



LAUREA
AMMATTIKORKEAKOULU

Uuden edellä

Turvajärjestelmien pääkäytön suuntaviivat

Jääskeläinen, Juuso

2014 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Turvajärjestelmien pääkäytön suuntaviivat

Juuso Jääskeläinen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2014

Juuso Jääskeläinen

Turvajärjestelmien pääkäytön suuntaviivat

Vuosi 2014 Sivumäärä 79

Kulunvalvontaa, avainhallintaa, kameravalvontaa ja rikosilmoittimia hallinnoidaan liikekiinteistöissä ja yksittäisissä yrityksissä pääkäyttäjien toimesta. Järjestelmien on tarkoitus edistää turvallisuutta, mutta tavoitetta on vaikea saavuttaa, mikäli hallinnointia ei suoriteta aktiivisesti ja yhtenäisiä linjauksia noudattaen. Havaitsin työelämässä, etteivät järjestelmäkohdattaiset käyttöohjekirjat sekä Finanssialan Keskusliiton ohjeet ja oppaat olleet riittäviä pääkäytön asiantuntijuuden perustaksi.

Tutkimuskysymyksiä lähestytään tutkimuksellisen kehittämistyön näkökulmasta. Työssä tutkitaan mitä pääkäyttäminen sisältää sekä miten pääkäyttämistä ja palveluprosesseja voidaan parantaa. Opinnäytetyön tarkoituksena on tuottaa informaatiota pääkäytön asiantuntijuuden perustaksi. Tavoitteena on luoda turvajärjestelmien hallinnointia varten yhtenäiset linjaukset, joita noudattamalla hallinnointiprosessit nopeutuisivat, samalla hyödyntäen järjestelmien maksimaalista kapasiteettia. Toisena tavoitteena on käsitteellistää turvajärjestelmien pääkäyttö terminä, jotta alalle vakinaistuisi yksi yhteinen näkemys siitä, mitä pääkäyttäminen tarkoittaa ja mitä tehtäviä sekä vastuita se lähtökohtaisesti sisältää.

Tiedonkeruumenetelminä on käytetty pääasiallisesti asiantuntijahaastatteluita. Menetelminä toimivat myös työelämäpohjainen systemaattinen havainnointi sekä alan kirjallisuus. Teoreettisessa osassa käsitellään käsitteen määrittelyn lisäksi ammattisanaston merkitystä ja tärkeyttä päivittäisessä hallinnointityössä.

Käsitteellistämistä varten työssä luodaan reaali-määritelmä termille turvajärjestelmien pääkäyttö. Tutkimuksessa havaitaan, että nykyisellään pääkäyttäminen ei yleisesti ole tehokkaimmalla tasolla, joten palveluprosesseja pystytään yhä kehittämään. Pääkäytön asiakas odottaa palvelun ulkoistaessaan, että omaan ydinliiketoimintaan vapautuu resursseja. Turvallisuustasoa ei kuitenkaan ole helppoa ylläpitää, mikäli kommunikoinnissa on puutteita. Tarve yhtenäisten suuntaviivojen määrittämiselle on siis molemminpuolinen.

Tuotoksena syntynyt Turvajärjestelmien pääkäytön suuntaviivat -opas on apuväline pääkäyttöpalvelua tuottaville tahoille tai palvelun asiakkaille. Opas sopii koulutuskäyttöön sekä turvallisuustietoisuuden levittämiseen. Tutkimustulosten perusteella voidaan todeta, että järjestelmän saaminen suuntaviivojen avulla korkean turvallisuustason ylläpitotilaan on avainjärjestelmän pitkälle elinkaarelle.

Tutkimusaiheena pääkäyttäminen on vielä antoisa. Järjestelmien sisältämien henkilötietojen luomat henkilörekisterit ja niiden käsittely ovat vailla yhtenäisiä pelisääntöjä. Lisäksi kulkuoikeuksien määrittelyperiaatteet isoissa monirakennuksissa kiinteistöissä aiheuttavat pääkäyttäjille päänvaivaa, joten ongelman ratkaiseva malli olisi hyvinkin tervetullut pääkäytön sektorille.

Asiasanat: Turvajärjestelmien pääkäyttö, pääkäyttäminen, turvajärjestelmä, kulunvalvonta, avainhallinta, kameravalvonta, rikosilmoitinjärjestelmä, liikekiinteistö, hallinnointi

Juuso Jääskeläinen

Guidelines for the Security System Administration

Year	2014	Pages	79
------	------	-------	----

Access control, key control, video surveillance and alarm systems are managed in commercial real estates and in individual companies by the security system administrators. Systems are intended to promote security, but the goal is difficult to achieve if the management is not performed actively and in accordance with the guidelines. In the working life, I noticed that the user manuals of the systems and other instructions and guides were not sufficient for the expertise base of a security system administrator.

The research questions are approached from the perspective of an empirical development work. The study examines what security systems administration includes and how the management and service processes can be improved. The purpose of this study is to provide information for the administrators as a basis of expertise. The aim of this thesis is to create coherent and uniform guidelines for the administration of security systems. By following these guidelines, the time of accomplishing a management assignment could be decreased while utilizing the maximum capacity of the system. The second objective is to conceptualize the administration of security systems as a term, in order to achieve a common and permanent vision of what it means and what tasks and responsibilities it includes in principle.

The main data collection method is the expert interviewing. Other methods are the workplace-based systematic observation and literature of the security field. The theoretical part handles with the specification of the concept, but also with the meaning and importance of the professional vocabulary in daily work.

The empirical real definition of the term Security system administration was created as a result of the research. It was discovered in the research, that the current level of administration in general is not the most efficient, thus the service processes can still be developed. The customer normally expects that their core business resources are freed by outsourcing the service. However, the security level is not easy to maintain, if the communication is insufficient. The need for determining uniform guidelines is therefore mutual.

The output of this thesis, Guidelines for the Security System Administration, is a tool for administration organizations or companies' internal administrators. The guide is applicable to educational use and to the dissemination of security awareness. Based on the results it can be concluded that with the help of the guidelines, obtaining the system in maintenance mode with high security level is the key to a long life cycle of the system.

The security systems administration as a subject is still rich for further research. Systems containing personal data are devoid of coherent guidelines and a model to specify the creation of access rights in large organizations would be very welcome to the sector of administration.

Keywords: Administration of security systems, Technical security system, Access control, Key control, CCTV, Video surveillance, Alarm system, Property management, Commercial real estate, Administration, Management

Sisällys

1	Johdanto.....	6
1.1	Tausta ja rajaus	7
1.2	Tarkoitus ja tavoitteet	8
1.3	Keskeiset käsitteet.....	8
2	Työn toteutus.....	10
2.1	Lähestymistapa	12
2.2	Tiedokeruumenetelmät	12
2.3	Tietoperustan rakentaminen.....	14
2.4	Oppaan tarkoitus	15
3	Liikekiinteistöjen turvallisuus	15
3.1	Liikekiinteistön turvallisuus asiakkaan näkökulmasta	18
3.2	Turvallinen liikekiinteistö pääkäytön näkökulmasta	19
4	Turvajärjestelmien pääkäyttö	21
4.1	Käsitteen määrittely.....	22
4.2	Turvajärjestelmät.....	23
4.2.1	Kulunvalvonta ja työajanseuranta	24
4.2.2	Avainhallinta	25
4.2.3	Kameravalvonta	27
4.2.4	Rikosilmoitinjärjestelmä	30
4.3	Pääkäytön tavoitteet	31
4.4	Turvallisuuden kehittäminen.....	31
4.4.1	Kulunvalvonnan aloitustyöt.....	32
4.4.2	Avainhallinnan aloitustyöt	34
4.4.3	Kameravalvonnan aloitustyöt	35
4.4.4	Rikosilmoittimen hallinnan aloitustyöt	36
4.5	Turvallisuuden ylläpitäminen & pääkäyttöprosessi	36
4.6	Rekisteriselosteet	37
4.7	Turvajärjestelmien pääkäytön ammattisanasto	39
5	Tulokset ja arviointi	39
5.1	Kehittämistyön tulokset.....	40
5.2	Tulosten arviointi	41
6	Pohdinta ja jatkotutkimus.....	42
6.1	Opinnäytetyöprosessi ja oma oppiminen.....	43
6.2	Jatkotutkimuksen aiheita	44
	Lähteet	45
	Kuvaluettelo	48
	Kuvioluettelo	49
	Taulukkuuettelo	50
	Liitteet.....	51

1 Johdanto

Vuoden 2012 lopulla aloitin työt turvajärjestelmien pääkäyttäjänä yrityksessä, joka tuottaa pääkäyttöpalveluja liikekiinteistöille. Nimikkeeni oli turvajärjestelmien pääkäyttäjä ja hoidin palvelusopimuksista riippuen liikekiinteistöjen kulunvalvonnan, avainhallinnan, kameravalvonnan sekä rikosilmoittimen pääkäyttöä. Havaitsin, etteivät järjestelmäkohtaiset käyttöohjekirjat sekä Finanssialan Keskusliiton ohjeet ja oppaat olleet riittäviä pääkäytön asiantuntijuuden perustaksi.

Tämä opinnäytetyö on työelämän prosesseja edistävä toiminnallinen kehittämistyö, jossa käsittelem liikekiinteistöjen turvallisuusratkaisuja; kulunvalvontaa, avainhallintaa, kameravalvontaa sekä rikosilmoittimen hallintaa turvajärjestelmien pääkäytön näkökulmasta. Opinnäytetyöprosessin tarkoituksena oli tutkia ja selvittää yleisesti turvajärjestelmien hallinnon nykytilaa sekä keinoja ja toimenpiteitä, joilla järjestelmistä on mahdollista saada maksimaalinen hyöty irti. Selvitetyistä toimintatavoista, ilmenneistä ongelmista sekä niiden parannustoimenpiteistä kokosin Turvajärjestelmien pääkäytön suuntaviivat -oppaan tueksi pääkäyttöprosessien parantamista ja yhtenäistämistä varten.

Opinnäytetyöni aihevalinta on rakentunut suoraan työnkuvastani liikekiinteistöjen turvallisuusratkaisujen palveluntoimittajana ja tarpeesta yhtenäiselle ohjeistukselle työn suorittamista varten. Työympäristössä on puhuttu tarpeesta esimerkiksi kirjalliselle ohjeistukselle tai käsikirjalle, jotta palvelun ja työn taustat olisivat helposti ymmärrettäviä. Palvelun kehittämiseksi on myös tärkeää, että pääkäyttäjillä on olemassa selkeät suuntaviivat, joilla turvajärjestelmiä on turvallisuuden kannalta syytä hoitaa (Avald ym. 2014). Pääkäyttäjän olisi hyvä osata hahmottaa eri kohteiden turvajärjestelmien funktiot; miksi esimerkiksi tietyllä alueella on kulunvalvonta, mutta ei kameravalvontaa (Hulkkonen 2014). Syyt vaihtelevat, miksi tietyt turvajärjestelmät ovat mihinkin liikekiinteistöihin valittu ja palvelusopimuksen piiriin sovitettu. Usein turvallisuuden parantamiseen ruvetaan vasta, kun jotain on jo tapahtunut tai riski on havaittu (Kyllästinen 2014).

Suuntaviivat (eng. guidelines) tarkoittavat sääntöjä tai periaatteita, jotka antavat opastusta tarkoituksenmukaiseen toimintaan. Suuntaviivat voivat olla lausuntoja periaatteista, joiden avulla voidaan määritellä toimintatavat tai standardit. Standardit taas tarkoittavat joidenkin esittämiä suosituksia siitä, miten joku asia tulisi tehdä. Pääkäyttöä ei ole ennen käsitteellistetty eikä yhtenäisiä suuntaviivoja ole määritetty, vaan viitekehyksenä ovat toimineet esimerkiksi Kansallinen turvallisuusauditointikriteeristö KATAKRI, Finanssialan keskusliiton suosituksukset, kuten Avainturvallisuusohje (2010), Kameravalvontaopas (Ellonen ym. 2010) sekä lainsäädäntö koskien muun muassa henkilötietojen käsittelyä (Henkilötietolaki 1999/523).

1.1 Tausta ja rajaus

Toiminnallisessa työssä on tarkoituksena järjeistää sekä parantaa käytännön toiminnan ohjeita (Airaksinen & Vilka 2003, 65). Kehittämistyön tavoitteeksi Ojasalo, Moilanen ja Ritalahti (2009, 14) ovat määritelleet kehittämällä ja uudistamisella hyödyn tuottamisen. Tällä työllä tuotetaan hyötyä asiakkaalle sekä palvelun tarjoajalle. Työssä syvennyttään selvittämään, mitä pääkäyttäminen turvajärjestelmien kontekstissa sisältää, millä keinoilla pääkäyttöprosessi paranee, sekä mitä hyötyjä voidaan saada ulkoistamalla järjestelmien pääkäyttö sekä avainten hallinnoinnin pääkäyttöpalvelua tuottavalle yritykselle. Samalla selvitetään turvajärjestelmien hallinnoinnin merkitystä liikekiinteistöjen turvallisuudessa. Pääkäytön tarkoitusta ja sisältöä liikekiinteistöjen toimintaympäristössä on tutkittu haastattelumenetelmin sekä havainnoinnin keinoin.

Pääkäyttäminen terminä on ollut monelle vieras, vaikka järjestelmiä on aina jonkun toimesta hallinnoitu. Usein turvajärjestelmiin on budjetoitu hankintavaiheessa valtavasti rahaa, mutta niiden hallinta- tai huoltotoimenpiteisiin ei ole varattu tarpeeksi tai ollenkaan resursseja, jolloin niiden funktiot turvallisuutta parantavina järjestelminä eivät kohtaa tarkoitustaan, sillä ylläpitämättöminä järjestelmistä saatavat tiedot ovat usein vanhentuneita (Avald, Jeskanen, Pietilä & Öhman 2014). Toinen usein esille noussut tilanne on, että edes pääkäyttöpalvelun tilaaja ei ole aina sisäistänyt tilaamansa palvelun laajuutta, kokonaisuutta tai tarkoituseriä. Samaa myötäilee kiinteistöpäällikkönä toimiva Kari Kyllästinen (2014): ”Manageroinnilta vaatii aktiivista otetta, että turvallisuustaso ei heikkene. Turvallisuus on valitettavasti asia, mitä mietitään kiinteistöissä liian vähän.”

Oppaan sisällöstä on rajattu pois hankinnalliset näkökulmat, sisältäen järjestelmän teknisen suunnittelun, toteutuksen sekä kustannukselliset puolet. Opas ei myöskään sisällä palvelusopimuskohtaisia asioita, vaan on täydennettävissä ja yksilöitävissä yritys- tai kohdekohtaisesti. Sitä voidaan käyttää myös niin sanottujen kohdekorttien eli kiinteistökohtaisten ohjeistusten ohessa ymmärtääkseen syyt, joilla tiettyjä kohteita pääkäytetään. Oppaan pohjalta voidaan kehittää kohteiden turvallisuutta päivittämällä ja arvioimalla mahdollisia aikaisempia olevia ohjeistuksia. Turvallisuuteen vaikuttaa toki myös tärkeänä osana tietoturva- sekä it-palveluratkaisut ja -mallit, kuten virustorjuntasovellukset tai ASP-palvelu (Application Service Provider = sovellusvuokraus) ym. joihin tässä työssä ei oteta kantaa. Pääkäyttäjällä on tärkeää olla toimiva tietotekninen ympäristö, jossa tekninen laitteisto toimii. Tällöin pääkäyttäjä voi keskittyä omaan työhönsä. Tietoturvan osalta täytyy toki muistaa omat, esimerkiksi varmuuskopiointiin liittyvät tehtävät, mutta muuten tietoturvan suuntaviivat tulisi olla määritelty yrityksen omassa tietoturvapoliitikassa (Avald ym. 2014).

1.2 Tarkoitus ja tavoitteet

Työn tavoitteena on määritellä ja käsitteellistää termi ”turvajärjestelmien pääkäyttäminen” (jäljempänä ”pääkäyttö”) ja koota yhtenäiset sekä kunnolliset suuntaviivat kaikkien pääkäyttöpäalveluitä tuottavien tai itse suorittavien tahojen käyttöön. Käsitteellistäminen tarkoittaa normin luomista käsitteen käyttämislle. Palveluntälaajan näkökulmasta työstä on hyötyä, koska suuntaviivojen avulla pääkäytön sisältö voidaan ymmärtää paremmin. Näin ollen palvelua ja turvallisuuskulttuuria voidaan kehittää entisestään. Suuntaviivat käsittävät sekä kokemuksen pohjalta hyväksi koetut tavat ja huomiot että elinkeinoelämän suositukset ja lainsäädännön. Pääkäytön kehittämislä on tarkoitus myös välttää tilanteet, joissa turvajärjestelmä ei vastaa sen hankinnan tarkoitusta.

Jotta pääkäyttöpäalvelu voi olla laadukkaalla ja turvallisuutta edistävällä tasolla, tulevat toimintatavat ja -mallit olla palveluntoimittajalla yhtenäiset ja ennalta määrättyt. Voidaan puhua formaatista, eli malleista ja tasosta, jolla palvelua tarjotaan. Formaatin ollessa laadukas myös turvallisuustaso on kelvollinen. Työssä selvitettyt suuntaviivat voivat olla näkökulmana laadukkaalle formaatille, jolla pääkäyttötöytä voidaan nykyajan turvallisuusvaatimusten mukaisesti tuottaa.

Tutkimuksen pohjalta tehtävä ohjeistus tulee kulkemaan nimellä ”Turvajärjestelmien pääkäytön suuntaviivat” ja se sisältää kattavan ohjeistuksen kootuista toiminnan kannalta hyväksi havaituista suosituksista ja lainsäädännöllisistä syistä, joilla turvallisuutta voidaan ylläpitää ja kehittää eri liikekiinteistöissä tai yrityksissä. Opas toimii erityisesti ohjeistuksena ja koulutusmateriaalina pääkäyttäjille. Oppaasta on apua myös siihen, että jokainen pääkäyttäjä pystyy suuntaviivojen avulla ymmärtämään, mihin tietyt tavat pääkäyttötöiden tekemiseen perustuvat ja miten pääkäyttöprosessit olisivat mahdollisimman tehokkaita. Palvelun tilaaja voi osaltaan taas nähdä oppaasta mallit, joilla työtä olisi suositeltavaa tehdä ja hänelle pystytään tarjoamaan turvallisuuden kannalta töiden suorittamiseen tehokkaampia vaihtoehtoja, jotka perustuvat selkeästi joko lakiin tai yleisiin suosituksiin.

1.3 Keskeiset käsitteet

Opinnäytetyön keskeisimmät käsitteet ovat turvajärjestelmä, pääkäyttö, suuntaviivat, pääkäyttäjä, kulunvalvonta, avainhallinta, kameravalvonta sekä rikosilmoitinjärjestelmä.

Turvajärjestelmä käsittää kaikki välineet, laitteet sekä keinot, joilla suojataan ja turvataan ihmisiä sekä omaisuutta erilaisia uhkia vastaan, kuten rikokset, tulipalot, onnettomuudet, sabotaaetit ja vakoilut. Toteutuessaan nämä uhat aiheuttavat vahinkoa. (Turvallisuusalan sanasto 1989.)

Pääkäyttäjä hallinnoi turvajärjestelmiä, valvoo, antaa sekä rajoittaa oikeuksia muille käyttää järjestelmää tai siihen liittyviä turvallisuusratkaisuja. Pääkäyttäjä on hierarkiamallissa käyttäjän yläpuolella, samoin tavoin kuin järjestelmänvalvoja tietokoneen käyttäjillä. Pääkäyttäjä on käyttäjän tukena järjestelmän käyttöön, niin käytönopastukseen kuin konsultointiin. Käyttäjä voi olla esimerkiksi yrityksen työajanhallintaa hoitava henkilö tai kameravalvonnan osalta kiinteistön huoltomies tai vartija.

Pääkäyttö/pääkäyttäminen on palvelua tai tehtäviä, jota pääkäyttäjä tuottaa. Pääkäyttäminen tarkoittaa järjestelmän hallinnointia sen ylimmällä tasolla. Pääkäyttö voi olla sisäisesti hoidettua tai ulkoistettua palvelua. Pääkäyttäjä valvoo, antaa sekä rajoittaa oikeuksia muille käyttää järjestelmää. Pääkäyttö voi olla sisäisesti hoidettua tai ulkoistettua palvelua, jota yrityksen tai esimerkiksi liikekiinteistön yhteyshenkilö voi kiinteistön järjestelmilleen tilata joko palvelukokonaisuutena tai yksittäisinä pääkäyttötöinä. Palvelu muodostuu palvelun käynnistys- ja tuotantovaiheesta. Pääkäyttöpalvelun tarkoituksena on muutos-, raportointi- ja ylläpitotehtävillä järjestelmien häiriöttömästä ja asianmukaisesta kunnossapidosta huolehtiminen. Avain- ja tunnistehallinnan osalta tämä tarkoittaa kulkutunnisteiden ja mekaanisten avainten hallinnointia alkaen niiden säilytyksestä siihen hetkeen, kun tarve kulkutunnisteelle tai avaimelle päättyy. Kulunvalvonnan pääkäyttämiseen liittyy kulkuoikeuksien määrittely ja ylläpito. Kameravalvonta- ja rikosilmoitinlaitteistojen pääkäyttöön kuuluu järjestelmien määrittelyjen ylläpito. (Ukkonen 2014.)

Kulunvalvonnalla tarkoitetaan tietyllä alueella tai tietyssä rakennuksessa liikkuviin henkilöihin kohdistuvaa, vartioinnilla tai teknisillä laitteilla toteutettua valvontaa (MOT Kielitoimiston sanakirja 2014). Kulunvalvonta on siis alueille, rajoille tai vyöhykkeille kohdistunut turvallisuusvalvonnan osa-alue ja pääkäytön kontekstissa kyse on teknisestä valvonnasta. Kulunvalvontajärjestelmillä on tarkoitus ohjata, valvoa ja rajoittaa kiinteistön kulkuaukoista eli ovisista, hisseistä, porteista jne. kulkemista (Sähköala 2014a). Kulunvalvontajärjestelmiin on integroitavissa myös työajanhallinta- sekä rikosilmoitinjärjestelmiä.

Avainhallintaa voidaan pitää prosessina, joka tarkoittaa lukostojen ja niihin liittyvien avaimien kokonaisuuden hallinnointia ja ylläpitoa (Iloranta 2014). Kiinteistön tai tilan turvallisuuskokonaisuuden kannalta ensimmäinen ja tärkein tavoite on ylläpitää sen lukostoon kuuluvia avaimia (Tyska & Fennelly 1998, 100).

Kameravalvonta kuuluu kulunvalvonnan ja murtovalvonnan lisäksi teknisiin turvasuojausmenetelmiin, joiden tavoitteena on estää tai rajoittaa henkilö- ja omaisuusvahinkoja. Rikostorjunnallisen tehtävän lisäksi kameravalvontaa käytetään prosessien valvonnassa, kulunohjauk-

sen tukena ja tuottamassa web-kamerakuvaa kaupunkien keskeisiltä paikoilta. (Ellonen ym. 2010, 6.)

Rikosilmoitinjärjestelmä on laitteisto, jolla on tarkoitus parantaa tilojen, rakennusten tai alueiden turvallisuutta havainnoimalla mahdollisia murto-, ilkivalta-, sabotaasi-, palovahinko- tai vesivahinkotapauksia. Järjestelmää kutsutaan myös hälytysjärjestelmäksi. Näistä eri tapauksista on tarkoitus välittyä hälytystieto valinnaisesti joko vartiointin hälytyskeskukseen, häätäkeskukseen, järjestelmän käyttäjälle, kiinteistön/tilan omistajalle tai muulle yhteyshenkilölle, tai kaikille edellä mainituille osapuolille. Rikosilmoitinjärjestelmä koostuu useimmiten erilaisista ilmaisimista, kuten liiketunnistimista, magneettikoskettimista, lasirikkoilmaisimista, ryöstöpainikkeista ja seismisistä -, savu- sekä kosteusilmaisimista. (Hulkkonen 2014.)

2 Työn toteutus

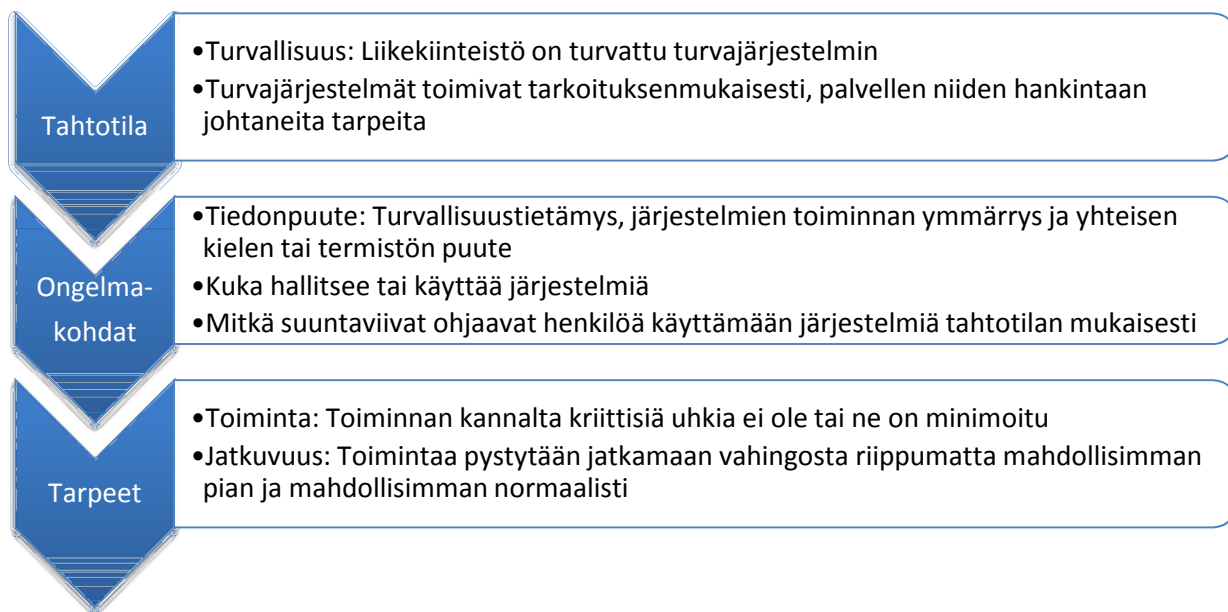
Ihmisillä ja yrityksillä on usein, toimialasta riippumatta, heidän toimintaansa vaikuttavia uskomuksia toimintaympäristöstään ja usein uskotaan, että tuotteet ja palvelut ovat kunnossa (Ojasalo ym. 2009, 21). Tämä pätee myös erittäin olennaisesti turvallisuuteen. Kun liikekiinteistön omistajan puolelta on hankittu turvallisuusratkaisuja kiinteistön suojaukseen, saataan kuvitella, että kiinteistön tai myös oman yrityksen turvallisuusasiat ovat kunnossa (Kylästäinen 2014).

Kiinteistön omistaja saattaa luottaa siihen, että hankkimalla aulavartiointin, järjestelmät ja pääkäyttöpalvelun on turvallisuus mitä parhaimmalla tasolla, vaikka todellisuudessa yksikin epäonnistunut linkki näiden välillä laskee turvallisuustasoa huomattavasti. Esimerkkinä tilanne, jossa kiinteistön vuokralaisia on vaihtunut, mutta aulapalvelun ja pääkäyttöpalvelun puutteellisen kommunikaation takia tieto muutoksesta ei ole päätynyt pääkäyttäjälle, josta syytä uusien kulkualueiden luonti ja määrittely kulunvalvontajärjestelmään on jäänyt tekemättä. (Ukkonen 2014.) Käyttäjien valinnalla on myös merkitystä, sillä yrityksissä on usein vain yksi henkilö, joka osaa käyttää järjestelmää, mikä johtaa ongelmiin esimerkiksi loma-aikoina tai kun henkilö lopettaa kyseiset työt (Ellonen ym. 2010, 45.)

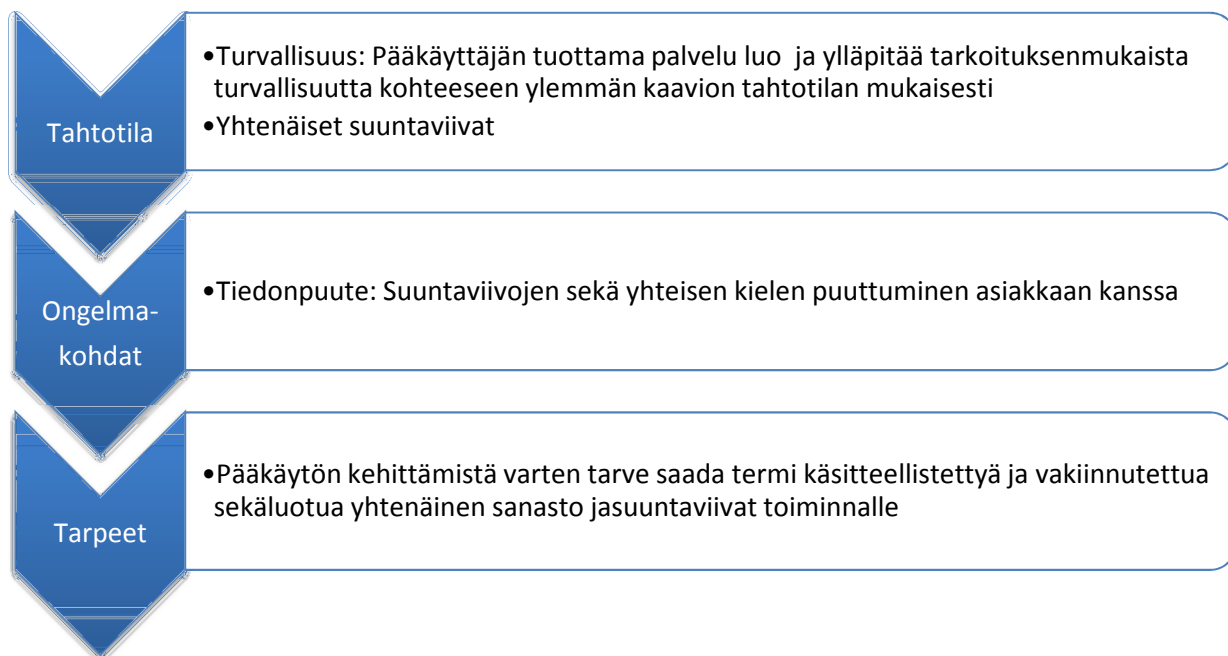
Työssä tutkitaan ja selvitetään, miksi turvajärjestelmien pääkäytön suuntaviivat on tärkeä tiedostaa niin pääkäyttäjän, kiinteistönjohdon, kuin asiakkaankin näkökulmasta. Opinnäytetyön päämääränä on tuottaa informaatiota pääkäytön asiantuntijuuden perustaksi. Taulukko 1 kuvastaa, miten tutkimuskysymykset vievät tarkastelun turvallisuuden tahtotilasta suuntaviivojen tarpeeseen sekä niiden määrittämisen tärkeyteen.

Tutkimuskysymykset: Mitä pääkäyttäminen sisältää, mitkä asiat ohjaavat pääkäyttöä turvallisuuden kontekstissa, miten kiinteistönjohdolle voidaan tuoda esiin pääkäytön mahdollisuudet kokonaisturvallisuuden parantajana sekä millä näitä asioita ja palveluprosesseja voidaan parantaa?

Liikekiinteistön näkökulmasta (kiinteistönjohto ja vuokralaiset):



Pääkäyttäjän näkökulmasta:



Suuntaviivat: Tuotoksena opas turvajärjestelmien pääkäytön suuntaviivoista, joita kiinteistönjohto, vuokralaiset sekä pääkäyttäjät voivat kaikki hyödyntää tarkoituksenaan turvallisempi liikekiinteistö.

Taulukko 1 Tutkimuskysymyksistä tuotokseen

2.1 Lähestymistapa

Tutkimuksellisessa kehittämistyössä pääpaino on varsinaisen kehittämistehtävän saavuttamisessa, mutta tärkeää on myös uuden tiedon tuottaminen käytännöstä. Tässä työssä se tarkoittaa työelämän hiljaisen tiedon dokumentointia, mikä voi uudistaa työelämän osaamis- ja tietoperustaa sekä luoda täysin uutta ammatillista tietoa. Tähän vaaditaan dokumentoinnin lisäksi myös julkisuuden korostamista ja juuri siihen tämä työ ja sen suuntaviivat toimivat hyvänä näkökulmana. Tiedon tuottamisen lisäksi tutkimuksellinen kehittämistyö on ihmisten välistä vuorovaikutusta sekä muutoksen hakemista ja ohjaamista (Ojasalo ym. 2009, 14), josta syystä olen työssä tutkinut myös ammattisanaston kehittämisen tärkeyttä.

Opinnäytetyössä tarkoituksena oli tutkia ja selvittää turvajärjestelmien hallinnoinnin nykytilaa sekä keinoja ja toimenpiteitä, joilla järjestelmistä on mahdollista saada maksimaalinen hyöty irti. Tarkoituksena pääkäytön tutkimukselle on rakentaa ratkaisut ja tuotettu tieto normaalien olemassa olevien käytänteiden päälle. Ojasalon ym. (2009, 21) mukaan kehittämistyössä tulisi näkyä kyky siirtää teoriapainotteista tietoa, eli pääkäytön tapauksessa suositusten ja lainsäädännön tietoja käytännön työhön. Parhaimmillaan tämän avulla voidaan luoda uutta teoriaa. Tämän selvityksen suuntaviivat antavat kuitenkin toimivan näkökulman aiheen perusteellisemmalle tutkimukselle.

Kokemuksellista ammattitietoa ja hiljaista tietoa on tarkasteltava kriittisesti, jotta tuotoksesta tulee tutkimuksellista tietoa (Ojasalo ym. 2009, 22). Tämä pätee erityisesti tätä aihetta käsiteltäessä, sillä suuntaviivoja ei ole ennen määritetty, vaan palveluntuottajat ovat toimineet pitkälti juuri ammattitiedon ja hiljaisen tiedon varassa, nojaten nämä näkökulmat tietysti lainsäädäntöön ja suosituksiin (Avald ym. 2014). Pääkäytön suuntaviivat tuovat samalla ilmi pääkäyttäjälle sekä palveluntilajalle miten turvallisuutta ja turvallisuusratkaisuja voidaan palveluntoimittajan tai yksittäisen pääkäyttäjän toimesta ylläpitää ja kehittää.

2.2 Tiedokeruumenetelmät

Ennen käytettävien menetelmien valintaa, oli kehittämistyön tavoitteeksi määritelty pääkäytön suuntaviivojen kokoaminen ja termin käsitteellistäminen. Menetelmiksi valitsin systemaattisen havainnoinnin ja asiantuntijahaastattelut, joista jälkimmäisin oli selvästi laajin ja tärkein tietolähde. Työn teoriatausta perustuu lisäksi alan kirjallisuuteen. Selvitystyöhön on käytetty empiiristä toimintaa, eli tarkoituksena on ollut saada kokemukseräistä tietoa liikekiinteistöjen turvallisuusratkaisuista ja -tavoitteista sekä niitä tukevista palveluntuottajien toimintatavoista. Tavoitteena on myös ollut omien valmiuksieni lisäksi tarkastella muita pääkäyttöön liittyviä tehtäviä kriittisesti, jotta tieto olisi selkeästi tutkimuksellista, eikä perustuisi vain yhden palvelua tuottavan yrityksen asiantuntijalausuntoihin.

Haastattelin kiinteistö-, turvallisuus- ja lukitusalan asiantuntijoita sekä pääkäyttöpäalvelun tilaajia. Koska pääkäyttöpäalvelut eivät ole vielä niin laajasti suuren käyttäjäkunnan tiedossa, eikä julkista sekä kattavaa materiaalia pääkäytön koulutukselle ole, valikoitui ensisijaisiksi lähteiksi pääkäyttöpäalvelua tuottavien yritysten pääkäytön asiantuntijat, kuten Flexim Security Oy:n pääkäyttöyksikkö sekä avainhallinnan asiantuntijat. Pääkäyttöpäalveluntoimittajia tavoitin haastatteluita varten yhdeksän eri asiantuntijaa kolmesta eri yrityksestä. Heistä kuusi teki kulunvalvonnan pääkäyttöä, kaksi kameravalvonnan sekä rikosilmoittimen hallinnointia, yksi oli erikoistunut työajanhallinnoinnin pääkäyttöön ja neljä suoritti myös avainhallinnan pääkäytön tehtäviä. Lisäksi asiantuntijahaastattelua hyödynsin julkisen sektorin eli poliisin puolelta haastatteleamalla Helsingin poliisilaitokselta teknisen tarkkailun yksiköstä rikoskomisario Markku Mäkistä liittyen kameravalvontaan. Avainhallinnan osalta haastattelin Abloy Oy:n ohjelmistoasiantuntijaa Riitta Räsästä. Liikekiinteistöjen edustajista haastattelin Ovenia Oy:n ylläpitöpäällikköä Niko Juntusta sekä Corbel Oy:n kiinteistöpäällikköä Kari Kyllästä.

Käytin haastatteluita tiedonkeruun menetelmänä, sillä pääkäyttöä käsitteleviä tutkimuksia tai muuta kirjallisuutta ei ollut saatavilla. Havainnointini pohjalta pääkäyttäminen ja hallinnointi ymmärrettiin laajuuksiltaan usein erilaisilla. Olin tehnyt haastatteluita varten kysymysrungot valmiiksi jokaista haastateltua varten, osittain samoilla kysymyksillä, mutta myös asiantuntijan ydinosaamisalueet huomioon ottaen. Tarkoituksena asiantuntijahaastatteluilla oli saada aikaan avointa keskustelua pääkäytöstä ja siihen liittyvistä näkökulmista. Ensimmäisellä pääkäyttäjän haastattelulla hain yleisempää katsausta pääkäytön sisältöön keskustelemalla muun muassa aiheista: ”Mitä pääkäyttö on?” ja ”ammattisanasto ja sen merkitys”. Tuloksia pystyin vertaamaan omaan työkokemukseen pääkäyttäjänä ja seuraavilla pääkäyttäjän haastatteluilla pystyin vertaamaan uusia näkökulmia aiempiin näkemyksiin. Haastatteluissa yhtenäisiksi havaitsemiani käytäntöjä hyödynsin suuntaviivojen kokoamisessa. Kiinteistönjohdon näkökulmia liikekiinteistöjen turvallisuuteen liittyen selvitin avoimilla haastatteluilla kiinteistöpäälliköiden kanssa. Painotin haastattelun aiheita turvajärjestelmiin liittyviin suojauskeinoinhin sekä vertasin tietoja omiin havainnoiteihin. Tarkoituksena oli myös selvittää pääkäyttöön liittyvät hyödyt, mahdolliset haitat ja muut näkökulmat hallinnointiin liittyen.

Systemaattista havainnointia on käytetty opinnäytetyöprosessin koko ajalta hyödyksi, kirjaimella systemaattisesti ylös kaikki pääkäyttötyössä havaitut ongelmat, puutteet sekä kehityskohdat henkilökohtaisesti että koko työyksikön kesken. Näistä havainnoista keskusteltiin säännöllisesti sekä sisäisesti laskettiin, mitkä tekijät vaikuttavat negatiivisesti pääkäyttöprosessien sujumiseen. Kirjallisuudella oli tarkoitus selvittää tämän hetken tutkimustietoa sekä ohjeistuksia liittyen avainturvallisuuteen ja kameravalvontaan. Lukitukseen, avainhallintaan ja kulunvalvontaan liittyen tutkin muutamia opintojen lopputöitä, kuten Waltteri Holmbergin ”Lukitusjärjestelmät ja niiden hankintaprosessi”, mutta moni näistä liittyi järjestelmien omi-

naisuuksiin sekä kustannuksiin, eikä niinkään varsinaisiin prosesseihin. Tutkin ja vertasin tuloksia myös lakiteksteihin mm. henkilötietojen säilyttämisestä, tarkoituksenani ymmärtää syvällisemmin, mitkä menetelmät ovat lainalaisia. Osa käytännöistä oli hyviksi ja toimiviksi havaittuja pääkäyttäjien keskuudessa ja täten myös itse sovellettavissa turvallisuus- ja palvelunäkökulman mukaan.

2.3 Tietoperustan rakentaminen

Tutkimuksellinen kehittämistyö voi olla perua organisaation kehittämistarpeista tai muutosten aikaansaamisen halusta. Kehittämistyöhön kuuluu täten käytännön ongelmien ratkaisuja ja esimerkiksi uusien käytäntöjen tai palvelujen tuottamista ja toteuttamista sekä ratkaisujen käyttöön ottamista. Kehittämistyön tarkoituksena on viedä asioita eteenpäin, kuten tässä työssä pääkäyttö on tarkoitus nostaa terminä vakiintuneeksi käsitteeksi ja omaksi kokonaisuudekseen turvallisuuden kentällä. Työssä on myös tieteellisen tutkimuksen piirteitä, sillä pääkäyttöön liittyville entuudestaan käytetyille prosesseille luodaan kokonainen viitekehys. Prosessien määrittelemisen ei itsessään johda käytännön uusiin ratkaisuihin (Ojasalo ym. 2009, 14), joten tieteelliselle selvitykselle oli tarvetta. Tietoperustaa onkin lähdetty rakentamaan miettimällä, miten pääkäyttöä voidaan kehittää, mitä parannuksia voidaan saada aikaan sekä miten uusia käytäntöjä voisi hyödyntää.

Työn tietoperusta pohjautuu työelämäkokemuksiin ja havainnointiin sekä alan kirjallisiin ohjeistuksiin ja asiantuntijoiden haastatteluihin. Teoreettista tietoa turvajärjestelmien pääkäyttämistä ei alan kirjallisuudesta löydy, joten omaa tutkimustietoa on täytynyt käsitellä vertaillen sekä erityisen kriittisesti. Aikaisempien tutkimusten puutteellisuuden vuoksi olen pyrkinyt kuvaamaan pääkäytön taustoja mahdollisimman tarkasti. Kehittämistyöni lähteinä olen käyttänyt suosituksia (esim. Kansallinen turvallisuusauditointikriteeristö KATAKRI, versio II), lakeja (esim. Henkilötietolaki 1999/523), pääkäyttöpalveluntoimittajien ja kiinteistönselityksen asiantuntijoiden haastatteluja, Finanssialan Keskusliiton ohjeistuksia (esim. Avainturvallisuusohje 2010) sekä kirjallisuutta, esim. Turvallisuustutkimuksen tekeminen (Heinonen, Keinänen, Paasonen 2013) ja Yrityksen turvallisuusopas (Heljaste ym. 2008).

Opinnäytetyön tavoitteena oli koota tutkimus-, havainnointi- ja selvitystiedon pohjalta liitteeksi tullut Turvajärjestelmien pääkäytön suuntaviivat -opas. Vaikka pääkäyttöä on onnistuneesti tehty jo pidemmän aikaa, ei työllä ole koskaan ollut yhtä selkeää raamistoa. Ratkaisut ovat pohjautuneet hyväksi koettuihin menetelmiin ja toimintatapoihin sekä järjestelmien rekisteriselosteisiin (Liljedahl 2014), mutta asiakasrajapinnasta tarkasteltuna nämä ovat usein hankalasti hahmotettavissa, jolloin tarpeet ja palvelusopimukseen kuvatut toiminnot eivät aina kohtaa toisiaan (Kyllästinen 2014).

Pääkäyttäjän työnkuvaa ja -sisältöä on vaikea kokonaisuudessaan hahmottaa ilman proaktiivista turvallisuusajattelua. Myöskään mitään pääkäyttöä suoraan opettavaa koulutusta ei ole, eikä julkista koulutus- tai oppimateriaalia. Tämän vuoksi tällä opinnäytetyöllä on merkittävästi uutuusarvoa, sillä tavoitteena onkin tehdä julkiset suuntaviivat, minkä avulla kuka vain voi ymmärtää pääkäytön tärkeimmät prosessit, menettelyt ja kehityssuunnat.

2.4 Oppaan tarkoitus

Valmista opasta on tarkoitus pystyä hyödyntämään niin yrityksen turvajärjestelmien käyttöönottilanteessa, pääkäyttötoimintaa aloittaessa tai sitä kehittäessä, kuin myös koulutuskäytössä tai imagonäkökulmasta. Tuotoksen tulee olla kenen vain käytettävissä ja hyödynnettävissä omaan toimintaansa. Turvajärjestelmien pääkäytön suuntaviivat -ohjeistus on hyödynnettävissä pääkäyttäjän sekä asiakkaan näkökulmista riippumatta siitä, onko pääkäyttöpalvelu ulkoistettua vai sisäisesti hoidettua. Prosessien, kommunikaation ja ymmärryksen tulisi kuitenkin olla samalla tasolla, jotta palvelu voi olla laadukasta.

Pääkäytön sanasto yhtenäistää turvajärjestelmiin ja niiden hallinnointiin liittyvän terminologian. Sanasto on tarkoitettu käytettäväksi niin pääkäyttäjille kuin kenelle muulle tahansa, jolla on yhteys kulkutunnisteisiin, avaimiin tai yleisesti turvallisuuteen. Pääkäyttäjillä, yrityksen pääkäyttöpalvelun yhteyshenkilöillä sekä yrityksen turvallisuudesta vastaavilla henkilöillä tulisi vähintään kuitenkin olla palvelusta riippuen käsitteiden perustuntemus. (Avald ym. 2014.)

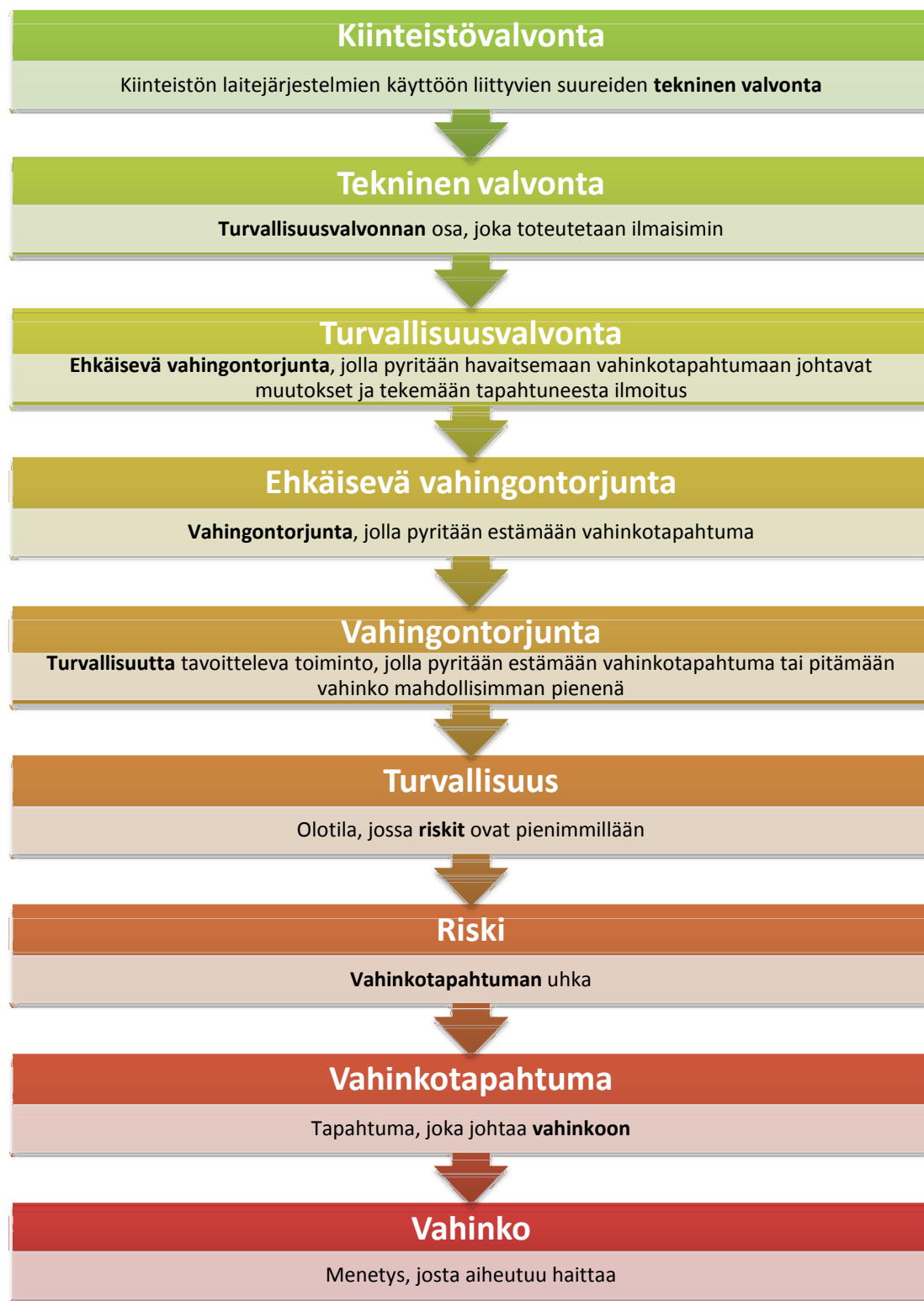
3 Liikekiinteistöjen turvallisuus

Pääkäyttäminen kokonaisvaltaisena palveluna, sisältäen kaikki turvajärjestelmät, keskittyy lähes yksinomaan liikekiinteistöihin, jonka vuoksi selvityksessä käytetään kontekstina liikekiinteistöjen pääkäyttöpalvelua. Asunto-osakeyhtiöissä esimerkiksi kulunvalvonta on harvinaisempi ratkaisu, mutta avainhallintaa voidaan hyvinkin hoitaa pääkäyttäjän toimesta. (Iloranta & Viljakainen 2014.)

Mikäli avainten tai kulunvalvontajärjestelmän hallinta ei ole kunnossa, turvallisuusratkaisut, kuten kiinteistön täysmittainen lukitus tai kulunvalvontalaitteisto, eivät itsessään kasvata tai ylläpidä turvallisuutta. Lukituksessa menetetään turvallisuushyöty, jos ei tiedetä kenellä mikäkin avain on hallussa, puhumattakaan esimerkiksi kadonneista yleisavaimista. Kulunvalvonnassa hyöty menetetään, mikäli kulkualueita ei ole suunnitellusti rajattu tai kulkutunnisteiden haltijoista ei ole tietoa. (Iloranta & Viljakainen 2014.) Myös ratkaisujen huomioiminen kokonaisuutena on erittäin tärkeää, jotta järjestelmät tukevat toisiaan. Edellä mainitut asiat huomioon ottaen, on silti muistettava, että olivat järjestelmät joko elektronisia tai mekaani-

sia, vaativat ne oikein toimiakseen huoltoa, ylläpitoa ja toiminnan tarkkailua. Tarkoitushan ei ole, että turvajärjestelmistä olisi haittaa vaivattomaan kulkemiseen. Hoitamaton kulunvalvontajärjestelmä voi rikkoutuessaan jättää tahattomasti henkilöitä lukkojen taakse paikkoihin, joista olisi tarkoitus päästä ulos. Ja tähän ei ole turvajärjestelmien tarkoitus. Toisaalta, mitä hyötyä on myöskään rikoksen selvittämisessä esimerkiksi valvontakameralla, jonka kuva on epätarkka tai tallennus ei ole toiminut. (Ukkonen 2014.)

Kuviossa 1 havainnoillistan Turvallisuusalan sanaston (1989) mukaisen määritelmän termistä kiinteistövalvonta, joka on suojaava tekijä liikekiinteistöjen turvallisuuden näkökannalta. Kiinteistöjä suojataan, jotta vahinkoja ei tapahtuisi. Vahingoilta eli haittaa aiheuttavilta menetyksiltä välttyminen on siis suojattava arvo. Kuviossa osoitan näiden suojaavan tekijän sekä suojattavan arvon väliset suhteet Turvallisuusalan sanaston mukaisilla termeillä.



Kuvio 1 Kiinteistövalvonta (Turvallisuusalan sanasto 1989)

3.1 Liikekiinteistön turvallisuus asiakkaan näkökulmasta

Kiinteistönjohdon näkökulmasta on tärkeää tietää, keitä kiinteistöissä liikkuu ja milloin. Syvemmin tarkasteltuna, tärkeintä on tietämys siitä, että nämä kulkutapahtumat tai kameratalenteet voidaan saada turvajärjestelmän avulla nähtäviksi. Liikekiinteistön johto, kuten yksittäisen kohteen kiinteistöpäällikkö, haluaa olla tietoinen siitä, että kohteeseen hankitut järjestelmät toimivat, tiedot ovat dokumentoitu ja ovat ajan tasalla. Nämä asiat luovat turvallisuuden tunnetta, ja se on tärkein mittari sille, että kiinteistönjohto voi sanoa uskoa kiinteistönsä olevan turvassa ja suojattu. Lisäksi tärkeä osa turvallisuuden tunnetta on se, että kiinteistön vuokralaiset ymmärtävät turvallisuuden tarkoituksen ja merkityksen. (Juntunen 2014.)

Ovenia Oy:n ylläpitöpäällikkö Niko Juntusen (2014) mukaan kiinteistöjen turvallisuus koostuu avainhallinnan, kulunvalvonnan, kameravalvonnan, rikosilmoittimen sekä vartiointin paloista. Juntunen myös mainitsee, että kameravalvonta ja vartiointi yhdistettynä ovat toimiva ratkaisu, sillä vaikka kaikkea ei pysty itse seuraamaan, niin kiinteistöllä on kuitenkin silmät. Hän kuitenkin näkee, että kulunvalvonta asiakkaan tai kiinteistön vuokralaisen näkökulmasta on ehdoton, sillä pelkkä mekaaninen lukitus nähdään vaikeana. Toisaalta myös rikosilmoitin integroituna kulunvalvontajärjestelmään on toimiva ratkaisu, joka edistää turvallisuustietoisuutta siten, että esim. auki teljettyt ovet aiheuttavat hälytyksen ja käyttäjät reagoivat tähän oppimalla sulkemaan ovet. Muutoinkin mahdollisimman moni järjestelmä integroituna yhteen yksinkertaiseen käyttöliittymään olisi kiinteistönjohdon näkökulmasta toimiva kokonaisuus, mutta raha ja kustannukset rajoittavat aina hankintoja.

Corbel Oy:n kiinteistöpäällikkö Kari Kyllästinen (2014) harmittelee, ettei turvallisuusasioita huomioida yleisesti ottaen tarpeeksi, eikä pääkäyttäjätasoiseen järjestelmien hoitoon varmasti olisikaan tarpeeksi resursseja. Tästä syystä kulunvalvonta ja avainhallinta ovat usein ulkoistettu aulapalveluille tai vartiointille ja kameravalvonnan hallinnointi huoltomiehille, vaikka pääkäyttölliset tehtävät ovatkin heille ylimääräistä tehtävää. Tämän vuoksi Kyllästinen uskoo, että turvallisuustaso voi vaihdella eri kiinteistöjen kohdilla paljonkin, ja selkeillä yhteisillä linjauksilla turvallisuuskulttuurin on mahdollista parantua.

Juntunen (2014) näkee, että mitä vähemmän turvajärjestelmien ylläpitämiseen käyttää resursseja, sitä isommaksi riskit kasvavat. Tällöin järjestelmien tiedot eivät ole enää ajan tasalla ja siten palvele tarkoitustaan. Tärkeintä ylläpidossa on dokumentointi kaikista järjestelmistä sekä niiden sisältävistä tiedoista. Järjestelmien hallinnoinnin ulkoistaminen pääkäyttöpäalvelua tuottavalle yritykselle Juntunen näkee toimivana, sillä usein henkilömäärät ja tietomas-
sat ovat liikekiinteistöissä niin suuret, että kiinteistöpäällikkö ja huoltomies eivät yhdessäkään pysty halutun ylläpitotason mukaisesti hoitamaan pääkäyttöllisiä tehtäviä, kuten avainten

luovuttamisia ja palautuksia, tunnisteiden aktivointeja sekä kameratallenteiden hakemisia ja tarkastuksia.

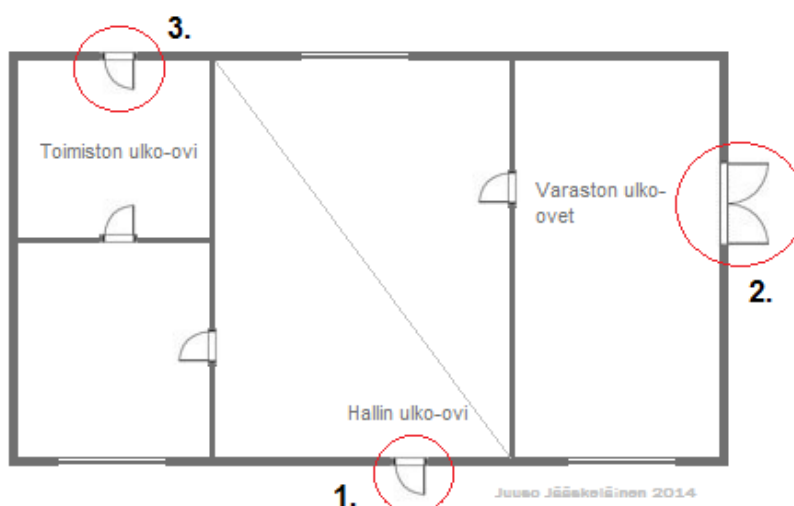
Turvajärjestelmien eheyttä tarkastellessa on jatkuvuussuunnittelu tärkeässä roolissa. Toimintaa haittaavien tapahtumien vaikutusta ja aikaa voidaan lyhentää huomattavasti onnistuneella pääkäytöllä. Järjestelmän pääkäyttäjä on tärkeää saada vika- tai rikostilanteessa mahdollisimman pian tavoitettua selvitystoimenpiteitä ja toipumista varten. Helsingin poliisilaitokselta Vakavan rikollisuuden toimintayksiköstä, tekniseen tarkkailuun erikoistunut rikoskomisario Markku Mäkinen sekä hänen kollegansa Otto Kurtelius (2014) toteavatkin, että turhan usein ilmenee tilanteita, joissa kiinteistön kameravalvonnasta vastaavaa henkilöä ei saada rikoksen selvittämistä varten kiinni, tai tallenteita ei osata ollenkaan ottaa ulos järjestelmästä. Suurimmaksi syyksi he näkevät tässä järjestelmän puutteellisen hallinnoinnin.

3.2 Turvallinen liikekiinteistö pääkäytön näkökulmasta

Pääkäyttäjä haluaa lähtökohtaisesti olla tietoinen ja varmistunut siitä, että hänen hallinnoimat turvajärjestelmät ylläpitävät kiinteistön turvallisuutta. Pääkäyttäjälle turvallisuuden tunne syntyy siitä, kun voidaan tiedostaa turvajärjestelmien hallinnan ja ylläpidon olevan kunnossa, sekä kun ratkaisut on turvattu ja tiedot varmuuskopioitu. Tärkeintä on kuitenkin tietoisuus ja luottamus siitä, että asiakkaat muistavat aina ilmoittaa järjestelmiin kohdistuneista tapahtumista ja niihin vaikuttavista muutoksista. (Hulkkonen 2014.)

Pääkäyttäjälle olisi selkeä etu tuntea kohdeorganisaatio ja -kiinteistö, mutta usein tämä ei asiakasvolyymien ja etäisyyksien takia ole mahdollista. Tällöin kiinteistön tai yrityksen yhteyshenkilön tulisi itse tiedostaa kohteen ominaisuudet sekä tiedottaa näistä pääkäyttäjille. Tarkoitus on, että pääkäyttäjä suorittaa tehdyn palvelupyynnön ja tukee tarvittaessa järjestelmiin ja kokonaisturvallisuuteen liittyvissä ratkaisuissa ja kehitysideoinnissa, mutta asiakkaan ei tule tukeutua siihen, että pääkäyttäjä havaitsisi pyynnöstä oleellisesti poikkeavia tekijöitä. (Ukkonen 2014.)

Esimerkkiongelmiana uuden kulkualueen luominen kulunvalvontajärjestelmään: Kuvan 1 kiinteistön yhteyshenkilöltä tulee pyyntö luoda uusi kulkualue tilan X uudelle vuokralaiselle. Pyyntö tulee ilman pohjakuvaa. Tilat ovat yhtä aluetta ja punaisella ympyröidyissä kuorioivissa on kulunvalvontalukijat. Ilmoituksen mukaisesti ”kulkualueeseen tulee oikeudet kulkea hallin sekä toimiston ulko-ovista”, eli ovista 1. sekä 3. Varaston ovista 2. pääsee kuitenkin samoihin tiloihin. Tällöin syntyy ristiriita, joka voi aiheuttaa kulkuongelmia. Mikäli pääkäyttäjä tuntee kyseiset tilat, voidaan ristiriita mahdollisesti havaita etukäteen, mutta tämä hidastaa pääkäyttöprosessia sekä heikentää oleellisesti turvallisuustasoa ja luottamusta dokumentaatioon sekä järjestelmän aukottomuuteen.



Kuva 1 Liikekiinteistön tila X: Pohjakuva

Voisi olettaa, että mikäli asiakkaalta ei koskaan tule palvelupyynnöitä tai tilauksia, ovat asiat kunnossa ja asiakas pysyy tyytyväisenä. Pääkäyttäjällä ei voi kuitenkaan olla varmaa, onko muutoksia tapahtunut ja ovatko järjestelmät ajan tasalla. Tällöin liikekiinteistö ei pääkäytön näkökulmasta ole täysin riskittömässä tilassa. Mikäli rikos tai muu kiinteistöön kohdistuva vahinko pääsee tapahtumaan, on pääkäyttäjällä yleensä ensisijaisena apuna tutkinnassa.

Kaikkia Liikekiinteistöjen tai yritysten turvallisuuden näkökulmasta pääkäyttäjällä on kiinnostunut tietämään kiinteistön ulkoisilla toimijoilla olevat kulkutunnisteet ja haltijat, jotta käyttäjien kokonaismäärästä ollaan tietoisia. Tiedolla pystytään myös todentamaan helposti kiinteistössä liikkuvat ulkopuoliset organisaatiot. Pääkäyttäjällä haluaa tietää, että vuokralaisilla olevien kulkutunnisteiden ajantasaiset nimilistaukset ovat joko yrityksellä itsellään tai pääkäytön hallussa. Avainhallinnan osalta tärkeää on tietää, kenelle mekaaniset avaimet on kuitattu. Jatkuvuuden kannalta tärkeää on tiedostaa, että avaimien ja kulkutunnisteiden eteenpäinkuittauskäytännöt ovat kunnossa, eikä avaimia ole kadoksissa.

Järjestelmien eheyden vuoksi tärkeää on, ettei muilla kuin pääkäyttäjällä itsellään ole pääsyoikeuksia tekemään muutoksia järjestelmään. Jokaisen turvajärjestelmän ylläpitämistä ajan tasalla edellyttää, että asiakas ymmärtää kommunikoinnin tärkeyden. Pääkäyttäjän oman dokumentoinnin osalta on tärkeää, että kiinteistön pohjakuvat on dokumentoitu ja ajan tasalla lukituksen että kulunvalvonnan osalta. Tämä sisältää lukoston sijoituspohjakuvat ja kulunvalvonnan pohjakuvat kulunvalvontalukijoiden osalta. Myös kameroiden, rikosilmoittimien silmukoiden sekä laitehuoneen sijainnit on hyvä dokumentoida pohjakuviin. Dokumentit voidaan tehdä kaikki ratkaisut kattaen, tai jokainen erikseen selkeyden vuoksi. Koska tiedot ovat luotamuksellisia, on pääkäyttäjällä tiedostettava ja varmistettava, että omat tiedot ja yhteydet ovat suojattuja sekä varmuuskopioituja. Palvelun keskeytyksettömyyden kannalta on hyvä

huomioida myös, että järjestelmät on suojattu varavirtajärjestelmillä, eli UPS:illa (=Uninterruptible Power Supply) toimivuuden takaamiseksi lyhyissä sähkökatkoksissa sekä syöttöjännitteen epätasaisuuksissa. (Avald ym. 2014; Hulkkonen 2014; Iloranta & Viljakainen 2014; Ukkonen 2014.)

4 Turvajärjestelmien pääkäyttö

Tässä luvussa käsitellään turvajärjestelmien pääkäyttöä käsitteenä, sen tavoitteita ja merkitystä turvallisuuden kehittämiseksi. Ensin täytyy ymmärtää käsite ja sen sisältö. Tämän jälkeen käsitteen tavoitteet on määriteltävä, ennen kuin päästään tarkastelemaan tilaa ja konkreettisia tehtäviä, joiden avulla tavoitteet saavutetaan. Näitä tehtäviä kutsutaan järjestelmien aloitustöiksi tai tietokannan siivoustöiksi.

KATAKRI:n fyysisen turvallisuuden F300 *Turvallisuustekniset järjestelmät* -osa-alueen kysymys F 306.0 antaa osviittaa tasosta, jolla pääkäyttöpalvelua voidaan ulkoistettua hoitaa. Viranomaisvaatimukseltaan korkea taso (II) määrittelee, että ”Kulunvalvontajärjestelmän hallinnointi voi olla ulkoistettu, jos se on hyvin hallinnoitu.” (2011, 72). Voidaan siis todeta, että korkeinkin turvallisuusluokitellun tilan kulunvalvonnan pääkäyttö voidaan ulkoistaa, mikäli palvelu tuotetaan tiettyjen suuntaviivojen mukaisesti. Tällöin voidaan puhua pääkäyttöprosessista, jonka tarkoituksena on siirtää vastuu erikseen nimetyyn turvatekniseen järjestelmän tai järjestelmien pääkäyttötoimenpiteistä sopimusteitse pääkäyttöyritykselle sekä vapauttaa asiakkaan resursseja muihin tehtäviin (Flexim Security 2014).

Pääkäyttöpalvelun yhtenä tarkoituksena on tuottaa asiakkaan turvajärjestelmien hallinnointiin liittyvät ratkaisut. Vain sellaisia ratkaisuja voidaan oikeasti ja turvallisesti hallita, joiden kopioiminen ja/tai tuottaminen on suojattua, joten esimerkiksi lukostoa, jonka patenttisuoja on päättynyt, ei voida mitenkään hallinnoida ilman riskejä (Viljakainen 2012).

Pääkäytön ulkoistamisella yritys saa siirrettyä suurimman osan päivittäisestä turvallisuus- ja riskienhallintatyöstä toisaalle, jolloin yrityksen omaan ydinliiketoimintaan jää enemmän resursseja (Flexim Security Oy 2014). Liikekiinteistön managerointiyhtiön edustajan eli esimerkiksi kiinteistöpäällikön osalta tämä tarkoittaa, että myöskään liikekiinteistöjen turvallisuusasiat eivät pelkästään ole enää yksittäisen henkilön vastuulla (Kyllästinen 2014).

Toisena tarkoituksena on kiinteistön tai yrityksen turvallisuustason jatkuva kehittäminen. Palvelun toimittajilla eli pääkäyttäjillä ydinosaaminen on juurikin turvallisuus, joten resurssit kehittämistyölle ovat sitä myöten vahvat. Räätelöimällä palvelusopimus voidaan samalla täyttää yrityksen tai kiinteistön tiettyjen tilojen turvallisuustason mukaiset vaatimukset Kansallisesta turvallisuusauditointikriteeristö KATAKRI:sta (Ukkonen 2014).

Pääkäyttäjä voi palvelusopimuksen rajauksien mukaan vastaanottaa ja selvittää palvelupyynn-
töjä esimerkiksi oviympäristön ongelmiin tai kameravalvontatallenteisiin liittyen. Optimi
(ihannetila) on, että järjestelmää tai samaa tietokantaa hallinnoi sujuvan tiedonvälityksen
vuoksi vain yksi pääkäyttäjät tai organisaatio. Järjestelmien käyttöönotosta ja konfiguroinnista
eli järjestelmän asetuksien palvelukohtaisesta yksilöinnistä sekä päivityksien huolehtimisesta
vastaa palveluntoimittaja. (Avald ym. 2014.)

4.1 Käsitteen määrittely

Kappaleessa 1.3 *Keskeiset käsitteet* käsiteltiin erikseen termit *Turvajärjestelmä* sekä *Pää-
käyttö*. Nämä ovat lähikäsitteitä, jotka määrittyvät aina asiayhteydestä. *Turvajärjestelmien
pääkäyttö* on syytä käsitteellistää siksi, että monesti erityisalan termit ovat alaa tuntematto-
mille vaikeita (Aalto-yliopisto 2014). Tämä vaikeus aiheuttaa pääkäyttöprosessin pitkittymistä
sekä pahimmillaan turvallisuusriskejä. Aalto-yliopiston Käsitteiden määrittely ja käyttö -
tekstin (2014) mukaan käsitteen määritelmän avulla vähennetään ilmausten monimerkityksi-
syyttä ja sillä esitetään sopimus siitä, mitä käsitteellä tarkoitetaan. Tässä yhteydessä on myös
hyvä olla selvitetty, miten muut ovat käyttäneet vastaavia käsitteitä.

Vastaavasta termistä ”pääkäyttäjäpalvelu” on saatavilla tietoa eri palveluntoimittajilta,
muun muassa Stanley Security Oy:ltä, BLC Turva Oy:ltä sekä Flexim Security Oy:ltä. Jokaiselta
kolmelta yritykseltä nousee selkeimmin esiin asiakkaan resurssien vapauttaminen omaan liike-
toimintaansa. Flexim Security Oy (2014, 3) kuvaa, että palvelun tavoitteena on varmistaa jär-
jestelmien häiriötön ja asianmukainen toiminta, kun taas Stanley Security Oy (2014) ilmaisee,
että pääkäyttäjäpalvelu huolehtii yrityksen turvallisuudesta katkeamattomasti. BLC Turva Oy
(2014) mainitsee palvelun kuvauksessaan, että palvelulla tarkoitetaan päivittäisiä muutos-,
raportointi- ja ylläpitotehtäviä, jotka ovat räätälöitävissä asiakkaan tarpeiden mukaisesti.
Palvelun sisällön puolesta yhteistä on se, että pääkäyttöpalvelua tuotetaan asiakkaan tarpeita
heijastellen. Stanley Security Oy kuvaa tätä siten, että palvelun tarkoituksena on suorittaa
tietojen hallintapalveluita asiakkaan palvelupyyntöjen mukaisesti. Flexim Security Oy:llä sa-
ma ilmenee palvelun tavoitteessa tukea järjestelmien pääkäyttöä.

Koska pääkäyttö voi olla myös sisäisesti hoidettua turvajärjestelmien hallinnointia, voidaan
termistä luoda reaalinmääritelmä, joka pyrkii sanomaan jotakin määriteltävän käsitteen tun-
nusomaisista piirteistä eli erittelemään kuvaamaansa käsitettä. Turvallisuuteen liittyvänä
terminä reaalinmääritelmä on myös sopivin, sillä Aalto-yliopiston (2014) mukaan reaalinmääri-
telmät ovat tavallisia juuri erikoisalojen oppi- ja sanakirjoissa.

Käsiteanalyysi tarkoittaa käsitteen sisällön määrittelyä eli käsitteen olennaisten piirteiden tunnistamista sekä niiden keskinäisten suhteiden osoittamista (Aalto-yliopisto 2014). Lisäksi sen avulla voidaan saavuttaa tila, jossa yleisesti käytetty termi tarkoittaa kaikille samaa asiaa. Käsiteanalyysin tavoitteena voi olla yhdenmukaisen määrittelyn löytäminen, jolloin ilmiötä tai asiasta kyetään kommunikoimaan täsmällisesti ja yhteneväisesti, joka puolestaan edistää viestintää. (Puusa 2008, 38.)

Käsiteanalyysissä määritellään ensimmäisenä termin laji. Termin ollessa ”turvajärjestelmien pääkäyttö”, määrittelen, että se kuuluu luokkiin hallinnointi sekä pääkäyttäminen. Seuraavaksi määritellään termin määrittelevä ominaisuus, joka tässä tapauksessa on ”turvajärjestelmät”. Termiä määritellessä tarvitaan vielä termiin kuuluvat rakenneosat, joita turvajärjestelmien pääkäytössä ovat kulunvalvonta, avainhallinta, kameravalvonta, rikosilmoittimen hallinta sekä työajanhallinta. Käsiteanalyysissä tarkastellaan viimeiseksi, miten termiä voidaan vielä siihen liittyvien tehtävien mukaan eritellä tarkemmin. Tehtäviä ovat turvallisuus, turvallisuuden edistäminen ja ylläpitäminen, järjestelmien hallinta, pääkäyttöpalveluna asiakkaan resurssien vapauttaminen, turvallisuuskulttuurin kohentaminen. Nämä huomioon ottaen olen tehnyt taulukon 2 mukaisen reaalityökalun turvajärjestelmien pääkäytölle. Määritelmä esittää käsitteen olennaiset sisällölliset piirteet sekä käsitteen alaan kuuluvat kohteet.

Turvajärjestelmien pääkäyttö

turvajärjestelmien, kuten kulunvalvonnan, avainhallinnan, kameravalvonnan, rikosilmoittimen hallinnan tai työajanseurannan organisoitu hallinnointi ja jatkuva ylläpito turvallisuutta edistäen sekä yleisiä pääkäytön suuntaviivoja noudattaen

Taulukko 2 Reaalityökalu - turvajärjestelmien pääkäyttö

4.2 Turvajärjestelmät

Finnsecurity Ry:n toimeksiannosta laaditun tutkimuksen *Turvallisuusalan yritysten suhdanne- ja toimialaraportti 2014:n* (Lith 2014) mukaan yritysten tuottamien turvallisuusalan tuotteiden ja palveluiden laskennallinen liikevaihto oli Suomessa vuonna 2013 arviolta noin 1,563 miljardia euroa. Liikevaihto koostuu laajasta tuote- ja palveluvalikoimasta, joista muutamia tärkeimpiä ovat sähköiset turvajärjestelmät sekä rakenteelliset turvatuotteet. Sähköisten turvajärjestelmien ja niiden ylläpito muodostavat arviolta viidenneksen yksityisen turvallisuusalan markkinoista. Tuoteryhmistä suurimman muodostavat kameravalvontajärjestelmät, jonka jälkeen tulevat murtohälytysjärjestelmät sekä kulunvalvonta- ja työajanseurantajärjestelmät yhtä suurella osuudella.

Sähköisiä turvajärjestelmiä kulunvalvonta-, kameravalvonta- ja rikosilmoitinjärjestelmän lisäksi ovat myös paloilmoitin- ja turvavalaistusjärjestelmät (Heinämäki 2009, 67), mutta jälkimmäiset eivät ole ns. pääkäytettäviä ratkaisuja. Seuraavissa alakappaleissa käsitellään pääkäytettäviä turvajärjestelmiä ja -ratkaisuja yleisellä tasolla, mutta myös pääkäyttäjän näkökulmasta, jolloin saadaan yhteys lakeihin perustuviin - tai yleisesti suositeltaviin toimintatavoihin ja suuntaviivoihin.

4.2.1 Kulunvalvonta ja työajanseuranta

Kulunvalvonta on erittäin yleinen turvasuojaamisen ja riskienhallinnan keino nykypäivänä. Turvajärjestelmien yhtenä osa-alueena kulunvalvonta on toimiva ratkaisu toimitilojen turvallisuuden ja omaisuuden suojaamisen kehittämiseksi. Kulunvalvonnan yhteydessä kuullaan usein myös puhuttavan kulunseurannasta ja kulunhallinnasta. Kulunvalvonnan perimmäinen syy on turvallisuuden lisääminen. Tämä tapahtuu tiedostamalla, että oikeilla henkilöillä on kulkuoikeudet eli pääsy oikeisiin tiloihin ja oikeisiin aikoihin. Kulunvalvonta on siis kulkemisen ohjaamista ja rajoittamista sekä luvattoman kulkemisen estämistä. Kulunvalvonta ei poista uhkaa tai väärinkäytöksiä kokonaan, mutta oikein hoidettu kulunhallinta minimoi riskit. (Ukkonen 2014.)

Kulunvalvonnan yhtenä tarkoituksena on korvata mekaanisia avaimia etäluettavilla kulutunnisteilla, jotta mekaaniset lukostot saadaan mahdollisimman yksinkertaisiksi ja näin ollen harvoin uusittavaksi, joka on myös kustannustehokasta (Sähköala 2014a).

Kulkemisen valvontaa voidaan myös toteuttaa lukituksen tai vartioinnin avulla (Turvallisuusalan sanasto 1989, 62). Tekniseen kulunvalvontaan liittyy oleellisesti kulunvalvontajärjestelmä, kulunvalvontalukijat eli ovilukijat ja kulutunnisteet. Näitä kaikkia löytyy eri merkkejä ja malleja. Kulutunnisteet ovat pääsääntöisesti etäluettavia avaimenperiä tai kulkukortteja. Lisäksi kulunvalvontajärjestelmiin on integroitavissa rikosilmoitinjärjestelmiä ja järjestelmäs- tä riippuen voidaan myös hoitaa työajanseurantaa. Kulunvalvonta ja kulutunnisteet eivät korvaa mekaanisia avaimia, vaan ne toimivat yhdistettynä kokonaisratkaisuna parantaen lukituksen käyttömukavuutta ja suojaustasoa. (Heljaste ym. 2008, 47.)

Joidenkin palveluntoimittajien kulunvalvontajärjestelmissä on mahdollisuus ottaa käyttöön kulunvalvontaan integroitu työajanseurantajärjestelmä, joka ensisijaisesti toimii työntekijöiden työajanhallintana eli työajanlaskennan apuna. Työajanseuranta ei ole riskienhallinnan keino, mutta ominaisuus voidaan liittää pääkäyttäjän hallinnoimaksi, sillä henkilötiedot ovat järjestelmässä yhteisiä kulunvalvonnan kanssa. Kulutunnisteita ja niiden tietoja voidaan hyödyntää myös maksupalveluissa, eli esimerkiksi mahdollisella maksu- tai ruokalapäätteellä

lounasta maksettaessa. Pääkäyttäjän on hyvä tietää, mihin kaikkien kulunvalvontajärjestelmät ovat kykeneviä, järjestelmistä riippuen. (Ukkonen 2014.)

4.2.2 Avainhallinta

Pääkäytettävistä turvajärjestelmistä tai -ratkaisuista avainhallinta on vanhin ja avaimia on hallittu jollain tasolla aina yksilöllisten avainten avaamien haittalukkojen olemassaolosta asti eli vuodesta 1778 (Walco 2008). Tällöin on siis haluttu parantaa turvallisuutta varmistamalla, että vain tietyillä henkilöillä on avaimet lukittuun tilaan, mikä on tänäkin päivänä avainhallinnan merkittävin syy. (Iloranta & Viljakainen 2014). Avainhallinnan pääkäyttäjä huolehtii lukitusturvallisuudesta, joka sisältää avainturvallisuuden, lukitustuotteet, sarjoitukset, ylläpidon ja huollon tai niiden organisoinnin. Käytännössä lukitusturvallisuudella tarkoitetaan sitä, että kiinteistö on turvassa varkailta. (Lukitusturvallisuus 2014.)

Pääsääntöisesti lukitus Suomessa on vanhentunutta, mikä tarkoittaa sitä, että avainjärjestelmien patenttisuoja on päättynyt. Murtoturvallisuuden kannalta taso Suomessa on kuitenkin hyvä, sillä lukitustekniikka on kehittynyt. Viimeisin patenttisuoja Abloy Oy:n avaimelle eli Exec-avainjärjestelmälle on päättynyt 25.3.2013. Lukitusturvallisuuden näkökulmasta pääkäyttäjä tulisi suositella vanhentuneiden avainjärjestelmien uusimista, sillä niiden käyttö alustaa kiinteistöjen avainten kopioinnin ilman valvontaa ja kirjanpitoa, jolloin avainhallinta menettää merkityksensä. (Holmberg 2014.)

Avainhallintaa voidaan määritellä eri tavoin ja eri näkökulmista (Räsänen 2014), joten edes Suomessa lukitusalan korkean markkinaosuuden hallitsijalla Abloy Oy:llä (Kilpailu- ja kuluttajavirasto 2009) ei ole virallista määritelmää sille. Suomen lukitusjärjestelmistä Abloyn osuus mekaanisissa - sekä elektromekaanisissa lukitusjärjestelmissä on arviolta yli 90 % (Holmberg 2014). Abloy Oy:n ohjelmistoasiantuntija Riitta Räsänen (2014) kuitenkin määrittelee, että avainhallinta tarkoittaa jonkin kokonaisuuden avaimien tietojen ylläpitämistä. Tämä käsittää kyseiseen kohteeseen kuuluvat avaimet ja niiden määrät, sekä kenellä ne ovat ja mistä ovista niillä pääsee kulkemaan. Mekaanisissa avainjärjestelmissä kulkuoikeudet eli avaukset ovat määritetty ennakkoon, ja ne määräytyvät avainten perusteella. Räsänen (2014) mainitsee vielä, että kirjanpito avaimista voi olla manuaalista tai apuna voidaan käyttää tietojärjestelmiä. Sähköisessä avainhallinnassa on huomioitava myös kulkuoikeuksien hallinta (kulunvalvonnallinen puoli), sillä kulkuoikeuksia voidaan muuttaa ohjelmallisesti.

Avainhallintaprosessissa lukostoon kuuluvien avainten ylläpito käsittää lukitussuunnittelun ja lukitustöiden jälkeisen lukoston käyttöönoton, eli avaimien varastoinnin, jakelun, kuittauskäytännöt, lukostokansion sisällön hoitamisen ja päivittämisen eli mahdollisten uusien tai poistuvien lukkojen tai avaimien merkinnät sekä sijoituspohjakuvien ja lukostokaavioiden päi-

vittämisen. Avainhallinnan perimmäinen syy on sama kuin kulunvalvonnassa. Erona kulunvalvontaan on, ettei mekaanisella avaimella ovesta kuljettuna jää käyttäjästä jälkeä, ellei ovi ole hälytysvalvonnassa. Hälytyskään ei tietysti paljasta kulkijaa, mutta voidaan tietää, että joku on kulkenut ovesta avaimella, mikäli murtojälkiä ei ole. (Iloranta & Viljakainen 2014)

Lukitussuunnittelussa tulee noudattaa samankaltaisia suuntaviivoja kuin kulunvalvontajärjestelmän kulkuoikeusryhmien suunnittelussa. Mikäli lukoston käyttöoikeudet eivät ole ajan tasalla, tulee lukitussuunnitelmassa määrittellä eri käyttäjäryhmien kulkuoikeustarpeiden mukaiset sarjoitukset niin, että kukin avaimen haltija pääsee vain niihin tiloihin, joihin hänellä on tarve päästä. Suuria yhtenäisiä yleisavainsarjoja tulee välttää. (Avainturvallisuusohje 2010, 4.)

Tänä päivänä Suomessa on yleisesti käytössä kolme avainturvallisuustasoa. Ensimmäinen, eli perustaso tarkoittaa, että lisäavaimen voi teettää kuka tahansa malliavaimella tai avaimen peitenumeraalla. Toinen, eli lukkoseppätaso tarkoittaa, että lisäavaimen voi teettää lukkoliikkeessä avaimelle kuuluvalla avainkortilla. Kolmas taso on tehdastaso, jossa lisäavaimen voi teettää vain nimetty vastuuhenkilö avainkortilla lukkovalmistajalta. (Avainturvallisuusohje 2010, 3.)

Mikäli avaimia säilytetään pääkäyttöpalvelua tuottavan yrityksen tiloissa, tulee avaimet säilöä Finanssialan Keskusliiton Avainturvallisuusohjeen (2010) mukaisesti hyväksytyissä olosuhteissa, valvotuissa ja rikossuojatuissa tiloissa ja oikean kokoisissa kassa- tai avainkaapeissa. Huomioitava FK:n ohjeen mukaisesti, että lukoston avaimien lukumäärä ei määrää avainkaapin kokoa, vaan avainten avausten määrä (=montako lukkoa tietty avain avaa).

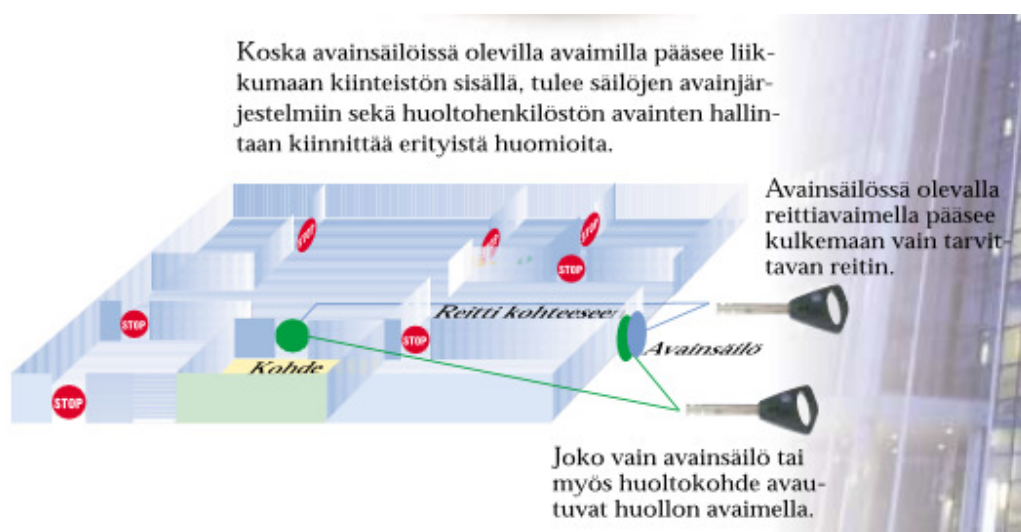
Säilytettävien avaimien yhteenlaskettu sopivuus eri oviin	Säilytysyksikkö	Rakenteellinen murtosuojaus	Murtohälytysjärjestelmä
1 – 50 ovea	Lukittu metallinen avainten säilytykseen tarkoitettu kaappi	1	1
51 – 500 ovea	Standardin SFS-EN 14450, SFS 5870, SS 3492 tai SFS 7020 mukaan testattu kaappi	2	2
yli 500 ovea	Standardin SFS-EN 1143-1 mukaan vähintään luokkaan 1 testattu kassakaappi	2	2

Taulukko 3 Avainsäilytysyksikkö (Avainturvallisuusohje 2010, 4)

Lisäksi on huomioitava taulukossa 3 mainitut Finanssialan Keskusliiton Rakenteellinen murtosuojaus- (2014) sekä Murtohälytysjärjestelmäohjeistusten (2008) vaatimukset. Nämä vaatimukset huomioon ottaen avainhallinnan ulkoistaminen on toimiva ratkaisu yrityksen tai kiin-

teistönjohdon turvallisuustoiminnan ja -vastuiden siirtämiseksi muualle (Iloranta & Viljakainen 2014).

Kiinteistön avainsäilössä ei saa säilyttää lukoston yleisavainta (Avainturvallisuusohje 2010). Pääkäyttäjän tulee lukitus suunnittelussa huomioida avainsäilöihin kuuluvien avainten tarpeelliset kulkureitit ja avaukset tulee olla vain näihin tarpeellisiin oviin. Sisätiloissa, esimerkiksi paloilmottimen luona oleva toinen putkilukko voi kuitenkin pitää sisällään kulunvalvonta- tai yleisavaimen ja kulkutunnisteen. Kuva 2 on Abloy Oy:n esimerkki avainsäilön sisältämistä reittiavaimista.



Kuva 2 Avainsäilön reittiavain (Avainsäilöt kiinteistöissä 2000, 2)

Myös avainhallinnan kirjanpidosta ja sen oheistiedoista muodostuu henkilörekisteri, riippumatta millä keinoilla sitä suoritetaan. Avainten haltijoilla ja lukkojen käyttäjillä on kuitenkin palvelussuhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan, jolloin ilmoitusvelvollisuutta avainhallinnan rekisteristä ei ole. (Henkilörekisteriasiat avainten- ja lukostonhallinnassa 2014). Rekisteriseloste on kuitenkin hyvä olla olemassa siksi, että yhteiset linjaukset koskien henkilötietojen keräämistä löytyvät tarvittaessa nopeasti.

4.2.3 Kameravalvonta

Kameravalvonta kuuluu kulunvalvonnan ja murtovalvonnan lisäksi teknisiin turvasuojausmenetelmiin, joiden tavoitteena on estää tai rajoittaa henkilö- ja omaisuusvahinkoja. Rikostorjunnallisen tehtävän lisäksi kameravalvontaa käytetään prosessien valvonnassa, kulunohjauksen tukena ja tuottamassa web-kamerakuvaa kaupunkien keskeisiltä paikoilta. (Ellonen ym. 2010, 6.) Kameravalvonnan suuntaviivat perustuvat hyvin pitkälti lakeihin sekä Kameravalvontaoppaan (2010) ohjeistuksiin, mutta pääkäyttöllisiä suuntaviivoja näistä ei ole aiemmin koottu yhteen.

Kameravalvontajärjestelmiä käytetään pääosin täydentämään muita turvallisuusjärjestelmiä ja on tärkeää määritellä järjestelmän käyttötarkoitus, jotta tiedetään minkälaista valvontaa varten järjestelmä hankitaan, kuten yleisvalvontaan tai henkilöiden tunnistamiseen (Sähköala 2014b). Huomioitavia asioita ovat myös valvonnasta tiedottaminen merkein, tarroin tai kyltein, sekä ennaltaehkäisevä vaikutus, jota näkyvä valvonta tuo mukanaan.

Kameravalvontaan ja sen tavoitteisiin liittyy myös oleellisesti kameravalvonnan rekisteriseloste sekä Finanssialan Keskusliiton K-menetelmä, josta kerrotaan Kameravalvonnan suunniteluohjeessa Kameravalvonnan K-menetelmä (Ahokas ym. 2006). Kameravalvonnan tuottama tallennettu ääni tai kuva rinnastetaan tietosuojavaltuutetun mukaan henkilötietolaissa tarkoitettuun henkilötietoon ja jos henkilö on kyseisistä tallenteista tunnistettavissa, syntyy niistä henkilötietolain mukainen henkilörekisteri. Henkilörekisteristä on laadittava rekisteriseloste, josta on ilmentävä rekisterinpitäjän nimi ja yhteystiedot, henkilötietojen käsittelyn tarkoitus ja se, mihin tietoja säännönmukaisesti luovutetaan. Rekisteriseloste on pidettävä kaikkien tarkkailtavien saatavilla. Tietosuojavaltuutetun kannanotto kameravalvontaan on kuitenkin hieman kyseenalainen, sillä tallenteet eivät aina täytä henkilörekisterin tunnusmerkistöä ja velvollisuuksista voidaan esimerkiksi valtion yleisen järjestyksen ja turvallisuuden vuoksi poiketa. (Ellonen ym. 2010, 50.)

K-menetelmä on Finanssialan Keskusliiton laatima kuvainformaation yksityiskohtaisuuden suunnittelu- ja tarkastusmenetelmä, joka on tarkoituksenmukainen kiinteillä kameroilla valvottavissa sisätiloissa, joissa olosuhteet eivät muutu esimerkiksi valaistuksen suhteen. (Ellonen ym. 2010, 30). Pääkäyttäjän on hyvä tietää ja ymmärtää valmiiden hallinnoitavien kameroiden tarkoitus ja K-menetelmän eri näkymien vaatimustasot rinnastettuna tarkoitukseen. Yleisimmät turvallisuuden valvontaan käytetyt näkymät ovat hahmotettu kuvassa 3. Vaatimustasot ovat:

- yksilöinti (K120), näköiskuva, kohteen oltava vähintään 120 % ruudun korkeudesta
- tunteminen (K50), kohteen oltava vähintään 50 % ruudun korkeudesta
- havaitseminen (K10), kohteen oltava vähintään 10 % ruudun korkeudesta
- yleiskuva (K5), kohteen oltava vähintään 5 % ruudun korkeudesta.



● Yksilöinti (K120), tunteminen (K50) ja havaitseminen (K10).

Kuva 3 K-menetelmän näkymien vaatimustasot (Kameravalvontaopas 2010, 31)

Pääkäyttäjän rooli kameravalvonnan prosessissa on käyttää, ylläpitää sekä kartoittaa kameravalvonnan tarpeita käytön mukaisesti. FK:n Kameravalvontaoppaan (2010, 8) Kameravalvonnan prosessiin on myös määritelty projektin suunnittelu, YT-menettely, tarjoukset, hankintapäätös sekä toteutus, mutta nämä eivät suoranaisesti kuulu pääkäyttäjän rooliin. Pääkäyttäjää ei myöskään suorita aktiivista valvontaa, vaan kyseessä on passiivinen - tai etävalvonta, riippuen palvelusopimuksesta. Passiivisessa valvonnassa toimivuutta ei ylläpidetä jatkuvasti, eikä toimintaa seurata aktiivisesti, vaan tarvittaessa tallentimelta haetaan informaatiota jonkin asian selvittämiseksi. Tässä on riskinä se, että pitkällä aikavälillä tallentimen toiminta on voinut heikentyä tai lakata toimimasta. Etävalvonnassa pääkäyttäjää saa tallentimeen suojatun etäyhteyden, jolloin tallenteiden saaminen on nopeampaa ja helpompaa, sekä pääkäyttäjää voi aktiivisesti seurata laitteiden toimivuutta etänä. (Ukkonen 2014.) Kameravalvontaoppaan (2010) määrittelemiä tarveselvityksen - sekä kameravalvonnan laillisuuden perusteita pääkäyttäjän näkökulmasta avataan enemmän liitteenä olevan oppaan osiossa 4: Kameravalvonta.

Kameravalvonnan pääkäyttäjän tulee järjestelmää hallinnoidessaan ottaa huomioon kameravalvonnan käyttökohteiden laillisuus, vaikka järjestelmä ei olisikaan pääkäyttöorganisaation toteuttama. Lisäksi pääkäyttäjän rooliin järjestelmän ylläpitäjänä kuuluu erilaisten olosuhteiden ja niiden muutosten huomioiminen, kuten valaistus, näkymäesteet ja katveet ja järjestelmän vakaus. Myös järjestelmän dokumentoinnin ajantasaisuuden huolehtiminen, tallenteiden käsittely ja lainsäädäntö, kuten salakatselu ja yksityiselämää loukkaavan tiedon levittäminen ovat tärkeitä tunnistettavia aiheita pääkäyttäjälle, jotta järjestelmä tuottaa enemmän tarkoituksenmukaista hyötyä kuin haittaa. (Ellonen ym. 2010.)

4.2.4 Rikosilmoitinjärjestelmä

Rikosilmoitinjärjestelmä on laitteisto, jolla on tarkoitus parantaa tilojen, rakennusten tai alueiden turvallisuutta havainnoimalla mahdollisia murto-, ilkivalta-, sabotaasi-, palovahinko- tai vesivahinkotapauksia. Järjestelmää kutsutaan myös hälytysjärjestelmäksi.

Valvontatasoja ovat kehävalvonta eli alueen valvonta, kuorivalvonta eli rakennuksen valvonta, tilavalvonta eli tilaryhmän tai tilan valvonta, kohdevalvonta eli erillisen kohteen tai esineen valvonta sekä ryöstöhälytykset (Sähköala 2014c). Näistä eri tapauksista on tarkoitus välittyä hälytystieto valinnaisesti joko vartioinnin hälytyskeskukseen, hätäkeskukseen, järjestelmän käyttäjälle, kiinteistön/tilan omistajalle tai muulle yhteyshenkilölle, tai kaikille edellä mainituille osapuolille.

Rikosilmoitinjärjestelmä koostuu useimmiten erilaisista ilmaisimista, kuten liiketunnistimista, magneettikoskettimista, lasirikkoilmaisimista, ryöstöpainikkeista ja seismisistä -, savu- sekä kosteusilmaisimista. (Hulkkonen 2014.) Näiden väylään kytkettyjen ilmaisimien silmukat voidaan usein liittää kulunvalvontajärjestelmään.

Rikosilmoitinjärjestelmien keskuksat tulee aina olla sijoitettuna hyvin suojattuun, lukittuun ja valvottuun tilaan. Tätä määrittelevät myös viranomaismääritykset perustasosta lähtien. Vertailun vuoksi, kameravalvonnalle ei ole perustason viranomaisvaatimuksia. Tasot ja vaatimukset nähtävissä KATAKRI:ssa F 301.0. Elinkeinoelämän suosituksena rikosilmoitinkeskuksen on oltava vähintään Finanssialan Keskusliiton luokiteleva luokan 2. mukainen. Järjestelmää tarvitaan, mikäli viranomaisvaatimuksen Perustaso (IV) luokiteltua aineistoa säilytetään tavallisessa lukitussa kaapissa/laatikossa. (KATAKRI 2011, 71.)

Pääkäyttäjän tulee ymmärtää rikosilmoitinjärjestelmää pääkäyttäessään järjestelmän perimmäinen tarkoitus, eli se, mitä suojellaan, miksi ja millä tasolla. Finanssialan Keskusliiton Kohteen murtoriskien arviointi ja suojaustason valinta -ohje (2008) mukaan suojaustasoluokkia on neljä: Alhainen suojaustaso (1), keskimääräinen suojaustaso (2), korkea suojaustaso (3) ja erittäin korkea suojaustaso (4). Suojaustaso riippuu rikosvahingon todennäköisyydestä ja vahingon seurauksista.

Pääkäytettäviin tehtäviin rikosilmoittimen hallinnoinnissa kuuluu hälytysalueiden/-vyöhykkeiden luominen, henkilökohtaisten pin-koodien tekeminen, muuttaminen ja toimittaminen sekä poikkeusjärjestelyiden tekeminen hälytysajankohtiin. Lakien ja suositusten määrittelemiä suuntaviivoja ei hallinnollisella puolella ole, sillä vaatimukset ovat lähinnä teknisiä ominaisuuksia koskevia. Pääkäyttäjän vastuulla on kuitenkin huolehtia siitä, että kaikille henkilöille/asiakkaille annetaan henkilökohtaiset hälytysjärjestelmän pin-koodit, ellei sisäisesti

toisin ole sovittu, sekä että hälytykset kytkeytyvät poikkeuspäivinä (arkipyhät ym.) oikein tai pyydetyn mukaisesti. Asiakkaalla itsellään on vastuu tehdä pyynnöt, sillä pääkäyttäjä ei voi itsenäisesti ilman työtilausta tehdä muutoksia järjestelmään. (Ukkonen 2014.)

4.3 Pääkäytön tavoitteet

Pääkäytön tavoitteena on taata turvajärjestelmien osalta korkealuokkainen turvallisuus. Pääkäyttö on palvelua, jonka avulla palveluntilaajan on entistä helpompi keskittyä omaan ydinliiketoimintaansa, sillä palvelun tavoitteena on varmistaa turvajärjestelmien häiriötön ja asianmukainen toiminta. Lisäksi palvelun avulla turvallisuustasoa ylläpidetään ja sitä voidaan kehittää paremmaksi. (Avald ym. 2014.) Viljakaisen (2012) mukaan pääkäytön tarkoituksena on tuottaa asiakkaalle turvallista ja ammattimaista palvelua järjestelmän koko elinkaaren ajaksi.

Korkean turvallisuustason ylläpitäminen helpottaa myös työntekijöiden kykyä omaksua turvallisuuskulttuuria. Matalalla profiililla ei ole samanlaista suojaavaa vaikutusta (Peltonen 2014). Tämä tarkoittaa sitä, että mitä enemmän työntekijät tiedostavat turvallisuustekijöitä ja riskejä, sitä helpompaa korkea turvallisuusprofiili on omaksua osaksi jokapäiväistä työtä. Kun pääkäyttämällä ylläpidetään kyseistä tasoa, on selvää, että palvelu on riskienhallintaa. Turvallisuustoimintaa arvottaa kielteinen tulevaisuuskuva ja riskienhallinta ovat kielteisen tulevaisuuskuvan toteutumisen estämistä (Peltonen 2014).

Kaikkeen toimintaan liittyy erittäin tärkeänä elementtinä tietoturvaluottisuus. Vaikka tästä työstä tietoturvan suuntaviivojen osuus on rajattu pois, on pääkäyttäjän ehdottoman tärkeää muistaa tietoturvan merkitys omassa toiminnassaan, koska Peltosen (2014) mukaan riskienhallinta on hyvin pitkälti toimintaan liittyvää ajattelua, eikä niinkään näkyviin asioihin paneutumista.

4.4 Turvallisuuden kehittäminen

Jotta turvallisuutta voidaan kehittää, on nykytilanne kartoitettava. Turvajärjestelmien pääkäyttöpalvelun aloitusvaiheessa on tärkeää tehdä kartoitus turvallisuuden sen hetkisestä tilasta. Tämä pätee myös päivitysprojekteihin sekä ns. ”siivousprojekteihin”, jotka tarkoittavat jo olemassa olevien järjestelmien alustamista virheettömään kuntoon. Turvallisuuskokonaisuutta ja -kulttuuria kehitetään palvelun käyttöönottoajanjaksolla siihen pisteeseen, millä tasolla palveluntuottaja on lupautunut ja sitoutunut tekemään työtä palvelusopimuksen puitteissa. (Avald ym 2014.) Voidaan puhua palveluntoimittajan formaatista. Tämä tarkoittaa sitä toimintamallia ja niitä keinoja, joilla yksittäisessä pääkäyttöpalvelua tuottavassa yrityksessä toimitaan. Luonnollisesti tason tulee olla korkealla laadukasta palvelua tuottaessa. Tason

vieminen formaatin määrittelemään pisteeseen helpottaa pääkäyttäjien työtä, sillä silloin kaikki tietävät asiakaslupauksen mukaiset toimintatavat. Esimerkiksi asiakaskohdetta ja palvelusopimusta tarkemmin tuntematta pääkäyttäjä pystyy kertomaan, miten esimerkiksi kohteen avaintenluovutusten ja -palautusten kuittausmenettelyt toimivat. (Hulkkonen 2014.)

Turvajärjestelmän aloitustöissä, eli uutta järjestelmää käyttöön otettaessa tai vanhan järjestelmän tietokannan siivoamisessa on huomioita järjestelmää sekä tietokantaa koskevia tehtäviä. Näiden lisäksi on muita yleisiä huomioita koskien järjestelmien pääkäyttöä. Tehtävät sekä niiden syyt ja seuraukset on kirjattu Turvajärjestelmien pääkäytön suuntaviivat -oppaaseen. Opinnäytetyön teoreettisessa osassa, kappaleissa 4.3.1 - 4.3.4 käsitellään kyseisiä aloitustöitä ja niiden merkitystä pääkäyttöprosessille. Kappaleet ovat jaettuina kulunvalvonnan, avainhallinnan, kameravalvonnan ja rikosilmoittimen hallinnan käyttöönottoprosessien tehtäviin. Kappaleissa on selvitetty, miksi aloitustyöt ovat tärkeä osa pääkäyttöä ja miten aloitustöissä huomioitavat asiat vaikuttavat jatkossa järjestelmän käytettävyyteen.

Aloitustöihin suositellaan varattavaksi reilusti aikaa ja tärkeimpänä kaikkia yhdistävänä tekijänä on saada kiinteistön yhteyshenkilöiden, vuokralaisten sekä ulkoisten toimijoiden, kuten huoltopalveluiden yhteystiedot kerättyä yhteen. On hyvä valtuuttaa ainakin kaksi yhteyshenkilöä, joista toinen toimii ensisijaisena yhteyshenkilönä ja toinen hänen sijaisenaan. Yhteystiedoista on hyvä olla asiakkaan täyttämä, palveluntuottajan toimittava formaatin mukainen lomake, jossa vastuut ja velvollisuudet ilmenevät. (Avald ym. 2014.)

4.4.1 Kulunvalvonnan aloitustyöt

Kulunvalvontajärjestelmän toimivuuteen ja luotettavuuteen vaikuttaa ensisijaisesti järjestelmän ikä, yleinen kunto sekä palvelimelle ja laitteistolle tehdyt päivitykset. Mikäli pääkäyttö siirtyy sellaisenaan jo olemassa olevassa muodossa vanhoine tietoineen, on tärkeää tarkastaa tai tarkastuttaa järjestelmän kunto teknisellä ja fyysisellä tasolla, jotta iän ja ajan tuomat häiriötekijät voidaan minimoida. Lisäksi on tärkeä tarkastaa järjestelmäversion mahdolliset uudet päivitykset, jotta pystytään myös varautumaan jatkuvuussuunnittelun mukaisesti kulunvalvonnan keskeytyksettömyyteen. Tähän vaikuttaa esimerkiksi tuotannosta poistuvat osat ja vanhojen versioiden korjauspäivitykset järjestelmätoimittajan osalta.

Vanhan järjestelmän tietokantaan liittyen on järjestelmästä syytä ottaa lähtötilanteen tiedot talteen. Täten tilaajalle voidaan näyttää toteen tehty työ. Myös siivoamattoman kannan aikaisemmin aiheuttamat turvallisuusriskit voidaan kunnollisella dokumenteilla havainnollistaa jälkikäteen. Lähtötilanteen tietoja ovat kulkutunnisteiden määrä, yritystiedot, kulkualueet, aikaryhmät.

Kulcutunnisteiden määrä vaikuttaa olennaisesti käytettävyyteen, tietojen paikkansapitävyyteen sekä turvallisuuteen. Mitä enemmän ylimääräisiä, varsinkin aktiivisia, kulcutunnisteita löytyy tietokannasta, sitä enemmän riskejä ne aiheuttavat. Tiedoista tulisi löytyä vain käytössä oikeasti olevat tai varalle kirjatut tunnisteet. Vanhoja yritystietoja on turha säilyttää. Järjestelmästä tulisi yritystiedoista suoraan nähdä sen hetkiset vuokralaiset, yritykset, osastot, jaokset ja muut yksilöintiä varten luodut tiedot. Kulkualueet tulee tarkastaa ja tarvittaessa määrittää uudelleen, mikäli alueissa havaitaan liian laajoja oikeuksia tai päällekkäisyyksiä. Kulkualueita olisi oltava vain sen verran kuin alueiden mukaan rajattuja pääsyoikeuksia tarvitaan. Varsinkin isoissa liikekiinteistöissä yritys saattaa vuokrata useita eri tiloja eri kerroksista. Tällöin vanhoja kulkualueita ei tulisi olla riskitekijänä, jotta väärä ihminen pääsisi väriin tiloihin. Mikäli järjestelmään on määritetty aikaryhmiä tai kellonaikoja esimerkiksi rajaamaan kulkuoikeuksia vain päiväsaikaan arkisin tai ovien aukiohjauksia varten, on ylimääräiset syyt poistaa. Näin virheellisten ajastusten määrittäminen kulkuoikeuksiin tai oviohjauksiin on epätodennäköisempää, kun ylimääräisiä vaihtoehtoja ei ole valittavissa. (Avald ym. 2014.)

Lisäksi nimeämiskäytännöt on huomioitava alusta lähtien, mitä käytäntöjä järjestelmässä on käytetty esimerkiksi kulkualueen tai henkilön nimeämisessä. Nämä tulisi yhtenäistää suunta- viivojen suositusten mukaisesti esim. Sukunimi Etunimi -muotoon tai kulkualueessa niin, että jokainen alkaa alue nimetään kerroksen mukaan. Mikäli kulunvalvonnan mukana kiinteistön tunnistehallinta siirtyy samalla pääkäyttöyritykselle, on kulcutunnisteet inventoitava ja niitä on oltava tarpeeksi varalla isompiakin tilauksia varten. Henkilöiden nimeämisessä vuokralaisyrittäjien ajan tasaisen nimilistan toimittaminen pääkäyttäjälle on tärkeää, jotta järjestelmässä näkyy kaikkien kulcutunnisteiden haltijoiden tiedot oikein. Vaihtoehtona yritys pitää henkilötiedot itsellään ja pitää huolen päivittämisestä sekä omasta kirjanpidosta. Tällöin nimeämiskäytäntönä järjestelmään toimii esim. Yritys X / 1- (juokseva numero). Tietokannan siivoamisessa henkilötietojen osalta tämä on helpoin ja vaivattomin tapa selvittää tarpeelliset kulcutunnisteet tietomassasta. Ulkoinen pääkäyttäjä ei todennäköisesti muutoin pysty edes selvittämään todellisia ja oikealla asialla kiinteistössä liikkuvia henkilöitä. (Ukkonen 2014.)

Mikäli järjestelmän tietokannassa on muita pääkäyttäjiä tai yrityskohtaisia käyttäjiä, tulee näiden tunnukset ja käyttöoikeudet tarkistaa. Ihannetilana on, että samoja tietoja hallinnoi sujuvan tiedonvälityksen vuoksi vain yksi pääkäyttäjä tai organisaatio. Vaikka muita yrityskohtaisia käyttäjiä olisi samassa järjestelmässä, tulee koko kiinteistön pääkäyttäjän huolehtia palvelimen kesä- ja talviaikojen sekä arkipyhäpäivien tarkistukset, jotta mm. ovien lukitukset toimisivat oikein. (Avald ym. 2014.)

Järjestelmän toiminta-alueella oleviin kiinteistön vuokralaisiin on otettava yhteys ja ilmoitettava palvelun alkamisesta tai palveluntoimittajan muuttumisesta. Vuokralaisten tulisi valtuuttaa yrityksen kulunvalvonnan yhteyshenkilöt, joille annetaan oikeus tehdä tilauksia sekä muu-

tospyyntöjä liittyen yrityksen kulutunnisteisiin ja tapahtumien raportointiin. Aloitustöiden yhteydessä tämä on ehdottoman tärkeää, että jokaisella vuokralaisella on virallinen kulunvalvonnan yhteyshenkilö. Mikäli kuka vain voi pyytää muutoksia tai lisäoikeuksia, ei turvallisuustasoa voida taata. Vuokralaisten informoiminen palvelun toimintatavoista on tärkeää, jotta palveluprosessi saadaan toimivaksi heti palvelun käyttöönotosta lähtien.

4.4.2 Avainhallinnan aloitustyöt

Ensimmäinen vaihe avainhallinnan pääkäyttöä aloitettaessa on lukostokansion tai -kansioiden vastaanottaminen sekä tarpeellisten dokumenttien tarkastaminen lukostokansiosista. Riippuen kohteesta, voi lukosto olla hyvinkin vanha. Aiempi hallinnointi on voinut olla esimerkiksi kiinteistö- tai ylläpitopäälliköllä, huoltoyhtiöllä, lukkoliikkeellä tai toisella pääkäyttöyrityksellä, joten hallinnointitapoja on paljon erilaisia. Uuden kiinteistön lukostokansio voidaan myös vastaanottaa suoraan rakennuttajalta tai lukkotehtaalta. Jotta avainhallinnan pystyy viemään suuntaviivojen mukaiseen formaattiin, tulisi lukostokansiossa olla seuraavat dokumentit: Lukostonumero, avainkortti ja tunnusluvut tilauksia varten, lukituskaavio, avainlista, avainkuittaukset, sijoitusohjeet sekä lukoston lisätiedot ja yleiset ohjeet. Mikäli kaikkia ei löydy, on hyvä selvittää onko kyseisiä dokumentteja koskaan ollut ja onko niitä vielä jostain saatavilla.

Lukoston sisällön osalta lähtötilanne tulee dokumentoida samaan tapaan kuin kulunvalvonnan osalta. Huomioon tulee ottaa lukoston kunto, ikä sekä turvallisuus. Turvallisuuteen vaikuttaa erityisesti kadoksissa olevat avaimet. Kadoksissa olevista avaimista ja näiden vaikutus lukitus- ja turvallisuuden kokonaisuuteen tulee tehdä selvitysdokumentti palveluntilajalle, jotta voidaan todentaa lähtötilanteen turvallisuustaso. Lisäksi kriittiset avaimet useilla avauksilla, kuten yleisavain, huoltoavain tai kulunvalvottujen ovien yleisavain eli kv-avain, tulee varmistaa, että kuittauksen tehneellä henkilöllä todella on kyseinen avain hallussaan.

Mikäli paperista listausta tai sähköistä versiota avaintenhaltijoista ei ole, on syytä koota tiedot avaimista ja avaintenhaltijoista yhdelle listalle ja siirtää ne suuntaviivojen mukaiseen, pääkäyttöyrityksen mahdollisesti räätälöimään yhtenäiseen formaattiin, jotta tiedetään kellä mikäkin avain on hallussaan. Kun aloitustyöt on saatu päätökseen, tulee avainhallinnan turvallisuustaso arvioida lopullisessa pääkäyttöformaatissa ollessaan. Palveluntilajaa tulee tiedottaa lähtötasosta ja formaatissa olevasta tasosta mahdollisine puutteineen ja jatkotoimenpidesuosituksineen, esim. sarjoitustyöt kadonneiden avainten takia. Täten palveluntilajalle siirretään vastuu lukoston sen hetkisestä turvallisuustasosta. (Iloranta & Viljakainen 2014.)

4.4.3 Kameravalvonnan aloitustyöt

Kameravalvontajärjestelmän toimivuuteen ja luotettavuuteen vaikuttaa ensisijaisesti järjestelmän ikä, yleinen kunto sekä tallentimelle ja laitteistolle tehdyt päivitykset. Mikäli pääkäyttö siirtyy sellaisenaan jo olemassa olevassa muodossa vanhoine tietoineen, on tärkeää tarkastaa tai tarkastuttaa järjestelmän kunto teknisellä ja fyysisellä tasolla, jotta iän ja ajan tuomat häiriötekijät voidaan minimoida. Kameravalvonta on pääkäytettävistä järjestelmistä kokenut teknistä kehitystä eniten, joten on arvioitava vastaako pääkäyttöön otettava järjestelmä vielä nykypäivän vaatimuksia ja onko mahdollisia lisä- tai varaosia vielä saatavilla huoltoa ajatellen. Lisäksi on tärkeää tarkastaa järjestelmäversion mahdolliset uudet päivitykset, jotta pystytään myös varautumaan jatkuvuussuunnittelun mukaisesti tallentavan kameravalvonnan keskeytyksettömyyteen. Tähän vaikuttaa esimerkiksi tuotannosta poistuvat osat ja vanhojen versioiden korjauspäivitykset järjestelmätoimittajan osalta. Mikäli ohjelmiston voi päivittää, kannattaa toiminnan varmuudeksi hankkia uusin versio. (Ukkonen 2014.)

Yksittäisten kameroiden toiminta on palvelua aloittaessa tarkastettava. Tarkastuksessa tulee ottaa huomioon, kuvaako jokainen kamera ja kuinka monesta toimivasta sekä rikkiäisestä kamerasta järjestelmä koostuu. Tallentimen ja tallenteiden toiminnasta on tarkastettava, että löytyykö jokaisen kameras kuvasta tallenteet halutulta ajalta tallenteet. Tallentimen suorituskyky ja suoritinkäyttö tulee toiminnan ja jatkuvuuden kannalta tarkistaa. Eheyteen vaikuttaa erityisesti, millä suoritinkäytöllä järjestelmä on käytössä ja voidaanko asetuksia muuttaa. Jatkuva kapasiteetin maksimikäyttö ei ole hyväksi tallentimelle. Myös tallentimen fyysinen sijainti voi kasvattaa toimintaikää, esimerkiksi palvelinkaapissa oletettu käyttöikä on pidempi kuin lattialla pölyssä. Kuvanlaatu tulee tarkastaa ja mahdolliset tai tarvittavat säädöt sekä parannukset tulee tehdä. Suorituskyky huomioiden, kuvanlaadun parantaminen on syytä myös ottaa huomioon, esim. fps eli frames per second -asetusta tai resoluutiota muuttamalla. Kameroiden suuntaukset tulee tarkastaa ja tarvittaessa tulee tilata uudelleensuuntaukset. (Ukkonen 2014.)

Lisäksi sujuvaan pääkäyttöön vaikuttaa etäyhteyksien toiminta. Etäyhteydellä tulisi pystyä katsomaan live-kuvaa sekä tallenteita mutkattomasti, ilman että kuvanlaatu heikkenee tai kuva pätkii. Yhteys on myös salattava asianmukaisesti. Salasana suositellaan vaihdettavaksi, mikäli käytössä on oletussalasana tai muutoin yksinkertainen salasana. On siis minimoitava mahdollisuudet, että kukaan ulkopuolinen pääsisi käsiksi kameroihin tai tallenteisiin. Järjestelmän sekä palvelimen kesä- ja talviaikojen muuttuminen tulee ottaa huomioon, jotta tallenteissa näkyy oikea kellonaika. (Hulkkonen 2014; Ukkonen 2014.)

4.4.4 Rikosilmoittimen hallinnan aloitustyöt

Rikosilmoitinjärjestelmän hallintaa käyttöönotettaessa tulee huomioida lähes samat asiat kuin kameravalvonnan aloitustöiden osalta, sillä niihin liittyvien pääkäyttötoimenpiteiden sisällöt ovat hyvin samankaltaisia. Järjestelmän ikä, kunto ja tehdyt huollot tulee kartoittaa, jotta tiedetään onko järjestelmä vielä nykypäivän vaatimuksia vastaava ja voiko sen tarvittaessa tuoda sille tasolle, sekä onko vara- tai lisäosia saatavilla.

Järjestelmän toiminta tulee varmistaa aiheuttamalla hälytyksen ja tiedustelemalla hälytyskeskukselta, onko hälytys tullut heille läpi. Käyttäjien määrä tulee myös tarkistaa ja kanta puhdistaa ylimääräisistä sekä vanhoista tiedoista. Master-koodi on vaihdettava riskienhallinnallisista syistä. Rikosilmoitinsilmukat on hyvä piirtää pohjakuviin, mikäli vastaavaa dokumentaatiota ei aiemmin ole tehty. Mahdollinen vanha dokumentaatio on tarkastettava ja pidettävä ajan tasalla. Rikosilmoitinjärjestelmän turvallisuustaso lopullisessa pääkäyttöformaatissa ollessaan on myös dokumentoitava. Tiedot lähtötasosta ja formaatissa olevasta tasosta on hyvä toimittaa palveluntilaaajalle. Samalla pääkäyttäjä voi suositella mahdollisia toimenpiteitä, kuten silmukoiden uusiminen, lisääminen tai muu huollon tarve. Järjestelmän kesä- ja talviaikojen sekä arkipyhäpäivien muuttaminen tulee huomioida, jotta hälytykset menevät päälle oikeina aikoina. (Hulkkonen 2014 & Ukkonen 2014.)

4.5 Turvallisuuden ylläpitäminen & pääkäyttöprosessi

Kun palvelusopimukseen kuuluvat kohdat on saatu pääkäyttöformaattiin, tästä ilmoitettu palveluntilaaajalle ja tarvittavat parannus- tai huoltotoimenpiteet on tehty, alkaa palvelun ylläpitovaihe. Ylläpitovaiheen alkuun on syytä sopia palveluntilaaajan kanssa tarkasteluajanjaksosta, jolloin sopimukseen ja sopimushintaan voidaan vielä tehdä muutoksia, mikäli arvioitu työmäärä onkin esimerkiksi ennakoitua suurempi. Tämän vuoksi on tärkeää dokumentoida aloitustöissä ja tarkasteluajanjaksolla tehdyt työ- ja tuntimäärät sekä palvelupyyntöjen määrät.

Pääkäyttötoimenpiteen suorittaminen eli pääkäyttöprosessi on osa järjestelmän ylläpitoa. Prosessi käynnistyy tarpeesta tai asiakkaan yhteydenotosta ja päättyy pääkäyttäjän toimenpiteen jälkeiseen raportointiin (Avald ym. 2014). Karkeasti kuvattuna prosessi etenee kuvion 2 mukaan seuraavasti:



Kuvio 2 Onnistunut pääkäyttöprosessi

Havainnoinnin perusteella, sekä kaikkein haastateltujen asiantuntijoiden mukaan (Avald ym. 2014; Hulkkonen 2014; Iloranta & Viljakainen 2014; Ukkonen 2014), voidaan sanoa, että suurin osa palvelupyynnöistä ei mene tämän yksinkertaisen prosessikaavion mukaisesti, vaan hoitamaton ja huonossa tilassa oleva turvajärjestelmä aiheuttaa usein seuraavanlaisen, kuvion 3 mukaisen prosessin:



Kuvio 3 Aikaavievä pääkäyttöprosessi

Tähän pidempään prosessiin ajaudutaan usein myös vain sen takia, että palvelupyyntö on joko epäselvä, siinä on ristiriitoja järjestelmän tietojen kanssa tai ei välttämättä osata pyytää oikeaa asiaa. Mikäli pääkäyttäjä ymmärtää ja suorittaa työpyynnön väärin, ajaudutaan prosessissa vielä takaisin alkuun, jonka lisäksi on voinut aiheutua mahdollisia uhkia tai turvallisuuspuutteita, jotka tulisi selvittää. (Avald ym. 2014.)

Turvallisuustasoa pystytään helpoiten ylläpitämään, kun järjestelmät, dokumentointi ja muut asiakirjat ovat formaatin mukaisesti kunnossa. Tämä vaatii hyvää vuorovaikutteista kommunikointia palveluntilaajien sekä asiakkaiden, ja ennen kaikkea heidän yhteyshenkilöidensä, kanssa. Hyvin tehdyt aloitustyöt voivat helposti valua hukkaan, mikäli yhteyshenkilö ei ole ymmärtänyt palvelun tarkoitusta ja omaa rooliaan palvelukokonaisuudessa. Tämä voi näkyä esimerkiksi vuokralaisen vaihtumisen tai avaimen katoamisen ilmoittamatta jättämisestä. Myöskin avaimien ja kulutunnusteiden jakaminen eteenpäin vuokralaiselta tai huoltomieheltä toiselle voi sotkea avainhallinnan. Kameravalvonnan ja rikosilmoittimen hallinnan kannalta pääkäyttäjän on syytä itse tehdä esimerkiksi viikoittaisia palvelimien ja tallenteiden toimintatarkistuksia. Omalla toiminnallaan pääkäyttäjä voi ylläpitää ja jopa kehittää entisestään hyvää turvallisuustasoa järjestelmien osalta. Tarkkailun ja asiakkaiden suuntaan oma-aloitteisen yhteydenpidon voisi laskea kuitenkin vain hyväksi palvelutasoksi, sillä lähtökohtaisesti töiden tulisi olla suoraan asiakkaalta pääkäyttäjälle suunnattuja, tarkkaan ilmaistuja työpyyntöjä. Asiakkaan ja pääkäyttäjän pitäisi olla samalla tasolla järjestelmän sisältämästä yrityksen tiedosta, jotta väärinymmärryksiltä vältyttäisiin. (Hulkkonen 2014.)

4.6 Rekisteriselosteet

Kulunvalvonta- sekä kameravalvontajärjestelmistä on laadittava henkilötietolain (523/1999) mukaiset rekisteriselosteet, sillä järjestelmä, joka sisältää luonnollista henkilöä koskevia henkilötietoja, on henkilötietolain mukainen henkilörekisteri. Näiden järjestelmien pääkäyt-

täjät eivät kuitenkaan ole rekisterinpitäjiä, vaan palveluntuottajia tai toimeksisaajia. Rekisterinpitäjä eli asiakas vastaa tietojenkäsittelyn ja muun toiminnan lainmukaisuudesta ja vastuu henkilötietojen käsittelystä on myös heillä, vaikka palvelu olisi ulkoistettu. Pääkäyttöpalvelusopimuksen perusteella tapahtuva henkilötietojen käsittely on tällöin rekisterin käyttöä. (Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset 2010, 3).

Rekisterinpitäjän tulee laatia jokaisesta eri henkilörekisteristään rekisteriseloste, eli kulunvalvonta- ja kameravalvontajärjestelmien osalta molemmista omansa, jotta henkilötietolain vaatimukset täyttyvät. Rekisterinpitäjä määrittelee kuitenkin itse tietojen tarpeellisuuden. Poikkeuksina henkilötietolaki määrittää arkaluonteisten tietojen keräämisen ja käsittelyn sekä henkilötunnuksen käsittelystä erikseen. Yleinen edellytys käsittelylle on, että henkilöä ei voida muuten yksiselitteisesti yksilöidä ja siten muut tiedot eivät ole tähän riittäviä. (Tietosuojavaltuutetun toimisto 2013).

Rekisteriselosteen luominen auttaa arvioimaan esimerkiksi henkilötietojen käsittelyn kannalta tarpeellisia tietoja ja rekisteriseloste on siten hyvä työkalu asiakassuhteen hoidossa asiakkaan sekä pääkäyttäjän välillä. Järjestelmien sisältämät henkilötiedot ja mm. kulkutapahtumien tai kameravalvontatallenteiden säilytysajat on aina voitava perustella rekisteröidyille. Tämä lisää avoimuutta ja luottamusta turvajärjestelmiä sekä niiden hallinnointia kohden sekä ohjaa myös suunnittelemaan, toteuttamaan ja kehittämään tietoturvallisuutta. (Henkilötietolain mukainen ilmoitusvelvollisuus 2010).

Kameravalvonnan osalta tallennettu kuva ja ääni rinnastetaan henkilötietoihin, jos yksityishenkilö on niistä tunnistettavissa. Yleislakina kameravalvontajärjestelmän tallentamaa tunnistettavaa kuvaa tai ääntä kohtaan sovelletaan lähtökohtaisesti henkilötietolakia (523/1999), sillä kyse on henkilötietojen automaattisesta käsittelystä. Tallenteiden säilytysajalla ei ole vaikutusta henkilötietolain soveltamiseen. Kameravalvonnan harjoittaja tai toimeksiantaja on henkilötietolaissa tarkoitettu rekisterinpitäjä, vaikka tallenteita säilytettäisiin esimerkiksi vain päivän ajan. Henkilötietolakia ei sovelleta kameravalvontaan, mikäli kuvamateriaalia ei tallenneta jollekin alustalle. (Tietosuojavaltuutetun toimisto 2014).

Lähtökohtaisesti kulunvalvontajärjestelmän sisältämien henkilötietojen käsittely on kiinteistön tai yrityksen asiakas- tai palvelusuhteen vuoksi pääkäyttäjälle perusteltua. Työsuhteensa lopettaneella henkilöllä ei kulkuoikeuksien päättymisen jälkeen kuitenkaan ole varsinaista asiakassuhdetta kiinteistön tai yrityksen tiloihin, mutta tietojen säilyttämistä voidaan perustella mahdollisten rikosten selvittämiseksi kulkutapahtumalokeja hyödyntäen. Tiedusteltuani asiaa puhelimitse Tietosuojavaltuutetun toimistolta (2014), virkailija totesi, että käytännössä henkilötietojen ja kulkutapahtumien säilytystä voidaan soveltaa täysin vapaasti ja riskittä-

mästi. Mikään laki ei ota siihen suoranaisesti kantaa, missä vaiheessa ns. asiakassuhde kiinteistön ja kulkutunnisteen käyttäjän välillä päättyy. Asiakkaan on kuitenkin oltava henkilötietojen käsittelyssä erittäin huolellinen ja varmistettava, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja pääkäyttäjän toimesta käsitellä.

4.7 Turvajärjestelmien pääkäytön ammattisanasto

Turvallisuus tulisi käsitellä yhdellä yhtenäisellä tavalla. Olisi kaikille eduksi, että olisi mahdollisimman pitkälle yksi yhteinen kieli. Turvajärjestelmiin, kulunvalvontaan ja lukituksiin liittyvä yhtenäinen sanasto hyödyttää sekä asiakasta että palveluntoimittajaa tilauksissa, koulutus- ja ongelmatilanteissa, jotta kaikki osapuolet ymmärtävät asiat samoin tavoin. (Avald ym. 2014).

Yksiselitteisillä ja yhteisillä termeillä sekä käsitteillä on suuri vaikutus pääkäyttöpalvelulle sekä -prosessille. Se on myös edellytys pääkäyttäjän ammattimaisuudelle sekä toimivalle yhteistyölle, samoin tavoin kuin Mikael Kiviniemi sekä Juhani Turunen toteavat Valtionhallinnon tietoturvasanaston (VAHTI 8/2008) saatesanoissa tietoturvaosaamisen osalta: ”Myös käynnissä olevissa hankkeissa ja kehitysohjelmissa on todettu henkilöstön tietoturvaosaamisen ja yhteistyön merkitys hallinnon toimintojen, prosessien ja palvelujen kannalta. Osaamisen ja hyvän tietoturvyhteistyön edellytys on, että henkilöstö tuntee tietoturvallisuuden keskeiset käsitteet.”

Työn liitteeseen Turvajärjestelmien pääkäytön suuntaviivat -oppaaseen Osio 1:een on koottu lista asiantuntijahaastatteluissa ilmenneistä yleisimmistä epäselvyyksiä tuottavista sanoista. Ensimmäinen pystysarake on oikea, yksiselitteinen ja suositeltava sanavalinta. Keskimmäinen pystysarake määrittelee, mitä termi tarkoittaa ja minkälaisia ja -mallisia näitä on. Oikepuoleisessa pystysarakkeessa lisäselityksiä ja kuultuja termejä, joista voidaan ymmärtää mistä on kyse, mutta mitä termejä käytettäessä voidaan ajautua kauas halutusta tarkoituksesta.

5 Tulokset ja arviointi

Opinnäytetyön tutkimuksessa havaittiin, että pääkäyttö on terminä turvajärjestelmien kontekstissa yhä sellainen, mikä luo kuulijalle eri mielikuvia kyseisestä toiminnasta tai palvelusta. Myöskään pääkäyttöpalvelun tilaaja tai itse pääkäyttäjä ei aina ole tietoinen siitä, mitkä suuntaviivat tiettyjä toimintoja määrittelee sekä millä keinoilla pääkäyttöprosessin tehokkuutta voisi lisätä. Tarve yhtenäisten suuntaviivojen määrittämiselle oli siis molemminpuolinen.

Pääkäyttöpalvelussa asiakas on palvelua ulkoistaessa odottanut, että omaan ydinliiketoimintaan vapautuu näin ollen resursseja ja järjestelmistä saa niiden maksimaalisen hyödyn irti,

jolloin turvallisuuden voidaan olettaa olevan hyvällä tasolla. Turvajärjestelmän pääkäyttäjä on taas saattanut kokea, että asiakkaan tarpeita on ollut vaikea tunnistaa, kommunikoinnissa on ollut haasteita sekä ei ole ollut selviä suuntaviivoja, millä tilanteita ja valintoja voisi perustella.

Tilanteessa on kuitenkin vielä kolmaskin osapuoli, josta ilmenee, että kyseessä on ollut asiakaslähtöinen ja kohtalaisen suuri tarve pääkäytön kehittämiseksi. Helsingin poliisilaitokselta Mäkinen ja Kurtelius (2014) tulkitsivat haastattelussani, että kameravalvonnan pääkäytön osalta järjestelmien hallinnoijat olisi hyvä motivoida tarkastamaan aktiivisesti tai säännöllisesti järjestelmiensä tilaa ja toimintoja sekä parhaat käytänteet tulisi yhtenäistää.

Kiinteistönjohdon edustajien kanssa käydyissä keskusteluissa liikekiinteistöjen turvallisuusratkaisuista esille nousi useimmiten resurssien, tietoisuuden ja koulutuksen puute. Mikäli pääkäytön tehtäviä ja vastuita ei oltu ulkoistettu, koettiin tehtävät helposti ylimääräisinä taakkoina. Korkeatasoinen järjestelmien tai ratkaisujen hallinnointi, kuten avainhallintaan liittyvä lukitussuunnittelu koettiin lii ylitsepääsemättömäksi tehtäväksi. Käyttäjätasoiset tehtävät, kuten kameravalvontatallenteiden tallentaminen ja avaimien kuittaaminen nähtiin sopivina tehtävinä omille resursseille varattuna. Tärkeiksi järjestelmien elinkaarta pidentäviksi ja mainetta parantaviksi asioiksi koettiin avoimen dokumentoinnin merkitys, käyttökoulutuksien järjestäminen sekä turvallisuustietoisuuden näkyvä jakaminen.

Vaikka turvajärjestelmien pääkäytöstä voisi koostaa kokonaisen opintokokonaisuuden, ei aihetta juurikaan käsitellä turvallisuusalan opintoja tarjoavissa koulutuslaitoksissa. Kehitettäväksi näkökulmaksi on myös ilmennyt turvajärjestelmiin liittyvän sanaston tuntemuksen laajentaminen. Asioista puhutaan usein väärillä nimillä, varsinkin lukitukseen ja kulunvalvontaan liittyen. Ammattisanaston yhtenäistämällä palveluntuottaja ja palveluntilaaja olisivat helpommin samalla aaltopituudella.

5.1 Kehittämistyön tulokset

Turvajärjestelmien pääkäytön suuntaviivat -opas luotiin opinnäytetyön ohella liitteeksi, jotta työn ja tutkimuksen tavoitteena ollut pääkäyttöprosessien parantaminen ja yhtenäistäminen saavutettaisiin tuotoksen käyttäjäryhmillä.

Opas soveltuu niin pääkäyttäjien, käyttäjien kuin asiakkaiden käyttöön, jotta pääkäytön tarkoitus olisi yhteisesti ymmärrettävissä. Pääkäyttäjäorganisaatiot voivat soveltaa opasta pääkäyttäjien koulutukseen tai yritysten sisäiset pääkäyttäjät voivat suorittaa helpommin pääkäyttöprosesseja oppaan avulla ollen aikaisempaa varmempia siitä, että kaikki tarpeelliset lainsäädännölliset näkökulmat tai turvallisuutta uhkaavat virhemääritykset ovat katettuja.

Palvelun asiakas voi hyötyä oppaasta ymmärtämällä sen avulla helpommin pääkäyttäjien pyytämiä tietoja ja esittämiä vaatimuksia.

5.2 Tulosten arviointi

Valmista opasta on arviointia varten tarkasteltu Flexim Security Oy:n pääkäyttäjäyksikön asiantuntijoiden toimesta sekä nimettömänä arviointiin osallistuneiden kulunvalvonnan pääkäyttöpäalvelun yhteyshenkilöiden kanssa. Lisäksi opasta on esitetty täysin palvelusta ja palvelunsisällöstä tietämättömille henkilöille, jotta on saatu näkökulmia oppaan ymmärrettävyydestä. Näin ollen eri näkökulmat on saatu otettua huomioon tuotoksen käytettävyyttä varten.

Tulosten arviointia varten selvitettiin myös kokemuksia mahdollisista aikaisemmista vastaavankaltaisista pääkäyttöpäalvelun työpyyntölomakkeiden käytöistä. Selvisi, että Helsingin Energia on räätälöinyt omaan käyttöönsä vastaavan lomakkeen kulkutunnisteiden tilauksia varten heidän turvallisuuspäällikkönsä Mats Fagerströmin (2014) mukaan pääkäyttöpäalvelu on kehittynyt, prosessit nopeutuneet sekä virhetilanteet vähentyneet. Tämän lisäksi palvelupyntöjen dokumentointi on pysynyt hyvällä mallilla ja ajan tasalla itsestään.

Flexim Security Oy:n pääkäyttöyksikön asiantuntijat arvioivat, että pääkäyttöprosessia saataisiin oppaan liitteeksi tehdyillä lomakkeilla nopeutettua sekä kehitettyä varsinkin kulunvalvonnan vikatilanteiden selvityksissä, sillä aikaa kuluu varsin usein pitkään kohde-, käyttäjä- ja tilannekohtaisissa tiedustelu- ja selvitysasioissa (Avald ym. 2014). He totesivat myös, että työpyyntölomakkeissa on otettu kaikki tarpeelliset asiat huomioon ja se on helposti myös räätälöitävissä eri pääkäyttäjille, eri organisaatioille, kuin myös avainhallintaa varten. Ulkopuolisille henkilöille opasta ja lomakkeita tarkastutettaessa oli tarkoitus saada selville, onko oppaan sisältöä ja tarkoitusta helppo ymmärtää. Nimettöminä tiedusteluun vastanneet henkilöt (5kpl) arvioivat, että he pystyisivät käyttäjänä tai pääkäyttäjänä saamaan sekä löytämään apuja pääkäyttämistä tai palvelupyntöjen tekemistä varten. Lisäksi asiakkaana he kokisivat työpyyntölomakkeiden täyttämisen helpoksi. Eräs pääkäyttöpäalvelun tilaaja-asiakas ja yrityksensä kulunvalvonnan sekä avainhallinnan yhteyshenkilö koki lisäksi, että oppaalla ja sen liitteillä on ehdottomasti lisäarvoa, sillä hän ei ollut aiemmin osannut ottaa huomioon kaikkia esimerkiksi vikatilanteisiin olennaisesti liittyviä asioita. Flexim Security Oy:n palvelupäällikkö Tatu Monto (2014) mainitsi palautteessaan palveluntoimittajan näkökulmasta, että oppaan avulla on mahdollista muodostaa asiakkaan kanssa yhteinen kieli, joka luo edellytykset palvelusisällön ymmärtämiselle mahdollisimman yksiselitteisesti.

6 Pohdinta ja jatkotutkimus

Opinnäytetyön tarkoituksena oli tutkia ja selvittää turvajärjestelmien hallinnoinnin nykytilaa sekä keinoja ja toimenpiteitä, joilla järjestelmistä on mahdollista saada maksimaalinen hyöty irti. Hyödyiksi voidaan lukea järjestelmien suorituskyvyn parantaminen sekä hallinnolliselta puolelta pääkäyttöprosessien selventyminen, samaan aikaan kuitenkin resursseja jopa vähentäen. Tarve tutkimukselle ja sen tuotoksena syntyneelle oppaalle oli työelämälähtöinen. Opasta on tarjottu käyttöön eräälle alan yritykselle ja he aikovat pilotoida sitä koulutuskäytössä, tietokantojen siivousprojekteissa sekä saada kulunvalvonnan pääkäyttöprosessien keskimääräistä läpiviemisaikaa lyhennettyä.

Turvajärjestelmien pääkäyttäjän töitä tehdessä kävi ilmi, että moni turvallisuuteen vaikuttava asia tai määräys perustui käytännössä toimiviksi havaittuihin tapoihin tai Finanssialan Keskusliiton suosituksiin. Rajapinnat olivat silti vaikeasti havaittavissa, eikä näistä saanut pääkäyttötyöhön yhtenäistä tietopakettia. Pääkäyttäjän ja asiakkaiden välejä häiritsi yhteisen kielen ja sanaston puute, sekä varsin yleisesti se, ettei asiakas ymmärtänyt, mistä pääkäyttöpalvelussa oli tarkasti edes kysymys. Yllättävänä havaintona ilmeni, että vaikka yhteisille suuntaviivoille on ollut tarvetta, on palvelua silti toimitettu ja suoritettu tiedostaen, että prosesseissa olisi parantamisen varaa. Suuntaviivojen luonnista huolimatta vaikuttaa siltä, että oppaasta on enemmän hyötyä pääkäyttäjille. Asiakkaan näkökulmasta tavoite on ollut saada resursseja omaan ydintoimintaan, joten suuntaviivoista voisi luoda vielä lyhyet suuntaviivat palveluntilaajan näkökulmasta. Rajapinnalle on kuitenkin tarvetta, sillä ilman kommunikointia hyvän turvallisuustason ylläpitäminen on hankalaa.

Liikekiinteistöjen edustajilta viesti oli selkeä, että turvallisuus on ehdottomasti tärkeä asia sekä maineen että houkuttelevuuden kannalta. Raha ja kustannukselliset asiat sekä resurssien puute olivat kuitenkin usein asioita, joiden vuoksi taso ei välttämättä ollut hyvä, josta syystä kiinteistöjen sekä asiakkaiden turvallisuus kärsivät. Usein reagoidaan vasta, kun jotain tapahtuu. Riskit eivät siis ole tiedostamattomia, vaan hyväksytyjä riskejä.

Yhteenvetona pääkäytöllisistä tehtävistä voitaneen sanoa, että järjestelmien saaminen tiettyyn formaattiin, ns. ylläpitotilaan, on avain järjestelmän pitkälle elinkaarelle sekä turvallisuuden pysymiselle hyvällä ja hyväksyttävällä tasolla. Poikkeamat tasosta eivät aiheuta välitöntä uhkaa, mutta poikkeamien määrä laskee kielteisten uhkakuvien toteutumisen estämisestä. Turvajärjestelmät tukevat toiminnoillaan toisiaan. Esimerkiksi mekaanisen avaimen käyttäjä ei kameravalvontatallenteen silmissä ole enää anonymi.

Käytännön toimien puolelta kommunikoinnin merkitys pääkäyttäjälle on ensiarvoisen tärkeää virheiden sattumisien ehkäisemiseksi sekä ylläpitotilan varmentamiseksi. Oikein käytetyillä

ammattitermeillä luodaan ammattimainen ja asiantunteva kuva pääkäyttäjän taholta, sekä edesautetaan oikeakielisuuden ja turvallisuuskulttuurin leviämistä. Hallinnoinnin näkökulmasta korostuu pääkäyttöprosesseihin liittyvä dokumentointi, jotta velvollisuudet tehtävistä, määräyksistä ja ilmoituksista sekä vastuut avaimista, tunnisteista ja pin-koodeista ovat selvillä, tai ainakin pystyttävissä osoittamaan jälkikäteen.

6.1 Opinnäytetyöprosessi ja oma oppiminen

Opinnäytetyön tekoprosessi oli pitkä ja melkoisen raskas, sillä suuntaviivojen ja oppaan luomisessa sekä tietojenkeruussa meni kokonaisuudessaan yli 10 kuukautta. Haasteiksi muodostui selvittäminen, onko kaikki mahdolliset osa-alueet otettu huomioon jokaista neljää järjestelmää tarkasteltaessa. Lisäksi omat haasteensa toi rajausten tekeminen, sillä pääkäytön eri asiantuntijoilla oli palvelunkuvaustenkin takia joillakin osa-alueilla eri näkemyksiä. Yhteinen sävel löytyi kuitenkin helposti.

Työ ei aikataulunsa puolesta pysynyt suunnitelmassaan, mutta jälkikäteen ajateltuna siitä ei ollut lainkaan haittaa. Koska tein töitä täyspäiväisesti koko prosessin ajan, sain uusia ideoita, näkökulmia ja myös uutta oppia lähes viikoittain. Nämä ovat omasta mielestäni kehittäneet työn sisältöä. Itse aihe ja varsinaisten pääkäyttöprosessien sisällöt olivat minulle hyvin entuudestaan tuttuja, joten tutkimuksen kannalta en saanut suurta oppimiskokemusta substanssin osalta. Tutkimuksen ja selvityksen sekä haastattelujen tekemisestä tosin opin paljon ja pystyn hyödyntämään taitoja jatkossa paremmin.

Alun perin olin ajatellut, että opas olisi paljon lyhyempi, mutta tulin nopeasti johtopäätöksen, että mitään näkökulmaa ei voi jättää kattamatta. Hyvän oppaan luomiseen en työssäni pureutunut, mutta aion kehittää oppaan vielä sellaiseksi, jossa tämäkin näkökulma on huomioitu. Siitä muodostuu täysin oma prosessinsa, joka vaatii oppaan käyttöönottoa, reflektointia ja palautetta niin asiantuntijoilta, asiakkailta kuin täysin pääkäytöstä tietämättömiltä henkilöiltä. Todennäköisesti luon vielä myöhemmin lyhyemmän, muutaman sivun mittaisen oppaan, joka on tarkoitettu suoraan asiakkaan avuksi. Nykyisessä oppaassa asiakkaan voi olla hankalaa hahmottaa heitä itseään hyödyttävät tiedot.

Kaiken kaikkiaan onnistuin opinnäytetyössäni hyvin ja tavoitteideni mukaisesti, varsinkin työn tuotoksen osalta. Sain hyviä kontakteja asiantuntijahaastatteluiden kautta ja uskon, että pystymme kehittämään pääkäyttöä yhdessä kohti sitä tavoitetta, että turvajärjestelmät ja pääkäyttäminen ovat tulevaisuudessa laajemmin ymmärretty turvallisuusalan osa-alue.

6.2 Jatkotutkimuksen aiheita

Turvajärjestelmien pääkäyttöön liittyvistä henkilötiedoista ja niiden muodostamista henkilörekistereistä ei ole selvityksen ja havainnoinnin perusteella yhteisiä suuntaviivoja. Vaikka tietojen keräämistä ja käyttöä sekä rekisteriselosteiden merkitystä käsiteltiin tässä työssä, olisi aiheelle varmasti lisätutkimuksen tarvetta. Tutkimusongelmana voisi olla ulkoistetun pääkäyttöpalvelun tietosuojaperiaatteet, sisältäen henkilötietojen ja henkilötunnusten käytön ja käsittelyn sekä ilmoitusvelvollisuuden vastuut.

Toisena ongelmana pääkäytön suuntaviivoilla on erikaltaisten ja suuruisten yritysten erilaiset tarpeet. Jatkotutkimuksen aiheena voisi olla kulunvalvonnan kulkualueiden eli kulkuoikeuksien suunnitteluun suuntaviivat esimerkiksi case-kohtaisesti siten, että tutkimuksessa luotaisiin ja eroteltaisiin tarpeet sekä parhaimmat mallit luoda toimivat sekä yksinkertaiset kulkuoikeudet 1) Pieneen tai keskisuureen yhden organisaation kiinteistöön, 2) Liikekiinteistöön, jossa useampia vuokralaisia, sekä 3) Organisaatioon, jossa useita toimipisteitä saman kulunvalvontajärjestelmän alla ja henkilöitä liikkuu satunnaisesti eri kiinteistöjen välillä. Aihetta voisi soveltaa myös avainhallinnan puolelle lukitussuunnitteluun. Tutkimusongelma voisi kuitenkin keskittyä kohtaan 3; miten kulkuoikeudet voidaan määritellä suuressa organisaatiossa siten, että oikeudet ovat samalla tarpeeksi rajatut, mutta ratkaisu huomio myös ylläpidon ja käytettävyyden. Tällä hetkellä ratkaisu on usein turhan laajaksi määritellyt oikeudet.

Lähteet

Aalto-yliopisto Kauppakorkeakoulu. Käsitteiden määrittely ja käyttö. Viitattu 9.9.2014.
<http://viestinnantietoaines.aalto.fi/Tieteellinen/kasitteet.htm>

Ahokas, J., Karkinen, P., Mero, P. & Pänkäläinen, A. 2008. Finanssialan Keskusliiton omaisuusrikostoimikunta. Kohteen murtoriskien arviointi ja suojaustason valinta -ohje 2008. Helsinki: Finanssialan Keskusliitto.
http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Kohteen_murtoriskien_arviointi.pdf

Ahokas, J., Kuisma, L., Laitinen, J., Lehtikangas, M., Pänkäläinen, A. & Vuonoranta, E. 2006. Kameravalvonnan suunnitteluohje Kameravalvonnan K-menetelmä. Helsinki: Finanssialan Keskusliitto.

Airaksinen, T. & Vilka, H. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi

Avainsäilöt kiinteistöissä. 2000. Abloy Oy.
<http://www.abloy.fi/Abloy/FI/Tuotevalintaopas/Tuotekohtaiset%20oppaat/Avains%C3%A4il%C3%B6t%20kiinteist%C3%B6iss%C3%A4.pdf>

Avainturvallisuusohje. 2010. Finanssialan Keskusliitto.
<http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Avainturvallisuusohje.pdf>

BLC Turva Oy. N.d. Pääkäyttäjäpalvelut. Viitattu 9.9.2014.
<http://www.blcturva.fi/fi/ammattilaisille/palvelut/paakayttajapalvelu>

Ellonen V., Kauppi V., Kinnunen H., Käyhkö P., Laitinen J., Lehtikangas M., Lehtinen T., Lehtonen R., Pänkäläinen A., Pöytä H., Sallinen P., Starck K. & Woitsch P. 2010. Kameravalvontaopas. Turva-alan yrittäjät ry & Poliisihallitus, turvallisuusalan neuvottelukunta. Sähköinfo Oy. Sähköinen versio osoitteessa
https://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Kameravalvontaopas_2010.pdf

Heinonen, J., Keinänen, A. & Paasonen, J. 2013. Turvallisuustutkimuksen tekeminen. Helsinki: Tietosanoma.

Heinämäki, A-K. 2009. Yksityinen turvallisuusala turvallisuuspalveluiden tuottajana. Selvitystyö Sisäasiainministeriön toimeksiannosta. Poliisin ylijohdon julkaisusarja 8/2009.
[http://www.poliisi.fi/intermin/biblio.nsf/D01294F77884C1E1C225768F00428356/\\$file/8-2009.pdf](http://www.poliisi.fi/intermin/biblio.nsf/D01294F77884C1E1C225768F00428356/$file/8-2009.pdf)

Henkilörekisteriasiat avainten- ja lukostonhallinnassa. Abloy Oy. Viitattu 19.10.2014.
<http://www.abloy.fi/Abloy/FI/Tekstiliitteit%C3%A4/Henkil%C3%B6rekisteri%20lukitusj%C3%A4rjestelm%C3%A4ss%C3%A4.pdf>

Henkilötietojen käsittelyn ulkoistaminen, yhteiset tietojärjestelmät, verkottuminen ja niihin liittyvät sopimukset. 2010. Tietosuojavaltuutetun toimisto. Viitattu 28.9.2014.
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetun-toimisto/6JfppPP8x/Henkilotietojen_kasittelyn_ulkoistaminen_yhteiset_tietojarjestelmat_verkottuminen_ja_niihin_liittyvat_sopimukset.pdf

Henkilötietolain mukainen ilmoitusvelvollisuus. 2010. Tietosuojavaltuutetun toimisto. Viitattu 28.9.2014.
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetun-toimisto/oppaat/6Jfpr4Tsl/Henkilotietolain_mukainen_ilmoitusvelvollisuus.pdf

Heljaste, J-M., Korkiamäki, J., Laukkala, H., Mustonen, J., Peltonen, J. & Vesterinen, P. 2008. Yrityksen turvallisuusopas. Helsinki: Helsingin seudun kauppakamari.

Henkilötietolaki 22.4.1999/523

Kansallinen turvallisuusauditointikriteeristö - KATAKRI, versio II. 2011. Puolustusministeriö. Helsinki. http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Kilpailu- ja kuluttajavirasto. 2009. Lukkojen ja helojen murtoturvallisuuteen liittyvät standardiehdotukset rtt-2009008 ja rtt 2009009. Viitattu 28.9.2014.
<http://www.kilpailuvirasto.fi/cgi-bin/suomi.cgi?luku=aloitteet-ja-lausunnot&sivu=aloit-laus/a-2009-20-0105>

Lith, P. 2014. Turvallisuusalan yritysten suhdanne- ja toimialaraportti 2014. Selvitys turvallisuusalan yritysten markkinoista, yritysprofiileista, kasvuyrittäjyydestä ja lähiajan suhdanne-odotuksista. Finnsecurity ry:n julkaisu.

Lukitusturvallisuus. Hyvinkään Turvalukko Oy. Viitattu 5.10.2014.
<http://www.hyvinkaanturvalukko.fi/lukitusturvallisuus>

MOT Kielitoimiston sanakirja. Kulunvalvonta. Viitattu 26.2.2014.

Ojasalo K., Moilanen T. & Ritalahti J. 2009. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro Oy.

Puusa, A. 2008. Käsiteanalyysi tutkimusmenetelmänä. Premissi 4/2008, 38.

Stanley Security Oy. 2014. Pääkäyttäjäpalvelu. Viitattu 9.9.2014
<http://www.stanleysecurity.fi/tuotteet-ja-palvelut/sopimuspalvelut/paakayttajapalvelu/>

Sähköala. 2014b. Kameravalvonta. Viitattu 13.4.2014.
http://www.sahkoala.fi/kiinteistoala/Turvallisuus/fi_FI/videovalvonta/

Sähköala. 2014a. Kulunvalvonta- ja työajanseurantajärjestelmät. Viitattu 9.9.2014.
http://www.sahkoala.fi/kiinteistoala/Turvallisuus/fi_FI/kulunvalvonta/

Sähköala. 2014c. Rikosilmoitin. Viitattu 13.4.2014.
http://www.sahkoala.fi/kiinteistoala/Turvallisuus/fi_FI/rikosilmoitin/

Tietosuojavaltuutetun toimisto. 2014. Kameravalvonta. Viitattu 28.9.2014.
<http://www.tietosuoja.fi/fi/index/useinkysyttya/kameravalvonta.html>

Tietosuojavaltuutetun toimisto. 2013. Minkälaisia henkilötietoja voi käsitellä? Viitattu 28.9.2014.
<http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/minkalaisiahenkilotietojavoikasitella.html>

Tyska L.A. & Fennelly L.J. 1998. 150 Things You Should Know About Security. Woburn, MA: Butterworth & Heineman.

Walcot, B. 2008. The history of locks. Viitattu 22.2.2014.
<http://www.londonlocksmiths.com/assets/history-of-locks.pdf>

Julkaisemattomat lähteet:

Avald, K., Jeskanen, N., Pietilä, S. & Öhman, P. 2014. Kulunvalvonnan asiantuntijat. Flexim Security Oy. Pääkäyttöyksikön ryhmähaastattelu 30.9.2014.

Fagerström, M. 2014. Turvallisuuspäällikön puhelinhaastattelu 24.10.2014. Helsingin Energia Oy.

Flexim Security Oy. 2014. Palvelukuvaus - Pääkäyttäjäpalvelut.

Holmberg, W. 2014. Lukitusjärjestelmät ja niiden hankintaprosessi taloyhtiöille. Opinnäyte. Vantaan ammattiopisto Varia. Julkaisu toimitettu sähköpostitse. Vastaanottaja Juuso Jääskeläinen. Lähetetty 15.10.2014 20:11. Viitattu 18.10.2014.

Hulkkonen, I. 2014. Turvajärjestelmien pääkäyttäjä. Secon Systems Oy. Haastattelu 24.9.2014.

Iloranta, K & Viljakainen, M. 2014. Avainhallinnan asiantuntijat. Flexim Security Oy. Haastattelu 22.9.2014.

Juntunen, N. 2014. Ylläpitopäällikön haastattelu puhelimitse 23.10.2014. Ovenia Oy.

Kyllästinen, K. 2014. Kiinteistöpäällikkö. Corbel Oy. Haastattelu 2.6.2014.

Liljedalh, T. 2014. Kulunvalvonnan entinen pääkäyttäjä ja kouluttaja. Flexim Security Oy. Haastattelu 15.6.2014

Monto, T. 2014. Flexim Security Oy. Sähköpostiviesti. Vastaanottaja Juuso Jääskeläinen. Lähetetty 10.11.2014 10:39. Viitattu 11.10.2014.

Peltonen, J. 2014. Ulkoasiainministeriö. Luento Laurea-ammattikorkeakoulussa syksyllä 2013.

Räsänen, R. 2014. Re: Opinnäytetyö. Sähköpostiviesti. Vastaanottaja Juuso Jääskeläinen. Lähetetty 16.5.2014 15:23. Viitattu 12.06.2014.

Tietosuojavaltuutetun toimisto. 2014. Keskusteltu toimiston puhelinneuvonnan kanssa koskien kulunvalvontajärjestelmän sisältämiä henkilötietoja 7.8.2014.

Ukkonen, O. 2014. Pääkäyttäjä. ISS Palvelut. Haastattelu 7.7.2014.

Viljakainen, M. 2012. Avain- ja tunnistehallinnan pääkäyttöpalvelun julkaisematon Powerpoint-esitys. Esitys toimitettu sähköpostitse. Vastaanottaja Juuso Jääskeläinen. Lähetetty 21.10.2014. Viitattu 22.10.2014.

Kuvaluettelo

Kuva 1 Liikekiinteistön tila X: Pohjakuva	20
Kuva 2 Avainsäilön reittiavain (Avainsäilöt kiinteistöissä 2000, 2)	27
Kuva 3 K-menetelmän näkymien vaatimustasot (Kameravalvontaopas 2010, 31)	29

Kuviluettelo

Kuvio 1 Kiinteistövalvonta (Turvallisuusalan sanasto 1989)	17
Kuvio 2 Onnistunut pääkäyttöprosessi.....	36
Kuvio 3 Aikaavievä pääkäyttöprosessi	37

Taulukkuuettelo

Taulukko 1 Tutkimuskysymyksistä tuotokseen..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

Taulukko 2 Reaalimääritelmä - turvajärjestelmien pääkäyttö .. **Virhe. Kirjanmerkkiä ei ole määritetty.**

Taulukko 3 Avainsäilytysyksikkö (Avainturvallisuusohje 2010, 4)**Virhe. Kirjanmerkkiä ei ole määritetty.**

Liitteet

Liite 1 Turvajärjestelmien pääkäytön suuntaviivat	52
Liite 2 Asiantuntijahaastatteluiden rungot	76
Liite 3 Flexim Security Oy:n palvelupäällikön palaute oppaasta	79

Liite 1 Turvajärjestelmien pääkäytön suuntaviivat



TURVAJÄRJESTELMIEN PÄÄKÄYTÖN SUUNTAVIIVAT

- Kulunvalvonta
- Avainhallinta
- Kameravalvonta
- Rikosilmoittimen hallinta

Juuso Jääskeläinen 2014

TURVAJÄRJESTELMIEN PÄÄKÄYTÖN SUUNTAVIIVAT

Tämän oppaan tarkoituksena on kuvata turvallisuuden eri osa-alueiden pääkäytön tärkeimmät suuntaviivat ja niiden avulla toimia tukena pääkäyttöpalvelussa sekä asiakkaalle että pääkäyttäjälle. Suuntaviivat sekä pääkäytön sanasto ovat käyttökelpoiset kaikille turvallisuuden kanssa tekemisissä oleville organisaatioille ja henkilöille.

Suuntaviivat tarkoittavat sääntöjä tai periaatteita, jotka antavat opastusta tarkoituksenmukaiseen toimintaan. Turvajärjestelmien pääkäytössä suuntaviivoilla päästään tilaan, jossa järjestelmien sekä tietojen hallinnointi on mahdollisimman tehokasta ja yksiselitteistä. Yhtenäiset suuntaviivat helpottavat pääkäyttöpalvelun kokonaiskuvan ymmärtämistä nopeuttaen palveluprosessia ja siten parantaen kokonaisturvallisuutta ja turvallisuuskulttuuria.

Tästä oppaasta on rajattu tietoturvan suuntaviivojen osuus pois, mutta pääkäyttäjän ehdottoman tärkeää muistaa tietoturvan merkitys omassa toiminnassaan, sillä se on erittäin tärkeä elementti turvallisuustoiminnassa. Tietoturvaan liittyvät toimintatavat tulisivatkin löytyä yrityksen omasta tietoturvaetiketistä. Myöskään teknisiin ratkaisuihin ei tässä oppaassa oteta kantaa.

Osiossa 1 käsitellään turvajärjestelmiin ja niiden pääkäyttöön liittyviä termejä ja käsitteitä. On suositeltavaa perehtyä sanastoon ensimmäiseksi, jotta perustuntemus käsitteistä on hallussa ennen osioita 2-5.

Osiossa 2 käsitellään kulunvalvonnan pääkäytön tärkeimpiä ylläpidollisia tehtäviä ja kulunhallinnan tarkoitusta.

Osiossa 2 käsitellään avain- ja tunnistehallinnan ylläpidollisia tehtäviä ja tarkoitusta.

Osiossa 4 käsitellään kameravalvonnan pääkäytön tärkeimpiä ylläpidollisia tehtäviä ja tarkoitusta.

Osiossa 5 käsitellään rikosilmoittimen hallinnan tärkeimpiä ylläpidollisia tehtäviä ja tarkoitusta.

Osiosta 6 löytyy liitteinä oman yrityksen käyttöön räätälöitävät tai sellaisenaan käytettävät kulunvalvonnan ja avainhallinnan tilaus-/työpyyntölomakkeet sekä avainten/tunnisteiden kuittauslomakemalli.

OPAS PÄÄKÄYTTÖ- PALVELUUN ASIAKKAALLE SEKÄ PALVELUN- TOIMITTAJALLE

Osiot 1:
Pääkäytön sanasto

Osiot 2:
Kulunvalvonta

Osiot 3:
Avainhallinta

Osiot 4:
Kameravalvonta

Osiot 5:
Rikosilmoittimen
hallinta

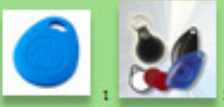





Osiot 6:
Liitteet

Osiot 7:
Lähteet

OSIO 1: PÄÄKÄYTÖN SANASTO

Pääkäytön sanasto yhtenäistää turvajärjestelmiin ja niiden hallintaan liittyvän terminologian. Sanasto on tarkoitettu käytettäväksi niin pääkäyttäjille kuin kenelle muulle tahansa, jolla on yhteys kulkutunnisteisiin, avaimiin tai yleisesti turvallisuuteen. Ei tule unohtaa, että turvallisuus on jokaisen vastuulla ja jokainen voi itse teoilla ja toiminnollaan vaikuttaa turvallisuuteen.

Pääkäyttäjillä, yrityksen pääkäyttöpalvelun yhteyshenkilöillä sekä yrityksen turvallisuudesta vastaavilla henkilöillä tulee vähintään kuitenkin olla käsitteiden perustuntemus, palvelukohtaisesti.

Oikea termi:	Tarhoittaa:	Huomioita
<p>Kulkutunniste</p> 	<ul style="list-style-type: none"> - Etälukuvaimenperä - Avaimenperätunniste - Etälukutunniste - Malleja: HID, Indala, Bewator ym. 	<ul style="list-style-type: none"> - Kuultuja termejä: Lätke, kulkuvain, kulkulupa, KV-avain, avain, sähköavain, nappi, tägi, mustikka, kapula ym. - Kyseessä ei ole avain, vaikka tunnisteella saakin lukon avattua - Voi olla integroitu henkilökorttiin
<p>Kulkukortti</p> 	<ul style="list-style-type: none"> - Korttimallinen kulkutunniste - Magneetikortti - Avainkortti 	<ul style="list-style-type: none"> - Kuultuja termejä: Kulkulupa, avain - Kyseessä on yhtä lailla kulkutunniste kuin edellisessä mainittu. Erona, että tämä on luottokortin mallinen - Voi olla integroitu henkilökorttiin
<p>Kulkulupa</p>	<ul style="list-style-type: none"> - Paperinen, laminoitu tms. lappu, jossa ilmenee, että henkilöllä oikeus kulkea ja/tai oleskella tilassa tai alueella 	<ul style="list-style-type: none"> - Ei sama asia kuin avain tai kulkutunniste - Henkilökortti ajaa yleensä saman asian kuin kulkulupa
<p>Henkilökortti</p>	<ul style="list-style-type: none"> - Kortti, jossa yrityksen nimi/logo sekä henkilön nimi ja kuva + muuta valinnasta tietoa 	<ul style="list-style-type: none"> - Ei kulkulupa, sillä henkilökortti ei varmenna, että henkilöllä oikeus liikkua omankaan yrityksen kaikissa tiloissa - Voi olla integroitu kulkutunniste
<p>Mekaaninen avain</p> 	<ul style="list-style-type: none"> - Normaali "kova" avain - Esim. Abloy, Kaba, Geze 	<ul style="list-style-type: none"> - Huomiona: Tilassa lisäavaimia on hyvä tietää avaimen malli, esim. Abloy Exec tai Sento - Avaimen leimaus tarkoittaa yleensä juoksevalla numeroinnilla avaimen leimattua tai kaiverrettua numero-/kirjainsarjaa, joka yksilöi avaimen

<p><u>Elektromekaaninen avain</u></p> 	<ul style="list-style-type: none"> - Kulcutunnisteellinen avain - Esim. iLoQ, Abloy Protec Cliq 	<ul style="list-style-type: none"> - Elektromekaanisista avaimista puhuttaessa on hyvä suoraan mainita, minkä merkkisestä avaimesta on kyse
<p><u>Oviympäristö</u></p>	<ul style="list-style-type: none"> - Yksittäinen ovi ja siihen liittyvä ympäristö, kuten lukitus, lukkorunko, karmit, lukijat, vedin, painike, kaapelointi ym. 	<ul style="list-style-type: none"> - Kohdatessa ongelmia oven tai oven lukituksen kanssa, on hyvä tarkistaa oviympäristö päällispuolisesti, mikäli vika paikantuisi oven johonkin tiettyyn osaan - Lukkorungon numero hyvä ottaa ylös ja ilmoittaa huoltotilauksessa
<p><u>Painike</u></p>	<ul style="list-style-type: none"> - Kädensija mistä painetaan, jotta ovi saadaan auki 	<ul style="list-style-type: none"> - Kuultuja termejä: Kahva, ovenkahva
<p><u>Sähköinen ovenavauspainike</u></p>	<ul style="list-style-type: none"> - Nappi, mitä painamalla lukko aukeaa 	<ul style="list-style-type: none"> - Kuultuja termejä: Avausnappi, painike
<p><u>Lukon telki</u></p>	<ul style="list-style-type: none"> - Lukkorungosta telkipesään menevä kieleke 	<ul style="list-style-type: none"> - Kuultuja termejä: Lukon kieli
<p><u>Riippulukko</u></p>	<ul style="list-style-type: none"> - Ulkopuolinen lukko, jonka saa irroitettua lukittavasta kohteesta, kuten oveen kiinnitetystä salvasta tai ketjusta 	<ul style="list-style-type: none"> - Kuultuja termejä: Munalukko - Suomen Vakuutusyhtiöiden keskusliitolla listaus heidän hyväksymistään lukoista
<p><u>Kulkualue / Kulkuoikeusryhmä</u></p>	<ul style="list-style-type: none"> - Kulunvalvonnassa määritellyt tilat/alue, jossa henkilöllä tai tietyllä ryhmällä oikeus kulkea 	<ul style="list-style-type: none"> - Kuultuja termejä: Taso
<p><u>Kulkukoodi</u></p>	<ul style="list-style-type: none"> - Henkilökohtainen pin-koodi, jolla pääsee kulkemaan koodinäppäimistöllä varustetuista ovista, missä koodin kysely on otettu käyttöön 	<ul style="list-style-type: none"> - Ei sama kuin kulcutunnisteen numero - Henkilö- tai yrityskohtainen - Ei saa luovuttaa toisen tietoon
<p><u>Tallentava kameravalvonta</u></p>	<ul style="list-style-type: none"> - Nykyajan mukainen termi kuvansiirtolaitteilla tapahtuvalle aktiiviselle tai passiiviselle kameravalvonnalle 	<ul style="list-style-type: none"> - Kuultuja termejä: Turvakamera, videokamera, videovalvonta - Vaikka puhutaan "valvonnasta", ei tallenteita välttämättä katsota

	- Kameravalvonnan rekisteriseloste määrittelee linjsukset	aktiivisesti, vaan vain jos jotain on sattunut
<u>Käyttölaite</u>	- Rikosilmoitinlaitteiston / hälytinlaitteiston käyttölaite, missä yleensä koodinäppäimistö sekä näyttö	- Käyttölaiteella käytetään järjestelmään keskus on suojatummassa paikassa
<u>Silmukka</u>	- Rikosilmoittimen ilmaisimen nimi ja numero - Hälyttäessä näkyy käyttölaiteella	- Antaa vartiointille, henkilökunnalle tai pääkäyttäjälle tiedon, mistä päin hälytys on tullut - Esim. Lasirikkoilmaisimen silmukka tai passiivisen infrapuna eli PIR- eli liikeilmaisimen silmukka

OSIO 2: KULUNVALVONTA

Kulunvalvontajärjestelmän ylläpitäminen:

Kaikki järjestelmän sisältämät tiedot tulee olla jatkuvasti ajan tasalla. Henkilöitä ja kulkuoikeuksia koskevat muutokset tulisi ilmoittaa mieluiten etukäteen, kuitenkin mahdollisimman pian kun muutostarve ilmenee. Kulkutunnisteen katoamistapauksessa muutostarve on kriittinen ja ilmoitusajalla on suuri vaikutus turvallisuuteen. Kulunvalvonnan pääkäytön tehtävistä on sovittava tarkemmin palvelusopimuksessa.

Kulkutunnisteet

Kuittauskäytännöt:

Kulunvalvontajärjestelmä ja sen sisältämät tunnistehallinnalliset tiedot saadaan pysymään dokumentoidusti ajan tasalla, kun jokainen luovutettu ja palautettu kulkutunniste on kuitattu luovutetuksi tai palautetuksi. Ilman kuittauksia on vaikea todentaa vastuullista osapuolta esimerkiksi tunnisteiden katoamistilanteissa.

Tämän oppaan liitteistä löytyy yksinkertainen malli kuittauslomakkeesta, joka sisältää tarvittavat tiedot. Kuittaamistilanteessa on kuitenkin tärkeä vielä mainita siitä, että kun tarve kulkutunnisteelle päättyy tai tunniste katoaa, tulee siitä ilmoittaa mahdollisimman pikaisesti tai se tulee palauttaa pääkäyttäjälle. Palautumattomat tunnisteet voivat aiheuttaa huomattavia lisäkustannuksia kulunvalvontaan, mikäli organisaatiolle joudutaan tilaamaan lisää tunnisteita siitä syystä, että käyttäjät eivät palauta ylimääräisiä tunnisteita takaisin.

Uuden luominen:

Jokainen kulkutunniste on henkilökohtainen, joten kaikille tunnisteille tarvitaan henkilötiedot tai muu yksilöllinen tieto, jolla tunnisteiden haltija pystytään tunnistamaan.

Kiinteistön tai yrityksen vuokratilojen kulkutunnistetarpeita tarkastellessa tulee ottaa huomioon eri käyttäjäryhmät:

- Sisäinen henkilöstö - tunnisteita saman verran kuin henkilöstöä
 - Pääkäyttöpyyntöjä voidaan tehokkaasti vähentää siten, että yrityksellä on henkilöstön koosta riippuen esim. 1 varatunniste 25 henkilöä kohden, joita voidaan hyödyntää esimerkiksi tilanteissa, jossa kulkutunniste on unohtunut kotiin
- Ulkoinen henkilöstö (mm. vartiointi, siivouspalvelut, vierailijat, lähetit, mattojenvaihtajat, remontointi, huoltoym.)
 - Pääkäyttöpyyntöjä voidaan tehokkaasti vähentää siten, että yrityksellä on ulkoisien palveluntoimittajien määrästä riippuen X määrä ns. huolto- tai vierailijatunnisteita, jotta lyhytaikaisia vierailuja tai remontointijaksoja varten ei tarvitse erikseen tehdä aktiivointia ja kuolettamista

Mikäli tunnisteista tulee taas määrääjäksi lainattavia varatunnisteita tai henkilötietoja ei haluta ilmoittaa, voidaan nämä nimetä/yksilöidä myös esim. nimellä *Yritys NN varatunniste 1-X*. Tällöin vastuu tunnisteilla tehtyjen kulkutapahtumien selvittämisessä on tunnisteiden luovuttajalla, eli henkilöllä, jolla on kirjanpito tunnisteista ja kuittaukset niiden luovutuksista ja palautuksista.

Tällaisessa selvittämistapauksessa, jossa tunnisteita ei ole nimetty tietokantaan, pääkäyttäjä pystyy ainoastaan kertomaan, että esim. *Yritys NN varatunniste 3* on kulkenut jostain ovesta. Vastuuhenkilön kirjanpidosta täytyy tällöin selvittää, kellä kyseinen varatunniste 3 on ollut tuolloin käytössä.

Kulcutunnisteiden tilauksissa / aktivointipyyntöissä tulee ilmetä seuraavat tiedot:

- Kulcutunnisteen numero
- Henkilön nimi
- Henkilön yritys - ja muut mahdolliset yksilöintitiedot (kustannuspaikka, henkilönumero, rooli/työnkuvaus tms. → Nämä räätälöitävä yrityskohtaisesti, mitä tietoja halutaan tietokannassa pidettävän.
- Kulkuoikeusryhmän nimi / tunnus
- Voimassaoloaika: Toistaiseksi vai määräajaksi
- Tarve pin- / kulkukoodille
- Mikäli tunniste on siirretty suoraan henkilön käytöstä toiselle, on hyvä ilmoittaa myös tämä lisätietona
 - Myös; mitä tunnisteen edelliselle haltijalle tehdään. Onko tarkoitus muuttaa edellinen haltija poistettavaksi

Tunnisteen kuolettaminen:

Kun kulcutunniste katoaa tai henkilöllä loppuu työsuhde = kun tarve kulcutunnisteelle loppuu
→ tunniste tulee deaktivoida mahdollisimman pian.

Pääkäyttäjän tarvitsee tietää seuraavat asiat kuolettamispyyntöön liittyen:

- Kulcutunnisteen numero
- Henkilön nimi
- Onko tunniste kadonnut tai henkilöllä loppunut työsuhde
 - Mahdolliset lisätiedot: Otetaanko aktivointi pois määräajaksi (esim. äitiysloma, varusmiespalvelus), eli tiedetään henkilön vielä myöhemmin käyttävän tunnistetta
- Huom. Mikäli kulcutunniste on tiedettävästi jäänyt esimerkiksi kotiin, ei tunnistetta tarvitse kuolettaa, vaan käyttöön voidaan ottaa varatunniste siksi aikaa, kunnes oma tunniste saadaan takaisin

Pääkäyttäjälle: Henkilötietojen ja kulkutapahtumien poistokäytännöt voidaan sopia yritys- / tapauskohtaisesti. Alla suuntaviivojen mukaiset suositukset ja huomiot:

- Kulunvalvontajärjestelmässä olevat henkilötiedot muodostavat henkilörekisterin
 - Henkilörekisterin käsittelyn syyt tulee ilmetä *Kulunvalvonnan rekisteriselosteessa*
- Rekisteriselosteeseen voidaan vapaasti määrittellä henkilötietojen ja kulkutapahtumien säilyttämisaika
 - Suositus: 1 vuosi
 - Perustelu: Mahdollisten rikostapausten selvittäminen kulkutapahtumia hyödyntäen
- Jotta aktiiviset ja deaktiiviset henkilöt / kulcutunnisteet voidaan erottaa järjestelmästä, olisi henkilötiedoissa suositeltavaa ilmetä jokin seuraavista:
 - Nimen perässä merkintä / *Ei käytössä* - nimet säilyvät aakkosjärjestyksessä
 - Nimen edessä merkintä * tai # - deaktivoidut näkyvät aakkosjärjestyksessä ensimmäisenä
 - Yritys- tai osastotieto *Lopettaneet* poistuneille henkilöille

Kulkuoikeudet

Uusien kulkuoikeuksien / kulkualueiden aktivointi- tai muutospyyntöissä tulee ilmetä sekä määrittelyissä huomioida:

- Kulkualueen numero/tunnus/nimi (nimeämiskäytäntöjen oltava yhteneväisiä tietokannan muiden kulkualueiden kanssa)
- Milloin kulkuoikeuksien astuttava voimaan
- Mitä tarkoitusta varten uusi kulkualue on
 - Onko uusi vuokralainen / uudet vuokratut tilat
 - Onko uusi kulkualue jo olemassa olevalle organisaatiolle
 - Voimassaoloaika: Toistaiseksi vai määräajaksi
 - Tuleeko uusi alue vanhantilalle → poistetaanko jokin tämän tilalta
- Mihin oikeudet:
 - ovet
 - portit
 - työaika- tai maksupäätteet
 - hissit + hissikerrokset

Kulkuoikeuksien antaminen henkilöille:

Henkilöllä tulisi olla kulkuoikeudet kaikkiin niihin ovipäätteisiin, jotka henkilön kulkemisen kannalta ovat oleellisia ja tarpeellisia. Myös leimausoikeudet voidaan antaa kaikkiin niihin työajanseurannan sekä maksupalveluiden päätteisiin, joihin oikeudet katsotaan hyödyllisiksi. Mitään erityistä sääntöä, lakia eikä asetusta ole, joka määrittelisi tarpeelliseksi katsottavat ovet. Suosituksena kulkuoikeuksien määrittelyä varten on hyvä huomioida seuraavat suuntaviivat:

- Mikäli henkilön ei koskaan tarvitse päästä tiettyyn tilaan tai alueelle, voidaan niiden tilojen kulunvalvonnan piirissä olevat ovet rajata oikeuksista pois
- Kulkuoikeuksien tai kulunhallinnan ei ole tarkoitus estää tai haitata kulkemista
 - Liian tiukkoja rajoituksia ei siis kannata tehdä
- Kulkualueiden kunnollisella suunnittelulla voidaan parantaa alueiden ja kulkureittien loogisuutta, käytettävyyttä sekä toiminnallisuutta
- Rajoituksia voidaan myös tehdä kellonaikojen perusteella siten, että tietyistä ovista ei pääse kulkemaan esimerkiksi työaikaliukuman päätyttyä
- Pienemmässä mittakaavassa kulkuoikeudet voidaan määrittellä henkilökohtaisesti jokaiselle kulkutunnisteen haltijalle
- Isommissa organisaatioissa kannattaa miettiä tiettyä rooli-, osasto- tai kustannuspaikkajakoa tms., jolloin esimerkiksi johtoryhmä saa laajemmat johtoryhmän kulkuoikeudet, IT-osaston henkilöstö saa ITC-tilojen kulkualueen tai kustannuspaikan X henkilöstö saa tietyn kulkualueen
- Järjestelmän ylläpitämisen, asiakkaan ja pääkäyttäjän kaikkien puolesta edullisinta olisi, että yksittäisellä henkilöllä olisi mahdollisimman vähän kulkualueita
 - Ovikohtaiset päällekkäisyydet kulkuoikeuksissa vähenee, kun henkilölle ei tarvitse luoda kulkuoikeuksia useista eri kulkualueista
- Vaikka yhden laajan, ns. ”kaikki ovet aina” -kulkualueen antaminen on helppoa ja pääkäyttötyön määrä kulkuongelmien takia varmasti ovat vähäiset, niin tätä ratkaisua ei turvallisuusnäkökulmista suositella
 - Vaikka kulkutapahtumista jää jälki kulkulokiin, niin tarpeetonta kulkemista on helpompi rajoittaa ja hallita ennakoiden, kuin myöhemmin selvittellen

Kulunvalvontajärjestelmän aloitustyöt / siivousprojekti:

Aloitustyöllä tarkoitetaan niitä määrityksiä ja tehtäviä, jotka tehdään järjestelmää tai palvelua toimeenpantaessa. Kulunvalvontajärjestelmää käyttöönottaessa, varsinkin vanhaa järjestelmää pääkäyttöön otettaessa eli tietokantaa siivotessa on huomioitava ja tehtävä seuraavat toimenpiteet:

Kulunvalvontajärjestelmä:

- Kulunvalvontajärjestelmän ikä, kunto, päivitykset

- Mikäli järjestelmä on uusi ja tietoja sisältämätön, voi vanhoja tietoja käsittelevät osiot jättää huomiotta ja tietojen (kulkualueet, henkilötiedot jne.) luomisen voi aloittaa suuntaviivojen mukaisesti.
- Mikäli pääkäyttö siirtyy sellaisenaan jo olemassa olevassa muodossa vanhoine tietoineen, on tärkeää tarkastaa/tarkastuttaa järjestelmän kunto teknisellä ja fyysisellä tasolla, jotta voidaan minimoida iän ja ajan tuomat häiriötekijät. Lisäksi on tärkeää tarkastaa järjestelmäversion mahdolliset uudet päivitykset, jotta pystytään myös varautumaan jatkuvuussuunnittelun mukaisesti kulunvalvonnan keskeytyksettömyyteen. Tähän vaikuttaa esimerkiksi tuotannosta poistuvat osat ja vanhojen versioiden korjauspäivitykset järjestelmäntoimittajan osalta.

Järjestelmän tietokanta:

- Järjestelmästä on syytä ottaa lähtötilanteen tiedot talteen, jotta tilaajalle voidaan näyttää toteen tehty työ ja jotta voidaan tiedostaa ns. siivoamattoman kannan aikaisemmin aiheuttamat turvallisuusriskit. Näitä tietoja ovat:
 - Kulcutunnisteiden määrä
 - Vaikuttaa olennaisesti käytettävyyteen, tietojen paikkansapitävyyteen sekä turvallisuuteen. Mitä enemmän ylimääräisiä (aktiivisia) kulcutunnisteita kannasta löytyy, sitä enemmän riskejä ne aiheuttavat. Tiedoista tulisi löytyä vain käytössä oikeasti olevat tai varalle kirjatut tunnisteet sekä deaktiiviset tunnisteet/lopettaneet henkilöt eroteltuna.
 - Yritykset
 - Vanhoja yritystietoja on turha säilyttää. Järjestelmästä tulisi yritystiedoista suoraan nähdä sen hetkiset vuokralaiset, yritykset, osastot, jaokset ym.
 - Kulkualueet
 - Kulkualueiden tarkastaminen ja tarvittaessa uudelleen määrittäminen, mikäli havaitaan liian laajoja oikeuksia tai päällekkäisyyksiä. Kulkualueita olisi oltava vain sen verran kuin alueiden mukaan rajattuja pääsoikeuksia tarvitaan. Varsinkin isoissa liikekiinteistöissä yritys saattaa vuokrata useita eri tiloja eri kerroksista. Tällöin vanhoja kulkualueita ei tulisi olla riskitekijänä, jotta väärä ihminen pääsisi väärin tiloihin.
 - Kulunvalvonnasta mahdollisesti poistuneet / ylimääräiset ovet. Nämä syytä poistaa järjestelmästä, jotta ne eivät pääse aiheuttamaan epäselvyyksiä
 - Aikaryhmät/kellonajat
 - Mikäli järjestelmään on määritetty kellonaikoja esimerkiksi rajaamaan kulkuoikeuksia vain päiväsaikaan arkisin tai ovien aukiohjauksia varten, on ylimääräiset syytä poistaa, jotta kulkuoikeuksiin tai oviohjauksiin olisi vähemmän mahdollisuuksia määritellä virheellinen ajastus.
 - Nimeämiskäytännöt
 - Mitä/minkälaisia käytäntöjä järjestelmässä on käytetty esimerkiksi kulkualueen, oven tai henkilön nimeämisessä. Nämä tulisi yhtenäistää suuntaviivojen suositusten mukaisesti esim. *Sukunimi Etunimi* -

muotoon tai kulkualueessa jokainen alkaa kerroksittain esim. 3. kerros toimistotilat.

- Ovien nimeämisessä tulee välttää yritysten nimiä tai muita mahdollisia usein vaihtuvia nimiä. Huoneiden tai tilojen käyttötarkoitukset voivat muuttua tai tila voidaan vuokrata toiselle yritykselle, ja tällöin uudelleennimeäminen teettää ylimääräistä muutostyötä.
 - Ulko-ovet on hyvä merkitä lyhenteellä UO, jotta ulkokuoren ovet voidaan havaita mahdollisimman helposti
- Nimeämiset tulee olla sellaiset, että ne voidaan ymmärtää mahdollisimman helposti kenenvain näkökulmasta
 - Huono esimerkki: *Duunariovi* tai *Yritys X postitus PRS*
 - Hyvä esimerkki: *1.krs länsipäätyporraskäytävä UO* tai *2.krs toimistoh. 201*

Lisäksi:

- Mikäli kulunvalvonnan mukana kiinteistön tunnistehallinta siirtyy samalla pääkäyttöyritykselle, on kulkutunnisteet inventoitava ja niitä on oltava tarpeeksi varalla isompiakin tilauksia varten
- Yhteyshenkilöiden informoiminen palvelun toimintatavoista ja valtuuttaminen yrityksen kulunvalvonnan yhteyshenkilöiksi, jolla oikeus tehdä tilauksia sekä muutospyyntöjä liittyen yrityksen kulkutunnisteisiin, -tapahtumiin ja -oikeuksiin
 - Järjestelmän toiminta-alueella olevien kiinteistön vuokralaisiin on otettava yhteys ja ilmoitettava palvelun alkamisesta. Aloitustöiden yhteydessä tämä on ehdottoman tärkeää, että jokaisella vuokralaisella on virallinen kulunvalvonnan yhteyshenkilö. Mikäli kuka vain saisi pyytää muutoksia tai lisäoikeuksia, ei turvallisuustasoa voitaisi taata.
- Yhteyshenkilöiltä tiedusteleminen yrityksen käytössä ja hallussa olevista kulkutunnisteista ja mahdollisista varatunnisteista
 - Yrityksen oman tahdon mukaan nimilistan toimittaminen pääkäyttäjälle, jotta järjestelmässä näkyy kaikkien kulkutunnisteiden haltijoiden tiedot tarkkaan
 - Vaihtoehtona yritys pitää tiedot itsellään ja pitää huolen päivittämisestä ja omasta kirjanpidosta. Tällöin nimeämiskäytäntönä toimii esim. Yritys X / 1- (juokseva numero)
 - Tämä on helpoin ja vaivattomin tapa selvittää tarpeelliset kulkutunnisteet ja henkilötiedot tietomassasta. Ulkoinen pääkäyttäjä ei todennäköisesti muutoin pysty edes selvittämään todellisia/oikealla asialla kiinteistössä liikkuvia henkilöitä.
- Mikäli muita käyttäjiä tai yrityskohtaisia pääkäyttäjiä; näiden tunnusten ja käyttöoikeuksien tarkistus
 - Muut mahdolliset käyttäjät, käyttäjätunnukset sekä -oikeudet tulee tarkastaa, sillä ihannetilana on, että samoja tietoja hallinnoi sujuvan tiedonvälityksen vuoksi vain yksi pääkäyttäjä tai organisaatio.
- Järjestelmän/palvelimen kesä- ja talviaikojen huomioiminen, jotta mm. ovien lukitukset toimisivat oikein

OSIO 3: AVAINHALLINTA

Lukoston ylläpitäminen:

Kaikki lukoston sisältämät tiedot tulee olla jatkuvasti ajan tasalla. Avaimia, lukkoja ja avainten haltijoita koskevat muutokset tulisi ilmoittaa mahdollisimman pian kun muutostarve ilmenee. Uusien avainten ja lukkojen sarjoitusten tilauksissa menee toimittajasta riippuen useampi päivä, mutta lähtökohtaisesti lukoston haltija voi saada uudet avaimet tehtaalta aikaisintaan seuraavana arkipäivänä. Avaimen katoamistapauksessa muutostarve on kriittinen ja ilmoitusajalla on suuri vaikutus turvallisuuteen.

Avaimet:

Kuittauskäytännöt:

Lukosto ja sen sisältämät avainhallinnalliset tiedot saadaan pysymään dokumentoidusti ajan tasalla, kun jokainen luovutettu ja palautettu avain on kuitattu luovutetuksi tai palautetuksi. Ilman kuittauksia on vaikea todentaa vastuullista osapuolta esimerkiksi avainten katoamistilanteissa. Lisäksi ajankohtaiset tiedot on päivitettävä avainhallintajärjestelmään.

Tämän oppaan liitteistä löytyy yksinkertainen malli avainten/kulikutunnisteiden kuittauslomakkeesta, joka sisältää tarvittavat tiedot. Kuittauslomakkeessa on kuitenkin tärkeä vielä mainita siitä, että kun tarve avaimelle päättyy tai avain katoaa, tulee siitä ilmoittaa välittömästi tai mahdollisimman pikaisesti tai se tulee palauttaa pääkäyttäjälle. Palautumattomat avaimet voivat aiheuttaa huomattavia lisäkustannuksia, mikäli ovi/ovia joudutaan sarjoittamaan uudelleen. Mitä vahvemmasta avaimesta on kyse, sitä suuremmalla syyllä asiakkaan on syytä olla tietoinen riskeistä ja avaimen katoamisesta johtuvista kustannuksista.

Avainten katoamiset / sarjoitustyöt:

Lukkojen uudelleensarjoituksia tehdään tarpeiden mukaisesti, asiakkaan tai kiinteistön edustajan toiveiden tai määräysten perusteella. Tilauksissa tulee ottaa huomioon, että pyyntö tulee oikealta yhteyshenkilöltä ja kiinteistön omistaja/manageri on hyväksynyt lukoston muutoksen. Myös tilauksen maksaja tulee olla selvillä ennen muutoksen täytäntöönpanemista.

Kun avain katoaa, on uudelleensarjoitus hyvin todennäköistä ja toivottavaa. Mikäli kyseessä on vahva avain, kuten yleisavain tai tarkkaan suojellun tilan avain, olisi suositeltavaa tehdä pikasarjoitus ns. ”villiin” sarjaan uudelle avaimelle siksi aikaa, kunnes uusi sarjoitus on valmis asennettavaksi. Myös paikallisvartiointia voidaan asiakkaalle suositella.

Muuta:

Pääkäyttäjän tulee huolehtia, että kiinteistön avainsäilytyksessä eli ns. putkilukossa on sinne kuuluva avain. Avainsäilytyksessä ei saa säilyttää kiinteistön yleisavainta, vaan putkilukoissa on oltava reittiavaimet huoltokohteelle, paloilmotimelle tai sisäputkilukon luokse. Sisäputkilukkoon voidaan suunnitella kiinteistön kulunvalvonta- tai yleisavain sekä kulikutunniste kaikilla oikeuksilla.

Pääkäyttäjän tulisi lukitusturvallisuuden näkökulmasta suositella avainhallinnan kohdeasiakkaita päivittämään avainjärjestelmä sellaiseksi, jossa patenttisuoja ei ole päättynyt. Tämä on ainut keino olla varma siitä, ettei avaimia voi teettää ilman pääkäyttäjän tietoa.

Avainhallinnan aloitustyöt / siivousprojekti:

Avainhallinnan käyttöönottaessa, varsinkin vanhaa lukostoa ja avainhallintaa pääkäyttöön siirrettäessä on huomioitava ja tehtävä seuraavat toimenpiteet:

Lukostokansio:

Ensimmäinen vaihe avainhallinnan pääkäyttöä aloitettaessa on lukostokansion/kansioiden vastaanottaminen sekä tarpeellisten dokumenttien tarkastaminen lukostokansiosta. Riippuen kohteesta, voi lukosto olla hyvinkin vanha. Aiempi hallinnointi on voinut olla esimerkiksi kiinteistömanagerilla, huoltoyhtiöllä, lukkoliikkeellä tai toisella pääkäyttöyrityksellä, joten hallinnointitapojakin on varmasti hyvin erilaisia. Uuden kiinteistön lukostokansio voidaan myös vastaanottaa suoraan rakennuttajalta tai lukkotehtaalta.

Jotta avainhallinnan pystyy viemään suuntaviivojen mukaiseen formaattiin, olisi lukostokansiossa olla seuraavat dokumentit:

- Lukostonumero, avainkortti ja tunnusluvut tilauksia varten
- Lukituskaavio
- Avainlistaus
- Avainkuittaukset
- Sijoitusohjekuvat
- Lukoston lisätiedot ja yleiset ohjeet

Mikäli kaikkia ei löydy, on hyvä selvittää onko kyseisiä dokumentteja koskaan ollut ja onko niitä vielä jostain saatavilla.

Lukoston sisältö:

Lähtötilanteen dokumentointi samaan tapaan kuin kulunvalvonnan osalta:

- Lukoston kunto, ikä, turvallisuus
 - Listauksen mukainen selvitys esimerkiksi kadoksissa olevista avaimista ja näiden vaikutus lukitusturvallisuuden kokonaisuuteen

→ Tärkeiden ja kriittisten avainten, kuten yleisavain, huoltoavain tai kulunvalvottujen ovien yleisavain eli kv-avain, varmistaminen, että kuittauksen tehneellä henkilöllä on kyseinen avain hallussaan

Lisäksi:

- Mikäli paperista listausta tai sähköistä versiota avaintenhaltijoista ei ole, on syytä siirtää ja koota tiedot avaimista ja avaintenhaltijoista yhdelle listalle, suuntaviivojen mukaiseen, pääkäyttöyrityksen mahdollisesti räätälöimään yhteiseen formaattiin, jotta tiedetään kellä mikäkin avain on hallussaan.
- Lukitussuunnittelussa tulee noudattaa samankaltaisia suuntaviivoja kuin kulunvalvontajärjestelmän kulkuoikeusryhmien suunnittelussa. Mikäli lukoston käyttöoikeudet eivät ole ajan tasalla, tulee lukitussuunnitelmassa määritellä eri

käyttäjäryhmien kulkuoikeustarpeiden mukaiset sarjoitukset niin, että kukin avaimen haltija pääsee vain niihin tiloihin, joihin hänellä on tarve päästä. Suuria yhtenäisiä yleisavainsarjoja tulee välttää.

- Kun edellä mainitut aloitustyöt on saatu päätökseen, tulee avainhallinnan turvallisuustaso arvioida lopullisessa pääkäyttöformaattissa ollessaan.
- Myös avainhallinnan kirjanpidosta ja sen oheistiedoista muodostuu henkilörekisteri, riippumatta millä keinoilla sitä suoritetaan. Avainten haltijoilla ja lukkojen käyttäjillä on kuitenkin palvelussuhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan, jolloin ilmoitusvelvollisuutta avainhallinnan rekisteristä ei ole. Rekisteriselosteen olemassaoloa kuitenkin suositellaan, että yhteiset linjaukset koskien henkilötietojen keräämistä löytyvät tarvittaessa nopeasti.
- Palveluntilaaaja tulee tiedottaa lähtötasosta ja formaattissa olevasta tasosta mahdollisine puutteineen ja jatkotoimenpidesuosituksineen, esim. sarjoitustyöt kadonneiden avainten takia. Täten palveluntilaaajalle siirretään vastuu lukoston sen hetkisestä turvallisuustasosta.

OSIO 4: KAMERAVALVONTA

Kameravalvontajärjestelmän ylläpitäminen:

Kaikki järjestelmän sisältämät kamerat tulee olla jatkuvasti ajan tasalla ja toimintakunnossa. Uusia kameroita, suuntauksia, valaistusten muutoksia koskevat tiedot tulisi ilmoittaa mieluiten etukäteen, kuitenkin mahdollisimman pian kun muutostarve ilmenee. Kameran häiriö-, vika- tai ilkeätilanteissa huoltotarve on lähtökohtaisesti kriittinen ja ilmoitusajalla on täten merkittävä vaikutus turvallisuuteen.

Kamerat ja tallennin:

Ylläpitotilassa olevan kameravalvontajärjestelmän pääkäyttöisiin tehtäviin kuuluu lähtökohtaisesti kameroiden ja tallentimen toiminnan testaaminen, sekä rikos- tai hälytystapauksissa selvitystehtävät ja mahdollisten tallenteiden ottaminen ja eteenpäin toimittaminen. Tehtävistä on sovittava tarkemmin palvelusopimuksessa.

Kameravalvonnan pääkäyttö voi olla joko etäkäyttöä tai passiivista valvontaa. Mahdollinen aktiivinen valvonta tulisi suorittaa esimerkiksi vartiointin toimesta. Käyttäjäorganisaation rakenne liikekiinteistössä voi olla seuraavanlainen:

1. Pääkäyttäjä/järjestelmänvalvoja

- etävalvoja tai passiivinen valvoja
- hallinnoi kaikkien käyttäjien toimintoja
- luo käyttäjäprofileja
- voi lukea, katsella ja tallentaa tallenteita sekä tapahtumalokeja
- tallentimen asetuksen muokkaaminen

2. Käyttäjä/vartija

- aktiivinen valvoja
- näkee kameroiden ja tallentimien kuvia
- pystyy tarvittaessa ohjaamaan kameroita
- osaa tallentaa ja luovuttaa materiaalia järjestelmästä viranomaisille.

3. Kehittäjä/järjestelmän toimittaja

- omaa käyttäjätunnuksen, joka sisältää kaikki pääkäyttäjän toiminnot
- tekee ohjelmistopäivitykset
- lisää ja poistaa laitteita järjestelmästä
- tekee muita pääkäyttäjän haluamia toimintoja.

Pääkäyttäjä ei ole taho, joka lähtökohtaisesti olisi mukana kameravalvonnan suunnittelemisessa, mutta pääkäyttäjän on hyvä sisäistää suunnittelun tarveselvityksessä määritellyt asiat:

- Mitä ja miksi halutaan kuvata?
- Missä ja milloin kuvia katsellaan?
- Miten kuvien tallennus, kuvansiirrot ja kuvien katselupisteet toteutetaan?

- Mitä lain mukaan saa ja voi kuvata?
- Kenelle tallenteita luovutetaan?

Lisäksi kameravalvonnan laillisuuteen liittyvistä asioista on pääkäyttäjän oltava tietoinen. Lakien ja oikeuskäytännön perusteella kameravalvonnan laillisuus riippuu eniten seuraavista tekijöistä:

- Kuka valvontaa suorittaa?
- Missä tarkoituksessa valvontaa suoritetaan?
- Missä paikassa oleskelevaan henkilöön valvonta kohdistuu?
- Onko kysymyksessä pelkkä katselu vai myös kuvan tallentaminen?
- Kuunnellaanko tarkkailtavaa tai talletetaanko puhetta?
- Kuinka salaista tai avointa valvonta on, eli miten valvonnasta on ilmoitettu?
- Mihin talletettuja tietoja käytetään ja kuinka kauan niitä säilytetään?
- Luovutetaanko tietoja johonkin tarkoitukseen?

(Kameravalvontaopas 2010)

Näillä tekijöillä lainsäädännön vaatima avoimuus kameravalvonnan toteuttamisessa saadaan toteutumaan.

Tallenteiden käsittely

Koska pääkäyttäjä ja mahdolliset käyttäjät (esim. vartiointi) voivat ottaa tallentimesta tallenteita, voidaan Kameravalvontaoppaan (2010, 46) osiota 6.2 *Tallenteiden käsittely* hyödyntää pääkäytön suurtaviivoihin kokonaisuudessaan:

- ”Tallenteita käytetään lähtökohtaisesti vain niihin tarkoituksiin, joita varten valvontaa on suoritettu. Tallenteiden käsittelyssä on noudatettava henkilötietolain periaatteita.
- Tallenteet on suojattava siten, että asiaton ja oikeudeton käyttö on estetty. Kun tieto on käsitelty ja säilytetty määritellyn ajan, se pyyhkiytyy automaattisesti kovalevyiltä uuden tiedon myötä.
- Mahdolliset ylimääräiset tulosteet ja tallenteet on hävitettävä niiden käytyä tarpeettomiksi. Vanhoja tallentimia hävitettäessä on kovalevyjen tietosisältö tuhoettava asianmukaisesti.
- Tallenteita ei saa käyttää tai tulostaa sukupuolisiveyttä loukkaavasti.
- Mahdolliseen esitutkintaan tai muuhun tutkintaan liittyvää materiaalia saa tarvittaessa säilyttää pidempäänkin tapahtumailmoitusten liitteenä. Tapahtumailmoituksissa on hyvä viitata kuvatallenteen olemassaoloon. Viranomaisille luovutetuista tallenteista ja niiden käyttämisestä vastaa asianomainen viranomainen.
- Vartiomistehtävissä havaituista rikoksista ja niissä epäillyiksi tai syylliseksi todetuista henkilöistä ei saa muodostaa omia rekistereitä. Sen sijaan esitutkintaviranomaisille voi sovittuja tietojenvaihtokanavia pitkin lähettää vihjeitä havaituista rikoksista. Tämän jälkeen esitutkintaviranomainen informoi parhaaksi katsomallaan tavalla muita toimijoita rikoksen vaarasta.”

Dokumentointi

- Kaiken dokumentaation on oltava sen tasoista, että järjestelmän huolto ja ylläpito onnistuu myös kolmannelta osapuolelta.

- Kaikkia kameravalvontaan liittyviä dokumentteja on säilytettävä siten, etteivät ne vahingossa joudu asiattomiin käsiin.
- Lopullinen käyttöönotton dokumentointi palvelee kameravalvontajärjestelmän käyttöä, ylläpitoa ja huoltoa. Dokumentoinnin on oltava riittävän tarkka. Siihen on kirjattava kaikki asennetut laitteet, laitteiden sijainnit ja ohjelmistot.

Kameravalvonnan pääkäyttäjää ensisijaisesti koskevat lait:

- Rikoslaisissa kameravalvontaa koskevat säädökset ovat 24 luvussa (531/2000), jossa säädetään yksityisyyden, rauhan ja kunnian loukkaamisesta
- Rikoslain 24 luvun 8 §:ssä säädetään yksityiselämää loukkaavasta tiedon levittämisestä
- Kameravalvontaa sivuaa rikoslain 38 luvun 9 §:n (525/1999) henkilörekisteririkos
- Salakatseluun syyllistyy rikoslain 24 luvun 6 §:n mukaan henkilö, joka oikeudettomasti teknisellä laitteella katselee tai kuvaa kotirauhan suojaamassa paikassa, käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaa henkilöä
- Laki yksityisyyden suojasta työelämässä (759/2004) ja siihen liittyvät yhteistoimintalain säännökset säätelevät kameravalvonnan käyttöä työpaikoilla ja virastoissa
- Lisäksi laki yksityisistä turvallisuuspalveluista (282/2002) kohdistuu turvasuojaustoimintaan

Kameravalvonnan aloitustyöt / siivousprojekti

Kameravalvontajärjestelmää käyttöönottaessa, varsinkin vanhaa järjestelmää pääkäyttöön otettaessa on huomioitava ja tehtävä seuraavat toimenpiteet:

Kamerat, tallennin ja järjestelmä:

- Kameravalvontajärjestelmän ikä, kunto ja tehdyt huollot
 - Sen hetkisen tilan kartoitus, jotta tiedetään onko järjestelmä vielä nykypäivän vaatimuksia vastaava ja voiko sen tarvittaessa tuoda sille tasolle, sekä onko vara- tai lisäosia saatavilla.
- Tarkastettava päivitysmahdollisuudet
 - Mikäli ohjelmiston voi päivittää, kannattaa toiminnan varmuudeksi hankkia uusin versio
- Yksittäisten kameroiden toiminta
 - Tarkastettava kuvaako jokainen kamera ja kuinka monesta toimivasta sekä rikkinäisestä kamerasta järjestelmä koostuu
- Tallentimen ja tallenteiden toiminta
 - Tarkastettava, että löytyykö jokaisen kameran kuvasta tallenteet halutulta (ja rekisteriselosteen mukaisesti määritellyltä) ajalta tallenteet
- Tallentimen suorituskyky ja suoritinkäyttö
 - Toiminnan ja jatkuvuuden kannalta on syytä tarkistaa, millä suoritinkäytöllä järjestelmä on käytössä ja voidaanko asetuksia muuttaa. Jatkuva kapasiteetin maksimikäyttö ei ole hyväksi tallentimelle. Myös tallentimen fyysinen sijainti voi kasvattaa toimintaikää (palvelinräkkikaapissa vs. lattialla pölyssä)
- Kuvanlaadun tarkastus ja mahdolliset tai tarvittavat säädöt/parannukset
 - Liittyen edelliseen suorituskykyyn; mahdollisuuksien mukaan voidaan parantaa kuvanlaatua, esim. fps (=frames per second) tai resoluutiota.
- Kameroiden suuntauksien tarkastus ja tarvittaessa uudelleensuuntauksen tilaus

- Kameran voidaan kohdekäynnillä itse suunnata paremmin mikäli mahdollista. Voidaan myös tilata huollolta

Lisäksi:

- Etäyhteyksien toiminta
 - Etäyhteydellä tulisi pystyä katsomaan live-kuvaa sekä tallenteita mutkattomasti, ilman että kuvanlaatu heikkenee tai kuva pätkii. Yhteys myös salattava asianmukaisesti
- Salasanan vaihto, mikäli oletussalasanana tai muutoin yksinkertainen
 - Minimoitava mahdollisuudet, että kukaan ulkopuolinen pääsisi käsiksi kameroihin tai tallenteisiin
- Järjestelmän/ palvelimen kesä- ja talviaikojen huomioiminen, jotta tallenteissa näkyy oikea kellonaika

(Hulkkonen 2014; Ukkonen 2014)

OSIO 5: RIKOSILMOITTIMEN HALLINTA

Rikosilmoitinjärjestelmän ylläpitäminen

Kaikki järjestelmän sisältämät tiedot ja ilmaisimet tulee olla jatkuvasti ajan tasalla ja toimintakunnossa. Uusia ilmaisimia, silmukoita ja aikataulumuutoksia koskevat tiedot tulisi ilmoittaa mieluiten etukäteen, kuitenkin mahdollisimman pian kun muutostarve ilmenee. Ilmaisimen häiriö-, vika- tai ilkeätilanteessa huoltotarve on lähtökohtaisesti kriittinen ja ilmoitusajalla on täten merkittävä vaikutus turvallisuuteen.

Järjestelmä ja käyttölaitteet

Ylläpitotilassa olevan rikosilmoitinjärjestelmän pääkäyttöisiin tehtäviin kuuluu lähtökohtaisesti järjestelmän ja ilmaisimien toiminnan säännöllisen testaamisen varmistaminen, sekä rikos- tai hälytystapauksissa selvitystehtävät liittyen hälytysaikoihin, hälyttäneisiin silmukoihin ja lokitapahtumiin. Lisäksi hallinnointiin kuuluu hälytysalueiden/-vyöhykkeiden luominen, henkilökohtaisten pin-koodien tekeminen, muuttaminen ja toimittaminen sekä poikkeusjärjestelyiden tekeminen hälytysajankohtiin. Tehtävistä on sovittava tarkemmin palvelusopimuksessa.

Pääkäyttäjän tulee ymmärtää rikosilmoitinjärjestelmää pääkäyttäessään järjestelmän perimmäinen tarkoitus, eli se, mitä suojellaan, miksi ja millä tasolla. Suojaustaso riippuu rikosvahingon todennäköisyydestä ja vahingon seurauksista. Finanssialan Keskusliiton Kohteen murtoriskien arviointi ja suojaustason valinta -ohje (2008) mukaan suojaustasoluokkia on neljä:

- Alhainen suojaustaso (1)
- Keskimääräinen suojaustaso (2)
- Korkea suojaustaso (3)
- Erittäin korkea suojaustaso (4)

Rikosilmoitinjärjestelmän yleisimmät ilmaisimet:

- liiketunnistimet
- magneettikoskettimet
- lasirikkoilmaisimet
- ryöstöpainikkeet
- seismiset -, savu- sekä kosteusilmaisimet

Silmukkatyyppejä on useita erilaisia ja pääkäyttäjän on hyvä tutustua näiden tuomiin eri mahdollisuuksiin. Yleisimmät silmukkatyypit ovat kuitenkin:

- Tavallinen - Havaitessaan poikkeaman silmukka antaa hälytyksen saman tien
- Viivesilmukka - Tällä mahdollistetaan tilaan / alueelle tuleminen erikseen määriteltävällä sisääntuloviiveellä, joka täytyessään antaa hälytyksen, mikäli valvonnan poiskytkevää koodia tai luetusta ei tapahdu

Rikosilmoittimen hallinnan aloitustyöt / siivousprojekti

Rikosilmoitinjärjestelmän hallintaa käyttöönottaessa, varsinkin vanhaa järjestelmää pääkäyttöön otettaessa on huomioitava ja tehtävä seuraavat toimenpiteet:

Rikosilmoitinjärjestelmä:

- Järjestelmän ikä, kunto ja huollot
 - Sen hetkisen tilan kartoitus, jotta tiedetään onko järjestelmä vielä nykypäivän vaatimuksia vastaava ja voiko sen tarvittaessa tuoda sille tasolle, sekä onko vara- tai lisäosia saatavilla.
- Järjestelmän toiminta ja testaus
 - Meneekö hälytyksestä soitto läpi hälytyskeskukselle
- Käyttäjien määrä ja kannan puhdistus
- Master-koodin vaihtaminen
- Rikosilmoitinsilmukoiden piirtäminen pohjakuviin, mikäli tällaisia ei vielä ole
- Rikosilmoitinjärjestelmän turvallisuustaso lopullisessa pääkäyttöformaatissa ollessaan → Tiedot palveluntilaaajalle lähtötasosta ja formaatissa olevasta tasosta
 - Mahdolliset toimenpiteet, esim. huollon tarve tai silmukoiden uusiminen, lisääminen tms.
- Järjestelmän/ palvelimen kesä- ja talviaikojen huomioiminen, jotta hälytykset menevät päälle oikeina aikoina

OSIO 6: LIITTEET

Kulunvalvonnan työpyyntölomakkeet pääkäytölle:

Kulcutunnisteen aktivoiminen tai kuolettaminen

1. Kenelle - Nimi ja yritys:

Esim. Kulkuri Kalle / AB Yritys Oy

2. Tunnisteen numero:

Esim. 562575

3. Tunniste aktivoidaan:



4. Tunniste kuoletetaan:

Lopullisesti - jää varalle

Määräajaksi: PVM

Tunniste kadonnut, eikä löydy etsinnöistä huolimatta

Tunniste kadonnut, mutta löytyessään aktivoidaan takaisin

Henkilö lopettanut - uusi aloittaa ja siirretään hänen käyttöön*

* Anna uuden henkilön tiedot täyttämällä lomake loppuun



5. Kulkuoikeusryhmän, kulkualueen tai oven tunnus tai nimi:

Esim. Kulkualue 101: Ab Yritys Oy esimiehet TAI ovipääte 220008 pääovi

6. Voidaanko joltain toiselta henkilöltä kopioida oikeudet - Anna nimi:

Esim. Turunen Tanja / Ab Yritys Oy

7. Alkaen milloin:

Esim. 01.11.2014 TAI heti niin pian kuin mahdollista

8. Tiedetäänkö kulcutunnisteen tarpeelle päättymispäivämäärä:

Esim. 31.01.2015 TAI oikeudet voimaan kuukaudeksi eteenpäin

9. Muut mahdolliset lisätiedot:

Mikäli sinulla on kysyttävää tai kaipaat lisätietoja, älä epäröi ottaa yhteyttä pääkäyttäjään.

Kulkuoikeuksien lisääminen tai poistaminen

1. Kenen kulkutunniste - Nimi ja yritys:

Esim. Kulkuri Kalle / AB Yritys Oy

2. Tunnisteen numero:

Esim. 562575

Kyllä

Ei

3. Onko tunniste henkilöllä jo aktiivisena ja käytössä:

4a. Henkilölle lisätään kulkuoikeusryhmä tai kulkualue:

4b. Kulkuoikeusryhmän tai kulkualan nimi tai tunnus:

Esim. Kulkualue 101: Ab Yritys Oy esimiehet TAI Ab Yritys Oy perusoikeudet

5a. Henkilölle lisätään poikkeuksellisesti oikeus yksittäiseen oveen:

5b. Oven/päätteen tunnus:

Esim. Ovipäätte 450001 (ATK-huone) TAI hissi 10004 kerroksiin 4-7.

6. Voidaanko joltain toiselta henkilöltä kopioida oikeudet - Anna nimi:

Esim. Turunen Tanja / Ab Yritys Oy

7. Tehdäänkö oikeuksiin muutoksia poistamalla vanhoja kulkualueita:

8. Mitä kulkuoikeusryhmiä / kulkualueita tai yksittäisiä ovia poistetaan:

Esim. Kaikki aiemmat oikeudet TAI ovipäätteen 120012

9. Mistä alkaen kulkuoikeusmuutoksen toivotaan tulevan voimaan:

Esim. Mahd. pikaisesti TAI alkaen 15.12.2014

10. Mikäli oikeuksille tiedetään päättymispäivämäärä, ilmoita se alla:

Esim. 31.01.2015 TAI oikeudet voimaan kuukaudeksi eteenpäin

11. Muut mahdolliset lisätiedot:

Mikäli sinulla on kysyttävää tai kaipaat lisätietoja, älä epäröi ottaa yhteyttä pääkäyttäjään.

Henkilö ei pääse kulkemaan kulkutunnisteella

1. Kenen kulkutunniste - Nimi ja yritys:

Esim. Kalle Kulkuri / AB Yritys Oy

2. Tunnisteen numero:

Esim. 562575

3. Milloin ongelma on ilmennyt - Pvm ja kellonaika:

Esim. Pe 31.10.2014 klo 07:00 alkaen

4. Mikä / mitkä ovat kyseessä - Oven/päänteen tunnus:

Esim. Ovipäätte 200010 sekä vasen hissi 100004 kerrokseen 3.

Kyllä

Ei

5. Tunnisteisiin tai kulkuoikeuksiin tehty muutoksia lähiaikoina:

6. Mitä / Milloin:

Jätä kohta tyhjäksi, mikäli vastasit edelliseen Ei

7. Mitkä kulkuoikeudet henkilöllä pitäisi olla:

Esim. Ab Yritys Oy henkilökunta 24/7-oikeudet

8. Muillakin ilmennyt sama ongelma:

9. Esimerkkihenkilö, kenellä ei myöskään toiminut:

Jätä kohta tyhjäksi, mikäli vastasit edelliseen Ei

10. Esimerkkihenkilö, kenellä kulkeminen onnistuu:

Jätä kohta tyhjäksi, mikäli vastasit edelliseen Ei

11. Kulkeminen on toiminut ennen normaalisti:

12. Milloin tunniste on toiminut viimeksi:

Esim. To 30.10.2014 klo 16:35 töistä lähdettäessä

13. Reagoiko ovilukija tunnisteen luetukseen:

14. Merkitse tähän, mikäli kyseessä pin-koodinäppäimistöllinen lukija:

15. Muut mahdolliset lisätiedot:

Mikäli sinulla on kysyttävää tai kaipaat lisätietoja, älä epäröi ottaa yhteyttä pääkäyttäjään.

YRITYKSEN LOGO

Avaimen/kulcutunnisteen kuittauslomake

Kiinteistö: _____
 Vastaanottaja: _____
 Yritys: _____
 Puhelinnumero: _____

Nimike	Avaimen leimaus / Kulcutunnisteen numero	Kappalemäärä
Yhteensä:		

Sitoudun pitämään tällä lomakkeella mainittuja avaimia ja kulcutunnisteita turvallisesti hallussani, kunnes sen käyttötarve osaltani päättyy. En luovuta avaimia tai kulcutunnisteita kolmannelle osapuolelle.

Avaimen tai tunnisteen katoamisesta ilmoitan välittömästi pääkäyttööni. Vastaan avaimen tai tunnisteen katoamisesta johtuvista kustannuksista täysimääräisesti.

Avaimiin ja tunnisteisiin ei saa liittää kiinteistöön, yritykseen tai henkilöön liittyviä tietoja

Päivämäärä: _____ Paikka: _____

Vastaanottajan allekirjoitus

Luovuttajan allekirjoitus

Nimen selvitys

Nimen selvitys

OSIO 7: LÄHTEET

Lähteet:

Ellonen V.; Kauppi V.; Kinnunen H.; Käyhkö P.; Laitinen J.; Lehtikangas M.; Lehtinen T.; Lehtonen R.; Pänkäläinen A.; Pöysä H.; Sallinen P.; Starck K. & Woitsch P. 2010. Kameravalvontaopas. Sähköinfo Oy Turva-alan yrittäjät & Poliisihallitus, turvallisuusalan neuvottelukunta. Sähköisenä versiona osoitteessa
https://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Kameravalvontaopas_2010.pdf

Ahokas, J., Karkinen, P., Mero, P. & Pänkäläinen, A. 2008. Finanssialan Keskusliiton omaisuusrikostoimikunta. Kohteen murtoriskien arviointi ja suojaustason valinta -ohje 2008. Helsinki: Finanssialan Keskusliitto.
http://www.fkl.fi/materiaalipankki/ohjeet/Dokumentit/Kohteen_murtoriskien_arviointi.pdf

Kuvien lähteet:

¹ Bewator. 2010. IB44EM. Viitattu 21.4.2014.
<http://www.bewator.com/internal/cimg!0/rbvvey5xb2jvxkjgpkngm041t1z9gg2>

⁴ Idesco. Idesco News #3, 2012. Viitattu 21.4.2014. <http://www.idesco.fi/wp-content/uploads/2012/01/keyring-300x300.jpg>

³ Serie Securite. ProxKey. Viitattu 21.4.2014. <http://www.serie-securite.fr/produits/controleac/rosslare/PROXKEY%5B1%5D.jpg>

^{*} HID Global. 2014. FlexKey® Keytag. Viitattu 21.4.2014
http://www.hidglobal.com/sites/hidglobal.com/files/keytag_1434_1454_1.png

² Hid Global. 2014. HID's Indala® FlexCard®. Viitattu 21.4.2014
<http://www.hidglobal.com/sites/hidglobal.com/files/indala-flexcard.png>

⁶ The Card Network. Access control cards. Viitattu 21.4.2014.
http://www.thecardnetwork.co.uk/media/catalog/category/bewator-ib-1_1.jpg

⁷ Keski-Suomen Lukko Oy. ABLOY-Avaimet. Viitattu 18.4.2014.
http://www.kslukko.fi/uploads/abloy_avaimet.jpg

⁹ Kaba. 2014. Keycards & key fobs. Viitattu 21.4.2014. <http://www.kaba.sg/media/495632/v5/resized170x-1/keycards-key-fobs-electronic-key.jpg>

⁸ iLOQ Oy. Avainhallinta. Viitattu 21.4.2014 http://www.ilq.com/fi/files/2013/01/challenge_2.jpg

¹⁰ Elektroniikkapiirilevy CLIQ-avaimessa. Abloy. Viitattu 18.4.2014
http://mpc.abloy_production.assaabloy.com/fileexplorer/Fetchfile.aspx?id=960&ft=.jpg&mh=153&mw=299

Liite 2 Asiantuntijahaastatteluiden rungot

ISS Palvelut. Pääkäyttäjä Olli Ukkosen haastattelu 7.7.2014. Haastattelun aiheet:

- Mitä pääkäyttäminen tarkoittaa?
- Pääkäyttö terminä?
- Mitä pääkäyttäjää tekee?
- Miten toiminta ilmenee;
 - o avain- ja tunnistehallinnassa sekä kulunvalvonnassa
 - o kameravalvonnassa ja rikosilmoittimen hallinnassa
- Mikä pääkäyttöpalvelun tarkoitus on?
- Miten pääkäyttö voi vaikuttaa palvelun tilaajan turvallisuustasoon?
- Miksi pääkäyttö kannattaa ulkoistaa?
- Mitä turvallisuusajattelu on? Miten se näkyy liikekiinteistöjen toimintaympäristössä?
- Linkit eri turvallisuuspalveluiden välillä? (Aulapalvelu, vartiointi, pääkäyttöpalvelu)
 - o Voidaanko palvelujen määrään panostamalla kuitenkin epäonnistua?
- Turvajärjestelmät kokonaisuutena: Mitä pitää huomioida?
- Mitä kulunvalvonta on?
- Mistä asioista pääkäyttäjän tulisi olla varma;
 - o avain- ja tunnistehallinnan puolelta
 - o hallinnolliselta näkökannalta
 - o viestinnälliseltä näkökannalta
 - o tekniseltä näkökannalta
- Miten turvallisuutta kehitetään järjestelmien näkökulmasta?
 - o Jo olemassa olevat järjestelmät
 - o Uudet järjestelmät
- Kameravalvonnan aloitustyöt?
- Rikosilmoittimen hallinnan aloitustyöt?
- Ammattisanasto?
 - o mitkä termit tuottavat eniten väärinkäsityksiä?
 - o mitä termejä käytetään väärin?

Flexim Security Oy. Pääkäyttöyksikön haastattelu 30.9.2014. Haastattelun aiheet:

- Onko pääkäyttäjälle olemassa tiettyä koulutusta? Miten pääkäyttäjää opittiin hyväksi pääkäyttäjäksi?
- Onko pääkäyttämiseksi selkeät yhtenäiset raamit jokaisella työntekijällä?
- Voiko pääkäyttöä suorittaa yksien tiettyjen suuntaviivojen mukaisesti?
 - o Voidaanko näillä suuntaviivoilla kouluttaa pääkäyttäjää?
 - o → ”ilman yhteisiä suuntaviivoja pääkäyttöä ei voida kutsua oikeasti hallituksi kokonaisuudeksi”
- Mitä pääkäyttäjän työhön kuuluu?
- Mitä pääkäyttöpalvelu tarkoittaa?
- Mikä on käyttäjän ja pääkäyttäjän ero?
- Kuinka monta pääkäyttäjää yhdellä järjestelmällä/kiinteistöllä/yrityksellä voi olla?
- Miten kulunvalvontajärjestelmän saa parhaiten vastaamaan asiakkaan toiveita?
- Pääkäyttöpalvelua on tuotettu jo useita vuosia (kuinka pitkään?). Minkä tiedon varassa on toimittu ja miten prosessit ovat muokkautuneet sellaisiksi kuin ne nykyään ovat? (Lainsäädäntö ja suositukset?)
 - o Onko tosiaan ammattitietoa ja hiljaista tietoa?
- Pääkäyttöprosessi?

- Prosessin eteneminen? Tavoitetila?
- Ongelmakohdat pääkäyttöprosessissa?
 - mikä aiheuttaa epäonnistuneen prosessin?
 - mitä voidaan tehdä prosessin nopeuttamisen ja sujumisen sekä uhkakuvien minimoimisen eteen?
- Ammattisanasto?
- Mistä asioista pääkäyttäjän tulisi olla varma;
 - avain- ja tunnistehallinnan puolelta
 - hallinnolliselta näkökannalta
 - viestinnälliseltä näkökannalta
 - tekniseltä näkökannalta
- Miten turvallisuutta kehitetään järjestelmien näkökulmasta?
 - Jo olemassa olevat järjestelmät
 - Uudet järjestelmät
- Kulunvalvonnan aloitustyöt?
- Kulunvalvonta
 - mitä on? Onko sama kuin kulunseuranta tai kulunhallinta?
- Työajanseuranta
 - onko riskienhallinnan työkalu/keino?
- Maksupalvelutoiminto kulunvalvontajärjestelmässä?

Secon Systems Oy. Turvajärjestelmien pääkäyttäjä Ilpo Hulkkosen haastattelu 25.9.2014.

Haastattelun aiheet:

- Minkälaiset pohjatiedot pääkäytettävistä kohteista pääkäyttäjällä on?
- Mistä rikosilmoitinjärjestelmä koostuu?
- Mitä rikosilmoitinjärjestelmän pääkäyttöön kuuluu?
- Ammattisanasto?
- Pääkäyttäjän rooli kiinteistön turvallisuuden ylläpitäjänä?
- Mistä asioista pääkäyttäjän tulisi olla varma;
 - avain- ja tunnistehallinnan puolelta
 - hallinnolliselta näkökannalta
 - viestinnälliseltä näkökannalta
 - tekniseltä näkökannalta
- Miten turvallisuutta kehitetään järjestelmien näkökulmasta?
 - Jo olemassa olevat järjestelmät
 - Uudet järjestelmät
- Kameravalvonnan aloitustyöt?
- Rikosilmoittimen hallinnan aloitustyöt?
- Pääkäyttöprosessit: Minkälainen on sujuva prosessin kulku? Mitä tekijöitä voi olla onnistuneen prosessin tiellä?
- Turvallisuustason ylläpitäminen: Palveluntoimittajan ja asiakkaan näkökulmista?
 - Mitä pääkäyttäjä voi tehdä ylläpitääkseen ja yhä kehittääkseen turvallisuustasoa?
 - Mitä haittatekijöitä voi olla tason laskemiseksi?

Corbel Oy. Kiinteistöpäällikkö Kari Kyllästisen haastattelu 2.6.2014. Haastattelun aiheet:

- Mikä merkitys turvallisuudella on liikekiinteistöissä?
- Miten turvallisuus näkyy ja miten sitä hoidetaan?
- Onko turvallisuus jokapäiväistä tai näkyvää toimintaa?

- Mitä turvajärjestelmien hankkimisella haetaan?
- Mitkä tekijät vaikuttavat hankintapäätöksiin, ylläpitoon sekä kehittämiseen?
- Turvajärjestelmien pääkäyttö terminä?
- Miksi turvallisuuspalvelut ulkoistetaan? Mitä etuja tai haittoja ulkoistamisella voi olla? Valvotaanko palveluiden tasoa?
- Kuuluuko kiinteistömanagerien koulutukseen turvallisuuskoulutusta?
 - o Pitäisikö olla enemmän?
- Miten hyvin (ulkoistettujen) turvallisuuspalveluiden rajapinnat ovat yleisesti tiedossa kiinteistönjohdon osalta?
- Millä perusteilla ulkoistettujen turvallisuuspalveluiden sopimusten sisällöt määritellään?
- Miten liikekiinteistöjen vuokralaiset näkevät kiinteistöjen turvajärjestelmät?
 - o Etuna vai vaivana?

Flexim Security Oy. Avainhallinnan asiantuntijoiden Kaisa Ilorannan sekä Mirva Viljakaisen haastattelu 22.9.2014.

- Avainhallinnan tarkoitus
 - o Mikä on avainten hallinnan merkittävin syy?
- Avainhallintaprosessi: Mitä käsittää, mitä siihen kuuluu, mitä eroja kulunvalvontaan?
- Miten avainhallinta on jakautunut liikekiinteistöjen ja asunto-osakeyhtiöiden välille?
- Mikä vaikutus turvallisuuteen on, jos avainhallinta ei ole kunnossa?
- Mistä asioista pääkäyttäjän tulisi olla varma;
 - o avain- ja tunnistehallinnan puolelta
 - o hallinnolliselta näkökannalta
 - o viestinnälliseltä näkökannalta
 - o tekniseltä näkökannalta
- Voidaanko korkeakin turvallisuusluokiteltu tila tai alue ulkoistaa pääkäyttöön?
- Ulkoistamisen hyödyt vs. Finanssialan Keskusliiton ohjeiden noudattaminen?
- Miten turvallisuutta kehitetään järjestelmien näkökulmasta?
 - o Jo olemassa olevat järjestelmät vs. uudet järjestelmät
- Avainhallinnan aloitustyöt?

Ovenia Oy. Ylläpitopäällikkö Niko Juntusen puhelinhaastattelu 23.10.2014

- Mitä kiinteistön turvallisuus on kiinteistönjohdon näkökulmasta?
 - o Mitä asioita se käsittää ja mitä siihen kuuluu?
- Mitkä turvallisuusratkaisut ovat parhaiten toimivia?
- Mitkä turvallisuusratkaisut ovat hankalia toteuttaa?
- Onko turvallisuudessa konkreettista kehitettävää?
- Kuinka tietoisia kiinteistön managerointipuolella koetaan olevan liiketilojen turvallisuudesta?
 - o Kuinka vastuu jakautuu kiinteistön ja vuokralaisten välillä?
- Mitä etuja turvajärjestelmien pääkäyttöpalveluista on / voi olla kiinteistönjohdon näkökulmasta?
- Pärjättäisiinkö pelkällä lukituksella? Ettei kulunvalvontajärjestelmää olisi.
- Mitkä asiat koetaan kulunvalvonnan hyödyiksi?
- Mistä turvallisuuteen liittyvistä asioista kiinteistöpäällikkö haluaa olla varma/tietoinen koskien hänen hallitsemiaan kiinteistöjä?
 - o Mistä turvallisuuden tunne syntyy?

Liite 3 Flexim Security Oy:n palvelupäällikön palaute oppaasta

Lähtettäjä: Tatu Monto

Vastaanottaja: Juuso Jääskeläinen

Lähetetty: ma 10.11.2014 10:39

Aihe: Vs: Turvajärjestelmien pääkäytön suuntaviivat -opas

Oppaassa on ansiokkaasti kiteytetty keskeiset asiasisällöt, jotka sekä asiakkaan että palveluita toimittavan yrityksen on syytä huomioida, jotta toimitettava pääkäyttöpalvelu (joka koskee oppaassa kuvattuja turvallisuusteknologioita) vastaa parhaalla mahdollisella tavalla palvelua kohtaan asetettuja odotuksia.

Oppaan avulla on mahdollista muodostaa asiakkaan ja palveluntarjoajan välille yhteinen kieli joka luo edellytykset ymmärtää palvelusisältö mahdollisimman yksiselitteisesti. Toisin sanoen se vähentää väärinkäsitysten mahdollisuutta. Opasta voidaan soveltaa osana palveluiden myynti/ostoprosessia.

Opasta sovelletaan osana Flexim Securityn perehdytystä (asiakaspalvelussa) sekä sen käyttö arvioidaan pääkäyttöpalvelun käynnistyksen osana.

Flexim Security Oy

Tatu Monto

Palvelupäällikkö | Palvelukeskuspalvelut

Puh: 010 700 7225

Kornetintie 3, PL 700

00381 HELSINKI

tatu.monto@flexim.fi

www.flexim.fi

KULJE HUOLETTA.



Information in this e-mail and any attachments is confidential and intended solely for the use of the intended recipient. If you have received this email in error please notify the sender.