. 2015: 106-107.] Seuraavassa käydään lävitse älyrakennuksen suunnittelu- ja toteutusprosessin vaiheita.

5.1 Tarveselvitys

Rakennus- ja suunnitteluprosessi lähtee käyntiin tarveselvitysvaiheesta, jossa pohditaan älyrakennuksen tarpeellisuutta. Tarveselvitysvaiheessa pohditaan rakennettavan älyrakennuksen mahdollisia älyluokitusvaihtoehtoja sekä sitä, millaista varustelua rakennettavaan älyrakennukseen tarvitaan, jotta saavutetaan mahdollisimman käyttäjäystävällinen, ekologinen ja toimintavarma älyrakennus. [Rantala ym. 2015: 111.]

5.2 Hankesuunnittelu

Kun rakennuksen tarpeellisuudesta on päästy yhteisymmärrykseen, voidaan hankesuunnitteluvaihe aloittaa. Hankesuunnitteluvaiheen tarkoituksena on päättää, minkälainen älyrakennus tarvitaan ja kuinka paljon rakennettavaan älyrakennukseen on mahdollista investoida rahaa. Hankesuunnitteluvaiheessa päätetään myös rakennettavan älyrakennuksen älykkyysluokitus, päätetään tarvittavat käyttäjälähtöiset sekä älykkyyttä parantavat järjestelmät, ratkaisut ja ominaisuudet sekä luodaan eritelty rakennushankkeen kustannusarvio. Osana hankesuunnittelua on tärkeä pitää alusta asti mukana myös ris-

kilähtöisyys, jonka yhtenä osana varaudutaan erilaisiin kyberuhkiin. Ratkaisujen ja teknologioiden valinnassa ja vertailussa on alusta asti kyettävä huomioimaan myös niiden heikkoudet ja niihin liittyvät riskit sekä mahdollisuudet ja keinot hallita näitä erilaisin suojauskeinoin. [Rantala ym. 2015: 112-113.]

5.3 Hankinta-aineistojen laatiminen

Hankinta-aineistojen laatimisvaiheen aluksi tarkastellaan ja vertaillaan hankesuunnitteluvaiheessa luotuja suunnitelmaratkaisuja, jotta saadaan selvitettyä hankittavien laitteistojen ja järjestelmien keskinäinen yhteensopivuus, näiden ratkaisujen vaatima tiedonsiirtotapa sekä päätetään järjestelmiin ja laitteisiin liittyvien oheistarvikkeiden hankinnan rajaukset kuten kaapeloinnin hankinnat, asennukset ja kytkennät. Kun edellä mainituista hankinnoista päästään yhteisymmärrykseen, voidaan luoda yksiselitteiset ja luotettavat älyrakennuksen toteuttamista varten vaadittavat hankinta-aineistot. [Rantala ym. 2015: 114-115.]

5.4 Toteutussuunnittelu

Toteutussuunnitteluvaiheen tarkoituksena on luoda yksityiskohtainen tekninen suunnitelma siitä, kuinka älyrakennuksen järjestelmät tullaan todellisuudessa toteuttamaan. Toteutussuunnitelman tulee olla mahdollisimman yksiselitteinen ja tarkka, jotta toteutusvaiheessa vältytään uusilta lisäkysymyksiltä ja ongelmilta. Toteutussuunnitelmasta tulee käydä ilmi muun muassa kaikki toteutusvaiheessa tarvittavat tiedonsiirtotavat, mistä ja miten älyrakennuksen järjestelmiä tullaan jatkossa hallinnoimaan sekä minkälaista kaapelointia toteutusvaiheessa tarvitaan. Toteutussuunnittelussa tulee myös ottaa huomioon tulevaisuuden näkymät esimerkiksi uusien älykkäiden toimintojen ja järjestelmien lisääminen tulevaisuudessa. Keskeinen osa älyrakennuksen toteutussuunnittelua on myös laadun, toimintavarmuuden ja kyberturvallisuuden suunnittelu. Myös nämä tulee huomioida yksityiskohtaisesti osana älyrakennuksen teknistä suunnittelua. [Rantala ym. 2015: 116.]

Kyberturvallisuus on osa älyrakennuksen laatua ja sitä tulee lähestyä riskilähtöisesti. Toteutussuunnitteluvaiheen aikana tunnistetaan älyrakennukseen kohdistuvat ulkoiset vaatimukset ja riskit, joiden pohjalta suunnitellaan kyberturvallisuuteen liittyvät suojauskeinot osaksi tietojärjestelmäkokonaisuutta ja arkkitehtuuria. Tehdyt suunnitelmat, arkkitehtuurikuvaukset ja tekniset määrittelyt tulee katselmoida ja arvioida suunnittelutyön aikana hyödyntäen uhkamallinnuksen keinoja mahdollisten heikkouksien tunnistamiseksi. Uhkamallinnuksessa mallinnetaan suunniteltu toteutus ja arvioidaan sitä mahdollisien käsittelemättömien uhkien ja haavoittuvuuksien tunnistamiseksi. Tarkoituksena on arvioida valittuja suojauskeinoja sekä niiden riittävyyttä varmistaen, että kaikkiin relevantteihin uhkiin on varauduttu asianmukaisesti. Uhkamallinnuksen avulla pyritään huomaamaan ongelmat ja puutteet mahdollisimman aikaisessa vaiheessa jo suunnittelun aikana, jotta niiden korjaaminen olisi vielä mahdollisimman helppoa. [Shostack 2014: 3-4; 29.]

Toteutussuunnittelun seurauksena älyrakennuksen toteuttamista varten tulisi olla mahdollisimman yksityiskohtainen kuvaus siihen liittyvästä teknisestä ympäristöstä ja sen suojaamisesta asianmukaisin kontrollein. Määritetyt suojauskeinot ovat valittu perustuen ulkoisiin vaatimuksiin, arvioituihin riskeihin ja yleisiin hyviin käytäntöihin. Tehdyt määrittelyt ovat myös katselmoitu ja arvioitu sen varmistamiseksi, että kaikki tarvittavat asiat on huomioitu sekä oikeat valinnat on tehty suojauskeinojen osalta. [Shostack 2014: 29.]

5.5 Rakentaminen, valvonta ja laadun varmistus

Kun kaikki tarvittavat suunnitelmat ovat tehty ja niistä on päästy yhteisymmärrykseen, voidaan älyrakennuksen varsinainen rakentaminen aloittaa. Rakennusvaiheessa on tärkeää, että laadittuja suunnitelmia noudatetaan tarkasti. Mikäli suunnitelmia ei rakentamisvaiheessa noudateta, voivat jotkin tarvittavat älyratkaisut toimia virheellisesti tai pahimmillaan ne menetetään kokonaan. Tämän vuoksi rakennusvalvonta ja laadun varmistus on erittäin tärkeässä roolissa. Laadun varmistuksella saadaan varmuus sille, että vaaditut älyratkaisut on toteutettu suunnitelmien mukaisesti ja ne toimivat loppukäyttäjän kannalta mahdollisimman optimaalisella tavalla. Koska kyberturvallisuus on osa älyrakennuksen laatua, myös asetettujen suojauskeinojen katselmointi, arviointi ja testaaminen ovat keskeinen osa toteutustyön valvontaa sekä valmiin toteutuksen hyväksyntää.

Tästä johtuen osana rakentamiseen ja sen valvontaan liittyviä suunnitelmia tulee määrittää myös se, miten kyberturvallisuuteen liittyvien suojauskeinojen oikeanlainen toteuttaminen ja kaikkien kontrollien huomioiminen varmistetaan. Tähän liittyvät olennaisesti erilaiset toteutusta koskevien kuvausten ja konfiguraatioiden katselmoinnit sekä tietojärjestelmien tekninen testaaminen. [Rantala ym. 2015: 117-118.]

5.6 Käyttö ja ylläpito

Älyrakennus valmistuu, kun rakentamisvaihe saadaan päätökseen. Tällöin älyrakennuksen käyttö ja ylläpito voi alkaa. Käyttö- ja ylläpitovaiheessa on tärkeää, että älyrakennusta ja sen järjestelmiä käytetään asianmukaisella tavalla. Tällä tavalla varmistetaan älyrakennuksen optimaalinen toimivuus ja vähennetään tarvittavia ylläpito- ja korjauskustannuksia. Asianmukainen käyttö ja ylläpito saavutetaan, kun käyttäjien ja ylläpitäjien kouluttamisesta ja perehdyttämisestä pidetään huolta. Älyrakennuksen suunnitteluvaiheen aikana tulee varmistaa, että tehdyt suunnitelmat mahdollistavat myös kyberturvallisuuden ylläpitämisen rakennuksen käytön ja ylläpidon aikana. Jos tehdyt suunnitelmat ja valinnat johtavat sellaiseen toteutukseen, ettei esimerkiksi päivityksiä tai lokienhallintaa voida helposti, keskitetysti ja automaattisesti toteuttaa, tai yksittäistä haavoittuvaa komponenttia ei voida helposti korvata, voi kyberturvallisuuden ylläpitäminen olla haastavaa ja työlästä. [Rantala ym. 2015: 118-119.]

5.7 Purku ja poisto

Purku- ja poistovaiheessa älyrakennus on saavuttanut elinkaarensa pään. Tässä vaiheessa on huolehdittava poistettavien laitteiden ja muiden materiaalinen asianmukaisesta poistamisesta jätehuolto- ja kierrätysmääräyksien mukaisesti. On myös otettava huomioon, tarvitaanko poistettavia laitteita varaosana esimerkiksi muissa järjestelmissä tai älyrakennuksissa. [Rantala ym. 2015: 119.]

6 Älyrakennuksen kyberturvallisuus

Seuraavissa alaluvuissa käsitellään ylätasolla yleisiä hyviä käytäntöjä ja suojauskeinoja, jotka on hyvä huomioida älyrakennuksen suunnittelu ja toteutusvaiheessa, kun määritetään ja käyttöönotetaan kontrolleja kyberturvallisuuden varmistamiseksi. Esiteltyjen suojauskeinojen on tarkoitus antaa yleiskuva huomioitavista asioista, joita tulee käsitellä osana älyrakennuksen riskilähtöisen kyberturvallisuuden toteuttamista.

6.1 Vaatimustenmukaisuus

Älyrakennuksiin, niissä käytettäviin ratkaisuihin ja tietojärjestelmiin voi kohdistua erilaisia ulkoisia vaatimuksia, jotka tulee tunnistaa ja huomioida osana suunnittelua sekä toteutusta. Ulkoisia vaatimuksia ja niissä mahdollisesti tapahtuvia muutoksia on kyettävä myös seuraamaan, jotta muutokset saadaan huomioitua käytännön toteutuksessa. Ulkoisia vaatimuksia muodostavat muun muassa lainsäädäntö ja viranomaisohjeet, sekä asiakkaiden, vuokralaisten ja tilojen käyttäjien mahdolliset sopimusvaateet rakennuksen tietojärjestelmien kyberturvallisuudelle. Sisäiset vaatimukset muodostuvat rakennuksen tilaajan ja toteuttajan itse määrittämistä periaatteista ja kontrolleista, jotka toteutukselle päätetään asettaa. Kaikki toteutukseen kohdistuvat vaatimukset on tärkeää kirjata ylös sekä viestiä ne jokaiselle tarpeelliselle älyrakennuksen toteuttamiseen osallistuvalle sidosryhmälle.

Suunnitteluvaiheen aikana määritetään, miten tunnistetut vaatimukset toteutetaan käytännössä, ja itse toteutusvaiheen aikana tulee seurata ja arvioida toteutustyötä varmistaen vaatimusten asianmukaisen huomioimisen.

6.2 Sisäänrakennettu kyberturvallisuus ja tietosuoja

Lähtökohtana koko älyrakennuksen suunnittelussa ja toteuttamisessa on, että kaikkiin siinä käytettäviin ratkaisuihin ja tietojärjestelmiin on sisäänrakennettu kyberturvallisuus ja tietosuoja (*Security by Design* ja *Privacy by Design*). Molemmat nähdään osana käytettävien ratkaisujen laatua ja kokonaisuutta eikä erillisinä asioina.

Kyberturvallisuus on sisäänrakennettuna käytettyihin ratkaisuihin jo niiden suunnittelusta lähtien huomioiden tarvittavat kontrollit kaikkiin järjestelmien elinkaaren vaiheisin. Elinkaaren vaiheita ovat tietojärjestelmien määrittely ja suunnittelu, kilpailutus ja hankinta, toteutus ja kehitys, käyttöönotto, ylläpito sekä käytöstä poisto. Kaikkien elinkaaren vaiheiden osalta määritetään ja toteutetaan älyrakennuksen tietojärjestelmiin kohdistuvien ulkoisten ja sisäisten vaatimusten sekä tunnistettujen riskien edellyttämät suojauskeinot kyberturvallisuuden varmistamiseksi. [Baseline Security Recommendations for IoT 2017: 63.]

Jos älyrakennuksen tietojärjestelmät keräävät ja käsittelevät henkilötietoja, tulee niiden osalta noudattaa voimassa olevaa tietosuojalainsäädäntöä, kuten Euroopan unionin tietosuoja-asetusta sekä kansallista tietosuojalakia. Jo älyrakennuksen suunnitteluvaiheessa on kyettävä tunnistamaan mahdolliset kerättävät henkilötiedot sekä toteutettava kokonaisuus niin, että henkilötietoja käsitellään lainmukaisesti ja niiden tietosuoja varmistaen. Kuten kyberturvallisuudenkin osalta, tietosuoja sisäänrakennetaan osaksi käytettyjä ratkaisuja sekä kokonaistoteutusta, jossa käsitellään henkilötietoja. Henkilötietoja tulee kyetä suojamaan asianmukaisesti kaikissa niiden säilytys- ja käsittelypaikoissa ja järjestelmissä sekä myös tiedonsiirron aikana. Älyrakennuksen tietojärjestelmäympäristö tulee toteuttaa tämä huomioiden. Myös henkilötietojen säilytysajat, henkilötiedon minimointi ja rekisteröidyn oikeudet sekä muut tietosuojasääntelystä tulevat velvoitteet tulee kyetä huomioimaan tietojärjestelmien suunnittelussa ja toteuttamisessa. [Baseline Security Recommendations for IoT 2017: 68.]

6.3 Omaisuuden hallinta ja ympäristön kuvaaminen

Suunnitelmallisella omaisuuden hallinnalla tunnistetaan ja hallitaan älyrakennukseen liittyviä tietojärjestelmiä läpi niiden elinkaaren. Omaisuuden hallinnan avulla varmistetaan, ettei hyväksymättömiä ja ilman asianmukaista suojausta olevia laitteita ja liittymiä liitetä rakennuksen ekosysteemiin. Sen avulla varmistetaan myös, että kaikki ympäristössä olevat tietojärjestelmät ja laitteet ovat muun muassa päivitysten ja haavoittuvuuksien hallinnan piirissä. Varjo-IT ja -IoT (*shadow IT & IoT*) muodostavat selvän riskin esimerkiksi tarjoamalla hyökkääjille heikommin hallittuja, kontrolloituja ja valvottuja kohteita ja hyök-

käyspinta-alaa organisaation tietojärjestelmiin ja verkkoon. [Baseline Security Recommendations for IoT 2017: 63; The CIS Critical Security Controls for Effective Cyber Defense 2016: 6-12.]

Älyrakennuksen ekosysteemiin kuuluvista tietojärjestelmistä ja niihin kuuluvista osista, kuten laitteista, antureista, ohjelmistoista ja lisensseistä laaditaan inventaario, jota saatetaan kutsua myös laiterekisteriksi tai -luetteloksi. Inventaarion lisäksi on tärkeää laatia kuvaukset ja dokumentaatio älyrakennuksen tietojärjestelmäarkkitehtuurista sekä tietovirroista. Inventaarion, arkkitehtuurin mallintamisen ja tietovirtojen kuvaamisen avulla varmistetaan osaltaan suojattavan omaisuuden asianmukainen hallinta ja suojaaminen, sekä riskien tunnistaminen ja hallinta. Kaikki ympäristöön liitettävät laitteet ja niihin liittyvä keskeinen tieto (mm. tekniset tiedot, omistajuus, vastuuhenkilöt) lisätään inventaarioon ja jokaisen järjestelmiä koskevan muutoksen on päivityttävä osaksi inventaariota. Sama koskee arkkitehtuuria ja tietovirtoja koskevia kuvauksia. Tämä edellyttää sekä oikeanlaisten toimintaprosessien käyttöönottoa että tarvittavien teknologioiden hyödyntämistä inventaarion ja kuvausten ylläpidossa. Inventaarion ylläpidossa voidaan hyödyntää automatisoituja ratkaisuja ja työkaluja, kuten *Asset-Inventory* –työkaluja, jotka aktiivisesti skannaavat rakennuksen IT-ympäristössä olevia laitteita. On ensiarvoisen tärkeää, että älyrakennuksen valmistuessa koko siihen liittyvästä IT-ympäristöstä on olemassa ajantasainen ja helposti ylläpidettävä inventaario ja kuvaukset, mikä mahdollistaa paremmin myös järjestelmien ylläpidon. Älyrakennuksen IT-ympäristöä koskevat tekniset ja arkkitehtuurilliset kuvaukset ovat aivan yhtä kriittisiä ja tärkeitä kuin muukin rakennusta koskeva keskeinen dokumentaatio. [Baseline Security Recommendations for IoT 2017: 63; The CIS Critical Security Controls for Effective Cyber Defense 2016: 6-12.]

6.4 Laiteturvallisuus

Älyrakennukseen liittyvien laitteiden ja sovellusten suunnittelussa ja valinnassa on huomioitava niihin kohdistuvat kyberuhkat ja varauduttava näihin asianmukaisin suojakeinoin [IoT Security Compliance Framework 2018: 6]. Teknologioiden ja laitteiden valinnassa huomioidaan niihin liittyvät mahdollisuudet suojautua älyrakennukseen kohdistuvia uhkia vastaan. Keskeisille ja etenkin kriittisille laitteille määritetään kovennusohje, jonka avulla pyritään niiden turvalliseen asennukseen ja konfiguraatioon, jossa keskeiset

kyberuhkat on huomioitu asianmukaisin suojakeinoin. Siltä osin kuin mahdollista, asennuksessa on hyvä käyttää yhdenmukaisesti valmiiksi määritettyä asennusimagea. [The CIS Critical Security Controls for Effective Cyber Defense 2016: 6-12.]

Järjestelmäympäristössä keskeistä on, että sulautetuille järjestelmille on luotettavan ja turvallisen tietojenkäsittelyn varmistava perusrakenne, TCB (*Trusted Computing Base*). TCB-pohjan muodostavat laitteisto, ohjelmistot ja protokollat yhdessä, ja se pyrkii varmistamaan laitteen eheyden, tunnistamaan muut laitteet sekä hallitsemaan tietoliikenteen ja sovellusten turvallisuutta. Keskeisessä roolissa TCB on luottamuksen lähteenä (*root of* trust) toimiva luottamusankkuri (*trust anchor*), joka esimerkiksi käsittelee ja säilyttää kryptografisia salaisuuksia kuten salausavaimia. Laitteessa luottamusankkuri on joku erillinen fyysinen siru tai turvallinen ydin prosessorin (*CPU*, Central Processing Unit) sisällä. Luottamusankkuria käytetään muun muassa autentikoimaan muita laitteita ja dataa viestinnän aikana. Luottamusankkurin on kyettävä turvallisesti varmistamaan, että viestit ja muiden laitteiden identiteetit voidaan autentikoida sekä kertoa näistä tuloksista TCB:lle sen päätöksenteon tueksi. Osana tätä on myös kyky varmistaa laitteen oman alustan eheys. [IoT Security Guidelines for Endpoint Ecosystems 2019: 23-27.]

TCB, jonka tehtävänä on vastavuoroinen autentikointi laitteiden välillä, auttaa luottamuksen lähteen muodostamisessa ja autentikoi itsensä kryptografisesti muille laitteille. Tällä osaltaan varmistetaan sitä, että verkossa olevat laitteet ovat, mitä väittävät olevansa. Esimerkiksi, jos joku verkossa oleva laite esiintyy päivityspalvelua tarjoavana laitteena, TCB autentikoi tämän laitteen ja varmistaa sen kuulumisen osaksi IoT-ratkaisun kokonaisuutta ennen päivitystiedoston vastaanottamista. [IoT Security Guidelines for Endpoint Ecosystems 2019: 25.]

TCB validoi verkossa olevat muut laitteet ja varmistaa datan luottamuksellisuutta ja eheyttä myös ilman taustapalveluiden tukea. Vaikka tietoliikenne taustapalveluihin katkeaisi, paikallinen IoT-ekosysteemi kykenee toimimaan turvallisesti määrätyn aikaa. TCB on kriittinen elementti IoT-arkkitehtuurissa ja keskeisessä roolissa turvallisessa kommunikaatiossa laitteiden välillä. Ilman TCB:tä ei ole yhtä keskitettyä komponenttia, joka hallitsee päätelaitteen turvallisuutta. [IoT Security Guidelines for Endpoint Ecosystems 2019: 25.]

Valittavien tuotteiden osalta on tärkeää varmistaa, että tämä toteutus on tehty oikein ja asianmukaisesti takaamaan riittävä suojaustaso, sillä esimerkiksi vääränlaisen luottamusankkurin valinta luo ainoastaan valheellisen turvallisuuden tunteen. On myös tärkeää, että IoT-laitteilla on koko niiden elinkaaren kestävä luottamusankkuri. [IoT Security Guidelines for Endpoint Ecosystems 2019: 23-24.]

Laitteiden kohdalla kaikki tietoliikenneportit, -protokollat ja palvelut on rajattu minimiin, mikä sallii ainoastaan toiminnan kannalta tarpeelliset. Kaikki käyttämättömät fyysiset ja virtuaaliset tietoliikenneportit, kuten USB ja RS232, poistetaan käytöstä tai niiden käyttö sallitaan vain tunnistetuille ja valtuutetuille laitteille. Laiteisiin kohdistuvia ja niiden välisiä valtuuttamattomia yhteyksiä rajoitetaan ja liikennettä suodatetaan palomuurein. [IoT Security Compliance Framework 2018: 19-23.]

Laitteiden käyttöjärjestelmistä on poistettu tarpeettomat palvelut ja käyttövaltuudet on rajattu minimiin. Käyttöjärjestelmän ytimen kutsuminen tietoliikenneporttien tai hyväksymättömien sovellusten toimesta on estetty. Käyttöjärjestelmän tukemia turvallisuusominaisuuksia käytetään soveltuvassa laajuudessa. Sovellusten tulee toimia vähimpien oikeuksien periaatteen mukaisesti, mikä sallii niille pääsyn ainoastaan niiden toiminnan kannalta tarpeellisiin resursseihin. Hyväksymättömien ohjelmistojen asentaminen laitteille on estetty. [IoT Security Compliance Framework 2018: 19-22.]

6.5 Vikaturvallisuus ja vikasietoisuus

Tietojärjestelmät suunnitellaan ja toteutetaan niin, että niissä on varauduttu myös erilaisiin häiriötilanteisiin toteuttaen ratkaisut vikaturvallisiksi (*fail-safe*). Toteutuksessa on tunnistettu tietojärjestelmään kohdistuvan häiriön mahdolliset vaikutukset ja seuraukset, jotka voivat aiheuttaa vahinkoa muulle ympäristölle tai rakennuksen käyttäjille. Rakennuksen tekniset järjestelmät eivät saa vika- tai häiriötilanteessa aiheuttaa fyysistä vahinkoa, muuttua vaarallisiksi, tai häiritä muita keskeisiä järjestelmiä, vaan tämä estetään toteuttamalla järjestelmät vikaturvallisiksi ja vikasietoisiksi. Tällaisia häiriöitä voivat aiheuttaa esimerkiksi odottamattomat laitteelle tulevat väärät syötteet ja järjestelmähäiriöt. [Baseline Security Recommendations for IoT 2017: 68-69; IoT Security Compliance Framework 2018: 20-21.]

Rakennuksen tärkeiden toimintojen tulee toimia myös tilanteissa, joissa esimerkiksi sähkönsyöttö tai verkkoyhteys on hetkellisesti poikki. Laitteet tulee toteuttaa niin, etteivät ne olisi vikaherkkiä vaan mahdollisimman vikasietoisia sekä kykeneviä toimimaan myös paikallisesti itsenäisesti tai manuaalisesti esimerkiksi tilanteissa, joissa verkkoyhteys on katkennut. Lähtökohtaisesti järjestelmien tulee olla myös sellaisia, että ne kykenevät poikkeamatilanteen jälkeen palaamaan normaalitoimintaan häiriöttä esimerkiksi verkkoyhteyden tai sähkönsyötön palautuessa. Häiriötilanteisiin tulee varautua jatkuvuus- ja toipumissuunnittelun avulla. [Baseline Security Recommendations for IoT 2017: 69; IoT Security Compliance Framework 2018: 25.]

6.6 Päivitysten hallinta

Osana älyrakennuksen suunnittelua, teknologioiden valintaa ja niissä käytettävien suojauskeinojen määrittämistä on tärkeää varmistaa ympäristöön liittyvien laitteiden ja ohjelmistojen päivittämistarve ja sen turvallinen toteuttaminen. Päivitysten avulla varmistetaan ympäristön ajantasaisuutta ja turvallisuutta sekä esimerkiksi korjataan havaittuja haavoittuvuuksia. Myöhemmässä ylläpitovaiheen määrittelyssä suunnitellaan itse päivitysprosessin toteuttaminen ja siihen liittyvät roolit, vastuut ja toimenpiteet.

Päivitysten osalta on myös tärkeä varmistaa päivitystiedostojen ja niiden lähteen luotettavuus. Laitteet estävät autentikoimattomien ohjelmistojen lataamista niihin ja esimerkiksi laitteiden etänä tapahtuvien päivitysten kohdalla päivityspaketeissa on digitaalinen allekirjoitus ja sertifikaatti, jotka autentikoidaan niiden alkuperäisyyden varmistamiseksi. Myös päivityspakettien tiedonsiirron salauksesta ja suojauksesta tulee huolehtia. Sellaisten laitteiden osalta, joiden päivittäminen ei syystä tai toisesta ole mahdollista, tulee suunnitella periaatteet ja toimintamalli laitteiden korvaamiseksi tietyn elinkaaren jälkeen. [IoT Security Compliance Framework 2018: 19-20.]

Päivitysten suunnittelussa on huomioitava myös mahdollinen tarve osittaiselle päivityksen asentamiselle sellaisiin laitteisiin, joiden verkkoyhteys on esimerkiksi rajallinen tai epävakaa. Päivitysprosessi tulee myös suunnitella niin, ettei se kuormita laitteita liikaa varsinkaan sellaisina aikoina, jolloin sillä voi olla negatiivista vaikutusta älyrakennuksen toimintaan ja käyttöön. [IoT Security Compliance Framework 2018: 21.]

6.7 Pääsynhallinta

Asianmukaisella pääsynhallinnalla mahdollistetaan älyrakennuksen tietojärjestelmien luvallinen käyttö sekä estetään oikeudetonta käyttöä. Pääsynhallintaan liittyvien suojakeinojen sekä käytettävän autentikoinnin ja autorisoinnin taso ja näihin käytettävät menetelmät suunnitellaan perustuen tietojärjestelmiin kohdistuviin vaatimuksiin ja tunnistettuihin riskeihin. Olennaista on, että kaikki järjestelmät ja laitteet autentikoivat riittävän luotettavasti käyttäjät, muut järjestelmät ja sovellukset sekä taustaprosessit. [Baseline Security Recommendations for IoT 2017: 70.]

Jokaisen yksittäisen käyttäjän toimet on oltava mahdollista selvittää yksilöiden ja yhdistäen suoritetut toimet henkilöön riittävän luotettavasti. Tästä johtuen käyttäjät kirjautuvat ympäristöön aina henkilökohtaisilla tunnuksilla, eikä yhteiskäyttöisiä tunnuksia käytetä. Käyttöoikeuksien ja -valtuuksien määrittäminen tehdään työroolipohjaisesti, jolloin tunnistetuille työrooleille määritetään ja lisätään työtehtävissä tarvittavat oikeudet ja henkilöt liitetään työnkuvansa mukaisesti työrooleihin. Käyttöoikeus on käyttäjälle myönnetty oikeus kohteen tai palveluelementin käyttöön ja käyttövaltuus taas määrittää sen, miten ja missä laajuudessa käyttäjä saa tätä käyttää. Roolipohjaisuudessa työroolien käyttöoikeudet ja -valtuudet perustuvat aina tehtäväkohtaisiin todellisiin tarpeisiin ja ”*kaikki on kielletty, ellei sitä ole erikseen sallittu*” -periaatteeseen, eikä niihin kiinnitetä tarpeettomia oikeuksia ja valtuuksia. Pääsynhallinnassa noudatetaan lisäksi aina ”*vähimpien oikeuksien periaatetta*” (*principle of least privilege*) antaen työrooleille ja käyttäjille suppeimmat mahdolliset oikeudet, joilla käyttäjä kykenee suoriutumaan työtehtävistään. Käyttöoikeudet ja käyttövaltuudet poistetaan välittömästi, kun niihin oikeuttava peruste päättyy esimerkiksi työsuhteen, toimeksiannon tai projektin päättyessä tai käyttäjän roolin muuttuessa. [Baseline Security Recommendations for IoT 2017: 72; Security and Privacy Controls for Federal Information Systems and Organizations 2013: F7-F13.]

Älyrakennuksen suunnitteluvaiheessa on jo hyvä pohtia, miten käyttövaltuushallinta toteutetaan. Käyttöoikeuksien ja -valtuuksien hallinta toteutetaan määritetyn prosessin mukaisesti ja jos mahdollista, tätä tukevaa identiteetin ja pääsynhallinnan järjestelmää (IAM,

Identity and Access Management). Siltä osin kuin on mahdollista, älyrakennuksen tietojärjestelmät voidaan integroida IAM-järjestelmään keskittäen ja automatisoiden käyttövaltuuksien lupienanto- ja provisiointiprosessia.

Pääsynhallinnassa käytettävien keinojen on perustuttava suunnitteluvaiheessa tehtyihin riskiarvioihin ja oltava riskeihin nähden asianmukaisia suojauskeinoja oikeudettoman käytön ennaltaehkäisemiseksi. Tunnistautumisessa käytetään kuitenkin aina vahvaa salasanaa tai monivaihteista tunnistautumista. Salasanoihin liittyvät laatuvaatimukset on teknisesti pakotettu kaikkialla, missä se on mahdollista, ja ne perustuvat johonkin luotettavaan lähteeseen, kuten valmistajan tai viranomaisen ohjeistukseen laadukkaista salasanoista. [IoT Security Guidance 2017.]

Pääsynhallinnan menettelyitä ja ympäristön koventamista suunnitellessa on tunnistettava keskeiset hyökkäysvektorit ja uhkat, joita vastaan varaudutaan. Tällaisia uhkia ovat esimerkiksi asennuksen aikana ympäristöön jäävät yleisesti tiedossa olevat oletussalasanat, selkokielisenä siirrettävät tai säilytettävät salasanat ja salasanojen arvaamiseen perustuva väsytyshyökkäys (*brute-force*). Tästä johtuen kaikki oletuskäyttäjätunnukset ja -salasanat vaihdetaan asennuksen ja tilien luonnin yhteydessä eikä heikkoja tai tyhjiä salasanoja sallita. Ympäristön tulee olla suunniteltu niin, ettei pääsynhallintaan liittyviä käyttäjätunnuksia ja salasanoja säilytetä tai siirretä selkokielisinä, eikä järjestelmien tule sisältää ikinä kovakoodattuja salasanoja. [Baseline Security Recommendations for IoT 2017: 72; IoT Security Compliance Framework 2018: 22.]

Laitteiden ja ohjelmistojen tulee toimia niin, että käyttäjätunnus lukkiutuu määräajaksi, kun määritetty lukumäärä vääriä kirjautumisyrityksiä täyttyy. Tällä ennaltaehkäistään muun muassa mainittujen väsytyshyökkäysten toimivuutta. Lukittuminen voi raueta määräajan kuluttua tai hallintatunnusten kohdalla se voi edellyttää myös manuaalista toimenpidettä. Myös käyttäjien istunnot katkaistaan määritetyn inaktiivisuusajan jälkeen muun muassa session kaappaukseen perustuvien hyökkäysvektorien minimoimiseksi. [Baseline Security Recommendations for IoT 2017: 71; IoT Security Compliance Framework 2018: 22, 28; IoT Security Guidelines for Endpoint Ecosystems 2019: 35-36.]

Pääsynhallinnan määrittelyitä ja ympäristön kovennuksia suunnitellessa varmistetaan, ettei älyrakennuksen teknisessä ympäristössä peruskäyttäjillä ole pääsyä muokkaamaan tietojärjestelmien ja laitteiden turva-asetuksia, laiteohjelmistoa tai ohjelmistokoodia. Vahvoihin hallintatunnuksiin (kuten pääkäyttäjien ja ylläpitäjien tunnukset), joilla on laajemmat käyttövaltuudet, tulee kohdistaa peruskäyttäjiä vahvempia kontrolleja, kuten monivaiheinen tunnistautuminen ja tarkempi lokivalvonta. Ideaalitilanteessa hyödynnetään mahdollisimman paljon *Just-enough (JEA)* ja *Just-in-time (JIT)* tyyppisiä hetkellisesti annettavia valtuuksia, kun laajemmille oikeuksille on tarvetta. Hallintatunnuksia ei tule myöskään koskaan käyttää normaalikäytössä, vaan ainoastaan niitä edellyttäviä toimenpiteitä suorittaessa. [Baseline Security Recommendations for IoT 2017: 72.]

Valvonnan avulla seurataan, että käyttäjätilit, käyttöoikeudet ja käyttövaltuudet ovat ajan tasalla, ja niiden käyttö on asianmukaista ja noudattaa sovittuja käytäntöjä. Osana älyrakennuksen suunnittelua on suunniteltava myös nämä valvontamekanismit ja niiden toteutus. Valvontaa voidaan toteuttaa sekä automaattisesti että manuaalisin katselmoinnein. Lokien keräämisen kannalta on tärkeää huomioida suunnittelussa, että myös kaikkien käyttövaltuushallintaan liittyvien tapahtumien tulee olla raportoitavissa. Kaikki käyttäjätileihin, työ- ja käyttäjärooleihin, käyttöoikeuksiin ja –valtuuksiin sekä muihin määrityksiin tehtävät muutokset ovat jäljitettävissä muutoksista syntyvien yksilöivien lokimerkintöjen kautta.

6.8 Salaus

Tiedon salaamisella varmistetaan tiedon luottamuksellisuus ja eheys tietoa tallennettaessa sekä siirrettäessä. Tieto salataan käyttämällä joko symmetristä tai epäsymmetristä salausmenetelmää. Symmetristä salausmenetelmää hyödyntävät salausalgoritmit käyttävät tiedon suojaamiseen yhtä salausavainta. Epäsymmetristä salausmenetelmää hyödyntävät salausalgoritmit suojaavat tiedon salausavainparin avulla, jossa toinen salausavain on julkinen ja toinen yksityinen. [Baseline Security Recommendations for IoT 2017: 74; Ohje salauskäytännöistä 2015: 24.]

Salausavaimien turvallisella hallinnalla varmistetaan salausratkaisun luotettavuus ja toimivuus niin, etteivät asiattomat tahot pääse purkamaan salausta. Salausavaimien hallinta pitää sisällään salausavaimen luomisen, jakamisen, säilyttämisen sekä ylläpidon. [Baseline Security Recommendations for IoT 2017: 74.]

Älyrakennuksen tietojärjestelmäympäristössä käytettävät salausratkaisut tulee suunnitella vaatimuksiin ja riskeihin pohjautuvan tarveanalyysin perusteella. Riskien arvioinnin avulla tunnistetaan tietoon kohdistuvia riskejä, joihin varaudutaan suhteessa riskiin riittävän vahvojen salausratkaisujen käytöllä. Salausratkaisujen suunnittelun ja valinnan tulee ottaa kantaa siihen, miten ja missä kaikkialla salausta käytetään. Tässä varmistetaan myös salaisratkaisun tarpeellisuus. Mikäli jälkikäteen havaitaan valitun salausratkaisun olevan väärä, on tilanteen muuttaminen ja korjaaminen haastavaa. [Ohje salauskäytännöistä 2015: 43-44.]

Salausratkaisuja suunniteltaessa on myös huomioitava mahdolliset ympäristön ja käytettyjen ratkaisujen muodostamat haasteet. Esimerkiksi perinteiset salausalgoritmit voivat olla liian raskaita ja hidastavia sulautetuille järjestelmille ja sensoriverkolle, jolloin on käytettävä kevyempiä algoritmeja. [Report on Lightweight Cryptography 2017: 2.]

6.9 Tietoverkko

Älyrakennuksen tietoverkko on keskeisessä roolissa koko sen toteutuksessa ja toimivuudessa sekä myös kyberturvallisuuden varmistamisessa. Oikeanlaisella verkkototeutuksella pyritään suojaamaan älyrakennuksen tietojärjestelmiä ja tietoa kyberhyökkäyksiltä. Tietoverkko on tärkeää suunnitella helposti hallittavaksi ja ylläpidettäväksi, jotta myös sen turvallisuus voidaan varmistaa. Tärkeässä osassa tätä on tietoverkkoarkkitehtuurin ja teknisten kuvausten dokumentointi. Dokumentaation tulee olla sellaista, että sitä myös ylläpidetään määritetyn toimintamallin mukaisesti, jotta kaikki tietoverkossa tapahtuneet muutokset pysyvät ajan tasalla osana kuvauksia. Dokumentaatiossa kuvataan kaikki älyrakennuksen tietoverkkoon liitetyt laitteet rooleineen, osoitteineen ja fyysisine sijainteineen. Myös vastuuhenkilöiden yhteystiedot kuvataan dokumentaatiossa. [Manageable Network Plan 2015: 3-7.]

Verkkoarkkitehtuuri ja verkkoon liittyvät suojauskeinot toteutetaan vaatimusten ja riskiarvion pohjalta tehtyjen määritysten mukaisesti. Tietoverkon toteutuksessa pyritään minimoimaan hyökkäyspinta-alaa rajoittamalla, suojaamalla ja hallitsemalla niitä kohteita, joihin kyberhyökkäykset on mahdollista kohdistaa. Osana hyökkäyspinta-alan pienentämistä ja hyökkäyksen rajoittamista on tietoverkon segmentointi eri alueisiin, jolloin esimerkiksi älyrakennuksen IoT-laitteet on konfiguroitu omaan virtuaalisen lähiverkkoon (*VLAN, Virtual Local Area Network*). Segmentoinnissa tietoverkko jaetaan eri alueisiin, joihin sijoitetaan erilaista turvatasoa ja toimintoa edustavia laitteita ja palveluita rajaten ja suodattaen liikennettä sekä pääsyä segmenttien välillä. Segmentoinnilla pyritään rajaamaan oikeudettomien käyttäjien pääsyä eri segmenteissä oleviin resursseihin sekä rajaamaan esimerkiksi haittaohjelmien leviämistä. Asianmukaisella verkon segmentoinnilla ja liikenteen suodatuksella pyritään muodostamaan suoraviivaista ja helposti erotettavaa oikeutettua liikennettä sekä tunnistettavissa olevaa pahantahtoista ja poikkeavaa (*anomaliat*) liikennettä, jonka kohdalla tulee ryhtyä toimenpiteisiin. [Manageable Network Plan 2015: 9-10; Donaldson ym. 2015: 459-465.]

Tietoverkkolaitteiden, kuten palomuurien ja reitittimien avulla pystytään suodattamaan älyrakennuksen tietojärjestelmiin saapuvaa pahantahtoista tietoliikennettä. Tietoverkkoliikennettä voidaan seurata tarkkailemalla tietoverkkolaitteiden loki- ja tilastotietoja. Käyttämällä erillistä tietoverkkolaitteisiin konfiguroitavaa tunkeilijan havaitsemisjärjestelmää (IDS, Intrusion Detection System), pystytään havaitsemaan älyrakennuksen tietojärjestelmiin kohdistuvat hyökkäysyritykset. Tietoverkkolaitteisiin konfiguroitavalla murron estämisjärjestelmällä (IPS, Intrusion Prevention System) pystytään estämään älyrakennuksen tietojärjestelmiin kohdistuvat hyökkäysyritykset. [Donaldson ym. 2015: 50; Configuring Cisco IOS Firewall Intrusion Detection System: SC-272.]

Älyrakennukseen kohdistuvien riskien perusteella tietoverkkolaitteet, kuten reitittimet ja kytkimet suojataan ja konfiguroidaan valittujen kovennusohjeiden mukaisesti. Tietoverkkolaitteita ei ole oletusarvoisesti konfiguroitu turvallisuuslähtöisesti, vaan mahdollisimman helppo käyttöönotto ja käytettävyys edellä. Oletuskonfiguraatioissa tarpeettomia portteja ja palveluja saattaa olla aktivoituna, jolloin niitä voidaan käyttää hyväksi kyberhyökkäyksen aikana. Tämän vuoksi on tärkeää, että vain käytössä olevat portit ja palvelut ovat avoinna ja aktiivisia. [Baseline Security Recommendations for IoT 2017: 76; The CIS Critical Security Controls for Effective Cyber Defense 2016: 38.]

Älyrakennuksen tietoliikenteen osalta huolehditaan siitä, että tietoverkoissa kulkeva tieto on suojattu käyttämällä tietoliikenteen salausprotokollia, esimerkkeinä TLS ja IPsec. Näiden salausprotokollien tehtävänä on varmistaa, että tietoverkossa liikkuva tieto ei kulje selkokielisenä vaan salattuna, jolloin arkaluontoinen tieto pysyy suojattuna myös tiedonsiirron aikana. [Manageable Network Plan 2015: 10-14.]

6.10 Sovellusten turvallisuus

Sovellustenhallinnan tavoitteena on saada älyrakennuksen tietojärjestelmien suunnittelijat, valmistajat ja toimittajat omaksumaan ja noudattamaan sovelluskehitysprosessia ja -käytäntöjä, joilla varmistetaan, että älyrakennukseen liittyviin ratkaisuihin kuuluvat mobiili-, työpöytä- ja verkkosovellukset on kehitetty turvallisiksi. Käytettävien sovellusratkaisujen kohdalla tulee saada riittävä varmuus siitä, että ne ovat asianmukaisesti suojattu yleisimpiä hyökkäysvektoreita vastaan. [Sovelluskehityksen tietoturvaohje 2013: 41.]

Osana sovelluksen turvallisuuden määrittelyä ja arviointia on tärkeä hyödyntää kyseiseen sovellustyyppiin liittyviä yleisiä turvallisuuskäytäntöjä ja suosituksia, kuten OWASP:n ohjeet yleisimmistä haavoittuvuuksista ja niihin liittyvistä suojauskeinoista. Alla muutamia keskeisiä OWASP-yhteisön laatimia suosituksia, joissa käsitellään yleisimpiä älyrakennuksen tietojärjestelmiin sulautettujen sovellusten suojaamismenetelmiä:

- Puskurin ja pinon ylivuodon turvaamisella estetään tunnettuja vaarallisia funktioita ja ohjelmointirajapintoja (*API, Application Programming Interface*) hyödyntämästä muistin korruptointia mahdollistavia haavoittuvuuksia [OWASP Embedded Application Security 2018].

- Injektiohaavoittuvuuksien ehkäisyllä varmistetaan, että kaikki arveluttava tieto ja käyttäjäsyöte vahvistetaan ja puhdistetaan. Tällä estetään tahaton sovellusten suorittaminen, esimerkiksi SQL-injektio. [OWASP Embedded Application Security 2018.]

- Laiteohjelmiston (*Firmware*) päivityksillä varmistetaan sovellusten haavoittuvuuksien paikkaaminen. Kun päivityspakettien kehittäjä hyödyntää sähköisiä allekirjoituksia, varmistutaan myös siitä, ettei ladattuja päivityspaketteja ole modifioitu tai muulla tapaa peukaloitu. [OWASP Embedded Application Security 2018.]

- Tiedon turvaamisella varmistetaan, ettei arkaluontoinen tieto joudu vääriin käsiin. Sovelluskehityksessä ei tule koskaan kovakoodata salasanoja, käyttäjätunnuksia tai avaimia suoraan laiteohjelmistojen julkaisuversioihin. Sama pätee myös, mikäli arkaluontoista tietoa tallennetaan kiintolevyille. Mikäli mahdollista, hyödynnetään arkaluontoisen tiedon tallentamisessa turvaelementtiä (*SE, Security Element*) tai TEE-tekniikkaa (*TEE, Trusted Execution Environment*). Muussa tapauksessa käytetään vahvaa salausta tiedon suojaamiseen. Kaikki mahdollisesti tarvittava selkokielinen tieto tallennetaan vain lyhytkestoisesti haihtuvaan muistiin (*Volatile*). [OWASP Embedded Application Security 2018.]

- Sovelluskehityksessä vältetään käyttöoikeuksien kovakoodaamista laiteohjelmistoon. Sen sijaan käytetään toimintoja, joiden avulla pystytään erottelemaan sekä paremmin hallinnoimaan sovelluksien käyttöoikeuksia ja käyttäjätunnuksia. Tällä estetään automatisoidut hyökkäykset. [OWASP Embedded Application Security 2018.]

- Varmistetaan, että kaikki tarpeettomat tuotantovaihetta edeltävässä testivaiheessa käytetyt ohjelmointikoodit ovat poistettu sovelluksesta ennen uusimman laiteohjelmiston julkaisua. Tämä pitää sisällään myös mahdolliset korkeimman käyttäjätason (*Root*) käyttöoikeudet, jotka ovat jääneet sovellukseen esimerkiksi ulkopuolisen palveluntuottajan toimesta. [OWASP Embedded Application Security 2018.]

- Varmistetaan kaiken sovelluksen välisen tietoliikenteen käyttävän TLS-salausprotokollaa. Tällä huolehditaan tiedonsiirron aikaisesta tiedon salauksesta. [OWASP Embedded Application Security 2018.]

- Rajoitetaan henkilökohtaisen arkaluontoisen sekä identifioitavan tiedon keruuta, tallennusta, sekä jakamista. Sovelluksen käyttäjien henkilökohtaisten tietojen vuotamisella saattaa olla vakavia ja oikeudellisia seurauksia sovelluksen valmistajille. [OWASP Embedded Application Security 2018.]

6.11 Syötteen- ja ulostulonhallinta

Älyrakennuksen tietojärjestelmien syötteenhallinta (*data input validation*) ja ulostulon suodatus (*output filtering*) varmistavat osaltaan datan eheyttä ja oikeellisuutta sekä turvaavat älyrakennuksen tietojärjestelmiä erilaisilta hyökkäysvektoreilta. Älyrakennuksen tietojärjestelmäkokonaisuuden suunnittelussa ja toteutuksessa on tärkeä varmistaa, ettei pahantahtoisen käyttäjän tai ulkopuolisen hyökkääjän ole mahdollista antaa tietojärjestelmälle haitallisia syötteitä, esimerkiksi haitallista koodia. Syötteenhallinta liittyy hyvin keskeisesti muun muassa aiemmin käsiteltyyn sovellusten turvallisuuteen. [Baseline Security Recommendations for IoT 2017: 77.]

Keskeistä on myös varmistaa se, että esimerkiksi antureiden tuottamat arvot ja data ovat oikeita ja niiden eheys säilyy. Jos esimerkiksi häiriö tai ulkopuolinen hyökkääjä pääsee vaikuttamaan antureiden tuottamaan dataan, voi sillä olla suuria vaikutuksia älyrakennuksen eri toiminnoille. Selvästi poikkeava data tulee voida tunnistaa ja käsitellä poikkeamana. [Baseline Security Recommendations for IoT 2017: 77.]

Älyrakennuksen laiteympäristöön täytyy toteuttaa tarvittavat tarkastuskeinot syötteiden ja ulostulojen validoimiseksi, jotta ne ovat määritetyn mukaisia ja hyväksyttävien rajaarvojen sisällä. Kaikki syötteet ja tuotokset voidaan validoida listaamalla sallitut (*White-listing*-periaate) datan lähteet ja dataan liittyvät keskeiset attribuutit. Esimerkiksi syötteenä tulevan ja rajapintojen välityksellä siirrettävän datan osalta voidaan tarkistaa datan tyyppi, pituus, formaatti, aitous, lähde ja frekvenssi. [IoT Security Compliance Framework 2018: 28.]

6.12 Valvonta ja havainnointikyky

Nykypäivän kyberturvallisuuden suunnittelussa ja toteutuksessa täytyy lähteä siitä olettamasta, että pelkkä ennaltaehkäisy ja suojautuminen eivät riitä, vaan on varauduttava riskien realisoitumiseen. Ajatuksen lähtökohtana on se, että häiriöitä, tietomurtoja ja niiden yrityksiä tulee tapahtumaan, eikä niitä kaikkia voida millään estää, jos halutaan myös itse kyetä toimimaan. Tällöin keskeiseen asemaan nousee kyvykkyys valvoa ja havaita erilaisia poikkeamia, jotta niihin voidaan reagoida.

Älyrakennuksen tietojärjestelmiin liittyviä tapahtumia kirjataan lokiin riskiarvion perusteella määritetyssä laajuudessa. Osana älyrakennuksen tietojärjestelmäympäristön suunnittelua on määritettävä luotavat valvonta- ja havainnointikyvykkyydet. Osana tätä on kerättävien lokien määrittäminen. Lokikirjauksessa huomioidaan ympäristöön liittyvät onnistuneet ja epäonnistuneet sisään- ja uloskirjautumiset, tietojärjestelmien ja tiedon käyttö, turvallisuusasetuksiin ja keskeisiin toiminnallisuuksiin tehtävät muutokset sekä järjestelmän toimintaan liittyvät häiriöt. Yksittäisten laitteiden käyttäytymistä seurataan sen varmistamiseksi, että ne toimivat ennalta määritettyjen hyväksyttävien normien rajoissa, eikä poikkeamia normaalitoiminnasta (*anomalia*) esiinny. Lokeja kerätään ja käsitellään määritettyjen lokiperiaatteiden mukaisesti ja ne suojataan muutoksilta. [Baseline Security Recommendations for IoT 2017: 78-79; IoT Security Guidelines for Endpoint Ecosystems 2019: 39.]

Lokit siirretään keskitettyyn lokienhallintajärjestelmään, jotta niiden avulla voidaan paremmin havaita kyberturvallisuutta koskevia uhkia ja poikkeamia sekä tuottaa näistä hälytyksiä, joihin reagoimalla ennaltaehkäistään ja rajataan vahinkoja. Jatkuvalla valvonnalla seurataan älyrakennuksen tietojärjestelmien toimintaa ja tunnistetaan siinä mahdollisia anomalioita ja häiriöitä, jotka edellyttävät toimenpiteitä. Ympäristön jatkuva valvonta ja havaintoihin reagointi on kriittisessä roolissa vahinkojen minimoinnissa ja riskien realisoitumisesta toipumisessa. [Baseline Security Recommendations for IoT 2017: 78-79.]

Laitteiden valvonnassa pyritään huomioimaan kolme peruskeinoa: anomalioiden havaitseminen, laitteiden lokien kerääminen ja diagnostiikka. Laitteet keräävät lokia omasta

toiminnastaan sekä käyttäjien toiminnasta ja välittävät nämä lokit taustajärjestelmälle käsiteltäväksi. Lokien lisäksi laitteet voivat kerätä itseensä liittyvää relevanttia diagnostiikkatietoa, kuten lämpötilaa, akun tilaa, muistinkäyttöä ja suoritusaikaa. Lokien ja diagnostiikkatiedon keräämisen ja anomalioiden tunnistamisen suunnittelun avulla pyritään luomaan keinot havaita toimenpiteitä vaativia poikkeamia ja häiriöitä älyrakennuksen käytön ja ylläpidon aikana. Valvonnalla ei pyritä havaitsemaan pelkästään kyberhyökkäyksiä, vaan myös laitteiden toiminnassa ilmeneviä häiriöitä ja vikoja. [IoT Security Guidelines for Endpoint Ecosystems 2019: 39.]

Havainnointikyvykkyyden ylläpitämisessä keskeiseen rooliin nousevat erilaisten teknologioiden hyödyntäminen ja automatisointi. Asianmukainen havainnointikyvykkyys edellyttää reaaliaikaista tilannekuvaa manuaalisten paikallisten lokien katselmoinnin sijaan. Havainnointikyvykkyyden rakentamisessa hyödynnettäviä teknologiaratkaisuja ovat muun muassa aiemmin mainittu IDS, lokikirjauksessa ja lokitiedon hallinnassa käytettävä SIEM (*Security Information and Event Management*) sekä analytiikkaan ja anomalioiden tunnistamiseen käytettävät UEBA-ratkaisut (*User and Entity Behavioral Analytics*). Älyrakennuksen suunnitteluvaiheessa on tunnistettava tarvittavat teknologiat ja määritettävä älyrakennuksen tietoturva-arkkitehtuuri, joka tukee myös riittävän havainnointikyvyn mahdollistamista. Myös lokienhallinnan kokonaisuus, mukaan lukien kerättävät lokit ja niiden valvonta, tulee määrittää älyrakennuksen suunnitteluvaiheessa ja huolehtia siitä, että tarvittavat lokikäytännöt luodaan toteutusvaiheessa.

6.13 Testaus ja katselmoinnit

Älyrakennuksen tietojärjestelmien kyberturvallisuuden ylläpitämiseksi ja siinä ilmenevien heikkouksien havaitsemiseksi ympäristöön kohdistetaan säännöllistä testausta ja katselmointeja, joiden tarkoituksena on tunnistaa puutteita ja kehityskohtia. Katselmointien yhteydessä käydään läpi ympäristöön liittyviä arkkitehtuurikuvauksia, dokumentaatiota ja määritettyjä periaatteita niiden ajantasaisuuden ja asianmukaisuuden varmistamiseksi. Muuttuva toiminta- ja uhkaympäristö sekä kehittyvät parhaat käytännöt edellyttävät omien suojauskeinojen jatkuvaa seurantaa ja arviointia niiden asianmukaisuuden ja riittävyyden varmistamiseksi. Testauksen avulla varmistetaan suojauskeinojen oikeanlainen toiminta ja varmistetaan, etteivät tietojärjestelmiin liittyvät väärinkäyttötapaukset ole

mahdollisia. Väärinkäyttötapausten mallintamisessa tunnistetaan tietojärjestelmän käyttäjien ja käyttöön liittyvien käyttötapausten lisäksi mahdolliset järjestelmää väärin käyttävät henkilöt ja tähän liittyvät väärinkäyttötapaukset. [Baseline Security Recommendations for IoT 2017: 79.]

Kyberturvallisuuden säännölliseksi seuraamiseksi ja arvioimiseksi erilaisia väärinkäyttötapauksiin liittyviä penetraatiotestauksia suoritetaan määritetyn testaussuunnitelman mukaisesti säännöllisin väliajoin läpi älyrakennuksen elinkaaren. Testaaminen on kuitenkin relevanttia myös älyrakennuksen toteutuksen aikana. Älyrakennuksen toteutusvaiheessa ja lopullisen toteutuksen hyväksymistestausvaiheessa on jo perusteltua suorittaa testausta varmistaen, että kontrollit on toteutettu oikein ja ne toimivat halutulla tavalla. Testaustapa, -kohteet, -laajuus ja -tiheys määritetään asetettujen vaatimusten ja riskiarvion pohjalta. Testaukseen liittyy manuaalista väärinkäyttötestausta sekä automaattisesti ajettavia skannauksia. [Baseline Security Recommendations for IoT 2017: 79.]

6.14 Elinkaaren päättymiseen varautuminen

Älyrakennuksessa käytettävien ratkaisujen ja tietojärjestelmien osalta on varauduttu niiden elinkaaren päättymiseen (*EOL, End of Life*), jolloin esimerkiksi tukea, päivityksiä ja tietoturvahaavoittuvuuksiin liittyviä korjauksia ei ole enää saatavilla. Elinkaaren liittyvä riski tunnistetaan ja ratkaisut toteutetaan niin, että ne ovat hallittavissa esimerkiksi toisiin teknologioihin tai ratkaisuihin siirtymällä tai käyttöönottamalla vaihtoehtoisia suojauskeinoja riskin hallitsemiseksi. Osana käytettävien ratkaisujen valintaa on kyettävä tunnistamaan niiden elinkaareen liittyvät tekijät ja mahdolliset riskit esimerkiksi lähiaikoina päättyvästä tuesta johtuen. Elinkaaren päättymiseen liittyvän riskin voi tuotteen ylläpidon päättymisen lisäksi aiheuttaa myös esimerkiksi toimittajan konkurssi. [Baseline Security Recommendations for IoT 2017: 79.]

Älyrakennuksen toteuttamisessa on hyvä käyttää yleisesti tunnettuja ja hyväksyttyjä ratkaisuja välttäen liian kustomoituja ja huonosti yhteen sovitettavia tai korvattavia ratkaisuja. Tämän avulla varaudutaan myös ympäristössä ilmeneviin muutoksiin ja niiden aiheuttamiin vaikutuksiin. [Baseline Security Recommendations for IoT 2017: 79.]

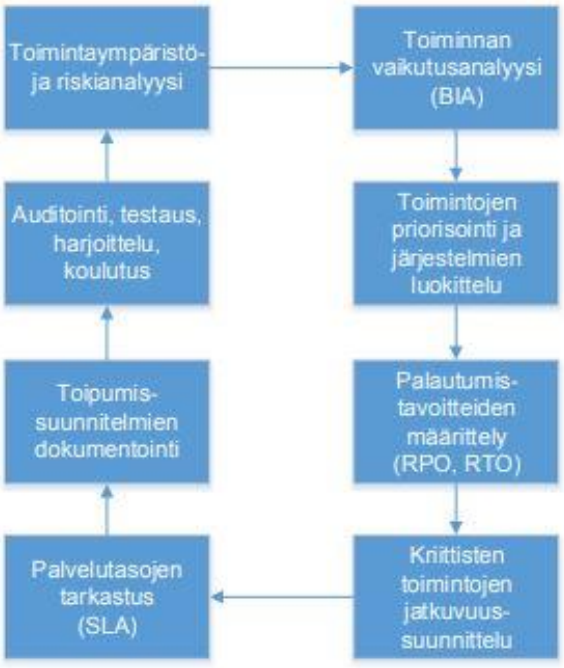
6.15 Haavoittuvuuksien hallinta

Haavoittuvuuksien hallinnan tavoitteena on luoda älyrakennukselle haavoittuvuuksia ennaltaehkäisevä, havaitseva, tutkiva ja hallitseva toimintamalli. Ennaltaehkäisevänä ja hallitsevana päämääränä on varmistaa, että tietojärjestelmissä havaitut haavoittuvuudet ehditään korjaamaan ja paikkaamaan esimerkiksi päivityksin, ennen kuin niitä ehditään hyödyntämään kyberhyökkäyksissä. Havaitsevana päämääränä on tarkkailla älyrakennuksen tietojärjestelmiä, jotta mahdolliset haavoittuvuudet, heikkoudet sekä kyberhyökkäykset ja -yritykset havaitaan ja niihin voidaan puuttua nopeasti. Tutkivana päämääränä on kerätä lokeja ja tietoa haavoittuvuuksista ja kyberhyökkäyksistä, jotta niitä voidaan myöhemmin tutkia ja analysoida sekä pyrkiä jatkossa paremmin ennaltaehkäisemään vastaavia poikkeamia. [Donaldson ym. 2015: 61.]

Älyrakennuksen suunnittelu- ja toteutusvaiheissa määritetään ja toteutetaan ne kyvykkyydet, joilla ylläpitovaiheen aikana havaitaan ja hallitaan haavoittuvuuksia. Yksi tällainen keino on liittää älyrakennukseen liittyvät uudet tietojärjestelmät olemassa olevien sisäisten ja ulkoisten haavoittuvuusskannausten sekä järjestelmävalvonnan piiriin, jotta haavoittuvuuksia on mahdollista havaita. Valittujen teknologioiden ja laitteiden osalta on tärkeää myös kirjata olennaiset tiedot osaksi laiteinventaariota, jotta tiedetään, missä ja mitä laitteita älyrakennuksessa on miltäkin toimittajalta. Yksi keskeinen osa haavoittuvuuksien hallintaa on seurata näiden toimittajien omaa viestintää ja tiedottamista heidän tuotteissaan havaituista haavoittuvuuksista ja niihin liittyvistä korjauksista. [Chapple 2018.]

6.16 Jatkuvuudenhallinta

Jatkuvuudenhallinnan suunnittelulla ja toteutuksella varmistetaan älyrakennuksen toiminnan jatkuvuus odottamattomien häiriöiden, poikkeamien ja onnettomuuksien sattuessa kohdalle. Olennaista toiminnan jatkuvuudelle on tunnistaa kaikki ne riskit, jotka voivat realisoituessaan vaikuttaa negatiivisesti älyrakennuksen kriittisiin toimintoihin. Jatkuvuutta uhkaavien riskien tunnistamisen ja hallinnan avulla pystytään varmistamaan älyrakennuksen ydintoimintojen häiriötön jatkuvuus. [Toiminnan jatkuvuuden hallinta 2016: 35-36.]



Kuva 6. Jatkuvuudenhallinnan suunnittelu [Toiminnan jatkuvuuden hallinta 2016: 43].

Kuvassa 6 on kuvattu ne suunnitteluvaiheessa hyödynnettävät toimenpiteet ja prosessit, joilla varmistetaan älyrakennuksen toiminnan jatkuvuus. Toimintaympäristö- ja riskianalyysin avulla tunnistetaan ne ulkoiset ja sisäiset riskit, jotka kohdistuvat älyrakennuksen toimintaympäristöön. Riskianalyysilla tarkastellaan näiden riskien vaikutusta älyrakennuksen toimintaan lyhyellä ja pidemmällä aikavälillä. [Toiminnan jatkuvuuden hallinta 2016: 43.]

Toiminnanvaikutusanalyysillä (*BIA, Business Impact Analysis*) arvioidaan riskien vaikutukset älyrakennuksen ja älyrakennuksessa toimivien käyttäjien ydin- ja liiketoimintaan. Tunnistamalla nämä riskit, voidaan valita riittävät ja tarpeelliset toimenpiteet jatkuvuuden varmistamiseksi. [Toiminnan jatkuvuuden hallinta 2016: 24, 44.]

Älyrakennuksen ydintoimintojen jatkuvuuden kannalta olennaista on määrittää kullekin älyrakennuksen toiminnolle alin hyväksyttävä palvelutaso. Mikäli älyrakennuksen toiminto laskee alle määritellyn palvelutason, kyseistä toimintoa ei enää pystytä käyttämään tai hyödyntämään. Kriittisimmille älyrakennuksen toiminnoille luodaan tarkat oh-

jeet toimenpiteistä, joiden avulla mahdollisten häiriöiden tai onnettomuuksien aiheuttamat vaikutukset minimoidaan ja älyrakennuksen toiminnot saadaan palautettua mahdollisimman nopeasti normaaliin tilaansa. Tärkeää on myös se, että älyrakennuksen toiminnot, tietojärjestelmät ja palvelut luokitellaan niiden käyttötarkoituksen, kriittisyyden, käytön laajuuden ja tietosisällön perusteella tärkeysjärjestykseen. Älyrakennuksen toiminnan jatkuvuuden kannalta on tärkeää, että ydintoiminnot palvelevat mahdollisimman korkeatasoisesti myös mahdollisista häiriöistä huolimatta. [Toiminnan jatkuvuuden hallinta 2016: 45-46.]

Toipumissuunnittelun ja -suunnitelmien (*DR, Disaster Recovery*) toimivuuden kannalta on olennaista määrittää älyrakennukselle ja sen toiminnoille erilliset palautumistavoitteet. Palautumistavoitteina käytetään älyrakennuksen toimintojen tavoiteltua toipumisaikaa (*RTO, Recovery Time Objective*) ja tavoiteltua toipumispistettä (*RPO, Recovery Point Objective*). RTO määrittää sen ajan, jonka kuluessa kyseinen älyrakennuksen toiminto tai palvelu on saatettava häiriötilanteesta takaisin normaaliin toimintaan. RPO määrittää sen tilan, johon kyseinen älyrakennuksen toiminto tai palvelu on saatava palautettua häiriötilanteiden jälkeen. Älyrakennuksen palautumistavoitteita määrittäessä on tärkeää huomioida, että lyhyillä palautumistavoitteilla saavutetaan useasti myös korkeat kustannukset. Kustannukset saattavat nousta yllättävän korkeiksi esimerkiksi korkean käytettävyyden (*HA, High Availability*) ratkaisuissa, joissa älyrakennuksen tietojärjestelmät ovat kahdennettu tai tietojärjestelmien komponentit hajautettu. [Toiminnan jatkuvuuden hallinta 2016: 25, 47-48.]

Esimerkki RTO- ja RPO-arvojen määrittelystä on, että älyrakennuksen toiminnolle annetaan RTO-arvoksi yksi tunti ja RPO-arvoksi neljä tuntia. Tämä tarkoittaa, että toiminnon on palauduttava takaisin normaaliin toimintaansa yhden tunnin kuluessa. Vastaavasti toiminnon täytyy pystyä palautumaan tilaan, joka ei saa olla neljää tuntia vanhempi, eli esimerkiksi häiriötilanteessa vajaan neljän viimeisen tunnin aikana syntynyt data on vielä hyväksyttyä menettää. Kun palautumistavoitteet ovat saatu määritettyä, suunnitellaan ja toteutetaan tietojärjestelmät, kumppanisopimukset ja ohjeistukset niin, että palautumistavoitteisiin päästään. [Toiminnan jatkuvuuden hallinta 2016: 48.]

6.17 Kolmansien osapuolien hallinta

Hankinoilla ja ulkoistuksilla ei voida kokonaan ulkoistaa riskiä ja asianmukainen kumppanien ja toimittajien hallinta onkin edellytys. Älyrakennukseen liittyy useita järjestelmä- ja laitetoimittajia sekä palveluntarjoajia, jotka liittyvät älyrakennuksen hallittavaan riskikokonaisuuteen. Jo älyrakennukseen liittyvien järjestelmien, ratkaisujen ja palveluiden hankintavaiheessa täytyy tunnistaa hankinnan kohteeseen liittyvät kyberturvallisuusvaatimukset sekä itse toimittajan omaan toimintaan kohdistuvat turvallisuus- ja salassapitovaatimukset, jotka tuodaan osaksi sopimuksia ja hankinnan kohteen vaatimusmäärittelyitä. Tavoitteena on saada kaikki älyrakennuksen tietojärjestelmiä kehittävät ja niitä hallinnoivat kolmannet osapuolet noudattamaan erillistä tietojenkäsittely- ja turvallisuussopimusta, jossa sovitaan tiedon käsittelystä ja suojaamisesta. Lisäksi järjestelmätoimittajat sitoutuvat sopimuksellisesti toteuttamaan hankittavaan ratkaisuun sovitut kyberturvallisuutta koskevat kontrollit. On myös ensiarvoisen tärkeää varmistaa sovittujen vaatimusten täyttyminen älyrakennuksen suunnitteluun ja toteuttamiseen osallistuvan kumppanin toiminnassa sekä näiden mahdollisesti toimittamissa ratkaisuissa. Tämä varmistetaan esimerkiksi auditoinnein ja teknisin testauksin. [Baseline Security Recommendations for IoT 2017: 81; The Seven Deadly Sins of Third-Party Cyber Risk Management 2018: 5-6.]

6.18 Fyysinen turvallisuus

Osana älyrakennuksen suunnittelua on myös laitteiden ja laitetilojen fyysisen turvallisuuden suunnittelu ja varmistaminen. Suunnittelussa tulee huomioida asianmukaisten suojauskeinojen määrittäminen sen varmistamiseksi, ettei älyrakennuksen toimintoihin liittyviä laitteita voi helposti väärinkäyttää niihin fyysisesti kajoamalla. Tätä estetään muun muassa itse laitteeseen liittyvillä peukalointiin liittyvillä suojauksilla sekä tilojen luvatonta pääsyä rajoittavilla fyysisillä suojauksilla ja valvontakeinoilla.

Älyrakennusten laitetilojen suojaus tulee määrittää suunnitteluvaiheessa niin, että keskeisiin tunnistettuihin riskeihin on varauduttu asianmukaisesti. Kiinteistön fyysisen laitetila- ja kaapelointikokonaisuuden muodostavat:

- tietotekniset laitetilat, joilla tarkoitetaan erityisesti konesalia, palvelinhotellia, viestiasemaa, tietoverkon valvomo- tai hallintatilaa tai muuta erillistä useita palvelimia sisältävää tilaa tai tilakokonaisuutta

- alue- ja talojakamot, joilla tarkoitetaan kiinteistön tai alueen laitetilaa, jossa yleinen viestintäverkko ja sisäverkko liitetään yhteen

- alijakamot eli toisiotalojakamot, joilla tarkoitetaan laitetilaa, johon on päätetty talo- tai alijakamosta tuleva aluekaapelointi sekä kerrosjakamosta tuleva nousukaapelointi

- kerrosjakamot, joilla tarkoitetaan toimitilahuoneistoon, kiinteistöön tai rakennukseen sijoitettua tilaa (huone, komero, kotelo, rasia tai niitä vastaava muu tila), jossa kerroskaapelointi ja nousukaapelointi liitetään yhteen

- kaapelointi ja kaapelireitit, joilla tarkoitetaan muun muassa kaapeloinnista, kaapelihyllyistä ja –tikkaista, johtokanavista, kaapelikouruista ja muista erilaisista kaapelikiinnitysjärjestelmistä sekä tiloista ja osastoista toisiin johtavista läpivienneistä syntyvää toteutusta. [Määräyksen 65 perustelut ja soveltaminen 2018: 17-19.]

Laitetilojen suojauksen suunnittelussa on huomioitava niiden sijoittelu, rakenteellinen suojaus, paloturvallisuus, olosuhteet (ilmanvaihto, lämpötila, kosteus ja valaistus), fyysinen pääsynhallinta sekä valvontaratkaisut. Laitetilojen sijoittelu suunnitellaan huomioiden tilaan pääsy, tilan koon tarve, kaapeloinnin toteuttaminen ja tilan asianmukaisen suojauksen toteuttaminen. Rakenteellinen suojaus (ovet ja aukot, seinät, lattia- ja kattorakenteet) suunnitellaan niin, että ne tarjoavat riskeihin nähden riittävän rakenteellisen suojan ja hidasteen tunkeutumiselle, jottei älyrakennuksen tietojärjestelmiin ja laitteisiin ole mahdollista tunkeutua fyysisen pääsyn avulla ennen kuin siihen ehditään reagoida. Laitetilojen paloturvallisuus suunnitellaan niin, että niitä koskevat vaatimukset täyttyvät ja olennaisiin riskeihin on varauduttu asianmukaisesti. Tämä edellyttää muun muassa palo-osastoinnin suunnittelua sekä oikeiden sammutusratkaisujen (sähköpalon sammuttaminen ja laitteiden suojaaminen vaurioilta) ja materiaalien (rakenteet ja kaapeloinnit)

valintaa. Olosuhteiden osalta on suunniteltava ratkaisut, joiden avulla varmistetaan laitetilan optimilämpötila ilmanvaihdon ja jäähdytysratkaisujen avulla sekä ennaltaehkäistään esimerkiksi vuotojen ja kondensaation aiheuttamat kosteus- ja vesivahingot. Fyysistä pääsynhallintaa koskevat samat periaatteet kuin aiemmin käsiteltyä loogista pääsynhallintaa. Laitetilojen osalta se tulee suunnitteluvaiheessa määrittää muun muassa oikeanlaisten lukitus- ja kulunvalvontaratkaisujen valinnalla sekä avainten ja vierailijoiden hallinnan määrittämisellä. Valvontaratkaisujen suunnittelulla pyritään valitsemaan oikeat teknologiat ja ilmaisimet muun muassa tunkeutumisyritysten ja tulipalojen havaitsemiseksi sekä tapahtumien jälkeenpäin selvittämiseksi. Tässä keskeisessä roolissa ovat rikosilmoitin-, kulunvalvonta-, kameravalvonta- ja palonilmaisujärjestelmät. [Määräys kiinteistön sisäverkoista ja teleurakoinnista 2018: 9-10; Määräyksen 65 perustelut ja soveltaminen 2018: 50-55.]

7 Yhteenveto

Insinöörityössämme perehdyttiin kyberturvallisuuteen älyrakennusten kontekstissa. Työn tavoitteena oli luoda ylätason ohjeistus sille, kuinka kyberturvallisuus tulisi huomioida tulevissa älyrakennuksen suunnittelu- ja toteutusprojekteissa.

Insinöörityöprosessin aikana huomasimme, että älyrakennuksiin kohdistuvaa materiaalia on saatavilla vain hieman, enimmäkseen englanninkielellä. Materiaalia, joissa kuvataan älyrakennusten kyberturvallisuutta kokonaisuutena, ei ole tuotettu lähes lainkaan. Englanniksi materiaalia löytyy hieman, mutta niissäkin sivutaan enimmäkseen yleisesti yritysturvallisuutta ja IoT-laitteiden kyberturvallisuutta. Kunnioitamme kaikkien insinöörityössä hyödyntämiemme tietolähteiden tekijöiden töitä ja referoimme kaikkia käyttämiämme tietolähteitä omin sanoin.

Kattavan ja nimenomaan älyrakennuksen kontekstiin viedyn kyberturvallisuutta koskevan lähdeaineiston löytäminen oli haastavaa. Tietoa oli hajanaisesti ja se liittyi usein erilaisiin toteutuksiin, kuten teollisuuslaitosten tuotantojärjestelmiin. Työn aikana onnistuttiin kuitenkin tunnistamaan oikea ja tarvittavan tiedon tuottava lähdeaineisto kattavan sekä monista lähteistä muodostuvan tietomassan koostamiseksi ja sen pohjalta luotavan mallin pohjaksi. Insinöörityö toteutettiin ylätason tutkimuksena, ja sen tulokset antavat

tärkeän yleiskuvan niistä teemoista ja suojauskeinoista, joita älyrakennuksen suunnittelussa tulee huomioida. Työn tulokset tukevat älyrakennusten suunnitteluun ja toteuttamiseen osallistuvia henkilöitä suojauskeinojen määrittelyssä ja valinnassa riittävän kyberturvallisuuden tason saavuttamiseksi.

Työn aihe antaa paljon mahdollisuuksia tuleville syvemmille yksittäisiin osa-alueisiin keskittyville lisätutkimuksille ja materiaaleille, joissa työn aihe rajataan vielä tarkemmin.

Lähteet

68% of the world population projected to live in urban area by 2050, says UN. 2018. Verkkoaineisto. United Nations. <https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html>. 16.5.2018. Luettu 16.4.2019.

Amazon Partner with Marriott Hotels to Launch Alexa for Hospitality. 2018. Verkkoaineisto. Memoori. <https://memoori.com/amazon-partner-marriott-hotels-launch-alexa-hospitality/ >. Luettu 8.5.2019.

Balani, Naveen. 2015. Enterprise IoT: A Definite Handbook. E-kirja. Balani, Naveen.

Baseline Security Recommendations for IoT. 2017. Verkkoaineisto. ENISA. <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>. 20.11.2017. Luettu 16.4.2019.

Building management and integrated/intelligent building management systems. Verkkoaineisto. i-SCOOP. <https://www.i-scoop.eu/building-management-building-management-systems-bms/>. Luettu 12.4.2019.

Chapple, Mike. 2018. Automated patch management and the challenges from IoT. Verkkoaineisto. SearchSecurity. <https://searchsecurity.techtarget.com/tip/Automated-patch-management-and-the-challenges-from-IoT>. Luettu 11.5.2019.

Chignell, Barry. 2017. How your business can benefit from system integration. Verkkoaineisto. Ciphr. <https://www.ciphr.com/advice/system-integration/>. 22.11.2017. Luettu 2.4.2019.

Configuring Cisco IOS Firewall Intrusion Detection System. Verkkoaineisto. <https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfids.pdf>. Luettu 28.3.2019.

Cooper, Rachel. 2017. Big Data: Big opportunity for smart buildings. Smart Buildings Magazine. <http://www.smartbuildingsmagazine.com/features/big-data-big-opportunity-for-smart-buildings>. 10.7.2018. Luettu 2.5.2019.

Data Breach Investigations Report. 2019. Verkkoaineisto. Verizon. <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>. Luettu 11.5.2019.

Donaldson, Scott; Siegel, Stanley; Williams, Chris K. & Aslam, Abdul. 2015. Enterprise Cybersecurity. Apress.

Hirsjärvi, Sirkka; Remes, Pirkko & Sajavaara, Paula. 2003. Tutki ja kirjoita. 6.-9. Painos. Vantaa: Dark Oy.

Improving Performance with Integrated Smart Buildings. 2012. Verkkoaineisto. Siemens Industry, Inc. <http://www.usa.siemens.com/intelligent-infrastructure/assets/pdf/smart-building-white-paper.pdf>. Luettu 15.4.2019.

IoT Security Compliance Framework. 2018. Verkkoaineisto. IoT Security Foundation. <https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf>. 2.12.2018. Luettu 19.3.2019.

IoT Security Guidance. 2017. Verkkoaineisto. OWASP. <https://www.owasp.org/index.php/IoT_Security_Guidance>. Luettu 3.5.2019.

IoT Security Guidelines for Endpoint Ecosystems. 2019. Verkkoaineisto. GSM Association. <https://www.gsma.com/iot/wp-content/uploads/2019/04/CLP.13-v2.1.pdf>. 31.3.2019. Luettu 9.5.2019.

Karlsen, Elisabeth B. 2017. Smart City – What Is It, Why Is It Important, and How to Get Started. Verkkoaineisto. eSmart Systems. <http://response.esmartsystems.com/hubfs/Content%20Offers/PDF/English/Ebook%20Smart%20City%20eSmart%20Systems.pdf>. Luettu 9.4.2019

Kyberturvallisuuden sanasto. 2018. Verkkoaineisto. Turvallisuuskomitea. <https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf>. Luettu 2.5.2019.

Limnéll, Jarno; Majewski, Klaus & Salminen, Mirva. Kyberturvallisuus. E-kirja. Jyväskylä: Docendo. Luettu 2.5.2019.

Lähdesmäki, Tuuli; Hurme, Pertti; Koskimaa, Raine; Mikkola, Leena & Himberg, Tommi. Menetelmäpolkuja humanisteille. Jyväskylän yliopisto, humanistinen tiedekunta. <http://www.jyu.fi/mehu>. 3.9.2014. Luettu 2.3.2019.

Manageable Network Plan. 2015. Verkkoaineisto. National Security Agency & Central Security Service. <https://apps.nsa.gov/iaarchive/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/security-configuration/networks/assets/public/upload/manageable-network-plan-guide.pdf&WpKes=aF6woL7fQp3dJih7UcXZRMVKEPHfpazxG5WZAw>. Luettu 27.3.2019.

Määräyksen 65 perustelut ja soveltaminen. 2018. Verkkoaineisto. Viestintävirasto. <https://www.finlex.fi/data/normit/44045/M_65_C_MPS_250118.pdf>. 25.1.2018. Luettu 9.5.2019.

Määräys kiinteistön sisäverkoista ja teleurakoinnista. 2018. Verkkoaineisto. Viestintävirasto. <https://legacy.viestintavirasto.fi/attachments/maaraykset/M_65_C_2018.pdf>. 25.1.2018. Luettu 9.5.2019.

Odom, Wendell. 2016. CCENT/CCNA ICND1 100-105 Official Cert Guide. Indianapolis: Cisco Press.

Ohje salauskäytännöistä 2015. Verkkoaineisto. VAHTI. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=8e28cd10-2e1e-4bd5-b6f1-f75a1fec2f5d&groupId=10229>. Luettu 17.4.2019.

OWASP Embedded Application Security. 2018. Verkkoaineisto. OWASP. <https://www.owasp.org/index.php/OWASP_Embedded_Application_Security#tab=Embedded_Top_10_Best_Practices>. Luettu 3.4.2019.

OWASP Internet of Things Project. 2018. Verkkoaineisto. OWASP. <https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project>. 12.4.2019. Luettu 8.5.2019.

Perry, Christopher. 2017. Smart Building: A Deeper Dive into Market Segments. Verkkoaineisto. American Council for an Energy-Efficient Economy. <https://aceee.org/sites/default/files/publications/researchreports/a1703.pdf>. Luettu 12.4.2019.

Qolomany, Basheer; Al-Fuqaha, Ala; Gupta, Ajay; Benhaddou, Driss; Alwajidi, Safaa; Qadir, Junaid & Fong, Alvis C. Machine Learning, Big Data, And Smart Building: A Comprehensive Survey. Verkkoaineisto. <https://arxiv.org/ftp/arxiv/papers/1904/1904.01460.pdf>. Luettu 1.5.2019.

Rantala, Reino; Mäkinen, Riika; Piikkilä, Veijo; Siren, Kari; Piira, Kalevi; Hast, Jukka; Federley, Maija; Seisto, Anu; Sarja, Asko & Åström, Gunnar. 2015. RIL 267-2015 Käyttäjälähtöinen älyrakennus – suunnittelu, rakentaminen, käyttö ja ylläpito. Helsinki: Suomen Rakennusinsinöörien Liitto RIL ry.

Report on Lightweight Cryptography. 2017. Verkkoaineisto. National Institute of Standards and Technology. <https://csrc.nist.gov/CSRC/media/Publications/nistir/8114/draft/documents/nistir_8114_draft.pdf>. Luettu 18.4.2019.

Security and Privacy Controls for Federal Information Systems and Organizations. 2013. Verkkoaineisto. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf>. Luettu 3.4.2019.

Seven Deadly Sins of Third-Party Cyber Risk Management. 2018. Verkkoaineisto. RiskRecon. <https://cdn2.hubspot.net/hubfs/2477095/Content%20PDFs/Whitepaper_7DeadlySins.pdf>. Luettu 11.5.2019.

Shostack, Adam. 2014. Threat Modeling, Designing for Security. Indianapolis, Indiana: John Wiley & Sons, Inc.

Smart Buildings: people and performance. 2013. Verkkoaineisto. Raeng. <https://www.raeng.org.uk/publications/reports/raeng-smart-buildings-people-and-performance>. Luettu 1.5.2019.

Sovelluskehityksen tietoturvaohje. 2013. Verkkoaineisto. VAHTI. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=03c32520-f3f8-4621-b0d4-ec4ca8edafb3&groupId=10128&groupId=10229>. Luettu 2.4.2019.

Talon, Casey & Goldstein, Noah. 2015. Smart Offices: How Intelligent Building Solutions Are Changing the Occupant Experience. Verkkoaineisto. Navigant Research. <https://info.switchautomation.com/hubfs/Switch_Content/Intel_sponsored_Navigant_White_Paper.pdf>. Luettu 16.4.2019.

The benefits of integrating enterprise-wide systems. Verkkoaineisto. AssetWorks LLC. <http://my.assetworks.com/rs/153-QDM-861/images/ASW-1606007-WhtPpr-Integrating-Enterprise-Wide-V01.pdf>. Luettu 2.4.2019.

Tietotermit. Verkkoaineisto. Finto. <https://finto.fi/tt/fi/page/t79>. Luettu 3.5.2019.

Toiminnan jatkuvuuden hallinta. 2016. Verkkoaineisto. VAHTI. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229>. Luettu 16.4.2019.

Verma, Urvashi. 2019. Smart buildings may soon deploy AI avatars to improve energy efficiency. Verkkoaineisto. In-Building Tech. <https://inbuildingtech.com/smart-buildings/smart-buildings-voice-assistance/>. Luettu 8.5.2019.

What is Cyber-Security?. Verkkoaineisto. Kaspersky. <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>. Luettu 3.5.2019.

What is the difference between a presence and motion sensor. 2018. Verkkoaineisto. KNX Association. <https://www.blog.knx.org/single-post/2018/01/22/What-is-the-difference-between-a-presence-and-motion-sensor>. 22.1.2018. Luettu 13.4.2019.

What Is The “Internet of Things”?. Verkkoaineisto. Postscapes. <https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/>. Luettu 12.4.2019.

What makes a building “smart” and why does it matter. 2018. Verkkoaineisto. Switch Automation. <https://info.switchautomation.com/hubfs/WHITE%20PAPER:%20What%20makes%20a%20building%20smart%20and%20why%20does%20it%20matter%3F.pdf>. Luettu 16.4.2019.

Wueest, Candid. 2019. Profiting from Hacked IoT Devices: Coin Mining, Ransomware, Something Else?. Verkkoaineisto. Symantec. <https://published-prd.lany-onevents.com/published/rsaus19/sessionsFiles/13089/SEM-M03D-Profiting-from-hacked-IoT-devices-coin-mining-ransomware-something-else.pdf>. Luettu 9.5.2019.