LAUREA

Turvallisuustekniikka osana toimitilaturvallisuutta: teknisten turvallisuusratkaisujen kartoitustyökalun tekeminen

• •

Päivärinta, Ari

2009 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

TURVALLISUUSTEKNIIKKA OSANA TOIMITILATURVALLISUUTTA: TEKNISTEN TURVALLISUUSRATKAISUJEN KARTOITUSTYÖKALUN TEKEMINEN

Ari Päivärinta
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu 2009

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Yhteiskuntatieteiden, liiketalouden ja hallinnon ala
Turvallisuusalan koulutusohjelma

Ari Päivärinta

Turvallisuustekniikka osana toimitilaturvallisuutta: teknisten turvallisuusratkaisujen kartoitustyökalun tekeminen

Vuosi 2009 Sivumäärä 68

Opinnäytetyö sai alkunsa kesällä 2008 teknisiä turvallisuusratkaisuja tuottavan Niscayah Oy:n entisen Julkishallinnon liiketoiminta-alueen Business Area Managerin, nykyisen turvallisuusjohtajan toimeksiannosta. Toimeksiantona oli tuottaa Niscayah Oy:lle teknisiä turvallisuusratkaisuja pintaa syvemmältä luotaava kartoitustyökalu. Työkalun avulla olisi tarkoitus pystyä kartoittamaan ja arvioimaan asiakkaiden olemassa olevia teknisiä turvallisuusratkaisuja osana toimitilaturvallisuutta.

Teknisiä turvallisuusratkaisuja kartoittamalla on tarkoitus pyrkiä varmistumaan siitä, että turvallisuusratkaisut vastaavat asiakkaiden turvallisuustarpeita ja palvelevat turvallisuudelle asetettuja tavoitteita mahdollisimman hyvin. Kyseessä on siis proaktiivinen sekä reaktiivinen työkalu, jonka avulla voidaan kartoittaa ja arvioida teknisiä turvallisuusratkaisuja suhteessa asiakkaan turvallisuustarpeisiin ja turvallisuudelle asettamiin tavoitteisiin, tunnistaa turvallisuusratkaisuissa mahdollisesti olevia puutteita ja kehityskohteita sekä auttaa korjaavien ja kehittävien toimenpiteiden kohdistamisessa oikein. Tällä Niscayah Oy haluaa tukea ja tuoda ilmi tavoitteitaan olla luotettava turvallisuuskumppani ja integraattori, joka tuottaa enemmän hyötyä asiakkaillensa teknisten turvallisuusratkaisujen tuottajana ja toteuttajana tarjoamalla asiantuntemuksensa asiakkaidensa käyttöön.

Kartoitustyökalu painottuu teknisten turvallisuusratkaisujen osalta kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmiin toimitilaturvallisuuden osana, rakenteellista turvallisuutta kuitenkaan unohtamatta. Toimitilaturvallisuuden ja teknisten turvallisuusratkaisujen lisäksi työkalussa kiinnitetään osin huomiota myös toimitilaturvallisuuteen läheisesti liittyviin turvallisuuden muihin osa-alueisiin. Itse kartoitustyökalu ei ole kuitenkaan osa opinnäytetyötä, vaan tarkoituksena on kuvata sitä ja sen tekoprosessia. Ennen tätä opinnäytetyössä kuitenkin tarkastellaan teknisiä turvallisuusratkaisuja toimitilaturvallisuuden osana edellä mainittujen järjestelmien osalta toimitilojen suojaamisen ja valvonnan näkökulmasta.

Työkalu toteutettiin yhteistyössä työn toimeksiantajan kanssa ja työssä hyödynnettiin myös yrityksen asiantuntijoita. Työkalun suunnittelussa tutustuttiin saatavilla olleisiin erilaisiin turvallisuuskartoituksiin ja riskianalyyseihin sekä esimerkiksi Finanssialan Keskusliiton antamiin ohjeisiin ja suosituksiin. Lopputuotoksena syntyi kolmesta osiosta kysymyssarjoineen koostuva kartoitustyökalu. Työkalun ensimmäinen osio kiinnittää huomiota yleisellä tasolla kartoitettavan kohteen turvallisuuteen ja omatoimiseen turvallisuussuunnitteluun ja turvallisuustoimintaan sekä turvallisuuden asemaan kyseisessä organisaatiossa. Toisessa osiossa keskitytään puolestaan kartoitettavan kohteen olemassa oleviin nykyisiin suojaus- ja valvontaratkaisuihin. Kolmas osio keskittyy Niscayah Oy:n toimintaan tilanteissa, joissa Niscayah Oy on ollut aikaisemmin toteuttamassa kartoitettavan kohteen nykyisiä teknisiä turvallisuusratkaisuja.

Asiasanat: kartoitustyökalu, tekninen turvallisuusjärjestelmä, kulunvalvontajärjestelmä, rikosilmoitinjärjestelmä, kameravalvontajärjestelmä

Laurea University of Applied Sciences **Abstract**
Leppävaara
Security Management Programme

Ari Päivärinta

Technical security as a part of securing premises: creating a mapping tool for technical security solutions

Year 2009 Pages 68

The idea for this thesis was born in summer 2008 on assignment of former Business Area Manager and current Security Manager of Niscayah. The assignment was to create a mapping tool for technical security solutions. The purpose of the tool is to map and evaluate client's existing technical security solutions in the view of securing premises.

The idea of the tool is to ensure that the security solutions match the security needs and serve the aims of security by mapping the security solutions. Therefore it is a reactive and proactive tool for mapping and evaluating existing security solutions. The tool can also be used to recognize possible shortcomings and lacks in security solutions and to help to adopt the right developing measures to the right target. Thus, Niscayah can support and express the company's desire to be a trusted partner and integrator in security. This is realized by producing more profit to clients by providing their expertise to the clients as a producer of technical security solutions.

The mapping tool concentrates on access control systems, alarm systems and video surveillance systems. Physical protection is taken partly into account. In addition, other fields of security relating to securing premises have been taken into account in the mapping tool. The mapping tool is not a part of the thesis but the process of creating the tool is described in it. It is preceded by a review of technical security solutions from the view of protecting and monitoring premises security.

The tool was produced in collaboration with the Security Manager of Niscayah. Moreover, the expertise of other experts of Niscayah was exploited. Different existing security mappings, risk evaluations, security guidelines and recommendations were used as a base when planning the tool. As an end product a tool consisting of three items with question series was developed. The first item concentrates on the security of an organisation on a common level and includes questions concerning independent security planning and activities. In addition, the first item emphasizes the role of security in an organisation. The second item includes questions of current protection and monitoring solutions. The third and last item concentrates on operations of Niscayah in situations where Niscayah has produced technical security solutions of today.

Key Words: mapping tool, technical security system, access control system, alarm system, video surveillance system

Sisällys

1 Johdanto

Toimitilaturvallisuuteen kuuluu oleellisena osana toimitilojen suojaamisen lisäksi myös toimitilojen turvallisuuden valvonta. Tekniset turvallisuusjärjestelmät tarjoavat oivia ratkaisuja toimitilojen suojaamisen ja turvallisuusvalvonnan toteuttamiselle. Tekniset turvallisuusjärjestelmät eivät kuitenkaan yksistään takaa turvallisuutta, mutta ne toimivat hyvinä työvälineinä ja keinoina toimitilaturvallisuuden varmistamiseen ja valvontaan. Teknisten turvallisuusjärjestelmien avulla voidaan suojata yrityksen tai organisaation henkilöstöä, asiakkaita, toimintaa sekä omaisuutta ennaltaehkäisemällä, vähentämällä, estämällä sekä selvittämällä yritykseen tai organisaatioon kohdistuvia rikoksia ja vahinkoja sekä pienentämään näiden seurauksia.

Teknisten turvallisuusjärjestelmien tulee vastata yrityksen tai organisaation turvallisuustarpeita ja palvella turvallisuudelle asetettuja tavoitteita, että niistä voidaan saada paras mahdollinen hyöty ja tehokkuus. Teknisillä turvallisuusjärjestelmillä saavutetun turvallisuustason säilyttämiseksi järjestelmät vaativat myös käyttäjiltään osaamista sekä säännöllistä ylläpitoa. Teknisiin turvallisuusjärjestelmiin voidaan liittää erilaisia palveluita liittyen järjestelmien käyttämiseen, toiminnan varmistamiseen sekä valvonnan tehostamiseen. Tällöin voidaan puhua teknisistä turvallisuusratkaisuista.

Toimitilaturvallisuuteen ja teknisiin turvallisuusratkaisuihin liittyen työn toimeksiantajalle kehitettiin opinnäytetyön osana teknisiä turvallisuusratkaisuja toimitilaturvallisuuden osana tarkasteleva kartoitustyökalu, olemassa olevien teknisten turvallisuusratkaisujen kartoittamiseen. Itse kartoitustyökalu ei kuitenkaan ole osa opinnäytetyötä, vaan tarkoituksena on kuvata kartoitustyökalua ja sen luomisprosessia. Ensin tarkastellaan kuitenkin teknisiä turvallisuusjärjestelmiä osana toimitilaturvallisuutta toimitilojen suojaamisen ja valvonnan näkökulmasta. Tarkastelun keskiössä ovat kulunvalvonta-, rikosilmoitin- sekä kameravalvontajärjestelmät.

2 Opinnäytetyön kuvaus, tarve ja tavoitteet

Tämä toiminnallinen ja työelämälähtöinen opinnäytetyö sai alkunsa työskennellessäni turvallisuusratkaisuja tuottavassa Niscayah Oy:ssä. Silloinen esimieheni, Julkishallinnon liiketoiminta-alueen Business Area Manager, yrityksen nykyinen turvallisuusjohtaja, toi esille tarpeen teknisten turvallisuusratkaisujen kartoitustyökalulle. Työkalun avulla olisi tarkoitus pystyä kartoittamaan asiakkaiden olemassa olevia teknisiä turvallisuusratkaisuja osana toimitilaturvallisuutta. Itse kartoitustyökalu ei ole osa opinnäytetyötä, vaan tarkoituksena on ainoastaan esitellä kyseinen työkalu ja kuvata sen luomisprosessia. Ennen kartoitustyökalun tekoprosessin kuvausta tarkastellaan ensin lyhyesti toimitilaturvallisuutta yritysturvallisuuden osa-alueena ja tarkastellaan yritysten ja organisaatioiden toimitiloihin ja omaisuuteen kohdistuvaa rikollisuutta toimitilojen suojaamisen ja valvonnan merkityksen korostamiseksi. Teknisistä turvallisuusjärjestelmistä käsitellään kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmiä toimitilaturvallisuuden osana näkökulman ollessa toimitilojen suojaamisessa ja valvonnassa.

Kartoitustyökalun avulla on tarkoitus pyrkiä varmistumaan siitä, että asiakkaiden olemassa olevat turvallisuusratkaisut vastaavat asiakkaiden turvallisuustarpeita ja palvelevat turvallisuudelle asetettuja tavoitteita mahdollisimman hyvin. Tarkoituksena on siis tunnistaa myös turvallisuusratkaisuissa mahdollisesti olevia puutteita ja kehityskohteita sekä auttaa korjaavien ja kehittävien toimenpiteiden kohdistamisessa oikein. Työkalun tarpeen taustalla on Niscayah Oy:n halu tukea ja tuoda ilmi tavoitteitaan olla luotettava turvallisuuskumppani ja integraattori, joka tuottaa enemmän hyötyä asiakkaillensa teknisten turvallisuusratkaisujen tuottajana ja toteuttajana tarjoamalla asiantuntemuksensa asiakkaidensa käyttöön.

Tavoitteena oli tuottaa Niscayah Oy:lle teknisiä turvallisuusratkaisuja pintaa syvemmältä luotaava kartoitustyökalu. Työkalun avulla tulisi pystyä kartoittamaan ja arvioimaan asiakaskohteissa olemassa olevien nykyisten teknisten turvallisuusratkaisujen todellista tilaa ja tasoa. Teknisten turvallisuusjärjestelmien tarkastelun tavoitteena on pohjustaa kartoitustyökalua ja tuoda esille teknisten turvallisuusjärjestelmien tarjoamia etuja, hyötyjä sekä mahdollisuuksia turvallisuusratkaisuina toimitilojen suojaamisen ja valvonnan näkökulmasta.

2.1 Aiheen rajaus

Aiheen rajaus teknisten turvallisuusjärjestelmien osalta perustuu opinnäytetyön toimeksiantajalle, Niscayah Oy:lle, tehtyyn teknisten turvallisuusratkaisujen kartoitustyökalun lähtökohtiin ja työn toimeksiantajan kartoitustyökalulle asettamiin tavoitteisiin. Itse kartoitustyökalu ei kuitenkaan ole osa opinnäytetyötä, vaan tarkoituksena on kuvata työkalun luomisprosessia. Kartoitustyökalu painottuu teknisiin turvallisuusratkaisuihin osana toimitilaturvallisuutta toimitilojen suojaamisen ja valvonnan näkökulmasta. Kartoitustyökalun painopiste on ennen

kaikkea kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmiin, sillä ne ovat Niscayah Oy:n päätuotelinjat turvallisuusjärjestelmien saralla. Teknisistä turvallisuusjärjestelmistä kyseiset järjestelmät ovat myös hyvin keskeisessä asemassa toimitiloihin ja omaisuuteen kohdistuvaan rikollisuuteen varautumisessa.

Näin ollen oli myös loogista keskittyä toimitilojen suojaamisen ja valvonnan näkökulmasta tarkastelemaan kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmiä osana toimitilaturvallisuutta. Tarkastelu katsottiin parhaimmaksi toteuttaa enemmänkin yleisellä tasolla eikä tarkastelussa ole tarkoitus keskittyä yksittäisiin tai tietyn merkkisiin järjestelmiin ja laitteisiin eikä pintaa syvemmälle meneviin teknisiin yksityiskohtiin laitteiden ja järjestelmien laajan kirjon takia. Teknisiä turvallisuusjärjestelmiä tarkasteltaessa käsitellään niiden hyödyntämistä toimitilojen suojaamisessa ja valvonnassa. Näkökulman ollessa hyvin vahvasti toimitilojen suojaamisessa ja valvonnassa toimitiloihin kohdistuvien rikoksien varalta, ei toimitilaturvallisuuden liittymäkohtia muihin yritysturvallisuuden osa-alueisiin tarkastelussa juurikaan huomioida.

2.2 Opinnäytetyön tekeminen ja aineisto

Toimitilaturvallisuuden ja teknisten turvallisuusjärjestelmien tarkastelu toimitilaturvallisuuden osana pohjautuu aihetta käsitteleviin painettuihin sekä sähköisiin lähteisiin sekä Niscayah Oy:n tarjoamaan asiantuntemukseen sekä tekijän omaan tietoon ja kokemukseen. Kartoitustyökalun tekoprosessissa otettiin puolestaan vaikutteita jo olemassa olevista erilaisista turvallisuuskartoituksista ja riskianalyyseistä sekä hyödynnettiin Niscayah Oy:n henkilöstön ja tekijän omaa asiantuntemusta. Tästä on kerrottu enemmän kartoitustyökalua käsittelevässä osiossa. Käytettyjä lähteitä on arvioitu tekijän omaan sekä työelämän ohjaajan kokemukseen ja näkemykseen perustuen.

2.3 Toimeksiantajana Niscayah Oy

Niscayah on Tukholman pörssissä noteerattu monikansallinen teknisiin turvallisuuspalveluihin keskittynyt konserni, joka on alansa johtava toimija maailmassa. Suomessa Niscayah Oy on toimialansa johtava yritys, joka tuottaa kokonaisvaltaisia turvaratkaisuja yrityksille, yhteisöille, julkisen sektorin ja yksityisten kotien tarpeisiin. Palvelutarjonta kattaa suunnittelusta toteutukseen lähes kaikki teknisten turvapalveluiden osa-alueet yksityistalouksien hälytysliittymistä korkean turvallisuustason kohteiden kokonaisturvallisuusratkaisuihin. Yrityksen missiona on auttaa turvallisuutta arvostavia yrityksiä ja yhteisöjä varmistamaan häiriöttömän toiminnan jatkuvuuden tarjoamalla kustannustehokkaita, luotettavia ja innovatiivisia ratkaisuja, jotka perustuvat asiakkaiden yksilöllisiin tarpeisiin. (K. Starck, henkilökohtainen tiedonanto 6.2.2009.)

Asiakasnäkökulmasta Niscayah tarjoaa kokonaisvaltaisia teknisiä turvallisuusratkaisuja asiakkaille, joille turvallisuus on tärkeää. Ratkaisut perustuvat nykyaikaisiin teknisiin järjestelmiin, palveluihin sekä konsepteihin. Teknisiä ratkaisukomponentteja ovat rikosilmoitin-, henkilöturva-, kulunohjaus-, työajanseuranta-, tuotesuojaus-, videovalvonta-, paloturva ja äänievakuointijärjestelmät. Palvelukomponentit koostuvat puolestaan erilaisista turvajärjestelmien huolto- ja ylläpitotoiminnoista, joihin kuuluvat mm. Security Operation Center (sisältäen etähallinnan, etävalvonnan ja hälytysvalvonnan), Call Center ja Help Desk-palvelut, ASP-palvelu, pääkäyttäjäpalvelu, dokumentointi, koulutus sekä ohjelmistojen ja järjestelmien ylläpitopalvelut. (K. Starck, henkilökohtainen tiedonanto 6.2.2009.)

Niscayah tunnettiin ennen nimellä Securitas Systems Oy. Entisen Securitas-konsernin yhtiöt pilkottiin syyskuussa 2006 ja Securitas Systems listautui Tukholman pörssiin omana konsernina. Oman nimen Niscayah otti käyttöön vuoden 2008 alkupuoliskolla. Tällä hetkellä Niscayah konserni käsittää 17 itsenäistä osakeyhtiötä, jotka toimivat 14 Euroopan maassa sekä Yhdysvalloissa ja Aasiassa. Suomessa yhtiön palveluksessa on lähes 300 henkilöä. (K. Starck, henkilökohtainen tiedonanto 6.2.2009.)

Niscayah Oy:n historia Suomessa alkoi vuonna 1986, jolloin Suomen Teollisuuden Vartioinnin turvapuolen ja Wärtsilän Walpass -kulunvalvonnan ympärille perustettiin STWS- Security Oy. Kaksi vuotta myöhemmin yhtiölle siirtyi Timecon- myynti ja vuonna 1992 Servi-turvapalvelu liitettiin osaksi liiketoimintoja. Vuotta myöhemmin yhtiö liittyi osaksi Securitas- konsernia ja samalla yhtiön nimi muuttui Securitas Tekniikka Oy:ksi, jolla yhtiö toimi seuraavat 11 vuotta. Vuonna 1994 yhtiö aloitti oman tuotekehitystoimintansa, jonka kohteina olivat Timecon ja Walpass. Vuonna 1996 alkoi yhtiössä voimakas panostaminen asiakkaiden toimialan mukaiseen organisoitumiseen, jolloin perustettiin pankkiliiketoimintayksikkö. Vuonna 1999 perustettiin kaupan liiketoimintayksikkö, samana vuonna alkoi myös paloliiketoiminta. Systems- divisioona syntyi vuonna 2001 ja yhtiön nimi muuttui divisioonan linjan mukaisesti vuonna 2004 muotoon Securitas Systems Oy. Suuri askel yrityksen kehityksessä oli listautuminen Tukholman pörssiin omana konserninaan syyskuussa 2006 ja oman nimen käyttöönotto huhtikuussa 2008. (K. Starck, henkilökohtainen tiedonanto 6.2.2009.)

3 Yrityksiin kohdistuva omaisuusrikollisuus ja siihen varautuminen

Keskuskauppakamari ja Helsingin seudun kauppakamari tekivät vuonna 2008 Yritysten rikosturvallisuus 2008- selvityksen, jossa yhteensä 1286 yrityksen edustajat arvioivat yrityksiin kohdistuvaa rikollisuutta, rikosriskejä ja niiden kehitystä vuosina 2005-2008. Selvitykseen osallistuneista yrityksistä 74 % arvioi, että yrityksiin kohdistuvat omaisuusriskit ovat pysyneet samoina tarkasteltavalla aikavälillä, kun noin neljännes yrityksistä arvioi omaisuuteen kohdistuvien riskien kasvaneen. Selvitykseen osallistuneista kaikista yrityksistä kuudesosa, suurista yrityksistä joka toinen oli joutunut murron kohteeksi. Joka neljänneltä yritykseltä oli varas-

tettu työvälineitä tai laitteita, suurista yrityksistä varkauksien kohteeksi oli joutunut joka toinen suuri yritys. Lisäksi noin kymmenys yrityksistä oli huomannut toiminnassaan epätavallista hävikkiä. Toimitiloihin kohdistunutta ilkivaltaa oli kokenut kuudesosa selvitykseen osallistuneista yrityksistä ja suurten yritysten kohdalla joka toisen toimitilat olivat joutuneet ilkivallan kohteeksi. Muuhun omaisuuteen kohdistuvan ilkivallan kohteeksi oli yrityksistä joutunut vajaa viidennes, 18 % selvitykseen osallistuneista yrityksistä. Lisäksi joka kymmenes yritys oli mielestään joutunut yritystiedon luvattoman urkkimisen tai vakoilun kohteeksi. 14 % yrityksistä ei tiennyt, oliko heidän yritystietoihin kohdistunut luvatonta mielenkiintoa ja urkintaa. (Yritysten rikosturvallisuus 2008: Riskit ja niiden hallinta 2008, 6-9, 24-46.)

Suomessa ei ole käytettävissä tarkkaa ja täysin luotettavaa tilastoa yrityksiin tai organisaatioihin kohdistuvasta rikollisuudesta ja sen kokonaismäärästä, sillä yrityksiin tai organisaatioihin kohdistuvia rikoksia ei erikseen tilastoida, omaisuuteen kohdistuvia rikoksia lukuun ottamatta. Omaisuusrikollisuudestakin osa jää piilorikollisuudeksi, koska osa, etenkin vähäisemmät teot, jäävät usein poliisille ilmoittamatta. Poliisin tietoon tulleiden yrityksiin ja organisaatioihin kohdistuva omaisuusrikollisuus on kuitenkin vähentynyt viime vuosina, samoin murtojen määrä on ollut laskussa liikemurtoja lukuun ottamatta. Poliisin tilastojen vertailukohdaksi ja piilorikollisuuden esiin tuomiseksi tehty Yritysten rikosturvallisuus 2008- selvityksen vertaaminen vuonna 2005 tehtyyn vastaavaan selvitykseen tukee myös poliisin tilastojen osoittamaa kehitystä yrityksiin kohdistuvan omaisuusrikollisuuden vähenemisessä. (Yritysten rikosturvallisuus 2008: Riskit ja niiden hallinta 2008, 6, 31-37.)

Täytyy ja on tärkeää kuitenkin muistaa, että kaikki yritykset ja organisaatiot ovat aina potentiaalisia omaisuusrikollisuuden kohteita, yrityksiin ja organisaatioihin kohdistuvan rikollisuuden vähentymisestä huolimatta. Rikoksen kohteeksi valikoitumiseen riittää se, että yrityksessä tai organisaatiossa on tai oletetaan olevan jotain varastettavaa tai vaihtoehtoisesti rikottavaa. Kummassakin tapauksessa vahingot ja seuraukset saattavat nousta yrityksen tai organisaation toiminnan kannalta huomattavan merkittäviksi. (Yritysten rikosturvallisuus 2008: Riskit ja niiden hallinta 2008, 31.) Yritykset ja organisaatiot voivat kuitenkin pienentää omaisuusrikosten kohteeksi joutumisen riskiä varautumalla heihin kohdistuviin rikoksiin ja uhkiin toimitilaturvallisuuden keinoin suojaamalla ja valvomalla toimitilojaan ja omaisuuttaan.

3.1 Toimitilaturvallisuus, tilojen suojaaminen ja valvonta

Kaikki yritykset ja organisaatiot tarvitsevat toimiakseen tyypillisesti toimitilat ja se korostaa toimitilaturvallisuuden merkitystä yrityksille ja organisaatioille. Toimitilaturvallisuuden keinoin, toimitilojaan suojaamalla ja valvomalla, yritykset ja organisaatiot voivat varautua henkilöstöönsä, toimitiloihinsa, toimintaansa sekä omaisuuteensa kohdistuviin rikoksiin. Toimitilaturvallisuuden voidaan todeta olevan yksi keskeisimmistä yritysturvallisuuden osa-alueista,

sillä toimitilaturvallisuus luo usein pohjan myös yrityksen tai organisaation monen muun toiminnon suojaamiselle. Toimitilojen turvallisuuden varmistaminen ja valvonta on usein myös ehdoton edellytys yrityksen tai organisaation toiminnalle. (Miettinen 2002, 91.)

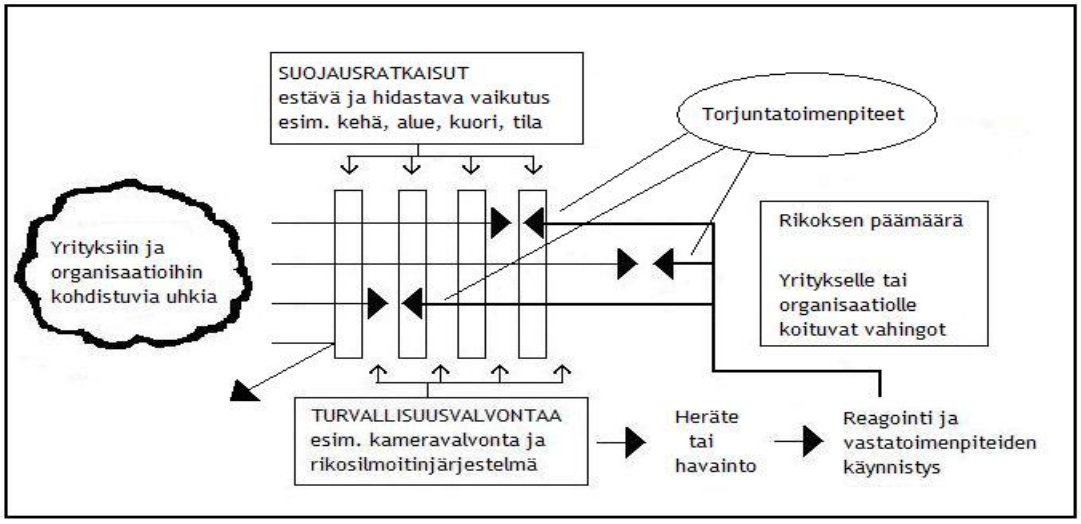
Toimitilaturvallisuus pitää sisällään yrityksen tai organisaation omistamien tai hallinnoimien kiinteistöjen tai toimitilojen, niissä olevan omaisuuden ja niiden piha-alueiden turvallisuuteen ja suojaamiseen liittyviä asioita, toimenpiteitä ja ratkaisuja. Toimitilaturvallisuuden keinoin yritys tai organisaatio pyrkii varmistumaan siitä, että sen toimitiloissa on turvallista työskennellä, toimitiloihin on pääsy vain siihen oikeutetuilla henkilöillä ja että toimitilat ja siellä oleva omaisuus on asianmukaisesti suojattu. Toimitilaturvallisuuden tavoitteena on turvata yrityksen tai organisaation toimintaa sekä estää yrityksen tai organisaation toimitiloihin sekä suojattaviin arvoihin, kuten ihmisiin ja omaisuuteen kohdistuvia uhkia ja riskejä pienentämällä niiden toteutumisen todennäköisyyttä ja toteutuneista riskeistä aiheutuneita vahinkoja sekä seurauksia. (Miettinen 2002, 91; Tikkanen ym. 2007, 161.)

Mary Lynn Garcia (2001, 53) mukaan toimitilojen fyysinen suojaaminen, toimitilaturvallisuus, muodostuu rakenteellisen turvallisuuden keinoista, teknisestä turvallisuusvalvonnasta sekä ihmisten, esimerkiksi vartiointiliikkeen vartijoiden sekä yrityksen tai organisaation oman turvallisuushenkilöstön toiminnasta ja toimenpiteistä. Yrityksen tai organisaation toimitilojen turvajärjestelyjen tarkoituksena on havaita ja estää toimitiloihin kohdistuvia uhkia sekä käynnistää asianmukaiset toimenpiteet rikosten ja uhkatapahtumien torjumiseksi ja rajoittamiseksi. (Garcia 2001, 53).

Toimitilaturvallisuuden voidaankin katsoa koostuvan rakenteellisesta turvallisuudesta ja turvallisuusvalvonnasta. Rakenteellisen turvallisuuden peruselementtejä ovat lähtökohtaisesti toimitilojen seinät, katto, lattia sekä ovet ja ikkunat. Rakenteellisesta turvallisuudesta puhuttaessa edellä lueteltujen rakenteiden kohdalla huomio kiinnittyy erityisesti esimerkiksi rakennusmateriaaleihin, seinien, lattioiden ja katon paksuuksiin sekä ovien ja ikkunoiden asianmukaiseen suojaamiseen ja lukitukseen. Rakenteellisen turvallisuuden toteutuskeinoihin kuuluvat myös aidat, portit, kalteroinnit, turvalukitusratkaisut ja muut rakenteisiin liittyvät turvajärjestelyt. (Miettinen 2002, 97; Tikkanen ym. 2007, 161.) Rakenteellisella turvallisuudella pyritään nostamaan tunkeutumiskynnystä sillä perusteella, että rikoksen toteuttaminen, esimerkiksi luvaton tunkeutuminen toimitiloihin, vaatii enemmän aikaa sekä työtä ja mahdollisesti apukeinoja (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 77). Turvallisuusvalvontaa voidaan määritellä siten, että se on ehkäisevää vahinkojen torjuntaa, jolla pyritään havaitsemaan vahinkoon johtavat muutokset ja tekemään tapahtumista ilmoitus (Rikosilmoitussanasto 1993, 28). Turvallisuusvalvonta koostuu tekniset turvallisuusjärjestelmät käsittävästä teknisestä valvonnasta sekä henkilösuoritteisesta turvallisuusvalvonnasta, esimerkiksi vartioinnista ja yrityksen tai organisaation henkilöstön, etenkin turvallisuushenkilöstön, suoritta-

masta valvonnasta. Tyypillisiä teknisiä turvallisuusvalvonnan välineitä ovat kulunvalvonta-, rikosilmoitin- sekä kameravalvontajärjestelmät. (Miettinen 2002, 98; Tikkanen ym. 2007, 161). Etenkin teknisellä turvallisuusvalvonnalla voidaan parantaa rakenteellisen turvallisuuden tehokkuutta ja suoja-arvoa (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 77).

Rakenteellisen turvallisuuden sekä teknisten turvallisuusjärjestelmien voidaan siis katsoa täydentävän toisiaan. Rakenteellisen turvallisuuden keinoin pystytään rakentamaan suoja-arvoltaan hyvä pohja toimitilojen suojaamiseksi ja toimitilaturvallisuutta voidaan tehostaa teknisten turvallisuusjärjestelmien tarjoamilla ratkaisuilla. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 77-78.) Suoja-arvoltaan parhaimmatkin rakenteelliset turvallisuusratkaisut tarvitsevat tuekseen turvallisuusvalvontaa tehokkaan toimitilaturvallisuuden toteuttamiseksi. Ilman valvontaa tehokkaistakaan rakenteellisista suojausratkaisuista ei pidemmän päälle ole apua, mikäli uhkatapahtumiin ei reagoida. Tekninen turvallisuusvalvonta tarjoaa tähän ratkaisun, kun vahinkoon johtavat muutokset voidaan havaita ja tehdä tapahtumista ilmoitus jatkotoimenpiteiden käynnistämiseksi (Rikosilmoitussanasto 1993, 28).



Kuva 1: Tekninen turvallisuusvalvonta rakenteellisen turvallisuuden tukena

Toimitilaturvallisuudella voidaan katsoa olevan useita liittymäkohtia muihin yritysturvallisuuden osa-alueisiin ja usein osa-alueista puhuttaessa niiden rajat tuntuvat varsin veteen piirretyn viivan kaltaisilta. Yritysturvallisuuden osa-alueiden voisi paremminkin nähdä liittyvän toinen toisiinsa, toiset enemmän ja toiset vähemmän, kuin nähdä ne tiukasti rajattuina erillisinä osa-alueina. Toimitilaturvallisuus tuleekin nähdä laajemmassa perspektiivissä kuin vain toimitilojen ja omaisuuden suojaamiseen tähtäävänä toimintana. Tätä voidaan perustella sillä, että varsin usein toimitiloihin ja omaisuuteen kohdistuvat riskit kohdistuvat samalla myös esimerkiksi henkilöturvallisuuteen. Esimerkiksi erilaiset rikosriskit sekä onnettomuus- ja vaaratilanteet kuten tulipalot yms. uhkaavat myös toimitiloissa työskenteleviä ja asioivia

henkilöitä. Kuten Miettisenkin (2002, 91) mukaan on jo edellä todettu, toimitilaturvallisuuden yhtenä tavoitteena on myös turvata työskentelyä toimitiloissa. Toimitilaturvallisuuden keinoin voidaan vaikuttaa ja varautua myös muihin yritysturvallisuuden eri osa-alueisiin sisällöllisesti kuuluviin riskeihin. Usein tehokkaasti toteutetut toimitilaturvallisuuden ratkaisut parantavatkin yrityksen tai organisaation muiden turvallisuuden osa-alueiden, kuten tietoturvallisuuden, pelastustoiminnan ja muun rikosturvallisuuden tasoa (Yritysten rikosturvallisuus 2008: Riskit ja niiden hallinta 2008, 31).

3.2 Tärkeysluokittelu suojauksen perustana

Yrityksen tai organisaation toiminnassaan tarvitsemat toimitilat eivät ole toimitilaturvallisuuden ja tilojen suojaamisen näkökulmasta aina samanarvoisia. Tilojen kriittisyys ja suojaamisen tarve riippuu useasta seikasta, kuten tiloissa suoritettavasta toiminnasta. On selvää, että esimerkiksi yrityksen tai organisaation johdon tilat tai tuotekehitystilat on suojattava eri tavoin kuin esimerkiksi yleiset tilat. Suojaamistasoon vaikuttaa myös se, kenelle ja minkälaiseen toimintaan kyseiset tilat ovat tarkoitettuja. Osaan tiloista voivat päästä esimerkiksi myös asiakkaat ja yhteistyökumppanit, kun joihinkin tiloihin on pääsy vain henkilöstöllä tai rajatulla osalla henkilöstöä. (Miettinen 2002, 92.)

Luokittelemalla tilat tärkeysjärjestykseen niiden kriittisyyden suhteen yrityksen tai organisaation toimintaan, voidaan toimitilojen suojaamisessa kohdistaa oikeat suojaus- ja valvontakeinot oikeisiin tiloihin. Tällä pyritään varmistumaan siitä, että tärkeimmät tilat tulevat asianmukaisesti myös kattavimmin ja oikein suojattua. Näin voidaan välttää se, että korkean suojaustason tilat jäisivät vaille asianmukaista ja kattavaa suojaamista ja vähemmän tärkeät tilat suojattaisiin puolestaan ylimitoitetusti. (Miettinen 2002, 92.) Tärkeysluokittelu voidaan tehdä usealla eri tavalla, mutta ensiarvoisen tärkeää on, että yrityksessä tai organisaatiossa ymmärretään tärkeysluokittelun merkitys sekä tarkoitus. (Miettinen 2002, 92.)

Juhat Leppänen (2006, 343-345) ja Miettinen (2002, 93) ovat kumpikin esitelleet tärkeysluokittelun yhdeksi periaatteeksi neljään suojaustasoon perustuvan luokittelun. Suojaustasoina tämän periaatteen mukaisesti ovat perussuojaus, tehostettu perussuojaus, erityissuojaus sekä täyssuojaus. Perussuojaus on tasoista alhaisin ja tarkoitettu tiloille, joihin ei kohdistu erityisiä riskejä tai riskejä, jotka aiheuttaisivat merkittäviä vahinkoja. Täyssuojaus on puolestaan tasoista korkein ja sitä käytetään puolestaan esimerkiksi rahan ja arvo-omaisuuden sekä salaisen tiedon säilytys- ja käsittelytiloissa, arkistotiloissa, henkilöturvallisuuden kannalta riskialttiissa toimitiloissa yms. tiloissa, joiden toimintaan kohdistuu huomattavia riskejä. Teknisiä turvallisuusjärjestelmiä käytetään pääsääntöisesti tehostettua perussuojausta, erityissuojausta tai täyssuojausta vaativissa tiloissa. (Leppänen 2006, 344-345; Miettinen 2002, 93).

3.3 Vyöhykkeittäin suojaaminen

Toimitilojen suojaustoimenpiteiden yhtenä toteuttamisperiaatteena voidaan pitää vyöhykkeittäin toteutettavaa suojausta. Tällöin suojattava kohde siihen kuuluvine piha-alueineen jaetaan suojausvyöhykkeisiin, joita ovat kehä, alue, kuori, tila sekä kohde. Jokaisella suojausvyöhykkeelle löytyy omat tekniset ja rakenteelliset suojaus- ja valvontamenetelmänsä. (Miettinen 2002, 94; Tikkanen ym. 2007, 161.) Miettisen (2002, 94) mukaan vyöhykkeittäin suojaaminen on yksi toimitilojen suojaamisen ja toimitilaturvallisuuden keskeisimmistä peruselementeistä. Seuraavassa tarkastellaan vyöhykkeittäin suojaamisen periaatetta lyhyesti pääpainon ollessa teknisissä suojaus- ja valvontamenetelmissä.

Ulommaisinta suojausvyöhykettä, johon suojattava alue rajautuu muusta ympäristöstä, kutsutaan kehäksi. Kehäsuojauksessa voidaan käyttää erilaisia rakenteellisia sekä teknisiä turvallisuusratkaisuja vaikeuttamaan alueelle tunkeutumista sekä havaitsemaan alueelle pyrkiviä henkilöitä. Yleisin kehäsuojauksen menetelmä on alueen aitaaminen. Teknisistä turvallisuusjärjestelmistä kehäsuojauksessa voidaan käyttää etenkin kameravalvontaa sekä erilaisia rikosilmoitinjärjestelmän ilmaisimia esimerkiksi aitalinjan valvonnassa. (Tikkanen ym. 2007, 161-162.) Myös kulunvalvontajärjestelmän käyttö aidatun alueen liikenteen ohjaamisessa on usein hyvin perusteltua.

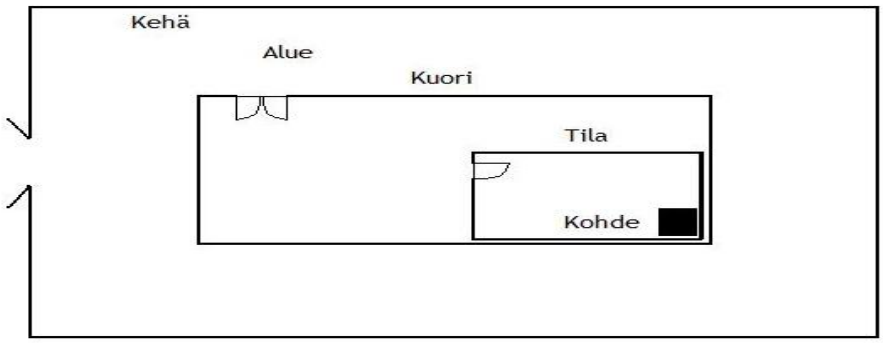
Aluesuojauksella tarkoitetaan kehän ja suojattavan kiinteistön välisen alueen, esimerkiksi piha-alueen, suojaamista ja valvontaa. Aluesuojauksen tarkoituksena on pyrkiä myös vaikeuttamaan, mutta ehkä vielä enemmän havainnoimaan luvatonta alueella liikkumista. Aluesuojauksessa yleensä käytettyjä teknisiä keinoja ovat yleensä alueen kameravalvonta sekä alueelle saapuvan ja alueelta poistuvan liikenteen kulunvalvonta, joka kuitenkin usein toteutetaan varsinaisesti kehävyöhykkeellä. Valaistukseen on myös syytä kiinnittää huomiota esimerkiksi kameravalvontaa ajatellen ja pimeän tarjoaman näkösuojan välttämiseksi. Aluevyöhyke, kuten myös kehävyöhyke kuitenkin jätetään tai joudutaan jättämään usein suojaamatta ja valvomatta. (Miettinen 2002, 95; Tikkanen ym. 2007, 162.)

Kuorisuojauksella tarkoitetaan suojattavan kiinteistön ulkokuoren suojausta. Kuorisuojaus on usein hyvin merkittävässä asemassa, sillä kiinteistön kuori on usein ensimmäinen suojattu vyöhyke. Kuorisuojauksen tarkoituksena on estää ja havaita luvaton tunkeutuminen sisälle yrityksen tai organisaation toimitiloihin ja aiheuttaa hälytys luvattomasta tunkeutumisesta. Teknisistä turvallisuusjärjestelmistä kuorisuojauksessa käytetään pääasiassa rikosilmoitinjärjestelmää kiinteistön ovien sekä ikkunoiden, muiden aukkojen ja luukkujen suojaamiseen ja valvontaan. Myös kameravalvontaa voidaan käyttää kuoren valvonnassa. Kameravalvonta luo ennaltaehkäisevää vaikutusta ja sen avulla havainnot asiattomasta toiminnasta voidaan tehdä välittömästi tai ainakin tallentaa tapahtumat jälkiselvitystä varten. Teknisen ja rakenteellisen

suojauksen välimaastossa lukitus on erittäin tärkeässä asemassa kuorisuojauksessa. Hyvät lukitusratkaisut rajoittavat ja estävät luvatonta liikkumista ja tunkeutumista tehokkaasti. Lukitusratkaisujen tehostamiseksi kuorisuojauksessa voidaankin käyttää kulkemisen kontrolloimiseksi ja luvattoman liikkumisen estämiseksi kulunvalvontajärjestelmää. (Miettinen 2002, 95-96; Tikkanen ym. 2007, 162-163.)

Tilasuojauksella tarkoitetaan suojattavan kiinteistön sisällä olevien tiettyjen suojaamista edellyttävien tilojen suojaamista. Tällaisen tilasuojauksen kohteina voivat olla esimerkiksi yksittäiset huoneet tai tilaryhmät. Tilasuojausta voidaan toteuttaa tehokkaasti kulunvalvonnan ja lukitusten sekä kulkuoikeuksien avulla ja valvomalla tiloja rikosilmoitinjärjestelmän tilailmaisimin sekä kameravalvonnalla. (Miettinen 2002, 96.) Tilasuojaus on kuorisuojauksen ohessa myös hyvin keskeisessä asemassa yritysten ja organisaatioiden toimitilojen suojaamisessa, sillä useimmiten suojaaminen perustuu hyvinkin pitkälti juuri kuoren ja tilojen suojaamiseen ja valvontaan kuoren ollessa ensimmäinen suojattu vyöhyke (K. Starck, henkilökohtainen tiedonanto 16.3.2009).

Kohdesuojauksella tarkoitetaan jonkin tietyn ja tarkasti yksilöidyn, yleensä hyvin arvokkaan, kohteen suojausta. Suojattava kohde voi olla esimerkiksi kassakaappi tai tietokone, jota voidaan suojata siten, että sen murtaminen, liikuttaminen tai muu ei-toivottu toimenpide havaitaan. Kohdesuojauksen vyöhyke on suojausvyöhykkeistä kaikista sisimpänä ja suojattavalla kohteella on siis ympärillänsä myös muut suojausvyöhykkeet. Kohdesuojausta vaativan kohteen suojaustaso saadaan tarvittaessa siis hyvinkin korkeaksi. (Miettinen 2002, 96; Tikkanen ym. 2007, 163.)



Kuva 2: Kiinteistön jaottelu suojausvyöhykkeisiin

4 Tekniset turvallisuusjärjestelmät osana toimitilaturvallisuutta

Teknisten turvallisuusjärjestelmien merkitystä yrityksen tai organisaation turvallisuudelle tulee käsitellä kokonaisvaltaisen turvallisuuden kautta ja miettiä, mitä hyötyjä yritys tai organisaatio teknisillä turvallisuusratkaisuilla saavuttaa. Turvallisuusjärjestelmien on tuettava

yrityksen tai organisaation jokapäiväistä toimintaa ihmisten, toiminnan ja omaisuuden sekä tiedon suojaamisessa. (Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät: opas tilojen omistajille ja käyttäjille 2004, 3-4, 8.) Tekninen turvallisuusvalvonta on erittäin perusteltua silloin, kun pelkkä toimitilojen suojaaminen ei riitä, vaan lisäksi tarvitaan myös valvontaa ihmisten, toimitilojen sekä omaisuuden suojaamiseksi ja turvallisuuden takaamiseksi. Tekninen turvallisuusvalvonta on perusteltu ratkaisu myös silloin, kun rakenteellisen suojauksen parantaminen ja ympäristöolosuhteiden muuttaminen suojaavammiksi on kallista, liian vaikeata tai jopa mahdotonta. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 79.)

Teknisen turvallisuusvalvonnan toteuttaminen käyttöä ja jokapäiväistä toimintaa tukevaksi kokonaisuudeksi vaatii tietämystä eri järjestelmistä, niiden käyttötarkoituksista, tekniikoista, toimintaperiaatteista ja niiden tarjoamista mahdollisuuksista niiden täysipainoiseksi ja tehokkaaksi hyödyntämiseksi. Ns. normaalin turvallisuustason kohteiden turvallisuusjärjestelmien ja suojausten suunnittelu voidaan tavallisesti hoitaa yhdessä kiinteistön muun sähkösuunnittelun kanssa. Teknisten turvallisuusjärjestelmien suunnittelu on usein kuitenkin perusteltua suorittaa omana erillisenä työnään ja mahdollisesti ulkopuolisen ammattilaisen tekemänä. Lähtötilanteessa selvitetään yrityksen tai organisaation turvallisuuden nykytilanne tai turvallisuustaso sekä määritellään turvallisuuden tavoitetaso, jolle yritys tai organisaatio haluaa turvallisuutensa saattaa. Seuraavaksi määritellään keinot, joilla tavoitetasoon pyritään. Massiivisissa ja korkean turvallisuustason tapauksissa suunnittelussa edetään uhkakartoituksen ja riskianalyysin kautta tarvekartoitukseen. Pienemmän mittaluokan tapauksissa voidaan laatia myös tarvekartoitus suunnittelun perustaksi. Tarvekartoituksella on tarkoitus selvittää yrityksen tai organisaation turvallisuustarpeet tilakohtaisesti. (Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät: opas tilojen omistajille ja käyttäjille 2004, 8-10.)

Toimivien ja tehokkaiden teknisten turvallisuusjärjestelmien aikaansaamiseksi on suunnitteluvaiheessa huomioitava myös hankittavan järjestelmän käyttäminen, sillä turvallisuusjärjestelmien käyttäminen vaatii resursseja ja käyttäjät on myös perehdytettävä järjestelmiin ja koulutettava niiden käyttöön. Huomioitavaa on mm. se, että toteutetaanko järjestelmien käyttö omilla henkilöresursseilla vai esimerkiksi ulkoistamalla. Turvallisuusjärjestelmien hankintaa suunniteltaessa on myös huomioitava suojattavassa kohteessa toimivat muut henkilöt, jotka järjestelmien vaikutuksen piiriin joutuvat. Ihmisten asenteilla ja motivaatiolla turvallisuutta kohtaan on suuri merkitys toteutuvan turvallisuuden suhteen, joten heidän motivointiaan ja perehdytystä turvallisuuteen, turvallisuusratkaisuihin ja niiden tarkoitukseen ei saa unohtaa. Teknisten turvallisuusjärjestelmien tehokkuuden ja toimivuuden nimissä on ajateltava myös järjestelmiä hankintojen jälkeen. Erilaiset turvallisuusjärjestelmiin liitettävät palvelut on huomioitava hankintavaiheessa turvallisuusjärjestelmien toiminnan ja tehokkuuden takaamiseksi. (K. Starck, henkilökohtainen tiedonanto 21.4.2009.)

Toimitilaturvallisuudessa tilojen suojaamisen ja valvonnan näkökulmasta keskeisimpiä teknisiä turvallisuusjärjestelmiä ovat kulunvalvonta-, rikosilmoitin-, kameravalvontajärjestelmät. Ne ovat keskeinen osa yrityksen tai organisaation toimitilaturvallisuutta ja tarjoavat hyviä keinoja toimitilojen suojaamiseen sekä valvontaan, kun halutaan ennaltaehkäistä, vähentää ja estää yrityksen tai organisaation toimitiloihin ja suojattaviin arvoihin, kuten mm. ihmisiin ja omaisuuteen kohdistuvia rikoksia ja vahinkotapahtumia sekä rajoittaa ja pienentää näiden seurauksia. Lisäksi teknisten turvallisuusjärjestelmien avulla voidaan pyrkiä jälkikäteen selvittämään tapahtuneita rikos- ja vahinkotapahtumia. Toimitilojen suojaamisen ja valvonnan näkökulmasta teknisten turvallisuusjärjestelmien tehtävät voidaan tiivistää neljään pääkohtaan, joita ovat ennaltaehkäisevän vaikutuksen luominen, ihmisiin sekä liikenteeseen kohdistuva kulkemisen ohjaaminen ja estäminen, rikosten ja uhkatilanteiden havaitseminen ja niistä hälyttäminen sekä tapahtuneiden rikosten ja vahinkotapahtumien selvittämisen mahdollistaminen. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.)

Teknisten turvallisuusjärjestelmien voidaan katsoa olemassa olollaan ennaltaehkäisevän rikoksia ja ilkivaltaa. Ennaltaehkäisevä vaikutus perustuu näkyvään valvontaan tai valvonnan olemassa olon ilmaisemiseen, jolla pyritään tuomaan esiin valvonnan ja kiinnijäämisriskin todellista olemassa oloa. Ennaltaehkäisevä vaikutus ei kuitenkaan aina ole riittävä keino rikosten torjunnassa eikä sen varaan tule yksistään laskea. Ihmisiin ja muuhun liikenteeseen kohdistuvalla ohjaavalla ja estävällä vaikutuksella kontrolloidaan ja ohjataan liikkumista ja liikennettä halutuille kulkureiteille, tarkoituksena tätä kautta ns. vapaan kulkemisen mahdollisuuden poistamisella ennaltaehkäistä ja estää rikoksia. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.) Ns. vapaan kulkemisen mahdollisuuden rajoittamisella tai poistamisella on tarkoitus poistaa osaltaan rikoksen tekemisen mahdollistavia tekijöitä ja rikostilaisuuksia ohjatun ja kontrolloidun kulkemisen avulla. Ennaltaehkäisyllä ja ns. vapaan kulkemisen poistamisella pyritään pienentämään motivaatiota ja kiinnostusta rikosta kohtaan ja poistamaan rikoksen mahdollistavia ja rikosta edesauttavia tekijöitä. Ennaltaehkäisevän vaikutuksen luominen sekä kulkemisen kontrolloiminen ovat sinällään merkittäviä tekijöitä toimitilojen suojaamisen kannalta, sillä niiden vaikutuksesta tekijä voi parhaimmassa tapauksessa luopua rikosaikeistaan jo ennen tekoa, jolloin vahingotkin jäävät syntymättä.

Teknisillä turvallisuusjärjestelmillä voidaan havaita yritykseen tai organisaatioon kohdistuva rikos esimerkiksi luvaton tunkeutuminen toimitiloihin. Yhtä tärkeää kuin itse havainnon tekeminen on se, että havainnosta kulkee tieto eteenpäin sovitulle taholle, joka reagoi tähän ennalta määriteltyjen toimenpiteiden aloittamiseksi. Tällöin rikos voidaan vielä mahdollisesti estää kokonaan tai osittain, jonka lisäksi voidaan rajoittaa vahinkoja ja torjua lisävahinkojen syntyä. Tämä kaikki kuitenkin edellyttää hälytystiedon kulkemista oikealle taholle, esimerkiksi vartiointiliikkeelle. Rikoksen havaitsemisella ja havaintoon ennalta määritellyin toimenpitein reagoimalla pyritään vähentämään rikoksen tekemiseen käytettävissä olevaa aikaa ja

lisäämään kiinnijäämisriskiä. Tekniset turvallisuusjärjestelmät voivat havaita rikoksen, mutta vastatoimenpiteiden käynnistäminen ja tapahtumiin puuttuminen edellyttävät myös havaintoon reagoimista. Myöhemmin tapahtumia voidaan tietysti pyrkiä selvittämään jälkikäteen tekijöiden edesvastuuseen saattamiseksi, mutta vahinkojen rajoittaminen ja torjuminen on usein jo myöhäistä. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.)

Tekniset turvallisuusjärjestelmät ovat tärkeä osa yritysten ja organisaatioiden suojaamista ja valvontaa. On kuitenkin muistettava, että tekniset turvallisuusjärjestelmät eivät yksistään takaa turvallisuutta, mutta ovat oikein ja tehokkaasti käytettyinä ne tukevat ja tehostavat rakenteellisia suojauskeinoja ja ovat hyviä turvallisuusvalvonnan välineitä toimitilojen suojaamisessa ja valvonnassa. (K. Starck, henkilökohtainen tiedonanto 29.1.2009.) Valvonnan mahdollisuus korostaa teknisten turvallisuusjärjestelmien merkitystä toimitilaturvallisuudessa. Yksistään rakenteelliset ratkaisut eivät ole aina riittävän tehokkaita toimitilojen ja omaisuuden suojaamiseksi, sillä suoja-arvoiltaan parhaimmatkaan rakenteelliset ratkaisut eivät ole ohittamattomia ilman valvontaa. Tekniset turvallisuusjärjestelmät täydentävät rakenteellisia ratkaisuja valvonnan kautta ja mahdollistavat reagoinnin ihmisiin, toimitiloihin ja omaisuuteen kohdistuviin rikos- ja uhkatapahtumiin. Tekniset turvallisuusjärjestelmät ikään kuin parantavat rakenteellisten ratkaisujen suoja-arvoa. Myös Tikkasen ym. (2007, 205) mukaan tekniikan tarjoamat keinot tehostavat rakenteellista turvallisuutta ja toimivat apuvälineenä ihmisen suorittamalle turvallisuusvalvonnalle. Usein tekninen valvonta voi myös vähentää esimerkiksi vartioinnin tarvetta. (Tikkanen ym. 2007, 205.)

5 Kulunvalvontajärjestelmä

Kulunvalvontajärjestelmän tarkoituksena on toimitilojen turvallisuuden varmistaminen ja omaisuuden suojaaminen ohjaamalla ja rajoittamalla kulkemista sekä estämällä luvatonta kulkemista toimitiloissa. Kulunohjaus, kulkemisen rajoittaminen sekä luvattoman kulkemisen estäminen kohdistuvat sekä yrityksen tai organisaation omaan henkilöstöön, että myös ulkopuolisiin henkilöihin. Kulunvalvontajärjestelmää voidaan hyödyntää myös muissa kuin suoranaisesti turvallisuuteen liittyvissä toiminnoissa. Kulunvalvontajärjestelmän osaksi voidaan liittää esimerkiksi työajanseurantajärjestelmä, joka toimii ensisijaisesti työntekijöiden työajanseurantamenetelmänä, mutta jonka avulla yhdessä kulunvalvonnan tietojen kanssa voidaan saada esimerkiksi tieto toimitiloissa sillä hetkellä olevista henkilöistä. Tällainen tieto voi olla tärkeää esimerkiksi erilaisissa uhka- ja vaaratilanteissa, erityisesti esimerkiksi suurilla teollisuusalueilla. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 41; Leppänen 2006, 366-367.)

Robert Gruberin (2006, 248) mukaan kulunvalvontajärjestelmällä pyritään estämään ulkopuolisten henkilöiden sisäänpääsyä ja kulkemista toimitiloissa sekä ohjaamaan ja rajaamaan kulkuoikeutettujen henkilöiden kulkua siten, että heillä on pääsy vain niihin tiloihin, joihin heille

on kulkuoikeus myönnetty. Työntekijöiden kulkuoikeudet voidaan rajoittaa esimerkiksi vain niihin tiloihin, joihin heidän on työtehtäviensä suorittamisen vuoksi päästävä. Kulunvalvontajärjestelmällä pyritään siis kontrolloimaan luvallista kulkemista ja estämään luvaton pääsy toimitiloihin ja luvaton kulkeminen toimitilojen sisällä. (Gruber 2006, 248.)

Ohjaamalla kulkemista liikenne voidaan keskittää tietyille reiteille ja kulun rajoittamisella voidaan rajata kulkeminen sallituksi esimerkiksi tiettyihin tiloihin vain tiettynä ajankohtana tai vain tietyille henkilöille, sillä yrityksen tai organisaation koko henkilöstöllä tarvitsee harvoin olla kulkuoikeudet kaikkiin tiloihin. Kuten aiemminkin on jo todettu, kulkemisen estäminen kohdistuu siis yrityksen tai organisaation ulkopuolisten henkilöiden lisäksi myös yrityksen tai organisaation omaan henkilökuntaan. Ulkopuolisten henkilöiden pääsyä yrityksen tai organisaation toimitiloihin on pyrittävä estämään jo esimerkiksi sisäänkäyntien kulunvalvonnalla. Mikäli sisäänkäynneiltä on vapaa kulku esimerkiksi aulatiloihin, on tärkeää, että aulatiloista varsinaisiin työ- yms. tiloihin johtavat kulkureitit ovat kulunvalvottuja vapaan kulkemisen estämiseksi ns. varsinaisiin työskentelytiloihin. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.)

Voidaankin katsoa, että kulunvalvontajärjestelmän tehtävänä laajemmassa perspektiivissä on estää ns. vapaa kulkeminen toimitiloissa ja kontrolloida luvallista kulkemista. Kulunvalvontajärjestelmän kulkemista estävän vaikutuksen voidaan sinänsä itsessään katsoa kuitenkin olevan rajallinen, sillä kulkemisen kontrollointiin ja estämiseen liittyy myös paljon muita tekijöitä kuin itsessään pelkkä kulunvalvontajärjestelmä. Murtosuojauksen kannalta kulkemisen estämiseen liittyvät esimerkiksi ovet ja niiden lukitukset, sillä mikäli ovi tai siinä oleva lukko eivät ole tarpeeksi jykeviä ja murtovarmoja, ei kulunvalvontajärjestelmäkään voi estää kulkemista, jos ovi helposti murrettavissa tai muuten ohitettavissa. Onnistuneen kulunvalvonnan, kulunvalvonnan tarkoituksen ja tavoitteiden toteutumisessa, on suuri merkitys myös kulunvalvontajärjestelmän piirissä olevilla kulkuoikeutetuilla henkilöillä ja heidän asenteillaan kulunvalvontaa kohtaan. Kulunvalvontajärjestelmä ei pysty estämään kulkemista, jos kulunvalvontajärjestelmä ohitetaan kulkuoikeutettujen henkilöiden huolimattomuuden tai välinpitämättömyyden seurauksena, esimerkiksi päästämällä ulkopuolinen henkilö sisään samalla oven aukaisulla tai kiilaamalla ovia auki kulkemisen helpottamiseksi. Tällaista kulkemista kulunvalvontajärjestelmä ei itse pysty estämään, vaan kulkuoikeutettujen henkilöiden on itse puututtava tähän. Ensiarvoisen tärkeää on kuitenkin muistaa, että kulunvalvontajärjestelmällä ei saa eikä sen tarkoitus ole hankaloittaa kulkuoikeudet omaavien henkilöiden kulkemista. Kulkemisen on tapahduttava sujuvasti, mutta turvallisuudesta tinkimättä. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.)

Luvattoman tunkeutumisen ja liikkumisen estämisen voidaan katsoa pohjautuvan hyvin pitkälti toimitilojen tila- ja lukitusratkaisuihin, sillä oletuksella, että toimitilojen kulunvalvotut

ovet olisivat lukittuja ilman kulunvalvontajärjestelmääkin. Kulunvalvontajärjestelmä ei itsessään estä kulkemista, mutta sen voidaan katsoa tarjoavan keinon ja erilaisia mahdollisuuksia toimitiloissa liikkumisen kontrollointiin sekä valvontaan. Kulunvalvontajärjestelmän ja sähköisen lukituksen avulla voidaan nostaa toimitilojen lukitusratkaisujen turvallisuustasoa ja mahdollistaa kulkemisen kontrollointi. Kulunvalvontajärjestelmä kontrolloi kulkemista epäämällä tai sallimalla kulkemisen kulkuoikeuksiin perustuen, lisäksi kaikki kulkutapahtumat ovat myöhemmin todennettavissa järjestelmästä. Tämä luonnollisesti edellyttää, että yrityksen tai organisaation kulunvalvontajärjestelmä on systemaattisesti toteutettu kattaen kaikki keskeisimmät kulkureitit. Kulunvalvontajärjestelmästä ei ole mitään hyötyä, niin kuin ei olisi mekaanisestakaan lukituksesta, mikäli kulunvalvottu ovi pystytään kiertämään kulkemalla esimerkiksi toista reittiä. Kulunvalvontajärjestelmän voidaankin sanoa ikään kuin hallinnoivan toimitilojen kulkureittejä, ovia ja niiden lukitusta.

Yksi kulunvalvontajärjestelmän keskeisimpiä tähän liittyviä etuja onkin se, että sen avulla voidaan vähentää mekaanisten avainten tarvetta tai korvata mekaanisten avainten käyttötarve käytännössä kokonaan. Tätä kautta kulunvalvontajärjestelmällä voidaan parantaa yrityksen tai organisaation lukitusturvallisuutta sekä avainhallintaa, sillä kulkuoikeuksien myöntäminen on yksinkertaista ja kulkuoikeudet voidaan määritellä henkilökohtaisesti. Mekaanisten avainten riskit liittyvät avainten katoamiseen sekä varastamiseen ja pahimmillaan yhdenkin avaimen katoaminen voi johtaa siihen, että yrityksen tai organisaation kaikki lukot, joihin kyseinen avain käy, on sarjoitettava uudelleen. Kulunvalvontajärjestelmän ”avaimen” eli kulkutunnisteen kadotessa tai joutuessa vääriin käsiin, voidaan kyseinen kulkutunniste poistaa kulkuoikeuksineen järjestelmästä yksinkertaisesti ja nopeasti. Keskeistä tässä on, että tämä ei vaikuta eikä tuo muutoksia muihin asioihin. Lukkoja ei esimerkiksi tarvitse sarjoittaa uudelleen, joka puolestaan pienentää esimerkiksi avainhävikin aiheuttamia kustannuksia. Sen jälkeen, kun kadonnut kulkutunniste on kuoletettu ja poistettu järjestelmästä, voidaan se korvata nopeasti uudella ja luovuttaa oikealle käyttäjälle. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 41.)

Kulunvalvontajärjestelmällä pystytään yhdistämään nykyään myös useampia rakennuksia tai eri toimipisteitä yhdeksi järjestelmäksi tietoverkon avulla. Tällöin yrityksen tai organisaation, jolla on useampia toimipisteitä, ei tarvitse hankkia jokaiseen toimipisteeseen omaa järjestelmää, vaan jokaisen toimipisteen kulunvalvonta toimii yhdellä ja samalla järjestelmällä. Tällainen ratkaisu voi tulla kyseeseen esimerkiksi tilanteessa, jossa henkilöiden on päästävä kulkemaan eri toimipisteissä. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 43.)

Kulunvalvontajärjestelmän keskusyksikön muistiin tallentuu tieto kaikista kulkutapahtumista, sekä sallituista, että estetyistä kuluista, joten kaikki kulkutapahtumat voidaan todentaa jälkikäteen. Kulunvalvontajärjestelmästä voidaan myös siirtää valvontatietoja rikosilmoitinjärjes-

telmään ja sitä kautta tarvittaessa esimerkiksi vartiointiliikkeelle, tämä helpottaa esimerkiksi ovien lukitusten valvontaa etenkin isoissa kiinteistöissä. Kulkutapahtumien tarkastelua varten kulunvalvontajärjestelmän keskusyksikön lokitiedostoista voidaan ottaa erilaisin kriteerein kulku- ja hälytysraportteja. Kriteereinä voidaan käyttää esimerkiksi tietyn henkilön kulkutapahtumia, tietyllä ovella tai tiettynä aikana tapahtuneita kulkuja tai ei sallittuja kulkuyrityksiä. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 41.) Esimerkiksi yrityksessä tai organisaatiossa sattuneen rikos- tai vahinkotapauksen selvittämiseksi kulunvalvontajärjestelmästä saatavilla kulkutiedoilla voidaan pyrkiä selvittämään tiloissa olleita ja käyneitä henkilöitä. (Leppänen 2006, 365). Tässä tosin täytyy muistaa se, mitä jo aiemmin todettiin, että kulunvalvontajärjestelmä ei itsessään estä asiatonta kulkemista, mikäli järjestelmä muuten ohitetaan. Tällaisessa tilanteessa ei siten voi aina täysin luottaa esimerkiksi kulkutapahtumatietoihinkaan.

5.1 Kulunvalvontajärjestelmän rakenne ja laitteet

Kulunvalvontajärjestelmä koostuu pääasiassa keskusyksiköstä, keskittimistä ja pääteohjaimista sekä kulunvalvontalukijoista ja kulkutunnisteista. Keskittimistä ja pääteohjaimista voidaan käyttää järjestelmästä riippuen myös nimityksiä kuten mm. paikallisohjain tai alakeskus. Keskitin ja pääteohjain voivat esimerkiksi olla samanlaisia laitteita, joita kuitenkin käytetään eri yhteyksissä eri tarkoituksiin. Kulunvalvontajärjestelmän piiriin kuuluvat ovet liitetään pääteohjaimien kautta keskusyksikköön. Ne ohjaavat niihin liitettyjen ovien ja kenttälaitteiden toimintaa itsenäisesti ja keräävät niihin liitetyiltä ovilta ja lukijoilta tietoja ja lähettävät ne edelleen keskusyksikölle. Kulunvalvontajärjestelmä tarvitsee luonnollisesti myös sähkönsyöttöä ja tarvittaessa sen akkuvarmennusta. Kulunvalvontajärjestelmän laitteet, keskuslaite, keskittimet ja pääteohjaimet, voidaan sijoittaa periaatteessa mihin tahansa tilaan, johon voitaisiin sijoittaa muitakin atk- ja elektroniikkalaitteita. Laitteiden sijoituspaikkaa valittaessa on kuitenkin huomioitava, että kyseessä on turvallisuusjärjestelmä. Sopivia tiloja ovat esimerkiksi ulkopuolisilta suljetut, valvonnan alla olevat tilat. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 43-45.)

Kulunvalvontajärjestelmän keskusyksikkönä toimii yleensä PC-palvelin käyttöjärjestelmineen sekä hallintaohjelmistoineen. Palvelimen hallintaohjelmisto voi sisältää erilaisia toiminnallisia ominaisuuksia, kuten esimerkiksi kulunvalvonnan valvomo-ohjelmiston, kulunvalvontaohjelmiston henkilöiden ja kulkuoikeuksien perustamiseksi järjestelmään, vieraskirjaohjelmiston vierailijoita varten sekä henkilökortin tulostusohjelmistosta. Kulunvalvontajärjestelmä voi sisältää myös erilaisia ohjelmistorajapintoja, kuten esimerkiksi henkilöstöhallinnon ohjelmistojen ja kulunvalvontajärjestelmän välistä tiedonsiirtoa varten. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 43.) Kulunvalvontajärjestelmän hallinnoimiseksi ja käyttämiseksi kulunvalvonnasta vastaavalle henkilölle tai henkilöille voidaan asentaa kulunvalvontajärjestelmän

työasemaohjelma eli ns. client. Tällöin kulunvalvontajärjestelmän keskusyksikkö voidaan sijoittaa muualle, esimerkiksi erilliseen laitetilaan, mutta kulunvalvonnasta vastaava henkilö voi hallinnoida ja käyttää kulunvalvontajärjestelmää esimerkiksi työhuoneestaan.

Järjestelmästä riippuen, joissain järjestelmissä kenttälaitteiden on oltava koko ajan yhteydessä palvelimeen, kun taas joissain järjestelmissä kulunvalvonnan toiminta ei vaadi jatkuvaa yhteyttä ovilta palvelimelle, tällöin edes palvelimen väliaikainen toimintakatkos ei vaikuta kulunvalvontajärjestelmän toimintaan esimerkiksi ovien kulunvalvonnan suhteen. Keskusyksikön sähkönsyötön varmennus on välttämätöntä, mikäli keskusyksikön on oltava koko ajan yhteydessä oviin. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 43-44.) Kulunvalvontajärjestelmän palvelinympäristö voidaan myös varmistaa kahdentamalla. Tällöin pääpalvelimen vikaantuessa pääpalvelimen ylläpitämä, normaalisti passiivitilassa oleva varapalvelin alkaa välittömästi toimia pääpalvelimen tilalla kulunvalvonnan häiriintymättä.

5.2 Kulunvalvontalukijat ja tunnisteet

Lähes kaikkien uusien kulunvalvontajärjestelmien lukijat ja kulkutunnisteet perustuvat passiiviseen etälukutekniikkaan. Lukijoita ja tunnisteita, joissa tunniste laitetaan osittain tai kokonaan lukijan sisään nähdään pääsääntöisesti enää vanhojen järjestelmien kohdalla. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 45.) Tästä johtuen, on tässä yhteydessä katsottu tarkoituksenmukaiseksi keskittyä etälukutekniikkaan jättäen muut tekniikat vähemmälle huomiolle.

Etälukutekniikan etuna on sujuvampi kulkutapahtuma, kun tunnistetta ei tarvitse asettaa lukijan aukkoon, vaan kulkutunnistetta ainoastaan ns. näytetään kulunvalvontalukijalle. Kulkutunniste voi olla tyyliltään esimerkiksi ns. avaimenperätunniste tai vaihtoehtoisesti luottokorttimallinen kortti. Lukuetäisyys voi olla muutamasta senttimetristä muutamaan kymmeneen senttimetriin. Passiiviseen etälukutekniikkaan periaatteena on, että kulkutunniste saa tarvitsemansa energian lukijan muodostamasta sähkökentästä, jolloin kulkutunniste lähettää tunnistenumeronsa lukijalle, joka puolestaan välittää tämän koodin kyseisen oven ohjauslogiikalle. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 45-46.)

Kulunvalvontajärjestelmässä käytettävistä lukijoista tyypillisimpiä ovat tavalliset lukijat sekä pin-koodilukijat. Kulkeminen tavallisella lukijalla varustetulla ovesta tapahtuu ainoastaan luettamalla kulkutunnistetta lukijalla ja pin-koodilukijalla varustetun oven avaamiseen tarvitaan kulkutunnisteen lisäksi myös henkilökohtainen pin-koodi. Pin-koodilukijoiden käyttö parantaa kulunvalvonnan turvallisuustasoa ja niiden käyttö on perusteltua esimerkiksi tärkeimpien tilojen kulunvalvonnassa tai ulko-ovilla. Vaatimalla pin-koodia sisäänpääsyyn voidaan torjua esimerkiksi varastetulla kulkutunnisteella sisään pyrkimistä. Myös esimerkiksi työajan

ulkopuolella tapahtuva sisään kulkeminen on usein perusteltua keskittää pin-koodilukijalla varustetulle ovelle. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 56.) Kulunvalvonnan turvallisuustasoa voidaan nostaa myös esimerkiksi edellyttämällä kahden kulkuoikeutetun henkilön kulkutunnisteen luetusta kulkemisen sallimiseksi. Vaihtoehtoisesti voidaan edellyttää myös, että henkilö on kulkenut tunnisteellaan ensin tietyn alueen kautta, ennen kuin henkilö voi päästä jollekin toiselle tietylle alueelle. Lisäksi kulkutunnisteita voidaan asettaa ns. seurantaan, jolloin kulunvalvontajärjestelmä tekee ilmoituksen, kun kyseistä kulkutunnistetta käytetään. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.)

Kuva 3: Tavallinen sekä pin-kulunvalvontalukija (Access Basic; Access 8 CM Pin)

Tavallisten kulunvalvontalukijoiden ja pin-koodilukijoiden lisäksi kulunvalvonnassa voidaan käyttää biometriseen tunnistukseen perustuvaa teknologiaa turvallisuustason parantamiseksi. Ne ovat kuitenkin verrattain kalliita perinteisiin lukijoihin ja tunnisteisiin nähden, eivätkä ole vielä levinneet kovin laajaan käyttöön. Biometriseen tunnistukseen liittyviä tunnistuskeinoja voivat olla esimerkiksi sormenjälki, ääni, kasvojen piirteet tai silmän verkkokalvo, joissa tunnistus perustuu matemaattisin algoritmein saatuihin yksilöllisiin koodeihin. Käytännössä esimerkiksi sormenjälkitunnistuksessa tunnistekortille on tallennettu henkilön sormenjäljen vastine. Kun henkilö luettaa tunnistettaan sekä sormeaan lukijassa, suorittaa lukija bioverifioinnin kulkutunnisteen ja aidon sormenjäljen välillä. Tämä vaatii kehittyneempää teknologia myös itse tunnisteen puolelta. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.)

5.3 Kulunvalvontajärjestelmään liitettävät ovet

Kulunvalvotuilla ovilla tarkoitetaan kulunvalvontalukijoilla ohjattuja ja valvottuja ovia. Oven kulunvalvonta voidaan toteuttaa ns. yksi- tai kaksipuoleisesti. Mikäli kulkemista halutaan kontrolloida vain toiseen suuntaan, toteutetaan kulunvalvonta yksipuoleisesti. Tällöin kulunvalvotussa ovessa lukija on vain oven toisella puolella ja vastakkaiseen suuntaan kulkiessa oven avaaminen tapahtuu esimerkiksi avaus-/poistumispainikkeen avulla. Mikäli ovella halutaan kontrolloida sekä sisään, että ulos kulkemista voidaan kulunvalvonta toteuttaa myös kaksipuoleisesti, jolloin oven kummallekin puolelle, sisä- ja ulkopuolelle, asennetaan lukijat.

Tällöin sekä sisään, että ulos kulkemiseen tarvitaan kulkutunnistetta. Yleensä tärkeimpien ja korkeampaa turvallisuutta vaativien tilojen ovet on syytä olla ns. kaksipuoleisesti kulunvalvottuja. Kulunvalvontaan voidaan liittää myös portteja, puomeja sekä hissejä. Tällöin porteista ja puomeista tapahtuu myös kulkutunnistetta kulunvalvontalukijassa luettaen. Hissikulunvalvonta puolestaan voidaan toteuttaa esimerkiksi siten, että hissin kulunvalvontalukija aktivoi kulkutunnisteen luetuksesta vain ne kerrokset valittaviksi, joihin kyseisellä kulkijalla on kulkuoikeus. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 56-58.) Vaihtoehtoisesti hissikulunvalvonta voidaan toteuttaa myös siten, että ainoastaan sellaisten henkilöiden on mahdollisuus käyttää hissiä, joille on tähän kulkuoikeudet myönnetty. Tällöin hissi toimii periaatteessa kuten kulunvalvottu ovi ja hissiin pääsee ainoastaan henkilöt, joilla tähän on kulkuoikeus.

Toimitilojen kaikkia ovia ei kuitenkaan aina ole välttämätöntä varustaa kulunvalvontalukijoilla, mutta ovien liittäminen kulunvalvontajärjestelmään ovien tilan ja lukituksen valvomiseksi tai ovien tilan ja lukituksen valvomiseksi ja ohjaamiseksi on kuitenkin monesti perusteltua. Tällaisia ovia voivat olla esimerkiksi hätäpoistumisteiden ovet, ne ulkokuoren ovet, joista ei haluta kuljettavan sisään sekä muut kiinteistön turvallisuuden kannalta tärkeät ovet, joita ei kuitenkaan ole tarpeen varustaa kulunvalvontalukijalla. Kulunvalvontajärjestelmään voidaan siis liittää kulunvalvottujen ovien lisäksi ns. valvottuja ovia tai ohjattuja sekä valvottuja ovia. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 52-53.)

Valvotun oven kohdalla kulunvalvontajärjestelmä voi valvoa itse oven sekä sen lukituksen tilaa. Valvontatietoja voidaan saada esimerkiksi siitä, onko ovi auki vai kiinni ja onko lukko auki vai kiinni. Valvotun oven lukon tilaa voidaan valvoa esimerkiksi teljen tilan perusteella, onko telki sisällä tai ulkona, tai telkipesän mikrokytkimellä, joka on kuitenkin herkkä vikaantumaan ja helposti sabotoitavissa. Pelkkää oven tilaa, eli onko ovi auki vai kiinni, voidaan valvoa myös esimerkiksi magneettikoskettimella. Valvontatietojen avulla voidaan siis valvoa esimerkiksi onko ovi kiinni ja lukossa tai kiinni lukon kuitenkin ollessa auki tai onko ovi kokonaan auki. Ovien tilan ja lukituksen valvonta helpottaa esimerkiksi vartiointia, kun jokaista ovea ei tarvitse erikseen kokeilla, vaan ovien tila nähdään kulunvalvontajärjestelmästä. Ohjattu ja valvottu ovi poikkeaa valvotusta ovesta siten, että ohjatun ja valvotun oven sähkölukkoa voidaan ohjata manuaalisesti tai aikaperusteisesti. Poistuminen ohjatun ja valvotun oven kautta on yleensä mahdollista toiseen suuntaan avaus-/poistumispainikkeen avulla, jota painamalla oven lukko avautuu. Toiseen suuntaan kyseisestä ovesta ei tällöin pääse vapaasti kulkemaan. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 52-55.)

6 Rikosilmoitinjärjestelmä

Rikosilmoitinjärjestelmällä ts. murtohälytysjärjestelmällä on tarkoitus suojata ja valvoa yrityksen tai organisaation suojattavia arvoja, kuten ihmisten sekä omaisuuden koskemattomuutta. Rikosilmoitinjärjestelmän ensisijaisena tehtävänä on valvoa yrityksen tai organisaati-

on toimitiloja sekä siellä olevaa omaisuutta luvattoman tunkeutumisen, luvattoman tiloissa liikkumisen ja muiden rikosten varalta. Rikosilmoitinjärjestelmän tavoitteena on havaita yrityksen tai organisaation toimitiloihin kohdistuvat mahdolliset rikokset ja luvattomat tunkeutumiset suojattuihin tiloihin nopeasti sekä välittää tästä hälytystieto ennalta määrätylle taholle, esimerkiksi vartiointiliikkeen hälytyskeskukseen. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 77-79.) Yhtä tärkeää kuin järjestelmän tekemä havainto esimerkiksi luvattomasta tunkeutumisesta, on hälytyksensiirto ennalta määritellylle taholle, esimerkiksi juuri vartiointiliikkeen hälytyskeskukseen, jolloin vartiointiliike voi käynnistää toimenpiteet rikoksen ja siitä syntyvien vahinkojen estämiseksi ja rajoittamiseksi. Havainnosta, josta ei välity hälytystä eteenpäin, ei käytännössä ole juurikaan hyötyä, sillä estäviä ja rajoittavia toimenpiteitä ei osata aloittaa, kun tietoa tapahtumista ei ole. Huomioitavaa on, että vartiointiliikkeellä on oltava valmius sekä ennalta määritellyt tavat ja toimenpiteet hälytyksiin reagoimiseksi. (Garcia 2001, 53.)

Rikosilmoitinjärjestelmällä suojattavat ja valvottavat kohteet voivat olla hyvinkin erilaisia, mutta kohteilla voidaan kuitenkin katsoa olevan olemassa ainakin yksi tai useampi yhteinen piirre. Tällaisia piirteitä kohteissa ovat huomattava määrä arvokasta tietoa tai omaisuutta, rahaa tai helposti rahaksi muutettavaa omaisuutta tai muista syistä, esimerkiksi toiminnan luonteesta johtuva, korkea riski joutua rikoksen kohteeksi. Yrityksen tai organisaation valitseman turvallisuustason toteutuminen tai turvallisuustason kehittäminen voivat myös olla kohteen suojaamista rikosilmoitinjärjestelmällä puoltavia tekijöitä. Rikosilmoitinjärjestelmän tarpeellisuutta kohteen suojaamisessa ja valvonnassa puoltavat myös sellaiset tilanteet ja tekijät, joissa esimerkiksi rakenteellisen turvallisuuden ja ympäristöolosuhteiden parantaminen on vaikeata, suhteettoman kallista tai jopa mahdotonta tai mikäli yritykseen tai organisaatioon on aikaisemmin kohdistunut rikoksia. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 79.)

Takalan (1998, 10-12) mukaan rikos edellyttää tapahtuakseen motivoitunutta rikoksentekijää, rikoskohdetta sekä kykenevän valvojan puuttumista. Kykenevällä valvojalla voidaan tarkoittaa jokaista, joka pystyy tapahtumien kulkuun puuttumalla vaikuttamaan rikokseen ehkäisevästi. Tapahtumien kulkuun puuttumisella tarkoitetaan esimerkiksi toimintaa rikostilanteessa, jolloin valvoja tulee rikoskohteen suojaksi tai hälyttää poliisit. Kykenevästä valvojasta voidaan puhua kuitenkin vain silloin kun rikoksen tekijä itse kokee valvonnan ns. rikoksen pilaavaksi. (Takala 1998, 10-12.) Näin rikosilmoitinjärjestelmää voitaisiin siis pitää kykenevänä valvojana, mikäli rikoksentekijä uskoo rikosilmoitinjärjestelmän hälytyksen estävän rikoksen tai aiheuttavan kiinnijäämisen esimerkiksi vartijan saapuessa paikalle hälytyksen johdosta.

Rikosilmoitinjärjestelmän kohdalla aika onkin hyvin merkittävä tekijä. Mitä aikaisemmin ja nopeammin tunkeutumisen alkamisesta saadaan havainto ja hälytystieto siirrettyä esimerkiksi

vartiointiliikkeen hälytyskeskukseen ja asianmukaiset toimenpiteet aloitettua, sitä lyhyemmäksi jää rikoksen tekemiseen käytettävissä oleva aika. Rikokseen käytettävissä olevan ajan pieneneminen puolestaan kasvattaa kiinnijäämisriskiä. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 77.) Rikosilmoitinjärjestelmän hälytys olisi siis tärkeää saada vartiointiliikkeen tietoon mahdollisimman nopeasti tunkeutumisen aloittamisesta ja mahdollisimman etäällä siitä suojattavasta kohteesta tai omaisuudesta, mitä tunkeutumisella tavoitellaan. Lisäksi on myös tärkeää, että rikosilmoitinjärjestelmän tekemän ensimmäisen havainnon jälkeen tunkeutujan ja tämän tavoitteleman kohteen välillä, on paitsi mahdollisimman paljon etäisyyttä, niin myös riittävästi suojausratkaisuja, jotka hidastavat tai estävät tunkeutujan tunkeutumista tavoitteeseensa, kunnes esimerkiksi vartiointiliikkeen vartija ennättää kohteeseen. (Garcia 2001, 5.)

Rikosilmoitinjärjestelmän avulla voidaan siis parhaimmassa tapauksessa estää tai keskeyttää tunkeutuminen, mikäli hälytykseen ehditään reagoimaan riittävän nopeasti ennen kuin tunkeutuja saavuttaa todellisen tavoitteensa, rikoksella tavoittelemansa hyödyn. Vaikka rikos sinänsä on jo tapahtunut, jäävät vahingot usein vähäisemmiksi ja tunkeutuja voidaan myös saada verekseltänsä kiinni. Mikäli tunkeutuja kuitenkin ehtii viedä rikoksensa loppuun ja poistumaankin paikalta, voidaan rikosilmoitinjärjestelmän hälytykseen reagoimalla kuitenkin pyrkiä rajoittamaan ja torjumaan lisävahinkoja. Kunhan tunkeutumisesta vain saadaan havainto ja hälytystieto esimerkiksi vartiointiliikkeelle, voidaan ainakin jälkivahinkojen torjunta ja tapahtumien selvittäminen aloittaa mahdollisimman pian. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.)

Rikosilmoitinjärjestelmä voi antaa myös näkyvän ja/tai kuuluvan paikallishälytyksen suojattavassa kohteessa esimerkiksi sireenin avulla. Paikallishälytys voi ikään kuin täydentää hälytystä siten, että järjestelmä hälyttää sekä suojattavassa kohteessa ja välittää samalla myös hälytystiedon esimerkiksi juuri vartiointiliikkeen hälytyskeskukseen. Nämä eivät siis ole toisiaan poissulkevia vaihtoehtoja. (Leppänen 2006, 364.) Paikallishälytyksen tarkoituksena voidaan katsoa olevan pelotevaikutuksen luominen ilmaisemalla tunkeutujalle, että hänet on havaittu. Parhaimmassa tapauksessa paikallishälyttimen hälytys voi saada tunkeutujan luopumaan rikoksen jatkamisesta. Lisäksi paikallishälytyksen tarkoituksena on pyrkiä kiinnittämään lähistöllä mahdollisesti olevien sivullisten henkilöiden huomio ja saada heidät esimerkiksi ilmoittamaan asiasta eteenpäin tai painamaan tekijöiden tuntomerkit ylös virkavallan jatkotoimenpiteitä varten. Aina rikosilmoitinjärjestelmään ei kuitenkaan haluta liittää paikallishälytintä ja paikallishälyttimen tarkoituksenmukaisuutta onkin harkittava aina tapauskohtaisesti. Pelkästään paikalliseen hälytykseen perustuva rikosilmoitusjärjestelmä ei kuitenkaan ole suositeltava vaihtoehto, sillä paikallishälytys ei kuitenkaan itsessään estä mitään eikä takaa sitä, että joku hälytykseen reagoisi. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 103.) Paikallishälytyksen etujen vastakohtana on punnittava paikallishälytyksen mahdollisia haittavai-

kutuksia. Paikallishälytyksen perusteella rikoksen tekijä voi ennakoida esimerkiksi vartijan saapumisen paikalle ja varautua tähän. Eikä ole tarkoituksenmukaista eikä suositeltavaa, että esimerkiksi sivulliset menisivät puuttumaan mahdolliseen rikokseen, jolloin seuraukset saattavat koitua vakaviksi, jopa kohtalokkaiksi.

Rikosilmoitinjärjestelmän kohdalla huomioitavaa on se, että perinteisesti rikosilmoitinjärjestelmällä valvotaan toimitiloja pääsääntöisesti aikoina, jolloin tiloissa ei ole toimintaa. Rikosilmoitinjärjestelmään voidaan kuitenkin soveltaa myös muuhun kuin perinteiseen tunkeutumisen valvontaan. Henkilöturvakäytössä rikosilmoitinjärjestelmää voidaan käyttää myös esimerkiksi päiväsaikaan. Rikosilmoitinjärjestelmää voidaan soveltaa esimerkiksi henkilöturvallisuudessa erilaisten uhkatilanteiden, kuten ryöstö- ja ns. päällekarkaustilanteiden varalta. Tällaista valvontaa voidaan kutsua esimerkiksi ryöstöilmaisuksi tai ryöstösuojaukseksi tai vain rikosilmoitinjärjestelmän avulla toteutetuksi henkilöturvajärjestelmäksi asiayhteydestä riippuen. Henkilöturvakäytössä rikosilmoitinjärjestelmän tarkoituksena on mahdollistaa avun hälyttäminen uhkaavassa tilanteessa. Avun hälyttäminen tapahtuu rikosilmoitinjärjestelmään liitetyillä painikkeilla, jotka voivat olla esimerkiksi kiinteitä tai mukana pidettäviä painikkeita tai varta vasten tiettyyn tarkoitukseen tarkoitettuja mekanismeja, kuten esimerkiksi kassan tyhjentämiseen reagoiva hälytysmekanismi. Henkilöturva- tai ryöstöhälytyksen ei tulisi laukaista paikallishälytystä, mikäli tällainen ominaisuus kyseisessä rikosilmoitinjärjestelmässä on. Hälytys tulisi aina välittää ns. hiljaisena hälytyksenä ennalta sovitulle taholle, kuten esimerkiksi vartiointiliikkeelle ja/tai muille työntekijöille. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 101.)

Rikosilmoitinjärjestelmän avulla voidaan saada myös hälytys esimerkiksi tulipaloista tai vesivahingoista. Tulipalon varalta rikosilmoitinjärjestelmään voidaan liittää jälleenannolla varustettu palovaroitin ja vesivahingon varalle järjestelmään voidaan liittää jonkinlainen vesivuotohälytin tai kosteusanturi. Hälytyksen tullessa rikosilmoitinjärjestelmä välittää hälytyksen eteenpäin ennalta määrätylle taholle. Tällaisten vaaratilanteiden valvonta voi olla aiheellista rikosilmoitinjärjestelmän avulla pienissä kohteissa, silloin kun edellä mainittujen tilanteiden valvontaan ei ole omaa erillistä järjestelmäänsä, esimerkiksi automaattista paloilmoitinjärjestelmää. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 80.)

6.1 Rikosilmoitinjärjestelmän rakenne

Rikosilmoitinjärjestelmä koostuu pääpiirteissään prosessoripohjaisesta keskuslaitteesta eli rikosilmoitinkeskuksesta, ilmoituksensiirtolaitteistosta sekä erilaisista ilmaisimista ja sähkönsyötöstä ja akkuvarmennuksesta. Rikosilmoitinjärjestelmään voidaan liittää myös erilaisia muita ilmaisimia tai hälytyspainikkeita, joilla voidaan valvoa esimerkiksi savunmuodostusta tai kosteutta tai henkilöturvallisuutta. Lisäksi rikosilmoitinjärjestelmään liittyy myös erilaisia

käyttö- ja ohituslaitteita sekä paikallishälyttimiä. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 81-84, 103.)

Käyttölaitteella voidaan käytännössä katsoen tehdä kaikki rikosilmoitinjärjestelmään liittyvät ohjaus-, ohjelmointi- ja käyttötoimenpiteet käyttäjän henkilökohtaisen koodin avulla. Käyttölaitteella voidaan esimerkiksi kytkeä rikosilmoitinjärjestelmä päälle tai pois päältä, ns. yö- tai päivätilaan tai tehdä yksittäisen tai useamman silmukan irtikytkentä silmukan tai silmukoiden kytkemiseksi pois valvontatilasta. Käyttölaitteet ovat yleensä varustettu näppäimistöllä ja esimerkiksi lcd-näytöllä ja ne asennetaan usein uloskäyntien läheisyyteen. Ohisulkijalla puolestaan voi olla koodilla tai mekaanisella avaimella toimiva ja sillä voidaan tehdä yleensä ainoastaan tietyn alueen ohitus- ja päällekytkentöjä. Ohisulkijoiden kohdalla on syytä muistaa, että niiden turvallisuustaso on usein kevyempi kuin käyttölaitteiden. Yleensä ohisulkijoissa on esimerkiksi led-valot indikoimassa rikosilmoitinjärjestelmän tilaa ja tällöin on syytä myös kiinnittää erityistä huomiota niiden sijoitukseen, sillä ohisulkijan merkkien perusteella ulkopuolinen henkilö voi osata päätellä rikosilmoitinjärjestelmän tilan, onko se päällä vai ei. Tietyissä tapauksissa tiettyjen laitteiden kohdalla rikosilmoitinjärjestelmää voidaan ohjata myös kulunvalvontajärjestelmän kulunvalvontalukijoilla ja kulkutunnisteilla. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 82-83.)

6.2 Rikosilmoitinkeskukset

Nykyiset rikosilmoitinjärjestelmät ovat pääsääntöisesti osoitteellisia järjestelmiä. Osoitteellisuus voidaan toteuttaa kahdella tavalla, osoitteellisilla ilmaisimilla tai erillisillä osoitepäätteillä rikosilmoitinkeskuksesta riippuen. Osoitteellisessa järjestelmässä rikosilmoitinkeskus tunnistaa hälyttävän ilmaisimen tämän osoitteen perusteella ja hälyttävä ilmaisin on helppo paikantaa kiinteistössä. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 88.)

Rikosilmoitinkeskukset luokitellaan EN- normien mukaan, SFS-EN-50131- normissa on esitetty rikosilmoitinkeskuksille mm. rakenteellisia ja toiminnallisia vaatimuksia. Kyseisen normin mukaan rikosilmoitinkeskukset luokitellaan nykyään tasoluokkiin 1-4, vaatimuksiltaan alhaisimman tason ollessa taso 1 ja korkeimman tason ollessa taso 4. Aiemmin keskukset luokiteltiin entisen Suomen Vakuutusyhtiöiden Keskusliiton (SVK), nykyisen Finanssialan Keskusliiton, toimesta A-, B- ja C-tasoluokkiin sekä langattomiin keskuksiin. Nykyiset ja entiset tasoluokat eivät ole identtisiä eivätkä siis täysin vastaa toisiansa. Voidaan kuitenkin sanoa, että taso 1 vastaa karkeasti entistä C– luokkaa ja taso 2 entistä B- luokkaa, tasojen 3 ja 4 ollessa vaatimuksiltaan korkeimpia luokkia, kuten entinen A- luokka. Tasoluokat määrittelevät keskusten vaatimuksia mm. keskukseen liitettävien silmukkatyyppien, silmukoiden määrään sekä keskusten eri tilanteissa antamien ilmoitusten suhteen. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 81.)

Entinen SVK, nykyinen Finanssialan Keskusliitto on antanut ohjeet myös siitä, minkä tasoisia rikosilmoitinjärjestelmiä olisi käytettävä missäkin kohteessa. Valittava rikosilmoitinjärjestelmän luokitustaso riippuu suojattavalle kohteelle, riskienarvioinnin perusteella, määriteltävään suojaustasoon. Esimerkiksi kultasepänliikkeeseen tulee asentaa vähintään luokan 3 mukainen rikosilmoitinjärjestelmä ja kauppaliikkeisiin puolestaan vähintään luokan 2 vaatimukset täyttävä järjestelmä. Kohteen suojaustason määritteleminen perustuu rakenteelliseen murtosuojaukseen ja sitä täydentävään toiminnalliseen suojaukseen. Rakenteellinen murtosuojaus perustuu yrityksen tai organisaation toimialaan ja se on kuvattu Finanssialan keskusliiton ohjeissa. Edellisiin esimerkkeihin viitaten, kultasepänliikkeelle edellytetään rakenteellisen murtosuojauksen suojeluohje 3:sta ja tällöin kohteeseen tulee siis asentaa myös vähintään luokan 3 mukainen rikosilmoitinjärjestelmä. Vastaavasti kauppaliikkeille edellytetään rakenteellisen murtosuojauksen suojeluohje 2:ta, jolloin kyseeseen tulee luokan 2 mukainen rikosilmoitinjärjestelmä. (Murtohälytysjärjestelmät ja –palvelut ohje 2008, 3, 5-6.)

Rikosilmoitinkeskus tulee sijoittaa turvalliseen, ulkopuolisilta suojattuun, mielellään valvottuun tilaan. Keskeistä on, että keskusta ei sijoiteta ns. viivealueelle. Prosessoripohjaisen keskuslaitteen lisäksi rikosilmoitinkeskus sisältää myös varakäyntiakun sähkökatkosten tai muun sähkönsyötön häiriön varalle. Vakuutusyhtiöiden ohjeiden mukainen minimivaatimus akun kapasiteetin mitoitukselle varakäyntiajan suhteen on 24 tuntia. Tämän ajan akun on pystyttävä tuottamaan rikosilmoitinjärjestelmälle sen tarvitsema virta, mikäli normaalissa sähkönsyötössä on katkos. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 81-82.)

6.3 Ilmoituksensiirto

Ilmoituksensiirrolla tarkoitetaan rikosilmoitinjärjestelmän tuottamien tietojen, hälytysten ja muiden ilmoitusten, siirtoa ennalta määritellylle taholle, esimerkiksi vartiointiliikkeen hälytyskeskukselle. Rikosilmoitinjärjestelmä pystyy välittämään esimerkiksi vartiointiliikkeen hälytyskeskukselle murtohälytyksen lisäksi tiedot mm. sabotaasi- ja ryöstöhälytyksistä sekä järjestelmän pois- ja päälle kytkennöistä sekä silmukoiden ohituksista. Lisäksi esimerkiksi ulko-oveen voidaan liittää ns. viivesilmukka, joka aiheuttaa hälytyksen, mikäli rikosilmoitinjärjestelmää ei kytketä pois päältä tietyllä aikaviiveellä. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 88.)

Rikosilmoitinjärjestelmän ilmoituksensiirtoyhteys esimerkiksi vartiointiliikkeen hälytyskeskukseen voidaan toteuttaa useammalla eri tavalla. Perinteisesti ilmoituksensiirtoyhteys toteutetaan puhelinlinjan välityksellä, mutta tiedonsiirto voidaan toteuttaa myös langattomasti esimerkiksi gsm- tai gprs-yhteyksien avulla. Nykyään tiedonsiirto voidaan toteuttaa myös IP-verkon välityksellä. Ilmoituksensiirron luotettavuutta parantaa tiedonsiirron varmistaminen varayhteydellä. Langattomat gsm- ja gprs-yhteydet tulevatkin kyseeseen lähinnä varayhteyk-

sinä tai silloin, kun mahdollisuutta kiinteään ilmoituksensiirtoyhteyteen ei ole. (K. Starck, henkilökohtainen tiedonanto 16.3.2009.) Ilmoituksensiirto voidaan toteuttaa ns. valvottuna tai valvomattomana yhteytenä. Valvotun yhteyden kohdalla yhteyttä valvotaan jatkuvasti, jolloin häiriöistä ilmoituksensiirtoyhteydessä saadaan tieto. Valvottu yhteys on aina suositeltava ja se auttaa esimerkiksi rikosilmoitinjärjestelmän sabotointiyritysten havaitsemisessa. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 103.) Valvotun puhelinlinjan valvonta voidaan toteuttaa esimerkiksi siten, että valvonnasta vastaa linjan tarjoava teleoperaattori. IP-yhteyttä voi puolestaan valvoa esimerkiksi hälytykset vastaanottava vartiointiliikkeen hälytyskeskus. (K. Starck, henkilökohtainen tiedonanto 16.3.2009.) Vahinkovakuutusyhtiöiden hyväksymät ilmoituksensiirtolaitteet määritellään nekin luokkiin 1, 2, 3 ja 4 ja ilmoituksensiirtolaitteiston tulisi aina vastata rikosilmoitinkeskuksen tasoa (Murtohälytysjärjestelmät ja –palvelut ohje 2008, 8).

6.4 Ilmaisimet

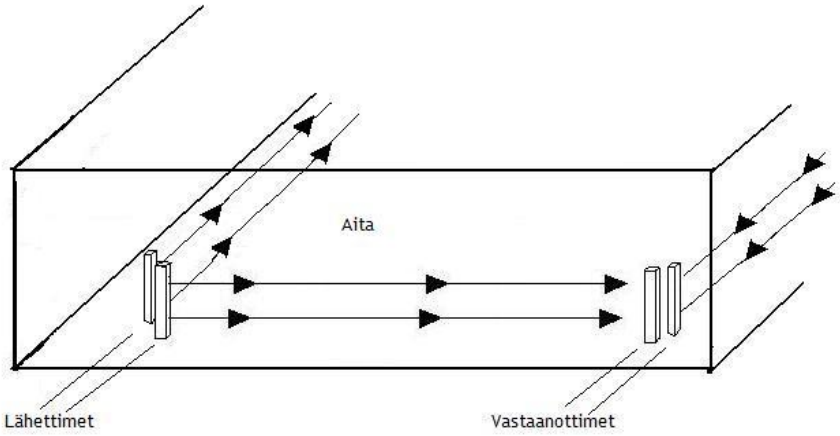
Rikosilmoitinjärjestelmän ilmaisimilla tapahtuva valvonta voidaan jakaa valvontavyöhykkeisiin, joita ovat kehä, kuori sekä tila ja kohde. Kehävalvonnalla valvotaan suojattavan kohteen, yrityksen tai organisaation, piha-alueita. Kuorivalvonnan tarkoituksena on valvoa kohteen kuorta ja siinä olevia sisäänpääsyreittejä kuten esimerkiksi ovia, ikkunoita sekä muita aukkoja ja luukkuja. Tilavalvonnan keinoin on tarkoitus valvoa suojattavan kohteen sisätiloja, kuten huoneita ja käytäviä. Kohdevalvonnalla puolestaan on tarkoitus valvoa yksittäisiä suojattavia kohteita, kuten esimerkiksi kassakaappia. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 79-80.) Useimmissa tapauksissa suojattavien kohteiden valvonta perustuu kuori- ja tilavalvontaan. Kehävalvontaa käytetään lähinnä erityisen korkean turvallisuustason kohteissa ja kohdesuojausta puolestaan käytetään yksittäisten arvokohteiden suojaamisessa. (K. Starck, henkilökohtainen tiedonanto 16.3.2009.)

Rikosilmoitinjärjestelmän ilmaisimet on luokiteltu samalla tavoin EN- normien mukaan neljään tasoluokkaan kuten rikosilmoitinkeskukset. Rikosilmoitinjärjestelmässä tulisi käyttää aina ensisijaisesti ilmaisimia, joiden luokitus vastaa vähintään rikosilmoitinkeskuksen luokkaa. Luokan 3 rikosilmoitinkeskukseen tulisi siis aina liittää ilmaisimien luokkaan 3 kuuluvia ilmaisimia. (Murtohälytysjärjestelmät ja –palvelut ohje 2008, 7.) Seuraavassa käsitellään erilaisia rikosilmoitinjärjestelmän ilmaisimia, ilmaisimilla tapahtuvan valvonnan valvontaperiaatetta mukaillen. Se, että ilmaisin esitellään jonkin tietyn valvontatavan yhteydessä, ei tarkoita sitä, että ilmaisinta voidaan käyttää vain tässä yhteydessä. Ilmaisimia voidaan käyttää tietyissä tapauksissa myös muilla valvontavyöhykkeillä. Huomion arvoista on, että yleisimmin käytetyillä kuori- ja tilavalvontamenetelmillä havainto esimerkiksi tunkeutumisesta saadaan usein vasta, kun tunkeutuja on jo päässyt tai pääsemässä sisään kohteeseen. Kehävalvonnan keinoin havainto voitaisiin saada aikaisemmassa vaiheessa.

6.4.1 Kehävalvonta

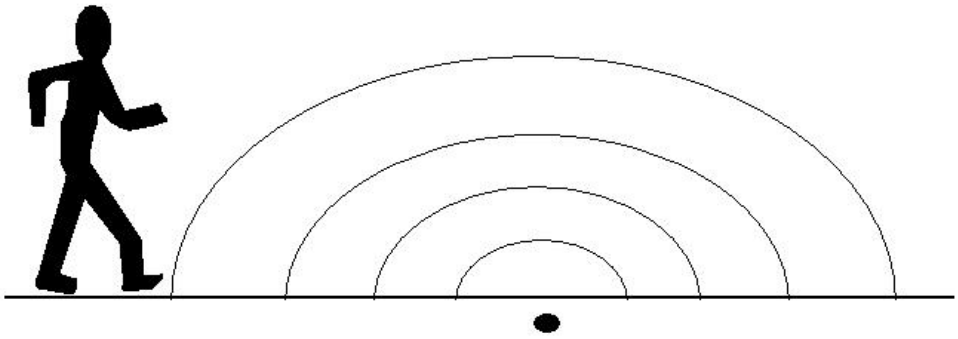
Kehävalvonnan tarkoituksena on havaita tunkeutuminen hyvissä ajoin jo alueen rajan tuntumassa. Kehävalvontaa toteutetaan yleensä aidan valvonnalla tai kehän ja kuoren välisen alueen valvonnalla asentamalla ilmaisimet heti aidan taakse, aidan ja suojattavan kiinteistön väliselle alueelle. Kehävalvonnassa käytettäviä ilmaisimia ovat esimerkiksi IR-linjailmaisimet, mikroaaltoaidat sekä vuotava kaapeli. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 90-92.) Myös itse aitaa voidaan valvoa erilaisilla aitavalvontalaitteilla, kuten esimerkiksi valokuituun perustuvalla aitavalvontakaapelilla, jota käytetään havaitsemaan aitaan kohdistuvaa liikettä. IR-linjailmaisimilla sekä mikroaaltoaidoilla voidaan valvoa esimerkiksi aitalinjaa tai sen taustaa, aitavalvontakaapelilla itse aitaa ja vuotavalla kaapelilla voidaan puolestaan valvoa esimerkiksi aidan ja suojattavan kiinteistön välistä aluetta. Kehävalvonnan toteuttaminen on kuitenkin yleensä ratkaisuna haasteellinen. Haasteita valvonnan onnistuneeseen toteutukseen tuovat mm. sää- ja ympäristöolosuhteet, mutta mahdotonta toimivan kehävalvonnan toteuttaminen ei suinkaan ole. (K. Starck, henkilökohtainen tiedonanto 16.3.2009.)

IR-linjailmaisinpari koostuu lähettimestä sekä vastaanottimesta, jotka muodostavat välillensä valvontalinjan infrapunasäteistä. Säteitä voi olla esimerkiksi kaksi tai useampi päällekkäin ja säteiden katkeamisesta aiheutuu hälytys. IR-linjailmaisinparin asennuksessa on huomioitava, että valvontasäteitä ei pysty helposti ylittämään eikä alittamaan. IR-linjailmaisinparin valvontasäde voi olla laitteista riippuen kymmenistä metreistä muutamaan sataan metriin. IR-linjailmaisinparin tapaan myös ns. mikroaaltoaita muodostetaan lähettimen sekä vastaanottimen avulla. ”Aita” muodostuu lähettimen vastaanottimelle lähettämästä mikroaaltosäteilystä. Valvonta perustuu muutoksiin säteilykentässä ja hälytys aiheutuu kun säteilykentässä havaitaan riittävän suuri muutos. Mikroaaltoaidan ja sen toimivuuden suhteen on erityisesti kiinnitettävä huomiota sää- ja ympäristöolosuhteisiin. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 91.)



Kuva 4: IR-linjailmaisinpari (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 91)

Ns. vuotava kaapeli, koaksiaalikaapelipari, muodostaa puolestaan maanpinnalle elektromagneettisen kentän. Koaksiaalikaapeliparin toinen kaapeli toimii lähetinantennina ja toinen vastaanotinantennina. Valvonta perustuu kaapeliparin muodostamassa elektromagneettisessa kentässä tapahtuviin muutoksiin. Esimerkiksi elektromagneettisen kentän läpi kulkeva henkilö tai ajoneuvo aiheuttaa hälytyksen edellyttämän muutoksen. Vuotavaa kaapelia voidaan pitää hyvin luotettavana, sillä kaapeli mukautuu maastoon ja sen elektromagneettisen kentässä tapahtuvan muutoksen herkkyys on myös säädettävissä. Vuotava kaapeli on myös täysin näkymätön, sillä koaksiaalikaapelipari asennetaan maan alle. Vuotavan kaapelin valvonta-alue voi olla n. 150 metriä pitkä. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 92-93.) Kehävalvonnan vähäiseen käyttöön haastavien ympäristöolosuhteiden lisäksi voi vaikuttaa myös se, että kehävalvonnan etuja ei osata täysin nähdä tai kustannuksia pidetään liian kalliina, varsinkin kuori- ja tilavalvonnan ratkaisuihin verratessa. Usein yrityksillä tai organisaatioilla ei kuitenkaan edes varsinaisesti ole omaa piha-aluetta, jolloin kehävalvontaa ei voida järkevästi toteuttaa.



Kuva 5: Vuotava kaapeli (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 93)

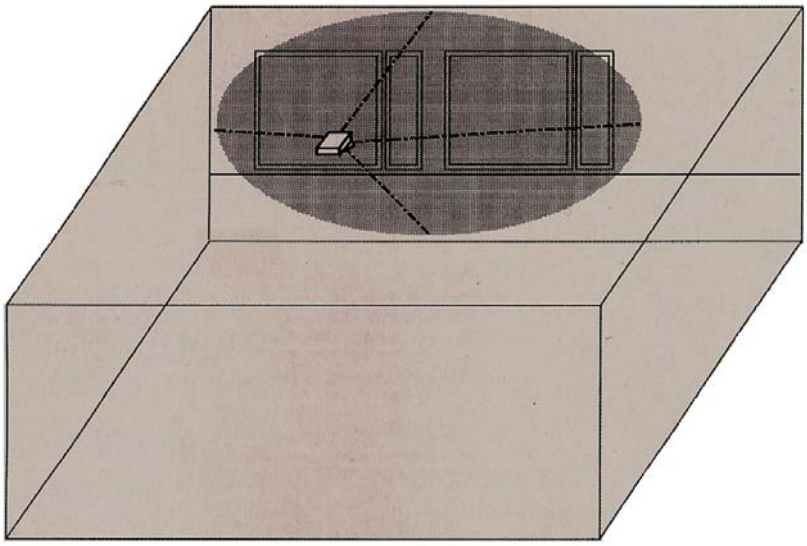
6.4.2 Kuorivalvonta

Kuorivalvonnan tarkoituksena on havaita tunkeutuja hänen tunkeutuessaan suojattavan kiinteistön ulkokuoren läpi. Tällöin havainto tunkeutumisesta pyritään saamaan siis välittömästi tunkeutumisen aloittamisesta. Tyypillisesti kuorivalvonnan keinoin valvotaan ulkokuoren ovia sekä ikkunoita sekä muita mahdollisia sisäänpääsyreittejä, kuten erilaisia luukkuja ja aukkoja. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 93.) Kuorivalvonta on tyypillisesti yhdessä tilavalvonnan kanssa useimmiten käytetty valvontamenetelmä (K. Starck, henkilökohtainen tiedonanto 16.3.2009).

Ovia ja erilaisia luukkuja sekä ikkunoita voidaan valvoa magneettikoskettimella. Magneettikoskettimia on olemassa sekä pinta-, että uppoasennusmallisia. Magneettikosketin asennetaan yleensä oven karmin yläreunaan lukkopuolelle, jotta rikosilmoitinjärjestelmä havaitsee pienenkin oven aukaisun. Pinta-asennettava magneettikosketin on aina suositeltavaa asentaa

oven suojatulle puolelle. Valvonnan tehostamiseksi oveen voidaan myös asentaa toinen magneettikosketin esimerkiksi alemmas oven karmiin. Magneettikoskettimen valintaan vaikuttaa aina se, minkälaiseen oveen ja karmiin magneettikosketin tulee, huomioitavaa on esimerkiksi se, onko kyseessä puu- vai metalliovi. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 93.) Uppoasennettavat magneettikoskettimet ovat turvallisuuden näkökulmasta parempia, sillä ne ovat huomaamattomampia ja siten vaikeammin sabotoitavissa kuin pinta-asennettavat magneettikoskettimet. Pinta-asennettavat magneettikoskettimet ovat kuitenkin yksinkertaisempia asentaa, etenkin vanhoihin olemassa oleviin oviin.

Kiinteistön kuoren ikkunoita voidaan valvoa kuuntelevilla tai itsessään lasiin kiinnitettävillä lasirikkoilmaisimilla tai inertiailmaisimilla. Myös edellä esiteltyjä IR-linjailmaisimia voidaan käyttää esimerkiksi ikkunarivistöjen valvonnassa. Kuunteleva lasirikkoilmaisin asennetaan tyypillisesti seinään tai kattoon ja se reagoi lasin rikkoutumisesta syntyviin ääniin. Kuunteleva lasirikkoilmaisin voi kuunnella yhtä, tai kuten yleensä, useampia eri taajuuksia. Kuuntelevan lasirikkoilmaisimen kuunteluetäisyydet rajoittuvat tyypillisesti alle kymmeneen metriin ja etäisyyttä voivat rajoittaa esimerkiksi verhot tai muut ääntä absorboivat materiaalit. Periaatteessa kuunteleva lasirikkoilmaisin tarvitsee parhaalla mahdollisella tavalla toimiakseen ns. näköyhteyden valvomaansa ikkunaan. Ikkunaan kiinnitettävän lasirikkoilmaisimen toimintatapa on pääpiirteissään sama kuin kuuntelevalla lasirikkoilmaisimella, mutta sen valvonta-ala on huomattavasti pienempi eikä sillä voi valvoa useampaa ikkunaa kerrallaan. Inertiailmaisin puolestaan on ikkunan karmiin asennettava ns. runkoääni-ilmaisin, joka reagoi asennusalustansa tärinään. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 95-96.) Kuuntelevien lasirikkoilmaisimien voidaan hyvin pitkälti katsoa syrjäyttäneen inertiailmaisimet ja myös itsessään ikkunaan kiinnitettävät lasirikkoilmaisimet.



Kuva 6: Kuunteleva lasirikkoilmaisin (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 96)

6.4.3 Tilavalvonta

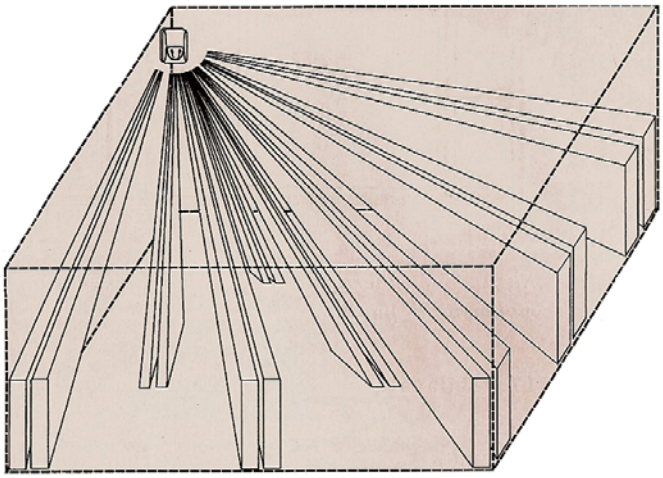
Tilavalvonnalla tarkoitetaan rakennuksen sisätilojen, huoneiden sekä käytävien valvontaa. Tilavalvonnan tarkoituksena on havaita luvattomasti tiloissa olevat ja siellä liikkuvat henkilöt. Huomioitavaa on, että tilavalvonnan keinoin havainto ja hälytys voidaan saada vasta tiloissa liikkumisesta, mutta itse sisälle tunkeutumisesta ei välttämättä aiheudu välittömästi hälytystä. Huonetilojen ja käytävien valvontaan tyypillisin ratkaisu on passiivinen infrapunailmaisin, PIR tai IR, kuten ilmaisinta usein nimitetään. IR-ilmaisin valvoo valvonta-alansa lämpökuvaa sektoreittain ja reagoi normaalista poikkeaviin muutoksiin valvontakeilojen lämpötiloissa. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 80, 97.)

Kuva 7: IR-ilmaisin antimasking toiminnolla (EV1012AMZ liikeilmaisin)

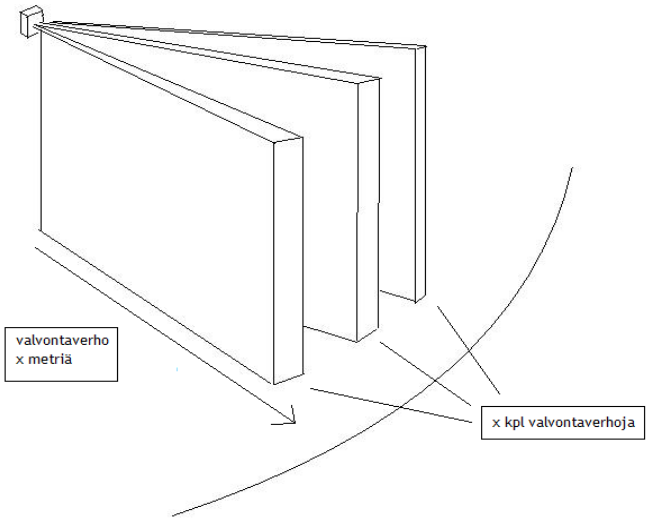
IR-ilmaisimia on olemassa ominaisuuksiltaan useita erilaisia erilaisiin käyttötarkoituksiin. Oikeanlaisen ilmaisimen valintaan vaikuttavat esimerkiksi ilmaisimien valvontakeilat ja niiden kantamat. Valvontakeilat voivat olla muodoltaan sädemäisiä valvontakeiloja tai verhomaisia valvontaverhoja. Ilmaisimien valvontakeilojen kantomatkat vaihtelevat yleensä noin kymmenestä pariinkymmeneen metriin ja pitkäkeilaisimmilla ilmaisimilla voidaan päästä jopa 150m pitkään valvontaetäisyyteen. Leveät valvontakeilat tai valvontaverhot sopivat esimerkiksi huoneiden ja muiden avointen tilojen valvontaan. Käytäviä voidaan valvoa puolestaan pitkäkeilaisilla ilmaisimilla käytävän suuntaisesti tai verhomaisen keilan tuottavalla ilmaisimella käytävän poikki. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 97.) Huoneiden ja avointen tilojen valvontaan on olemassa myös kattoon asennettavaksi tarkoitettuja ilmaisimia, jotka valvovat 180° tai 360° ympärillensä. Kattoilmaisinta on perusteltua käyttää mm. silloin, kun valvottavassa tilassa on paljon esteitä, jolloin tilan valvominen normaalein ilmaisimin on haasteellista. (EV669 kattoilmaisin.) Tiloissa, joissa on vaarana IR-ilmaisimiin kohdistuva sabotointi, voidaan käyttää ns. antimasking-toiminnolla varustettuja ilmaisimia. Antimasking eli peittämisvalvottu ilmaisin antaa hälytyksen mikäli ilmaisin yritetään peittää.

Nyrkkisääntönä voidaan pitää sitä, että IR-ilmaisin tulisi aina asentaa siten, että mahdollinen tunkeutuja joutuu kulkemaan poikittain valvontakeiloihin nähden. Asennuspaikkaa mietittäessä on myös muistettava huomioida mahdollisiin virhehälytyksiin vaikuttavat tekijät. Virhehälytyksiä voivat aiheuttaa mm. lämpötilaan vaikuttavat tekijät, kuten ilmaisimeen suoraan pais-

tava aurinko tai valvontakeilassa oleva tehokas lämpöpatteri. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 100.) IR-ilmaisimissa käytettävissä peilioptiikoissa ja signaalinkäsittelyssä tapahtuneen kehityksen myötä ilmaisin pystyy käsittelemään liikkeen aiheuttamaa havaintoa nykyään entistä tarkemmin eivätkä ilmaisimet enää ole niin herkkiä edellä mainituille mahdollisten virhehälytysten aiheuttajille. Nykyisen 5D-signaalinkäsittelyn myötä ilmaisin tunnistaa ja käsittelee liikkuvan kohteen kokoa, muotoa, nopeutta, kestoa ja lämpötilaa. Mikäli ilmaisin yritetään ohittaa hitaasti liikkumalla, siirtyy ilmaisin 5D toimintaan ja erottelee hitaasti liikkuvan tunkeutujan ympäristön muista lämmönlähteistä. Tällöin esimerkiksi auringon valon heijastus ei aiheuta hälytystä eikä ilmaisinta voida myöskään huijata esimerkiksi sateenvarjolla tai muilla ohuilla materiaaleilla. (EV1012AMZ liikeilmaisin.)



Kuva 8: IR-ilmaisin valvontakeiloin (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 98)



Kuva 9: IR-ilmaisin valvontaverhoin

Tilavalvonnassa voidaan käyttää myös mikroaalto- sekä yhdistelmäilmaisimia. Mikroaaltoilmaisin havaitsee tiloissa tapahtuvan liikkeen lähettämänsä ja vastaanottamansa mikroaaltosäteilyn perusteella. Mikroaalto ilmaisimelle optimaalisin asennuspaikka on IR-ilmaisimesta poiketen sellainen, jossa tunkeutujan liike tapahtuu ilmaisinta kohden. Mikroaaltoilmaisimen asentamisessa on erityisiä haasteita oikean asennuspaikan suhteen, sillä mikroaaltosäteily läpäisee myös seiniä, jolloin hälytyksiä voi aiheutua myös valvottavan tilan ulkopuolelta. Myös valvottavassa tilassa kaikki liike kuten esimerkiksi verhojen liikkeet yms. voivat aiheuttaa virhehälytyksiä. Oikein ja optimaaliseen paikkaan asennettuna mikroaaltoilmaisin on kuitenkin erittäin luotettava ilmaisin. Yhdistelmäilmaisimella tarkoitetaan ilmaisinta, jossa on samassa ilmaisinkotelossa joko IR- ja mikroaaltoilmaisin tai IR- ja ultraääni-ilmaisin, useimmiten yhdistelmäilmaisimia käytetään ensin mainitussa kokoonpanossa. Yhdistelmäilmaisin hälyttää vasta, kun molemmat ilmaisimet havaitsevat liikkeen. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 100.) IR-mikroaaltoyhdistelmäilmaisimen kohdalla on kuitenkin syytä kiinnittää huomioita esimerkiksi siihen, että näiden kahden ilmaisimen optimaaliset asennustavat suhteessa havaittavaan liikkeeseen poikkeavat toisistaan, jolloin molempien on vaikeampi saada havaintoa samanaikaisesti, hälytyksen kuitenkin edellyttäessä samanaikaisia havaintoja.

6.4.4 Kohdevalvonta

Kohdevalvonnalla valvotaan yksittäisiä kohteita tai jopa yksittäisiä esineitä, esimerkiksi kassaholvia, kassakaappia, taulua tai tietokonetta. Kohdevalvonnan tarkoituksena on havaita suojattavan kohteen liikuttaminen tai murtaminen. Kohdevalvonnassa voidaan käyttää valvontaa myös muita kuin kohdevalvonnan keinoja, esimerkiksi koko kyseistä tilaa voidaan valvoa tilavalvonnan ja kuorivalvonnan keinoin. Erityisesti yksittäisen kohteen valvontaan on olemassa erilaisia seismisiä runkoääni-ilmaisimia esimerkiksi kassa- tai arkistokaapin valvontaan. Esimerkiksi tauluja puolestaan voidaan valvoa ns. taulukoskettimin, jotka havaitsevat taulun liikuttamisen tai pois paikaltaan nostamisen. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 100-101.)

7 Kameravalvontajärjestelmä

Lainsäädännössä kameravalvonta määritellään jatkuvaksi kuvaa välittävän tai tallentavan teknisen laitteen käyttöön perustuvaksi valvonnaksi (Laki yksityisyyden suojasta työelämässä, 759/2004). Kameravalvonnan tarkoituksena on lisätä ja tehostaa näköhavaintoihin perustuvaa valvontaa ja antaa heräte henkilö- tai omaisuusvahinkoja estävien tai rajoittavien toimenpiteiden aloittamiselle. Toisekseen kameravalvonta ennaltaehkäisee olemassa ololla rikoksia sekä muita väärinkäytöksiä ja auttaa niiden selvittämisessä jälkikäteen. Kameravalvonnan tallenteiden perusteella voidaan tarkastella ja selvittää tapahtumia, niiden kulkua sekä tunnistaa ja yksilöidä niihin liittyviä henkilöitä. (Leppänen 2006, 368; Kameravalvonnan K-

menetelmä 2006, 3). Heräte kameravalvonnan aloittamiselle voidaan myös saada muiden turvallisuusjärjestelmien kautta, esimerkiksi rikosilmoitinjärjestelmän hälytyksestä. Kameravalvontajärjestelmä voidaan liittää usein myös muihin teknisiin turvallisuusjärjestelmiin, kuten kulunvalvonta- tai rikosilmoitinjärjestelmään, jolloin videokuvaa voidaan hyödyntää näistä järjestelmistä saatavien tietojen tukena. (Videovalvontajärjestelmät 2003, 36). Uudet ja monipuoliset kameravalvontajärjestelmät voivat myös kerätä tietoa kameroiden havainnoista, analysoida itsenäisesti tätä tietoa verraten sitä esimerkiksi aiemmin tuottamamaansa kuvamateriaaliin ja tehdä johtopäätöksiä kuvissa tapahtuvien muutosten perusteella sekä antaa esimerkiksi hälytyksiä näiden muutosten suhteen määriteltyjen parametrien perusteella. (Leppänen 2006, 369-371.)

Kameravalvonta voidaan jakaa kahteen osaan valvonnan suhteen, rikosten paljastamiseen tähtäävään valvontaan ja valvontaan rikoksentekijöiden toteamiseksi (Takala 1998, 7). Rikosten paljastamiseen tähtäävässä aktiivisessa valvonnassa havainto rikoksesta pyritään saamaan välittömästi rikoksen tekohetkellä. Passiivisella valvonnalla pyritään jälkikäteen tunnistamaan tekijät ja selvittämään tapahtumien kulkua kameravalvonnan tallenteiden avulla. (Tikkanen ym. 2007, 205.) Starckin (henkilökohtainen tiedonanto 21.1.2009) mukaan aktiivinen kameravalvonta on tehokas keino turvallisuusvalvontaan ja toisaalta kameravalvonta on myös arvokas työkalu rikosten selvittämisessä. Kameravalvonta luo myös ennaltaehkäisevää vaikutusta ja sen voidaan todeta vähentävän tehokkaasti etenkin esimerkiksi ilkivaltaa. (K. Starck, henkilökohtainen tiedonanto 21.1.2009.)

Kameravalvonnan suorittaminen ainoastaan passiivisena valvontana vesittää osan kameravalvonnan tarkoituksesta, kun rikoksiin ja häiriöihin ei voida reagoida nopeasti niiden tapahtuma hetkellä (Takala 1998, 33). Aktiivinen kameravalvonta, etenkin ympärivuorokautisesti, vaatii kuitenkin aina yritykseltä tai organisaatiolta mittavia resursseja niin rahallisesti kuin henkilöstönkin suhteen, jolloin kameravalvonta jää usein, etenkin työaikojen ulkopuolella, passiivisen valvonnan varaan. Tällöin kameravalvontajärjestelmään tukeudutaan yleensä vasta silloin, kun rikos tai vahinko on jo tapahtunut. Verkotetusti keskitetty kameravalvonta tuo kuitenkin kustannustehokkaampia mahdollisuuksia aktiivisen valvonnan järjestämiseen, jos yrityksellä tai organisaatiolla on useampia toimipisteitä. Tällöin useammankin kiinteistön kameravalvontaa voidaan suorittaa yhdestä ja samasta paikasta. Ympärivuorokauden miehitettyjä valvomoja, joista suoritetaan aktiivista valvontaa, voidaan todeta olevan kuitenkin vain isoimmilla ja korkean turvallisuustason yrityksillä ja organisaatioilla. Toisaalta kameravalvontaa voidaan myös esimerkiksi ulkoistaa etäpalveluna suoritettavaksi valvonnaksi, tosin valvontaa ei tällöinkään suoriteta jatkuvasti vaan esimerkiksi tietyin aikavälein tai hälytysperusteisesti, joten aktiivisesta kameravalvonnasta ei voitane puhua sen varsinaisessa merkityksessä. Tällaisissa tilanteissa on kuitenkin aina oltava myös valmius reagoida kameravalvonnan kautta tehtäviin havaintoihin.

Usein kameravalvonnan kohdalla nousee esiin kysymys kameravalvonnan todellisesta vaikutuksesta ja ennaltaehkäisevyydestä. Martin Gillin toimittamassa teoksessa CCTV (2003, 81-91), Gill ja Karryn Loveday ovat lähestyneet kameravalvontaa ja sen vaikutusta rikollisten näkökulmasta haastattelemalla mm. varkauksista, ryöstöistä ja murroista tuomittuja rikollisia selvittääkseen heidän näkemyksiään kameravalvonnasta ja sen vaikutuksesta. Heidän tutkimuksensa mukaan enemmistö rikollisista ei katso kameravalvonnan itsessään vaikeuttavan rikoksen suorittamista, tätä mieltä oli n. 64 % haastatelluista rikollisista. Myös vain n. 46 % haastatelluista katsoi kameravalvonnan lisäävän kiinnijäämisriskiä, vastaavan prosenttiosuuden vastaajista ollessa päinvastaista mieltä. Syitä haastateltujen rikollisten piittaamattomuudelle kameravalvonnan suhteen olivat mm. että kameravalvonnan ei uskottu kohdistuvan itseen tai, että kameroita ei uskottu seurattavan. Huomion arvoista on kuitenkin huomata se ero, mikä kameravalvonnan perusteella kiinnijääneiden ja muiden tutkimukseen osallistuneiden rikollisten välillä on. Lähes 65 % haastatelluista, jotka olivat jääneet kameravalvonnan perusteella kiinni, pitivät kameravalvontaa rikosta hankaloittavana tekijänä. Samoin hieman yli 70 % kameravalvonnan perusteella kiinnijääneistä katsoi kameravalvonnan lisäävän kiinnijäämisriskiä. (Gill 2003, 81-91.)

Yleisesti kameravalvonnan ennaltaehkäisevä vaikutus näyttäisi toteutuvan parhaiten siis silloin, kun kameravalvonnan tehokkuuden on ns. kerran jo kokenut. Takalan (1998, 10-12) mukaan kameravalvonnan vaikutusta rikosten ehkäisemisessä voidaan tarkastella myös kykenevän valvojan kannalta. Kameravalvontaa voidaan pitää kykenevänä valvojana, mikäli rikoksentekijä luopuu rikosaikeestaan sen takia, että uskoo jonkun ns. pilaavan rikoksen tai saavan hänet kiinni rikoksesta puuttumalla tapahtumiin kameravalvonnan perusteella. Kameravalvonnan ennaltaehkäisevän vaikutuksen toimivuutta voidaan katsoa siis siltä kannalta miten rikoksentekijä kokee valvonnan, tiedostaako ja uskooko tekijä häntä valvottavan. Mikäli rikoksentekijä ei usko kameravalvonnan vaikuttavan rikoksen tekemiseen, ei kameravalvontaa voida pitää kykenevänä valvojana. Huomionarvoista on se, että kameravalvontajärjestelmä ei itsessään valvo, vaan valvontaa suorittaa se, joka kameravalvontaa käyttää. Tästä johtuen passiivista kameravalvontaa, joka vain tallentaa rikoksen, ei voida pitää kykenevänä valvojana, sillä tällöinhän rikos on jo tapahtunut. (Takala 1998, 10-12.) Kameravalvonnan vaikutukseen ei siis pidä luottaa kuitenkaan sokeasti. Yleisesti voinee todeta, että kameravalvonnan ennaltaehkäisevä vaikutus toimii tietyissä tilanteissa, jotka ovat luonteeltaan esimerkiksi sellaisia, missä tilaisuus tekee varkaan. Rikoksia yritettäneen kameravalvonnasta riippumatta ja siitä huolimatta, mikäli rikoshyödyn koetaan olevan riittävän suuri verrattaessa kiinnijäämisriskiin. Näkyvä ja kattava kameravalvonta, jonka olemassaolosta ilmoitetaan näkyvästi, luonee tehokkaimmin ennaltaehkäisevää vaikutusta.

Toimitilojen suojaamisen ja valvonnan näkökulmasta kameravalvontaa on perinteisesti käytetty tiettyjen alueiden ja tilojen sekä ulko-ovien valvontaan luvatta alueella tai tiloissa ole-

vien havaitsemiseksi ja rikosten estämiseksi ja selvittämiseksi. Parhaimmassa tapauksessa kameravalvonnan avulla yksi henkilö voi hoitaa valvonnan, johon aikaisemmin ilman kameravalvontaa tarvittiin useampi henkilö. Kameravalvontaa voidaan hyödyntää aluevalvonnan työkaluna, jolloin jotain tiettyä, usein laajaa, aluetta voidaan valvoa kokonaisuutena esimerkiksi yhdestä valvontapisteestä. Aluevalvonnan tavoitteena on tunnistaa ja kontrolloida alueella oleskelevia ja siellä liikkuvia henkilöitä. Toinen perinteinen kameravalvonnan käyttökohde on tilavalvonta, jolla tarkoitetaan yksittäisten tilojen, usein yksityiskohtaisempaa, valvontaa. Kameravalvontajärjestelmän kohdalla on aina tärkeää huomioida ja määritellä se, mikä on kameravalvonnan tarkoitus ja mitä tarpeita se asettaa kameravalvontajärjestelmälle. On esimerkiksi aivan eri asia valvoa jotakin tiettyä laajaa aluetta siellä tapahtuvan liikkeen havaitsemiseksi kuin se, että tietyissä tiloissa oleva henkilö voidaan tunnistaa kamerakuvasta. Kameravalvontajärjestelmän suunnitteluvaiheessa täytyy määritellä se, mitä kameravalvonnalla halutaan valvoa ja minkälaista tietoa ja kuvaa järjestelmällä halutaan valvonnan kautta saada. (Videovalvontajärjestelmät 2003, 31-37; Leppänen 2006, 369.)

Usein kameravalvontajärjestelmässä onkin kameroita eri valvontatarkoituksiin ja järjestelmällä suoritetaan paikoin tila- ja kohdevalvontaa ja paikoin aluevalvontaa. Kriittisimmät tilat tai kohteet vaativat tarkempaa valvontaa kuin vähemmän kriittiset kohteet. Kriittisimpiä tiloja tai kohteita on perusteltua valvoa siten, että henkilö voidaan tunnistaa kamerakuvasta kun taas esimerkiksi joidenkin alueiden valvonnassa voi riittää ainoastaan havainto siellä tapahtuvasta liikkeestä. (Videovalvontajärjestelmät 2003, 32-33.) Kameravalvonnan K-menetelmä määrittelee vaatimukset valvottavasta kohteesta tuotetun kuvan yksityiskohtaisuudelle kun valvonnan kohteina ovat henkilöt. Esimerkiksi kuvattavan henkilön yksilöintiin ja tunnistamiseen vaaditaan, että kuvattavan henkilön on oltava vähintään 120 % kuvaruudun korkeudesta, jolta kuvaa katsotaan. Tuntemistasoisen kuva puolestaan edellyttää, että kuvattavan henkilön on oltava vähintään 50 % kuvaruudun korkeudesta. Valvotulla alueella liikkuvan henkilön havaitsemiseen tarkoitetussa valvonnassa kuvattavan henkilön tulisi olla vähintään 10 % kuvaruudun korkeudesta. Yleiskuvaksi on määritelty kuva, jossa henkilö täyttää vähintään 5 % kuvaruudun korkeudesta. (Kameravalvonnan K-menetelmä 2006, 3.)

Laajojen ulkoalueiden valvontaan voi usein riittää esimerkiksi se, että kamerakuvasta voidaan havaita ulkoaluilla tapahtuva liike. Ulkoalueiden kohdalla on kuitenkin usein perusteltua valvoa tarkemmin esimerkiksi paikoitusalueita, kiinteistön seinustoja ja mahdollisia lastausalueita ja ajoväyliä tai alueita, joilla säilytetään arvokasta omaisuutta. Sisätiloissa on usein perusteltua valvoa esimerkiksi sisäänkäyntejä, käytäviä, aula- ja asiakaspalvelutiloja, kerrostasanteita ja erilaisia kriittisiä erityistiloja. Ulko-ovilla voi olla perusteltua kohdistaa valvonta sekä sisään tulevaan, että myös ulos menevään liikenteeseen. Sisätiloissa valvonnan tulisi myös olla tarkempaa, tunnistamis- tai tuntemistasoista kuvaa henkilöiden yksilöimiseksi. Mikäli kameravalvonnalla saatava kuvamateriaali ei ole riittävän tarkkaa eli tunnistamis- tai tunte-

mistasoista, voi kameravalvonnan tehtävä, etenkin rikosten selvittämisen työkaluna vesittyä. Leppäsen (2006, 371) mukaan kameravalvonnan rooli rikoksen selvitysprosessissa voi olla parhaimmassa tapauksessa hyvinkin ratkaiseva, sillä kameravalvonnan tallenteita voidaan käyttää esimerkiksi todistelutarkoituksessa rikoksen selvitysprosessissa aina oikeusprosessia myöden. Kameravalvonnan tarkka ja hyvälaatuinen videomateriaali, josta tapahtumat ja henkilöt ovat riittävissä määrin tunnistettavissa, on todisteena pelkkää näköhavaintoa kiistattomampi. Videomateriaali toimii niin ikään epäiltyjen, kuten myös muiden osapuolten oikeusturvana. (Leppänen 2006, 371.)

7.1 Kameravalvontajärjestelmän rakenne, IP- ja analoginen järjestelmä

Yksinkertaisimmillaan kameravalvontajärjestelmä voi koostua yhdestä kamerasta ja sen seurantaan tarkoitetusta monitorista ja laajimmillaan järjestelmä voi sisältää satoja kameroita sekä useita tallentimia. Kameravalvontajärjestelmän voidaan katsoa sisältävän yleensä ainakin kameran ja näytön kameran seurantaa varten, lisäksi kameravalvontajärjestelmään kuuluu useimmiten myös tallennin, useampia kameroita sekä jokin käyttölaite ja käyttöliittymä. Lisäksi järjestelmä vaatii sähkönsyöttöä sekä siirtoyhteydet kuvien siirtoa varten. Kameravalvontajärjestelmän ns. keskuslaitteilla on perinteisesti tarkoitettu mm. automaattiajoittimia, multipleksereitä, nelikuvajakajia ja videomatriiseja. (Leppänen 2006, 368-370.) Nykyisissä järjestelmissä ns. keskuslaitteet ovat kuitenkin hyvin pitkälti korvautuneet samat toiminnallisuudet ja ominaisuudet sisältävillä nykyisillä tallentimilla (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009).

Perinteisten analogisten kameravalvontajärjestelmien rinnalle ovat viime aikoina nousseet verkkopohjaiset IP-kameravalvontajärjestelmät. Tosin nykyiset ns. analogiset kameravalvontajärjestelmät eivät nekään enää perustu täysin analogitekniikkaan. Nykyiset analogiset järjestelmät pohjautuvat analogisuuteen ainoastaan kuvien siirtoyhteyksien ja osittain kameroiden osalta, tallentimina näissä järjestelmissä käytetään digitaalitekniikkaan perustuvia DVR (digital video recorder)-tallentimia. IP-järjestelmässä tallentimina puolestaan käytetään tietoverkkoon liitettäviä NVR (network video recorder)-tallentimia. Edellä mainittujen kameravalvontajärjestelmän laitteiden lisäksi, erilaisten järjestelmäratkaisujen ja -kokoonpanojen aikaansaamiseksi, etenkin IP-järjestelmissä, tarvitaan paikoin myös muita laitteita, kuten esimerkiksi videopalvelimia sekä verkkokytkimiä.

IP-järjestelmien vahvasta tulosta huolimatta, analogiset järjestelmät eivät ole poistumassa käytöstä lähitulevaisuudessa. Analogijärjestelmiä puoltavia tekijöitä ovat mm. analogijärjestelmien tuttuus niiden käyttäjille sekä myös toimittajille. Lisäksi monessa yrityksessä ja organisaatiossa on entuudestaan toimiva analogijärjestelmä ja sille valmis kaapelointi. (Älykkäät ip-kamerat yläkastiin - analogiakameroista keskiluokka. 2009. Turvallisuus 1/2009, 33.) Ana-

logisten järjestelmien etuina voidaan nähdä myös niiden yksinkertaisuus, sillä ne eivät vaadi ylläpitoa samalla tavalla kuin IP-järjestelmät vaativat ylläpitoa esimerkiksi verkon suhteen. Analogisten järjestelmien asennus on myös tuttua niitä toimittaville yrityksille ja siten analogisten järjestelmien asennus on myös yksinkertaisempaa kuin IP-järjestelmien rakentaminen. Analoginen järjestelmä on myös turvallinen, IP-järjestelmän kohdalla on aina huomioitava myös tietoturvallisuuden asettamat vaatimukset verkon turvallisuudelle. (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.) Analogijärjestelmät ja etenkin kamerat ovat myös pitkän kehityskaarensa ja jatkuvan kehitystyön myötä IP-tekniikka edellä ja paikoin analogikameroilla voidaan saada suuri määrä sellaisia etuja, joihin IP-kamerat eivät vielä yllä. Analogikamera on usein esimerkiksi hämäränäön ja vastavalon suhteen IP-kameraa edellä, analogikameroita on myös tarjolla laajempi valikoima etenkin erikoiskäyttöön. (Tolonen 2/2009, 22-24.) Eräänä analogisia järjestelmiä puoltavana tekijänä voidaan nähdä myös niiden alhaisempi hintataso IP-järjestelmiin verrattuna.

Kameravalvontajärjestelmää hankittaessa IP-järjestelmien uutuuden viehätyksen ei pidä olla ratkaiseva tekijä valinnassa analogisen ja IP-järjestelmän välillä. Järjestelmän valinnan on perustuttava järjestelmän ominaisuuksiin ja käyttöön liittyviin tarpeisiin. IP-järjestelmien etuina voidaan nähdä sen mukanaan tuomat ominaisuudet skaalattavuutta, joustavuutta ja etäisyyttä vaativien järjestelmäratkaisujen käyttöön. Skaalattavuutensa ja joustavuutensa ansiosta IP-järjestelmää on helppo laajentaa hyvinkin kattavaksi järjestelmäksi ja järjestelmään tehtävät muutokset, lisäykset ja laajennukset ovat toteutettavissa pienin toimenpitein. IP-tekniikka tuo myös joustavuutta kaapeloinnin suhteen, etenkin, jos järjestelmässä käytetään wlan-kameroita ja langatonta verkkoa. Lisäksi IP-tekniikka poistaa myös fyysiseen etäisyyteen ja välimatkoihin liittyvät ongelmat, analogisessa järjestelmässä kuvaa voidaan siirtää koaksiaalikaapelissa maksimissaan noin 500m päähän, kun taas IP-järjestelmässä kuvadatan siirtäminen tietoverkossa poistaa tällaiset rajoitteet. Kuvia voidaan myös seurata tietoverkon välityksellä periaatteessa mistä tahansa. Kameroiden kohdalla puolestaan IP-tekniikan merkittävin etu syntyy perinteisiä kameroita tarkempien megapikselikameroiden kautta. (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.)

IP-järjestelmä mahdollistaa myös enenevissä määrin kameravalvonnan kuvaprosessoinnin erilaisin kuvaprosessointi- ja videoanalyysisovelluksin. Ns. älylliset järjestelmät ja kamerat mahdollistavat erilaisten reaaliaikaisten herätteiden ja/tai tilastollisten tapahtuma-analyysien tuottamisen automaattisesti. Automaattista kameravalvontaa, valvontadatan muuntamista herätteiksi, voidaan hyödyntää mm. henkilöiden ja ajoneuvojen tunnistamisessa, tilannelaskennassa tai kameran ns. normaalissa näkymässä tapahtuvien poikkeamien automaattiseen havaitsemiseen dynaamisesti tai staattisesti tai. (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.)

7.2 Tallentimet, kameroiden liittäminen ja kuvan katselu

Tallennin on prosessoripohjainen yhdellä tai useammalla kiintolevyllä varustettu laite kameroiden kuvien tallentamiseen. Analogisessa kameravalvontajärjestelmässä kamerat liitetään jokainen omalla koaksiaalikaapelillaan DVR-tallentimeen. DVR-tallentimessa on tavallisesti tallentimesta riippuen liitännät 4-32 kameralle. Kamera- ja näyttöliitäntöjen lisäksi tallentimet ovat usein varustettuja hälytystuloliitännöillä ja kameraohjauksiin tarkoitetuilla sarjaporteilla. Kehittyneimmissä DVR-tallentimissa on nykyään myös verkkoliitäntä, jonka kautta järjestelmä voidaan liittää myös verkkoon. NVR-tallentimen periaate on DVR-tallentimen kanssa kutakuinkin samanlainen, mutta NVR-tallentimen kohdalla kamerat liitetään tallentimeen aina tietoverkon välityksellä, tallentimessa ei ole ollenkaan liitäntöjä analogisille kameroille. Myös järjestelmän käyttö tapahtuu tietoverkon kautta.(E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.)

Kehittyneimpien DVR-tallentimien kohdalla voidaan puhua myös ns. hybriditallentimista tai DVR/NVR-tallentimista, sillä niihin voidaan liittää myös IP-kameroita. Samoin myös NVR-tallentimeen voidaan liittää analogikameroita videopalvelimien välityksellä. Tallentimiin voidaan siis liittää tietyissä tapauksissa sekä analogisia, että IP-kameroita. Tällaista järjestelmää voidaan kutsua ns. hybridijärjestelmäksi. (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.)

Perinteisesti kameravalvontajärjestelmän kamerakuvia ja tallenteita on katsottu paikallisesti tallentimeen liitetyltä valvontanäytöltä. Tietoverkon hyödyntäminen tuo etuja myös kameravalvonnan suorittamiseen ja tallenteiden katsomiseen. Tietoverkkoon liitetyltä tallentimelta, joka voi olla siis joko DVR- tai NVR-tallennin, voidaan katsoa videokuvaa ja hakea tallenteita esimerkiksi tietoverkossa olevalta työasemalta siihen asennetun käyttöliittymän kautta. IP-kameroissa on usein myös omat selainpohjaiset käyttöliittymänsä, joten niitä voidaan tarkastella myös selaimen avulla tietoverkon kautta yksitellen ilman erillistä käyttöliittymää.

Edellä mainitulla videopalvelimella ts. videoserverillä tarkoitetaan laitetta, jolla muutetaan kameroiden signaali toiseen muotoon. Videopalvelimella, enkooderilla, voidaan muuttaa analogisten kameroiden signaali tietoverkossa käytettävään muotoon, jolloin tavallisia analogisia kameroita pystytään liittämään osaksi IP-järjestelmää. Dekooderilla puolestaan voidaan muuttaa tietoverkossa kulkeva signaali analogiseksi. Enkooderi mahdollistaa esimerkiksi vanhojen olemassa olevien kameroiden hyödyntämisen edelleen, vaikka vanha järjestelmä muuten uusitaan ja korvataan uudella IP-järjestelmällä. Enkooderia voidaan hyödyntää paikoin myös silloin, mikäli kaapelointimatka on liian pitkä koaksiaaliyhteydelle. Dekooderia voidaan hyödyntää esimerkiksi muuntamalla kuvasignaali ensin tietoverkkoon kulkevaksi ja sitten takaisin

analogiseksi, jos tallentimessa ei ole verkkoliitäntää ja etäisyys on koko matkalta muuten liian pitkä koaksiaalikaapeloinnille. (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.)

7.3 Valvontakamerat

Kameravalvonnan K-menetelmä määrittelee kameran tekniseksi laitteeksi, joka poimii heijastunutta valoa kuvattavasta näkymästä ja kohteesta ja muuttaa valon sähköiseksi signaaliksi, jota voidaan siirtää, käsitellä ja muuttaa takaisin näkymäksi optisena näytteenä. (Kameravalvonnan K-menetelmä 2006, 9.) Kamera on yksi kameravalvontajärjestelmän keskeisimpiä ja tärkeimpiä laitteita, sillä kamera on ratkaiseva tekijä kuvanlaadun kannalta (Videovalvontajärjestelmät 2003, 81). Kamera koostuu pääpiirteissään kameran rungosta, optiikasta sekä jalustasta. Kamera voidaan myös suojata ympäristöolosuhteita ja ilkivaltaa vastaan näihin tarkoituksiin sopivilla suojakoteloilla.

Optiikan tehtävänä on projisoida kuvattavan kohteen kuva kameran sensorikennon pintaan. Valvontakameroissa käytettävät sensorikennot ovat yleensä 1/3", 1/2" ja 1/4" kennoja, joista suurin eli 1/2" kenno tarjoaa suurimman valoherkkyyden. Kennossa on ikkuna, jonka läpi valo varaa valoherkät kuvaelementit eli ns. pikselit kennoon. Kennossa kameralla kuvattavaa kohdetta mukailevat sähkövaraukset luetaan ja muutetaan videosignaaliksi. Oikean optiikan valinta on tärkeää, sillä vain oikealla optiikalla voidaan optimoida kameran suorituskyky. Optiikan suhteen keskeisimmät seikat liittyvät valovoimaan ts. valoherkkyyteen sekä polttoväliin. Optiikka voi olla polttoväliltään joko kiinteä tai muuttuva, kuten zoom- ja varifocal-optiikat. Esimerkiksi varifocal-optiikan suurin etu verrattuna kiinteä polttoväliseen optiikkaan on se, että kuva-alue voidaan säätää tarkalleen halutuksi polttovälialueen puitteissa, tämän jälkeen varifocal toimii kuitenkin ikään kuin kiinteä optiikka. Kameran kennon koko, kuvattavan kohteen etäisyys kamerasta ja halutun kuvan leveys ratkaisee tarvittavan polttovälin. Esimerkiksi, 1/3" kennon kameran kohdalla on valittava polttoväliltään 12 mm optiikka, jotta saataisiin 2,5m leveää kuvaa 5 metrin etäisyydeltä. (Videovalvontajärjestelmät 2003, 81, 95-96, 101.)

Valovoimaa kuvaava aukkoluku ilmaisee optiikan valoherkkyyttä. Mitä pienempi aukkoluku on, sitä herkempi optiikka on valolle. Optiikka voi toimia käsitoimisella tai automaattisella aukonsäädöllä. Automaattinen aukonsäätö voidaan toteuttaa ns. autoiirisoptiikalla, jossa aukonsäätömekanismi sähkömagneettisesti avaa tai sulkee optiikan mekaanista suljinta tai sähköisellä suljinautomatiikalla, joka säätää kameran herkkyyttä automaattisesti valaistuksen mukaan. (Videovalvontajärjestelmät 2003, 95, 104-106.)

Tunnetuinta valvontakameran tyyliä edustaa varmasti tavallinen ja perinteinen ns. box-kamera. Se koostuu yleensä kamerarungosta sekä erillisestä optiikasta, kotelosta sekä jalustasta. Box-kameroita on olemassa ominaisuuksiltaan laajin valikoima ja erillisen optiikan sekä

sen vaihtomahdollisuuden ansiosta kulloiseenkin käyttötarkoitukseen on helppo valita oikea kamera. Myös yksi yleisimmin käytetyistä kameroista on kiinteä kupukamera, jossa kamera on sijoitettu puolipallonmuotoisen kuvun sisään. Seinään tai kattoon asennettuina kupukamerat ovat huomaamattomia ja niiden kuvaussuuntaa on vaikeasti havaittavissa esimerkiksi tummennetun kuvun alta. (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.)

Kuva 10: Box-kamera ja kiinteä kupukamera (Bosch Product Catalog)

Kääntöpääkameralla tarkoitetaan ohjattavaa kääntöpäällä varustettua kameraa, jota voidaan ohjata sekä vaaka-, että pystysuunnassa. Perinteisesti kääntöpääkameroiden ohjaus on ollut hidasta, joten kääntöpääkamera on yleensä jouduttu sijoittamaan kauemmas kuvattavasta kohteesta. Ohjattavat kupukamerat ovatkin osaksi syrjäyttäneet perinteiset kääntöpääkamerat. Ohjattavan kupukameran kuvauskulma on puolipalloavaruus eli 360˚ ympäri ja 90˚ pystysuunnassa, joten se pystyy katsomaan myös suoraan alaspäin. Ohjattavat kupukamerat ovat myös paljon nopeampia kuin perinteiset kääntöpääkamerat, joten ohjattava kupukamera voidaan asentaa esimerkiksi juuri suoraan kuvattavan kohteen tai tilan yläpuolelle. Ohjattavista kameroista voidaan käyttää myös nimitystä ptz-kamera. Kupukameran kääntönopeus voi olla 100-600˚ sekunnissa kun perinteisen kääntöpään kääntönopeus on ollut tästä vain murto-osan. (Videovalvontajärjestelmät 2003, 92-93.) Nykyään hitaiden kääntöpäiden tilalle on kuitenkin tullut myös nopeampia kääntöpäitä, kääntönopeuden ollessa n. 50-60˚ sekunnissa. Perinteisten ptz-kameroiden lisäksi on olemassa myös kameroita, joissa ptz-toiminto on toteutettu ns. digitaalisesti ilman liikkuvia osia. Tällöin kameran kennolta valitaan tietty alue, jota halutaan valvoa. Sen jälkeen kun katseltava otos on valittu, kamera toimii käytännössä kuitenkin kuin pieniresoluutioinen kiinteä kamera. (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.)

Kuva 11: Kääntöpääkamera sekä ohjattava kupukamera (Bosch Product Catalog)

IP-kamerat voivat myös olla perinteisen box-mallin lisäksi myös ohjattavia sekä kupumallisia ja joko ns. langallisia tai wlan-kameroita. IP-kamerat, etenkin wlan-versiot tuovat joustavuutta kamerasijoitteluun ja kaapelointiin. Wlan-kameroiden kohdalla on kuitenkin huomioitava mahdolliset ongelmat liittyen langattoman verkon toimintavarmuuteen ja ruuhkaisuuteen. IP-kameroiden virransyöttö on mahdollista toteuttaa myös samassa kaapelissa, jota käytetään kuvan siirtämiseen. Tämä edellyttää kuitenkin PoE (Power over Ethernet)- ominaisuudella varustettujen kameroiden ja PoE-virransyöttöön tarkoitettujen verkkokytkinten käyttämistä. Merkittävin edistysaskel IP-kameroissa liittyy perinteisiä kameroita tarkempiin megapikselikameroihin. Megapikselikamerat mahdollistavat paremman tarkkuutensa ansiosta kuvan tuottamisen tuntemis- ja tunnistamistarkkuudella laajoiltakin alueilta. Tietyissä tilanteissa tämä voi vähentää myös tarvittavien kameroiden määrää, kun megapikselikamera pystyy tallentamaan enemmän yksityiskohtia suuremmalta alueelta kuin tavallinen analogikamera. (E. Vuonoranta, henkilökohtainen tiedonanto 28.4.2009.)

Kuva 12: Megapikseli- (Bosch Product Catalog) ja wlan-kamera (Axis Photo Archive)

Nykyään on olemassa myös 360˚ ympärillensä valvovia kattokameroita. Kyseessä on megapikselikamera, joka näkee joka puolelle ympärillensä ilman liikkuvia osia. Kameran tuottamasta kuvasta voidaan valita tietty kohta, jota voidaan katsella geometriakorjattuna. Katseltavaa kuvaa voidaan käännellä ympäri kameran valvomaa tilaa, samalla kamera voi myös tallentaa kuvaa koko 360˚ alueelta. (Tolonen 1/2009, 31.)

Kamerat on aina hyvä asentaa mahdollisuuksien rajoissa niin korkealle, että niihin ei voi tahallisesti kohdistaa mitään toimenpiteitä tai, että niihin ei törmätä vahingossakaan. Paikoin on kuitenkin perusteltua suojata kamera myös ilkivaltaa vastaan tukevalla alumiini- tai teräsvalmisteisella ns. vandaalisuojakotelolla. Kamerat voidaan suojata myös ympäristöolosuhteita vastaan ns. sääsuojakoteloilla. Ulkona sääsuojakotelot ovat välttämättömiä, mutta ne voivat olla perusteltuja myös esimerkiksi pölyisissä tiloissa. Sääsuojakotelon luokitus ilmoitetaan luvulla, esimerkiksi IP54, jossa ensimmäinen luku ilmaisee kotelon tiiviyttä. Luku viisi tarkoittaa, että pölyä pääsee kotelon sisään, mutta ei haitallisessa määrissä. Esimerkin luku neljä ilmaisee puolestaan kotelon vesisuojauksen tasoa, joka tässä tapauksessa kertoo, että kotelo on roiskevesisuojattu. Lian ja kosteuden lisäksi sääsuojakotelo suojaa kameraa myös kylmyy-

deltä lämmitysvastuksensa ansiosta. Sääsuoja- ja vandaalisuojakoteloiden lisäksi kameroille on olemassa myös erikoissuojattuja koteloita esimerkiksi teollisuusalueilla tapahtuvaan valvontakäyttöön. (Videovalvontajärjestelmät 2003, 86-89.)

Kuva 13: Vandaalisuojattu sääsuojakotelo (Videotec S.p.A.)

Kameroiden kohdalla on aina huomioitava myös, että riittävä valaistus on yksi hyvän videokuvan edellytyksistä. Valaistustason suhteen on olemassa kaksi ääripäätä, päivänvalo, jolloin valaistus on täysin riittävä ja yö, jolloin tarvitaan usein myös keinovalaistusta. Valaistuksen tulee olla riittävä kameran koko näkymässä eikä näkymässä olevan kirkkaimman ja pimeimmän kohteen valaistustason suhde saa olla liian suuri, sillä muuten kameran dynamiikka ei enää pysty käsittelemään valaistuseroja. Olennaisesti kuvaan vaikuttaa myös kuvattavan kohteen heijastama valo. Pimeissä ja hämärissä olosuhteissa voidaan käyttää näkyvän keinon valon lisäksi myös esimerkiksi IR-valaisimia. Saatavilla on myös kameroita, joissa on sisäänrakennetut IR-ledvalot. Erillisiä IR-valaisimia käytettäessä täytyy kuitenkin huomioida, että kyseisen kameran on myös oltava infrapunavalolle herkkä. (Videovalvontajärjestelmät 2003, 115-116.)

Kuva 14: Kamera sisäänrakennetuin IR-ledvaloin (Bosch Product Catalog)

8 Järjestelmäintegraatiot

Turvallisuusjärjestelmien integroinnilla tarkoitetaan erillisten teknisten turvallisuusjärjestelmien liittämistä toisiinsa. Turvallisuusjärjestelmien integraatioiden tarkoituksena on tehostaa järjestelmillä suoritettavaa valvontaa järjestelmien tukiessa ja täydentäessä toisiaan. Integroinneilla on mahdollista muodostaa turvallisuusjärjestelmien kokonaisuus, jossa järjestelmät tehostavat ja palvelevat toinen toisiaan. Esimerkiksi rikosilmoitinjärjestelmä on vain osa teknisten turvallisuusjärjestelmien kokonaisuutta, jota voidaan tehostaa liittämällä siihen esi-

merkiksi kameravalvontajärjestelmä ja/tai kulunvalvontajärjestelmä. Vastaavasti myös kulunvalvontajärjestelmän tueksi voidaan liittää rikosilmoitin- ja/tai kameravalvontajärjestelmä. Integraatiota tulisi aina kuitenkin miettiä sen mukanaan tuoman lisäarvon kannalta, tuottaako se lisäarvoa vai ei. (Leppänen 2006, 363-366.)

Järjestelmäintegraatioiden kohdalla voidaan puhua ns. aidosti integroiduista tai ns. toiminnallisesti integroiduista järjestelmistä. Aidosti integroidulle järjestelmäkokonaisuudelle on tunnuksenomaista, että esimerkiksi kulunvalvonta ja murtovalvonta käyttävät samaa järjestelmää yhteisenä alustanaan. Tällöin voidaan puhua ns. monivalvontajärjestelmästä. Yleensä ns. aidosti integroidut järjestelmät ovat ensisijaisesti kulunvalvontaan tarkoitettuja järjestelmiä, joiden avulla voidaan toteuttaa myös murtovalvonta ja/tai kameravalvonta tai vastaavasti ensisijaisesti rikosilmoitinjärjestelminä tunnettuja järjestelmiä, joilla voidaan toteuttaa myös kulunvalvontaratkaisut. Tällöin järjestelmät käyttävät esimerkiksi osittain samoja keskus- ja kenttälaitteita, joihin on sitten liitettävissä sekä kulunvalvonnan-, että murtovalvonnan laitteita ja komponentteja. Toiminnallisella integroinnilla tarkoitetaan erillisten, jopa eri valmistajien järjestelmien liittämistä yhteen kokonaisuudeksi, jossa toinen tai kumpikin järjestelmä tukee ja tehostaa toista järjestelmää. Erillisten yksittäisten järjestelmien liittämisessä toisiinsa tulee kuitenkin huomioida tekniikan, järjestelmäkohtaisten ominaisuuksien ym. seikkojen asettamat rajoitukset järjestelmien yhteensopivuudelle.

Turvallisuusjärjestelmien integroinneilla saavutettavat edut ja mahdollisuudet liittyvät valvonnan ja suojaamisen tehostamiseen. Esimerkiksi integroidussa kulunvalvonta- ja rikosilmoitinjärjestelmässä esimerkiksi kulunvalvontajärjestelmän ovivalvonta voi tukea rikosilmoitinjärjestelmän suorittamaa valvontaa ja toisaalta kulunvalvonnan lukijoilla voidaan mahdollistaa rikosilmoitinjärjestelmän ohjaus. Kulunvalvontajärjestelmään liitetyllä kameravalvontajärjestelmällä voidaan puolestaan saada kuvamateriaalia henkilöiden liikkumisesta kulunvalvontajärjestelmän kulkutapahtumatietojen tueksi. Samalla periaatteella rikosilmoitinjärjestelmään liitetyllä kameravalvontajärjestelmällä voidaan mahdollistaa hälytyksen aiheuttaneiden tapahtumien tallennus ja/tai esimerkiksi reaaliaikainen seuranta valvomosta käsin. Rikosilmoitinjärjestelmä voi esimerkiksi ohjata kameravalvontajärjestelmän kääntyviä kameroita hälytysten perusteella. (Leppänen 2006, 363-366.)

Järjestelmien integroinnilla voidaan saavuttaa myös järjestelmien käytettävyyteen ja hallinnointiin liittyviä etuja ja mahdollisuuksia. Integroitujen järjestelmäkokonaisuuksien, etenkin ns. aidosti integroitujen järjestelmien, kohdalla järjestelmien käyttöä helpottaa yhteinen hallintaohjelmisto. Järjestelmiä voidaan käyttää ja hallinnoida samasta käyttöliittymästä samalla valvonta-ohjelmalla. Valvontaohjelma voi olla varustettu esimerkiksi kiinteistön pohjakuvat sisältävällä grafiikalla, joista voidaan nähdä ja paikantaa esimerkiksi hälyttävän ilmaisimen sijainti, olemassa olevat kamerat ja kulunvalvonnan piirissä olevat ovet. Tällöin

valvontaohjelmassa voidaan katsoa esimerkiksi kamerakuvaa kulku- tai hälytystapahtumista reaaliajassa tai tallenteena. Kameravalvonnan kuvamateriaalin saaminen esimerkiksi kulunvalvontajärjestelmän kanssa samaan käyttöliittymään on mahdollista myös erillisten järjestelmien integraatioissa, mikäli kyseiset erilliset järjestelmät vain tukevat toisiansa. Ns. aidosti integroitujen monivalvontajärjestelmien kohdalla voidaan paikoin integraation tuomaksi eduksi laskea myös laitekustannuksista mahdollisesti syntyvät säästöt, kun järjestelmät käyttävät osittain samoja laitteita. Tämä tosin on suoraan riippuvainen järjestelmien laajuudesta, käytettävistä komponenteista yms.

9 Teknisiin turvallisuusjärjestelmiin liittyvät palvelut

Teknisten turvallisuusjärjestelmien toiminnan ja tehokkuuden kannalta on ajateltava myös aikaa jälkeen asennusten ja käyttöönoton. Tekniset turvallisuusjärjestelmät vaativat osaamista niiden tehokkaaksi hyödyntämiseksi sekä huoltoa ja ylläpitoa toimintavarmuuden takaamiseksi. Teknisiin turvallisuusjärjestelmiin liittyvät palvelut ovat usein perusteltuja ratkaisuja, sillä turvallisuusjärjestelmät ja niiden käyttö harvoin liittyvät yrityksen tai organisaation omaan liiketoimintaan, mutta ne ovat kuitenkin välttämättömiä toiminnan turvaamiselle. Aina yrityksellä tai organisaatiolla ei välttämättä ole riittäviä resursseja, osaamista tai mielenkiintoakaan turvallisuusjärjestelmien käyttöön, valvontaan tai ylläpitoon. Usein nämä tai osa näistä toiminnoista ulkoistetaan näitä ratkaisuja tarjoaville palveluntarjoajille. Näin teknisiin turvallisuusjärjestelmiin liittyvien palveluiden avulla turvallisuusjärjestelmistä on saatavissa paras mahdollinen hyöty ja tehokkuus sekä varmuutta järjestelmien käyttöön ja ylläpitoon. Lisäksi palveluilla voidaan myös lisätä valvonnan tehokkuutta. Teknisiin turvallisuusjärjestelmiin liittyvät palvelut voidaan periaatteessa jakaa järjestelmien toiminnan varmistamiseen, järjestelmien käyttämiseen sekä valvonnan tehostamiseen liittyviin palveluihin. Toimintavarmuuden lisäämisen ja valvonnan tehostamisen lisäksi palveluilla voidaan siis myös vapauttaa yrityksen tai organisaation omia henkilöresursseja muuhun käyttöön. (K. Starck, henkilökohtainen tiedonanto 21.4.2009.)

Koulutuspalvelut ovat hyvin perusteltuja etenkin uusia järjestelmiä hankittaessa, sillä teknisten turvallisuusjärjestelmien hankinnassa on huomioitava myös tulevan järjestelmän käyttäjät sekä järjestelmän piiriin kuuluvat henkilöt. Kouluttamisen avulla pyritään siihen, että turvallisuusjärjestelmien ominaisuuksia osattaisiin hyödyntää tehokkaasti. Koulutuksen järjestäminen yrityksen tai organisaation ihmisille on erityisen tärkeää turvallisuusjärjestelmien käyttöönoton onnistumisen kannalta, mittavien muutosten yhteydessä tai käyttäjien vaihtuessa, sillä turvallisuusjärjestelmien häiriöttömän ja tehokkaan toiminnan yksi osatekijä on järjestelmien käyttäjien osaaminen ja järjestelmien tuntemus. (K. Starck, henkilökohtainen tiedonanto 21.4.2009.)

Yleisimmin tunnettu palvelu on varmasti perinteinen hälytysvalvontapalvelu. Hälytysvalvontapalvelulla mahdollistetaan reagointi tyypillisesti rikosilmoitinjärjestelmän antamiin hälytyksiin torjunta- ja jatkotoimenpiteiden käynnistämiseksi. Hälytysvalvonta sisältää yleensä hälytysten edelleen käsittelyn, jatko ja torjuntatoimenpiteiden käynnistämisen, kuten vartijan hälyttämisen sekä tapahtumien kirjaamisen ja järjestelmän omistajalle ilmoittamisen. Etäkuvayhteyspalveluilla voidaan tehostaa hälytysvalvontaa, hälytysten vastaanottamista, käsittelyä sekä oikeiden jatkotoimenpiteiden käynnistämistä. Etäkuvavalvonnan avulla saadaan pelkän hälytystiedon tueksi myös videokuvaa hälyttävästä kohteesta. Tämä nostaa kohteen turvallisuustasoa ja helpottaa esimerkiksi tilannearvion tekoa, edesauttaa oikeiden jatkotoimenpiteiden käynnistämistä ja vähentää esimerkiksi vikahälytyksistä aiheutuvia kustannuksia. Etäpalveluiden avulla voidaan vähentää myös henkilövartioinnin tarvetta kustannustehokkaasti, kun kameravalvontaa voidaan suorittaa etänä esimerkiksi palveluntarjoajan valvomohenkilöstön suorittamina ns. kamerakierroksina aina tiettyinä ajankohtina. (K. Starck, henkilökohtainen tiedonanto 21.4.2009.) Hälytysvalvonnan ja hälytyksiin reagoimisen merkitystä turvallisuudelle on jo aiemmin käsitelty rikosilmoitinjärjestelmän kohdalla. Hälytysvalvontapalvelu pitäisi olla ikään kuin itsestään selvyys esimerkiksi rikosilmoitinjärjestelmän kohdalla. Rikosilmoitinjärjestelmän tarkoitus vesittyy heti mikäli, sitä ei ole liitetty hälytysvalvontaan ja hälytyksiin ei reagoida.

Teknisten turvallisuusjärjestelmien toimintavarmuutta voidaan parantaa ja mahdollisiin vikatilanteisiin voidaan varautua erilaisin ylläpitopalveluin. Ylläpitopalveluilla tarkoitetaan sopimustasosta riippuen järjestelmille suoritettavia huolto-, korjaus sekä ylläpitotoimenpiteitä. Ylläpitopalveluin pyritään ennaltaehkäisemään järjestelmien vikaantumista, takaamaan toimintavarmuus sekä varautumaan vikatilanteisiin, sen sijaan, että vikatilanteisiin reagoitaisiin vasta sen jälkeen, kun jotain on jo mennyt rikki. Ennakkohuollolla voidaan ennaltaehkäistä järjestelmien vikaantumista ja parantamaan toimintavarmuutta. Yllättävät järjestelmähäiriöt ja vikaantumiset saattavat aiheuttaa järjestelmille pitkiäkin toimintakatkoksia, lisäksi suunnittelemattomat korjaustoimenpiteet voivat aiheuttaa välittömien kustannusten lisäksi myös huomattavia välillisiä kustannuksia käyttäjäyritykselle tai -organisaatiolle. Laitteiden vikaantumisen varalle palvelu voi puolestaan sisältää esimerkiksi ns. korjaushuoltopalvelun sovitun vasteajan puitteissa, jolloin voidaan myös estää järjestelmien toimintakatkosten venyminen. Ohjelmistojen ylläpitopalveluilla pyritään puolestaan varmistumaan siitä, että turvallisuusjärjestelmien ohjelmistot tulevat aina päivitetyiksi uusimpiin versioihin. Ylläpidollisiin palveluihin sisältyy usein myös ns. puhelintuki, jonka kautta esimerkiksi eri järjestelmien asiantuntijat ovat käytettävissä järjestelmien käyttöön liittyvissä asioissa. Etäyhteyksien avulla voidaan saada myös ylläpitotehtäviin kustannustehokkuutta ja nopeutta, kun ongelmia voidaan pyrkiä ratkaisemaan ns. etänä. (K. Starck, henkilökohtainen tiedonanto 21.4.2009.)

Eräs ylläpidollinen ratkaisu palveluna on myös ns. asp-palvelu, joka ulkoistaa teknisten turvallisuusjärjestelmien käyttämisen, hallinnoinnin ja ylläpidon palveluntarjoajalle. Kyseessä on ikään kuin ns. palvelinhotelliperiaatteella toimiva palvelu, jossa turvallisuusjärjestelmän keskuslaitteet tai palvelin sijoitetaan palveluntarjoajan suojattuihin ja valvottuihin tiloihin, jossa myös tietoliikenneyhteydet ovat tehokkaasti suojattuja. Palveluntarjoaja vastaa myös palvelinympäristön hallinnoinnista ja ylläpidosta, kuten myös käyttäjäyrityksen tai –organisaation tiloihin asennettujen järjestelmän muiden laitteiden ylläpidosta. Teknisen turvallisuusjärjestelmän käyttö voidaan ulkoistaa myös ns. pääkäyttöpalveluna. Pääkäyttöpalvelu takaa osaamisen ja asiantuntijuuden turvallisuusjärjestelmän päivittäisessä käytössä sekä muutostilanteissa. Tämä paitsi tehostaa järjestelmän käyttöä, vapauttaa myös käyttäjäyrityksen tai –organisaation henkilöresursseja. (K. Starck, henkilökohtainen tiedonanto 21.4.2009.)

Ylläpitopalveluilla on suora yhteys turvallisuustason ylläpitoon. Laiteviat ja yllätykselliset toimintakatkokset teknisissä turvallisuusjärjestelmissä aiheuttavat heti turvallisuustason alenemisen, joka vaikuttaa negatiivisesti ihmisten, toimitilojen ja omaisuuden koskemattomuuden ja turvallisuuden varmistamiseen. Ylläpitopalveluilla varmistetaan ja nostetaan teknisillä järjestelmillä saavutettavaa turvallisuustasoa. Käyttämiseen ja sen ulkoistamiseen liittyviä palveluita tulee tarkastella myös muustakin kuin yrityksen tai organisaation henkilöresursseja vapauttavasta näkökulmasta. Osaamisella on vahva merkitys myös teknisten turvallisuusjärjestelmien tehokkuuteen ja ennen kaikkea turvallisuuteen. Mikäli turvallisuusjärjestelmien käyttämiseen ei ole osaamista, voi käytössä tapahtua suuriakin turvallisuutta vaarantavia tai heikentäviä virheitä. Osaaminen ja ammattitaito takaavat järjestelmien turvallisen käytön. Eri asia on, näkeekö asiakasyritys tai –organisaatio mielekkääksi kouluttaa omaa henkilöstöään vai ulkoistaa ja ostaa tarvitsemansa palveluina. Eräänä näkökantana voisi olla se, että mikäli järjestelmiä tarvitsee käyttää usein ja paljon, voi olla perusteltua kouluttaa tähän omaa henkilöstöä, tosin tällöin on huomioitava myös varahenkilöt yms. Mikäli järjestelmät tarvitsevat vähäisissä määrin käyttöä, voi palvelu olla perustellumpi ratkaisu, sillä vähäisen käytön vuoksi osaamisen säilyminen voi olla kyseenalaista.

10 Teknisiä turvallisuusjärjestelmiä koskeva lainsäädäntö

Vastuu teknisten turvallisuusjärjestelmien lainmukaisesta käytöstä kuuluu pääsääntöisesti järjestelmän tilaajalle/haltijalle, mutta vastuu voi kuulua joissakin tapauksissa myös esimerkiksi suunnittelu- tai asennusliikkeelle. Teknisiä turvallisuusjärjestelmiä koskevia lakeja lainsäädännössämme ovat rikoslaki (39/1889), henkilötietolaki (523/1999) sekä yksityisyyden suojasta työelämässä annettu laki (759/2004). Voimakkaimmin lainsäädännössä on säädelty kameravalvontaa. Kameravalvonnan kohdalla tulee huomioida rikoslain 24. luvun sisällään pitämät salakatselu sekä salakuuntelusäännökset, sekä henkilötietolain henkilötietojen käsittelyä koskevat säännökset sekä yksityisyyden suojasta työelämässä annetun lain työntekijän

yksityisyyttä ja sen suojaamista koskevat säännökset. Henkilötietolaki sekä laki yksityisyyden suojasta työelämässä on huomioitava kameravalvontajärjestelmän lisäksi myös kulunvalvontajärjestelmän kohdalla. Lisäksi, erityisesti suunnittelu- ja asennusliikkeiden kannalta, on huomioitava mitä yksityisistä turvapalveluista annetussa laissa (282/2002) on säädelty koskien turvasuojaustoimintaa. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 11-12.)

10.1 Laki yksityisistä turvapalveluista ja turvasuojaustoiminta

Turvasuojaustoiminnalla tarkoitetaan rakenteellisen turvallisuuden ja teknisten turvallisuusjärjestelmien, kuten kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmien, suunnittelua, asentamista ja huoltoa. Turvasuojaustoimintaa on säädelty kuitenkin enemmän turvasuojaustehtäviä hoitavan henkilöstön taustan ja rehellisyyden tarkistamisen kannalta kuin ammatillisen pätevyyteen liittyen. (Tikkanen ym. 2007, 207.) Yksityisistä turvallisuuspalveluista annetussa laissa turvasuojaustoiminta luetaan kuuluvaksi yksityisiin turvallisuuspalveluihin vartioimisliiketoiminnan ohella. Turvasuojaustoiminta elinkeinonharjoittamisena ei kuitenkaan ole luvanvaraista toimintaa kuten vartioimisliiketoiminta (Turvallisuusalan valvontayksikkö). Laki määrittelee turvasuojaustoimintaa siten, että se on ansiotarkoituksessa ja toimeksiantosopimukseen perustuvaa turvasuojaustehtävien hoitamista. Turvasuojaustehtävän lainsäädäntö määrittelee siten, että se on rakenteellisten suojausten tai sähköisten valvontajärjestelmien suunnittelemista, asentamista, korjaamista tai muuttamista ja muiden turvallisuusjärjestelyjen suunnittelemista. (Laki yksityisistä turvallisuuspalveluista, 282/2002).

Turvasuojaustehtäviä hoitavan henkilöstön taustan ja rehellisyyden tarkistamiseen liittyy yksityisistä turvallisuuspalveluista annetussa laissa (282/2002) määritellyt hyväksymistä edellyttävä turvasuojaustehtävä ja turvasuojaaja. Hyväksymistä edellyttävällä turvasuojaustehtävällä tarkoitetaan turvasuojaustehtävään, jonka suorittamiseen liittyy pääsy toimeksiantajan luottamuksellisiin turvallisuusjärjestelyjä koskeviin tietoihin, joiden avulla on mahdollista tunkeutua tai olennaisesti helpottaa tunkeutumista toimeksiantajan hallitsemaan ulkopuolisilta suljettuun paikkaan. Turvasuojaajalla puolestaan tarkoitetaan turvasuojausta harjoittavan liikkeen palveluksessa olevaa hyväksymistä edellyttäviä turvasuojaustehtäviä suorittavaa henkilöä. (Kulunvalvonta- ja rikosilmoitinjärjestelmät 2007, 12-13.) Turvasuojaajaksi hyväksytyllä henkilöllä on oltava turvasuojaajakortti mukana suorittaessaan hyväksymistä edellyttäviä turvasuojaustehtäviä. Turvasuojaajaksi hyväksymisen myöntää kihlakunnan poliisilaitos. (Turvallisuusalan valvontayksikkö.)

10.2 Rikoslaki ja sen 24. luku

Rikoslain (39/1889) 24. luvun säädökset liittyvät teknisistä turvallisuusjärjestelmistä kameravalvontajärjestelmään ja valvonnan suorittamiseen. Rikoslain mukaan salakatseluun syyllistyy

henkilö, joka oikeudettomasti teknisellä laitteella, kameralla, katselee tai kuvaa henkilöä tämän yksityisyyttä loukaten. Salakatselu on rangaistavaa myös yrityksenä. Henkilön katselu ja kuvaaminen teknisellä laitteella kotirauhan suojaamassa paikassa ilman tarkkailtavan suostumusta on aina rangaistavaa, jollei tarkkailuun poikkeuksellisesti ole laissa säädettyä oikeutta tai muuta oikeutusta. Säännösten lähtökohtana on siis, että ihmisten yksityiselämä tarvitsee suojaa tekniseltä tarkkailulta myös muualla kuin kotirauhan suojaamassa paikassa. Kotirauhan suojaaman alueen ulkopuolella salakatselun suoja on rajattu koskemaan sellaisia huoneistoja, rakennuksia ja niiden aidattuja piha-alueita, jotka voivat olla julkisrauhan rikkomisen kohteena. Salakatselusäännökset eivät siten koske paikkoja, kuten katuja, toreja, kauppoja, pankkeja yms., joihin yleisöllä on vapaa pääsy. (Tietosuoja ja tekniset valvontajärjestelmät 2005, 4.)

Salakatselulta suojataan kotirauhan piiriin kuuluvien alueiden lisäksi siis esimerkiksi käymälöitä, pukeutumis- ja pesutiloja, vaatetusmyymälöiden sovituskoppeja ja muita vastaavia tiloja sekä virastoja, toimistoja ja liikkeitä silloin, kun ne eivät ole auki yleisölle. Näissä yleisöltä suljetuissa paikoissa oleskelevan katseleminen ja kuvaaminen teknisellä laitteella, kuten kameravalvontajärjestelmällä, on rangaistavaa, jos se tapahtuu oikeudettomasti ja tarkkailtavan yksityisyyttä loukaten. Säännös suojaa salakatselulta esimerkiksi yksityisten yhdistysten tilaisuuksissa tai sairaalassa oleskelevia. Kameravalvonta ei ole oikeudetonta, mikäli siihen on saatu tarkkailtavan suostumus tai kun kotirauhan tai julkisrauhan suojaamassa paikassa teknisesti tarkkaillaan oikeudettomasti paikassa oleskelevaa. (Tietosuoja ja tekniset valvontajärjestelmät 2005, 4.) Tietyissä tapauksissa kameravalvontajärjestelmällä on kuvan katselun ja tallentamisen lisäksi myös mahdollista kuunnella ja tallentaa ääntä, puhetta. Turvajärjestelmäkäytössä tällainen on kuitenkin suhteellisen harvinaista, mutta mikäli kameravalvontajärjestelmällä on tarkoitus tai edes mahdollisuus tallentaa kuvan lisäksi myös ääntä on rikoslain salakatselusäännöksien lisäksi syytä kiinnittää huomiota myös rikoslain 24. luvun salakuuntelusäännöksiin.

10.3 Henkilötietolaki ja laki yksityisyyden suojasta työelämässä

Henkilötietolain (523/1999) yhtenä tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä. Laki edellyttää, että henkilötietoja käsitellään huolellisesti. Henkilötietolain noudattamista edellyttää henkilötietojen käsittelyä sisältävät toimenpiteet, kuten tiedon kerääminen, tallettaminen, käyttö, luovuttaminen, siirto, säilyttäminen ja hävittäminen. Rikosten torjunnassa kameravalvonnan avulla kerätään tietoa pääsääntöisesti henkilöistä ja henkilön kuva yhdessä aikaan ja paikkaan liittyvien tietojen kanssa voi usein olla riittävä henkilön yksilöimiseksi ja tunnistamiseksi. Henkilön tunnistamisen mahdollistavia ominaisuuksia sisältävien kameravalvonnan tallenteiden käsittelyn katsotaan olevan henkilötietojen käsittelyä, joka edellyttää henkilötietolain

soveltamista kameravalvontajärjestelmän käyttöön. Kameravalvontajärjestelmä ja sen tallenteet muodostavat siis henkilörekisterin, josta on laadittava henkilötietolain edellyttämä rekisteriseloste. Kameravalvontajärjestelmän kohdalla tallennus on henkilötietolain soveltamisen kannalta ratkaiseva tekijä, sillä pelkästään henkilön katselu kameran kautta ilman tallennusta ei täytä henkilörekisterin määritelmää. Myös kulunvalvontajärjestelmän keräämiä tietoja ja näiden käsittelyä pidetään henkilötietojen käsittelynä, joten myös kulunvalvontajärjestelmä muodostaa henkilörekisterin, josta on laadittava rekisteriseloste. Rekisteriselosteessa on mainittava henkilörekisterinpitäjä, jonka käyttöä varten henkilörekisteri perustetaan ja kenellä on oikeus määrätä rekisterin käytöstä, ja jonka tehtäväksi rekisterin pito on laissa säädetty. Rekisterinpitäjä voi olla yksi tai useampi henkilö, yhteisö tmv. Rekisteriselosteessa on mainittava myös henkilötietojen käsittelyn tarkoitus, kuvaus henkilörekisterin piirissä olevasta ryhmästä tai ryhmistä ja ryhmiin liittyvistä tiedoista, kuvaus tietojen säännönmukaisesta luovutuksesta ja mainina siitä, siirretäänkö tietoja EU:n tai Euroopan talousalueen ulkopuolelle. Rekisteriselosteesta on käytävä ilmi myös rekisterin asianmukaisen suojaamisen periaatteet. Rekisterinpitäjän tulee myös ilmoittaa rekisteröitävälle häntä koskevien tietojen keräämisestä. Kameravalvonta- tai kulunvalvontajärjestelmän kautta tapahtuva henkilötietojen käsittely ei kuitenkaan edellytä ilmoituksen tekoa tietosuojaviranomaisille. (Tietosuoja ja tekniset valvontajärjestelmät 2005, 5; Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät: opas tilojen omistajille ja käyttäjille 2004, 6-7; Leppänen 2006, 372-373.)

Yksityisyyden suojasta työelämässä annettu laki (759/2004) eli ns. työelämän tietosuojalaki täydentää henkilötietolakia. Siinä on säädetty keskeisimmistä työelämään liittyvistä tietosuojakysymyksistä. Lailla ei luoda valvontaa koskevia oikeuksia, vaan sen tavoitteena on se, että yrityksissä ja organisaatioissa on olemassa tietyt menettelytavat teknisen valvonnan järjestämisestä, teknisen valvonnan on oltava avointa. Laki koskettaa sekä kameravalvonta- ja kulunvalvontajärjestelmiä. Yhteistoimintalainsäädännössä on säännökset, joiden mukaan henkilöstöön kohdistuvan teknisen valvonnan tarkoitus, aloittaminen ja siinä käytettävät menetelmät kuuluvat yhteistoiminnassa käsiteltäviin asioihin. Teknisellä valvonnalla tarkoitetaan tässä kulunvalvonta- tai kameravalvontajärjestelmällä suoritettavaa valvontaa. Mikäli yritys tai organisaatio ei kuulu yhteistoimintalainsäädännön piiriin, niin työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus, jossa he tulevat kuulluiksi. Yhteistoiminta- tai kuulemismenettelyn jälkeen työnantajan on määriteltävä valvonnan tarkoitus ja menetelmät sekä tiedotettava niistä työntekijöille. (Tietosuoja ja tekniset valvontajärjestelmät 2005, 5-6; Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät: opas tilojen omistajille ja käyttäjille 2004, 6-7.)

Kameravalvonnan, etenkin tallentavan, tarvetta tulisi aina tarkastella ensisijaisesti välttämättömyyden näkökulmasta, sillä muutkin tapahtumat ja henkilöt kuin rikokset ja rikoksentekijät tallentuvat kameravalvontajärjestelmään. Ennen kameravalvonnan harkintaa olisi selvitettävä

muiden mahdollisten, henkilöiden yksityisyyteen vähemmän puuttuvien, turvallisuusratkaisujen soveltuvuus haluttuun tarkoitukseen. Tämä ei kuitenkaan aina ole mahdollista ja työturvallisuus, henkilöturvallisuus ja omaisuuden suojaaminen ovat usein perusteltuja ja oikeutettuja syitä kameravalvonnan järjestämiselle. Työnantaja saa suorittaa kameravalvontaa työtiloissa, jos tarkkailun tarkoituksena on työntekijöiden ja muiden tiloissa olevien henkilöiden turvallisuuden varmistaminen tai omaisuuden suojaaminen. Myös turvallisuutta, omaisuutta tai tuotantoprosessia vaarantavien tilanteiden ennaltaehkäiseminen ja selvittäminen ovat perusteltuja syitä kameravalvonnan järjestämiselle, kuten myös tuotantoprosessien asianmukaisen toiminnan valvominen. Kameravalvonta ei kuitenkaan saa puuttua työntekijöiden yksityisyyteen enempää kuin valvonnan tarkoituksen kannalta on tarpeellista. Kameravalvonnasta on myös ilmoitettava näkyvästi niissä tiloissa, joihin kamerat on asennettu ja työntekijöillä on oikeus myös tietää kameroiden sijainnista, jos ne on kohdennettu työpisteisiin, joissa työskentelee työntekijöitä. Työnantajan on huomioitava myös se, että kameravalvonnan tallenteita käytetään vain niihin tarkoituksiin, joita varten tarkkailua on suoritettu. (Tietosuoja ja tekniset valvontajärjestelmät 2005, 5; Leppänen 2006, 372-374.)

Pääsääntöisesti kameravalvontaa ei saa kohdistaa tietyn työntekijän valvontaan eikä valvontaa saa suorittaa työntekijöiden käymälä- ja pukeutumistiloissa, henkilöstötiloissa tai työntekijän henkilökohtaiseen käyttöön osoitetussa työhuoneessa. Kameravalvontaa voidaan kuitenkin kohdistaa tiettyyn henkilöön, jos tarkkailu on välttämätöntä työntekijän työhön liittyvän ilmeisen väkivallan uhkan tai hänen turvallisuudelleen tai terveydelleen haitan tai vaaran ehkäisemiseksi tai omaisuuteen kohdistuvien rikosten estämiseksi, jos työntekijä työtehtävissään olennaisena osana käsittelee huomattavaa määrää arvo-omaisuutta, kuten rahaa tai arvopapereita. Edellä mainitussa tilanteessa kameravalvontaa voidaan kohdistaa henkilöön myös työntekijän etujen ja oikeusturvan varmistamiseksi, jos ko. työntekijä näin itse pyytää ja asiasta on sovittu työnantajan ja työntekijän välillä. (Tietosuoja ja tekniset valvontajärjestelmät 2005, 5.)

Työnantajalla puolestaan on edellä mainituista kameravalvonnan suorittamista rajoittavista säännöksistä huolimatta oikeus käyttää tallenteita työsuhteen päättämisen perusteen toteennäyttämiseksi, naisten ja miesten välisestä tasa-arvosta annetussa laissa tarkoitetun häirinnän tai työturvallisuuslaissa tarkoitetun häirinnän ja epäasiallisen käytöksen selvittämiseksi ja toteennäyttämiseksi. Tallenteita voidaan käyttää työtapaturman tai muun työturvallisuuslaissa tarkoitettua vaaraa tai uhkaa aiheuttaneen tilanteen selvittämiseksi. Kameravalvonnan tallenteet on pääsääntöisesti hävitettävä heti, kun ne eivät ole tarpeen valvonnan tarkoituksen toteuttamiseksi ja viimeistään vuoden kuluessa. Tallenteen saa kuitenkin säilyttää myös tämän määräajan jälkeen, mikäli se on tarpeellista edellä mainittujen asioiden käsittelyn loppuun saattamiseksi. (Tietosuoja ja tekniset valvontajärjestelmät 2005, 5.)

11 Teknisten turvallisuusratkaisujen kartoitustyökalu

Teknisten turvallisuusratkaisujen kartoitustyökalu on yritysten ja organisaatioiden toimitilaturvallisuusratkaisujen kartoittamiseen tarkoitettu työkalu. Kartoitustyökalua on tarkoitus soveltaa yritysten ja organisaatioiden olemassa olevien nykyisten toimitilaturvallisuuden ratkaisujen kartoittamiseen pääpainon ollessa teknisissä turvallisuusratkaisuissa. Työkalu painottuu toimitilaturvallisuuden teknisiin turvallisuusratkaisuihin kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmien osalta niihin liitettävissä olevat palvelut huomioiden, rakenteellista turvallisuutta kuitenkaan unohtamatta. Toimitilaturvallisuuden ja teknisten turvallisuusratkaisujen lisäksi työkalussa kiinnitetään osin huomiota myös toimitilaturvallisuuteen läheisesti liittyviin turvallisuuden muihin osa-alueisiin, kuten henkilö- ja palo- sekä pelastusturvallisuuteen.

Kartoitustyökalu on kehitetty teknisiä turvallisuusratkaisuja tuottavan Niscayah Oy:n käyttöön yrityksen entisen Business Area Managerin, nykyisen turvallisuusjohtajan Kim Starckin toimeksiannosta ja yhteistyössä hänen kanssaan. Kartoitustyökalun avulla on tarkoitus pyrkiä arvioimaan asiakaskohteen nykyisiä turvallisuusratkaisuja suhteessa asiakkaan turvallisuustarpeisiin ja turvallisuudelle asettamiin tavoitteisiin sekä tunnistamaan turvallisuusratkaisuissa mahdollisesti olevia puutteita ja kehityskohteita. Kyseessä on siis proaktiivinen sekä reaktiivinen työkalu, jonka avulla voidaan arvioida asiakaskohteen nykyisten turvallisuusratkaisujen tarkoituksenmukaisuutta, systemaattisuutta ja riittävyyttä, tunnistaa turvallisuusratkaisuissa olevia puutteita ja kehityskohteita sekä auttaa työkalun tuottaman tiedon perusteella oikeiden korjaavien ja kehittävien toimenpiteiden kohdistamisessa oikein.

Turvallisuusratkaisun tarkoituksenmukaisuuden huomioimisella tarkoitetaan toteutetun ratkaisun vertaamista sen tarkoitukseen, turvallisuustarpeisiin sekä turvallisuustavoitteisiin yrityksessä tai organisaatiossa. Laadukkuudella tarkoitetaan puolestaan olemassa olevissa järjestelmäratkaisuissa käytettyjen laitteiden sekä niiden toteutustavan laatua ja toimivuutta. Kattavuudella ja systemaattisuudella tarkoitetaan puolestaan järjestelmien laajuutta ja hyödyllisyyttä suhteessa edellä mainittuihin turvallisuustarpeisiin ja tavoitteisiin sekä ratkaisun tarkoitukseen.

Kartoitustyökalu on tarkoitettu työvälineeksi teknisten turvallisuusratkaisujen arviointiin sekä kehittämiseen esimerkiksi tilanteissa, joissa yrityksen tai organisaation toiminnan luonteessa tai kiinteistöissä tapahtuu muutoksia ja laajennuksia tai tilanteissa, joissa turvallisuus vain priorisoidaan aiempaa korkeammalle. Kartoitustyökalu ei kuitenkaan ole toimitilaturvallisuuden suhteen kaiken kattava, sillä se keskittyy pääasiassa vain teknisiin turvallisuusratkaisuihin kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmien osalta. Kartoitustyökalulla ja kartoituksen suorittamisella ei voida näin taata kartoitettavan yrityksen tai organisaation omien turvallisuussitoumusten tms. täyttymistä. Työkalu on pikemminkin teknisiin turvalli-

suusratkaisuihin keskittyvä tiedonkeruun työväline, jolla voidaan osoittaa mahdolliset puutteet ja kehityskohteet nykyisissä turvallisuusratkaisuissa tarkoituksenmukaisuuden, laadun sekä kattavuuden ja systemaattisuuden suhteen. Kerätyn tiedon perusteella voidaan tehdä kehittämisehdotuksia ja pyrkiä näin parantamaan turvallisuusratkaisujen tilaa turvallisuustarpeita ja tavoitteita vastaaviksi, mikäli asiakas katsoo tämän tarpeelliseksi.

11.1 Kartoitustyökalun tarve ja tavoitteet

Olemassa olevien teknisten turvallisuusratkaisujen kartoittamiseen tarkoitetun kartoitustyökalun ja kartoitusten tarpeen taustalla voidaan nähdä useampia syitä. Ensinnäkin olemassa olevat tekniset turvallisuusratkaisut vanhenevat jollain aikavälillä ja tekniikan kehitys tuo koko ajan markkinoille uusia ratkaisuja. Myös esimerkiksi muutokset tai laajennukset kiinteistöissä, muutokset yrityksen tai organisaation toiminnan luonteessa tai vain turvallisuuden aiempaa korkeampi priorisointi vaikuttavat usein yritysten ja organisaatioiden, asiakkaiden, turvallisuustarpeisiin. Teknisten turvallisuusjärjestelmien hankintavaiheessa on myös saatettu sivuuttaa jotain, esimerkiksi kustannussyistä tai syystä, että kaikkia tarpeita ei vain ole osattu huomioida tai ne on jätetty huomioimatta muista syistä johtuen. Turvallisuusratkaisujen toteutus saattaa paikoin myös poiketa hankintavaiheen alkuperäisistä suunnitelmista ja visioista monestakin syystä, kuten esimerkiksi pitkän hankinta- ja toteutusprosessin takia, kun mukana on ollut monta eri tahoa esimerkiksi kohteen edustajasta turvallisuuskonsulttiin ja turvallisuusasiantuntijaan, suunnittelijasta, turvallisuusratkaisujen myyjään sekä projektipäällikköön ja asentajaan.

Lähtökohta teknisten turvallisuusratkaisujen kartoitustyökalulle on syntynyt Niscayah Oy:n halusta tuottaa enemmän hyötyä asiakkaillensa tarjoamalla asiantuntemuksensa heidän käyttöönsä toteuttamalla kokonaisvaltaisia teknisiä turvallisuusratkaisuja laadukkaasti ja ammattitaitoisesti. Niscayah Oy haluaa tuoda ilmi tahtoaan ja tavoitteitaan olla luotettava turvallisuuskumppani ja –integraattori teknisten turvallisuusratkaisujen tuottajana ja toteuttajana. Tarjoamalla asiantuntemustaan teknisistä turvallisuusratkaisuista asiakkaidensa käyttöön ja toteuttamalla tekniset turvallisuusratkaisut ammattitaitoisesti ja laadukkaasti Niscayah Oy panostaa asiakkaisiinsa, jolloin he voivat keskittyä paremmin omiin ydintoimintoihinsa. Työkalun toteutus aloitettiin, koska kartoitukselle asetettua tarkoitusta ja tavoitteita vastaavaa teknisiä turvallisuusratkaisuja pintaa syvemmältä luotaavaa kartoitustyökalua ei ollut saatavilla.

Kartoitustyökalun avulla on siis tavoitteena pyrkiä selvittämään ja varmistamaan ovatko turvallisuusratkaisut tarkoituksenmukaisia, riittävän kattavia ja laadukkaita sekä systemaattisesti toteutettuja turvallisuustarpeisiin nähden ja palvelevatko ne turvallisuudelle asetettuja tavoitteita mahdollisimman hyödyllisesti ja tehokkaasti. Lisäksi työkalun avulla olemassa olevia

ratkaisuja voidaan pyrkiä kehittämään edelleen sekä tunnistamaan nykyisissä turvallisuusratkaisuissa mahdollisesti olevat puutteet ajoissa. Tavoitteena on tuottaa tietoa asiakkaan turvallisuustarpeista pintaa syvemmältä, sillä vain tieto siitä, että asiakkaalla on esimerkiksi kameravalvontajärjestelmä, ei kerro itse järjestelmästä, kameravalvonnasta ja sen laadusta kovinkaan paljoa.

11.2 Kartoitustyökalun rakenne

Kartoitustyökalu rakentuu kolmesta osiosta kysymyssarjoineen. Ensimmäisen osion voidaan lyhyesti sanoa keskittyvän yrityksen tai organisaation turvallisuustarpeisiin, turvallisuuden toteuttamisen lähtökohtiin sekä periaatteisiin. Toisessa osiossa keskitytään kartoitettavan kohteen nykyisiin olemassa oleviin suojaus- ja valvontaratkaisuihin. Kolmas ja viimeinen osio käsittelee puolestaan Niscayah Oy:n toimintaan tilanteissa, joissa Niscayah Oy on ollut aikaisemmin toteuttamassa kartoitettavan kohteen nykyisiä teknisiä turvallisuusratkaisuja. Osiot sisältävät kukin tietyn määrän kysymyksiä, joihin vastataan joko ns. rasti ruutuun periaatteen mukaisesti, sanallisella vastauksella, numeerisella arviolla tai näiden yhdistelmillä. Työkalun soveltamista ajatellen työkalun rakennetta voidaan myös muokata. Kartoitettavasta kohteesta riippuen, työkalusta voidaan tiputtaa pois ylimääräisiä asiakokonaisuuksia, mikäli tämä katsotaan tarpeelliseksi.

Ensimmäisen, yrityksen tai organisaation turvallisuutta käsittelevässä osiossa keskitytään tarkemmin kartoitettavan kohteen eli yrityksen tai organisaation suojattaviin arvoihin, niiden kautta kohteen turvallisuustarpeisiin, turvallisuuden nykytilaan ja turvallisuudelle asetettuihin tavoitteisiin. Lisäksi ensimmäisessä osiossa keskitytään yrityksen tai organisaation omatoimiseen turvallisuustoimintaan ja turvallisuussuunnitteluun henkilöstöön, toimitiloihin ja omaisuuteen kohdistuviin riskeihin varautumiseksi sekä turvallisuuden hallinnointiin, resursseihin ja asemaan yrityksessä tai organisaatiossa. Ensimmäisen osion tarkoituksena on saada kuva yrityksen tai organisaation turvallisuustarpeista, nykytilasta ja nykytilan ja turvallisuudelle asetettujen tavoitteiden vastaavuudesta yrityksen tai organisaation oman näkemyksen pohjalta. Kohteessa jo olemassa olevia teknisiä turvallisuusratkaisuja käsitellään ensimmäisessä osiossa siten, että huomiota kiinnitetään olemassa olevien teknisten turvallisuusratkaisujen tarkoitukseen kyseisessä organisaatiossa. Huomiota kiinnitetään myös järjestelmiin liittyviin palveluihin, niiden tarkoitukseen ja tarpeellisuutteen sekä itsessään järjestelmien hallinnointiin, turvallisuuteen ja luotettavuuteen liittyviin seikkoihin. Osion kysymyspatteriston kysymyksiin vastataan ns. rasti ruutuun periaatteen mukaisesti sekä sanallisella vastauksella.

Kartoitustyökalun toisessa osiossa kiinnitetään huomiota kartoitettavan kohteen suojaus- ja valvontaratkaisuihin. Suojaus- ja valvontaratkaisuja lähestytään kartoituksessa vyöhykkeittäin suojaamisen periaatetta mukaillen ja huomiota kiinnitetään kullakin vyöhykkeellä teknisen

valvonnan ratkaisuihin sekä yleisimpiin rakenteellisen turvallisuuden keinoihin. Teknisten turvallisuusratkaisujen kohdalla huomiota kiinnitetään mm. suojaus- ja valvontatapoihin, niiden tarkoituksenmukaisuuteen, turvallisuusratkaisujen kattavuuteen ja systemaattisuuteen. Rakenteellisen turvallisuuden kohdalla huomiota kiinnitetään mm. aitoihin, portteihin, puomeihin ja oviin. Lisäksi huomiota kiinnitetään esimerkiksi myös valaistusratkaisuihin sekä piha- ja tilaratkaisuihin. Suojausten ja valvontaratkaisujen kohdalla kartoituksessa kiinnitetään huomiota niin ratkaisujen ennaltaehkäisevään vaikutuksen sekä estävän ja ohjaavan vaikutuksen luomiseen, rikosten yms. tapahtumien havaitsemiseen ja hälyttämiseen sekä tapahtumien selvittämisen mahdollistavaan tapahtumien tallentamiseen. Suojaus- ja valvontaratkaisuja kartoitettaessa kysymyksiin vastataan kyllä ja ei vaihtoehdoin, jonka lisäksi ratkaisujen tasoa arvioidaan myös asteikolla 1-3. Taso kolme tarkoittaa korkeinta tasoa ja yksi puolestaan alinta tasoa

Kartoituksen kolmas osio käsittelee Niscayah Oy:n toimintaa hankkeissa, joissa Niscayah Oy on jo toteuttanut kohteen tekniset turvallisuusratkaisut. Kyseessä voivat olla juuri äskettäin tai jokin aika sitten toteutetut tekniset turvallisuusratkaisut. Tarkoituksena on mahdollistaa Niscayah Oy:n oman toimintansa ja käyttämiensä järjestelmien arviointi samassa yhteydessä muun kartoituksen kanssa. Tässä osiossa kartoitettavan kohteen, Niscayah Oy:n asiakkaan edustaja, arvioi Niscayah Oy:n toteuttamia turvallisuusratkaisuja ja toimintaa hankkeessa. Huomion keskipisteessä on asiakastyytyväisyys ja Niscayah Oy:n ammattitaito ja asiantuntijuus sekä toteutettujen ratkaisujen toimivuus. Myös tässä osiossa käytetään sanallisen arvion lisäksi numeerista arviota asteikolla 1-5, parhaimman arvion ollessa viisi ja heikoimman yksi.

11.3 Kartoitustyökalun muotoutuminen

Kartoitustyökalun suunnittelu ja toteutus aloitettiin kesällä 2008 Niscayah Oy:n Julkishallinnon liiketoiminta-alueella. Työkalua lähdettiin suunnittelemaan ja kehittämään silloisen esimieheni, Niscayah Oy:n Julkishallinnon liiketoiminta-alueen Business Area Managerin, nykyisen turvallisuusjohtajan toimeksiannosta ja yhteistyössä hänen kanssaan. Työkalun tekoprosessiin osallistui myös muita Niscayah Oy:n asiantuntijoita samalta liiketoiminta-alueelta tarjoamalla näkemyksiään ja antamalla palautetta kulloisiinkin ratkaisuihin. Työkalua lähdettiin toteuttamaan muiden työtehtävien ohessa, joten aivan yhtäjaksoista työskentely ei ollut. Kaiken kaikkiaan työkalun tekoa ohjattiin alkuvaiheessa yhteisten suunnittelupalavereiden kautta ja prosessin aikana pidettiin väliaikakatsauksia aina kun siihen nähtiin tarvetta, yleensä isoimpien työkaluun liittyvien linjausten ollessa ajankohtaisia.

Työkalua toteutus käynnistettiin siis Niscayah Oy:n Julkishallinnon liiketoiminta-alueella, joten työkalun ensisijaisena kohderyhmänä pidettiin Julkishallinnon liiketoiminta-alueen asiakaskuntaa. Suunnitteluvaihe käynnistettiin asiakaskunnan turvallisuustarpeiden haarukoinnin

kautta kartoitustyökalulle asetettuja tavoitteita mukaillen. Julkishallinnon liiketoiminta-alueen asiakaskunta sisältää pieniä, keskisuuria ja suuria, turvallisuustarpeiltaan hyvin erilaisia organisaatioita, joten laaja asiakaskunta erilaisine turvallisuustarpeineen palveli myös ajatusta kartoitustyökalun kokonaisvaltaisuuden ja sovellettavuuden suhteen kohteesta ja sen turvallisuustasosta riippumatta.

Työkalun haluttiin keskittyvän, kuten aikaisemmin on jo todettu, teknisten turvallisuusratkaisujen todelliseen tilaan, niiden tarkoituksenmukaisuuteen, toteutuksen laatuun sekä systemaattisuuteen ja kattavuuteen suhteessa turvallisuustarpeisiin ja tavoitteisiin. Turvallisuusratkaisujen tarkoituksenmukaisuuden huomioimisella haluttiin kiinnittää huomiota siihen, että vastaavatko nykyiset tekniset turvallisuusratkaisut niiden tarkoitusta yrityksessä tai organisaatiossa, mitä yritys tai organisaatio haluaa niillä saavuttaa ja miksi ne on hankittu. Laadukkuudella tarkoitetaan puolestaan järjestelmäratkaisuissa käytettyjen laitteiden ja niiden asennusten laatua ja toimivuutta. Kattavuuden ja systemaattisuuden kautta haluttiin kiinnittää huomiota järjestelmien laajuuteen, järkevyyteen ja hyödyllisyyteen. Tällä pyritään esimerkiksi selvittämään onko kameravalvontajärjestelmä riittävän laaja ja kattava, suhteessa kameravalvonnan tarkoitukseen ja tavoitteisiin kartoitettavassa yrityksessä tai organisaatiossa tai onko esimerkiksi kulunvalvonta toteutettu sillä tavalla systemaattisesti, että tietyn kulkureitin kulunvalvontaa ei voida ohittaa käyttämällä muita kulkureittejä. Tai vaihtoehtoisesti, mikäli yksi sisäänpääsyreitti on kulunvalvottu, niin ovatko myös muut sisäänpääsyt kulunvalvottua ja mikäli eivät ole, niin miksi tällaiseen ratkaisuun on päädytty. Näiden asioiden kautta kiinnitettäisiin huomiota siihen, vastaavatko olemassa olevat tekniset turvallisuusratkaisut yrityksen tai organisaation turvallisuustarpeita ja palvelevatko ne turvallisuudelle asetettuja tavoitteita mahdollisimman tehokkaalla ja hyödyllisellä tavalla.

Kartoitustyökalua lähdettiin toteuttamaan siis siltä pohjalta, että sen olisi oltava käyttökelpoinen kohteesta ja sen turvallisuustasosta ja tarpeista riippumatta. Toteutusprosessin alkuvaiheessa tutustuttiin saatavilla olleisiin erilaisiin turvallisuus- ja riskikartoituksiin, turvallisuutta ja teknisiä turvallisuusjärjestelmiä koskeviin ohjeisiin sekä suosituksiin. Saatavavilla olleista kartoitusmalleista saatiin hyviä vaikutteita ja ideoita työkalun toteuttamiseen rakenteellisesti sekä sisällöllisesti. Vaikuttimina toimivat mm. Finanssialan Keskusliiton antamat erilaiset ohjeet sekä suositukset, yksittäisten vakuutusyhtiöiden suojelu- ym. ohjeet, PK-RH-foorumin erilaiset riskianalyysit sekä rikosturvallisuuden toimintamallin pilottiversio ja logistisen toiminnan turvallisuuteen liittyvä TAPA-auditointimalli. Myös Niscayah Oy:n henkilöstön asiantuntemusta sekä yrityksen sisäisiä materiaaleja käytettiin työkalun suunnittelua ja toteutusta ohjaavina tekijöinä.

Suunnittelu- ja perehtymisvaiheen jälkeen kartoitustyökalun varsinainen työstäminen aloitettiin kysymyssarjojen laatimisella ja kartoitustyökalun alustavan rakenteen hahmottelemisella.

Kysymyssarjojen kokoamisessa lähdettiin liikkeelle teknisistä turvallisuusjärjestelmistä sekä yleisesti yrityksen tai organisaation toimitilaturvallisuuteen ja omatoimiseen turvallisuussuunnitteluun ja -toimintaan liittyvistä asioista. Työkalussa haluttiin kiinnittää teknisiin turvallisuusjärjestelmiin huomiota, ei pelkästään teknisinä järjestelminä tai laitteina, vaan teknisinä turvallisuusratkaisuina. Tällä tarkoitetaan sitä, että työkalun ensimmäiseen osioon otettiin mukaan teknisiin turvallisuusjärjestelmiin liitettävissä olevat erilaiset palvelut järjestelmien käyttämiseen, valvonnan tehostamiseen sekä järjestelmien toiminnan ja ylläpidon varmistamiseen liittyen. Näitä asiakokonaisuuksia käsittelevistä kysymyksistä koottiin lopulta yksi kysymyssarja, josta muodostui lopulta työkalun ensimmäinen osio. Kyseinen osio sopi hyvin kartoituksen ensimmäiseksi osaksi, koska siinä kiinnitetään huomiota yrityksen tai organisaation turvallisuuteen, omaan turvallisuustoimintaan sekä turvallisuuden asemaan ja turvallisuusratkaisujen tarkoitukseen kartoitettavassa kohteessa eli yrityksessä tai organisaatiossa sen omaan näkemykseen perustuen. Vastaustavaksi tähän osioon päätettiin ottaa kyllä ja ei vaihtoehdot, jonka lisäksi vastausta voisi tarvittaessa täydentää kirjallisesti avoimella vastauksella.

Itse järjestelmien ja laitteiden osalta tultiin siihen tulokseen, että suojaus- ja valvontaratkaisuihin tulisi kartoituksessa perehtyä ns. havainnointikierroksen avulla, jotta erilaisista suojaus- ja valvontaratkaisuista sekä menetelmistä, niiden todellisesta tilasta ja tasosta saataisiin tietoa pintaa syvemmältä. Suojaus- ja valvontaratkaisuihin keskittyvän kysymyssarjan laadinnassa oli huomioitava työkalun suunnitteluvaiheen kohderyhmän laajuus sekä erilaisten turvallisuustarpeiden kirjo aina hyvin korkean turvallisuustason kohteisiin asti. Kysymyssarjan tuli olla riittävän kattavia kulloisenkin asiakkaan turvallisuustarpeita vastaavasti sekä myös huomioida erilaisia vaihtoehtoisia suojaus- sekä valvontatapoja ja ratkaisuja. Kartoituksen toisen osion suorittamistavaksi suunniteltu, havainnointiin pohjautuva ns. kenttäkierros kartoitettavassa kohteessa, asetti haasteita myös työkalun rakenteen suhteen, sillä itse kartoitusten suorittamisen olisi kuitenkin tapahduttava sujuvasti. Suojaus- ja valvontaratkaisuihin suuntautuvan työkalun toisen osion kysymyssarjaa lähdettiin jaottelemaan havainnointiin soveltuvaksi. Kysymyssarjan jaottelussa päädyttiin mukailemaan aiemmin kuvattua vyöhykkeittäin suojaamisen periaatetta, sillä tämän periaatteen mukaisen jaottelun eri vyöhykkeisiin katsottiin olevan hyvin selkeä ja kattava. Tämän mallin ajateltiin palvelevan myös kartoitusten suorittamista selkeän lähestymistapansa ja jaottelunsa ansiosta. Vastaustavaksi tähän osioon päätettiin kehittää kyllä ja ei vaihtoehtojen lisäksi myös numeerinen arviointi. Vastauksia täydentävän sanallisen vastaamisen tai kommentoinnin mahdollisuus katsottiin myös tarpeelliseksi sisällyttää vastausvaihtoehtoihin.

Numeerisen arvion katsottiin palvelevan kartoitustyökalun tarkoitusta ja tavoitteita paremmin kuin pelkän ns. rasti ruutuun vastauksien, koska tavoitteenahan on saada tietoa turvallisuusratkaisujen todellisesta tasosta ja tilasta. Numeerisella arviolla on siis tarkoitus pyrkiä kohti

tarkempaa ja syvempää tietoa nykyisten turvallisuusratkaisujen tarkoituksenmukaisuudesta, todellisesta tasosta ja laadusta, sillä esimerkiksi vain tieto siitä, että kohteessa on kameravalvontajärjestelmä, ei kerro itse järjestelmästä, kameravalvonnasta, sen kattavuudesta ja laadusta itsessään kovinkaan paljoa. Tasoarviolla haluttiin pyrkiä siihen, että kartoitusten tuottaman tiedon perusteella nähtäisiin turvallisuusratkaisujen todellinen tila, jonka perusteella voitaisiin myös nähdä mahdolliset puutteet ja kehityskohteet nykyisissä turvallisuusratkaisuissa. Näin mahdollisesti tarvittavat turvallisuusratkaisuja parantavat ja kehittävät toimenpiteet osattaisiin myös kohdistaa paremmin ja tarkoituksenmukaisesti. Numeerisen arvioinnin perustaksi suunniteltiin tasoasteikkoa välillä 1-3, jossa taso kolme tarkoittaisi korkeinta tasoa ja yksi puolestaan alinta tasoa.

Kartoitukseen haluttiin sisällyttää myös Niscayah Oy:tä teknisten turvallisuusratkaisujen tuottajana ja toteuttajana käsittelevä osio. Tarkoituksena on mahdollistaa Niscayah Oy:n oman toiminnan ja käyttämiensä järjestelmien arviointi samassa yhteydessä muun kartoituksen kanssa tilanteissa, joissa Niscayah Oy on ollut toteuttamassa kohteen nykyisiä turvallisuusratkaisuja. Myös tässä osiossa päädyttiin käyttämään numeerista arviota, ainoastaan asteikkoa laajennettiin välille 1-5. Vastausperiaatteena toimii asiakastyytyväisyyskyselyistä tuttu täysin samaa tai täysin eri mieltä oleva periaate, parhaimman arvion ollessa viisi ja heikoimman yksi.

Kaiken kaikkiaan kysymyssarjoja laadittaessa oli pohdittava hyvin tarkkaan mm. kysymysten asettelua ja kattavuutta erityisesti suojaus- ja valvontaratkaisuihin keskittyvässä kysymyssarjassa, että työkalu palvelisi kattavasti ns. normaalin turvallisuustason kohteiden lisäksi myös korkeamman turvallisuustason kohteita. Toisin sanoen, kartoitustyökalun oli sovelluttava ympäristöltään, olosuhteiltaan sekä turvallisuustasoltaan ja -tarpeiltaan hyvin erilaisiin kohteisiin, joten kysymyssarjojen tulisi vastata asiakkaiden tarpeita näiden toiminnan luonteesta ja turvallisuustarpeista riippumatta. Tämän johdosta päädyttiin siihen ratkaisuun, että työkalun tulisi olla modifioitavissa kartoitettavan kohteen mukaan. Käytännössä tämä toteutettiin siten, että kartoitustyökalun osioiden asiakokonaisuudet valittaisiin aina kohteen, yrityksen tai organisaation, mukaan. Vyöhykeperiaatetta mukaileva rakenne palveli myös tätä ajatusta, sillä kartoitettavasta kohteesta riippuen esimerkiksi kehäsuojausta käsittelevät kysymyssarjan kysymykset tai osa niistä olisi helppo jättää sivuun, mikäli niitä ei tarvittaisi.

Kun työkalun osiot kysymyssarjoineen oli saatu muotoiltua ja koottua, aloitettiin kartoitustyökalun toisessa osiossa käytettävien tasoluokkien määrittelyt numeerisille arvioille. Numeeristen tasoluokkien perustana käytettiin yleisesti turvallisuusalalla tunnettuja esimerkiksi Finanssialan Keskusliiton sekä eri vakuutusyhtiöiden tuottamia ohjeita ja suosituksia siinä laajuudessa kuin niitä oli olemassa ja saatavilla. Tässä kohdin jouduttiin soveltamaan paljon toimeksiantajayrityksen asiantuntemuksen ja kokemuksen perusteella hyväksi havaittuja käy-

täntöjä, sillä kaikkiin kartoitustyökalun käsittelemiin aiheisiin tai kysymyksiin ei ollut ohjeita, suosituksia tms. olemassa. Haasteena tässä kohdin oli myös lukuisien erilaisten suojaus- ja valvontamenetelmien vaihtoehtojen huomioiminen. Toimeksiantajayrityksen sisäinen asiantuntemus ja kokemus olivat arvokasta pääomaa tässä vaiheessa. Tasoarviointia päädyttiin soveltamaan siten, että taso arvioidaan vain, kun vastaus ao. kysymykseen on kyllä. Näin kartoitettavan kohteen suojaus- ja valvontaratkaisuista voitaisiin myöhemmin muodostaa turvallisuusratkaisujen tason mittaamiseksi esimerkiksi pistetaulukko tai keskiarvo.

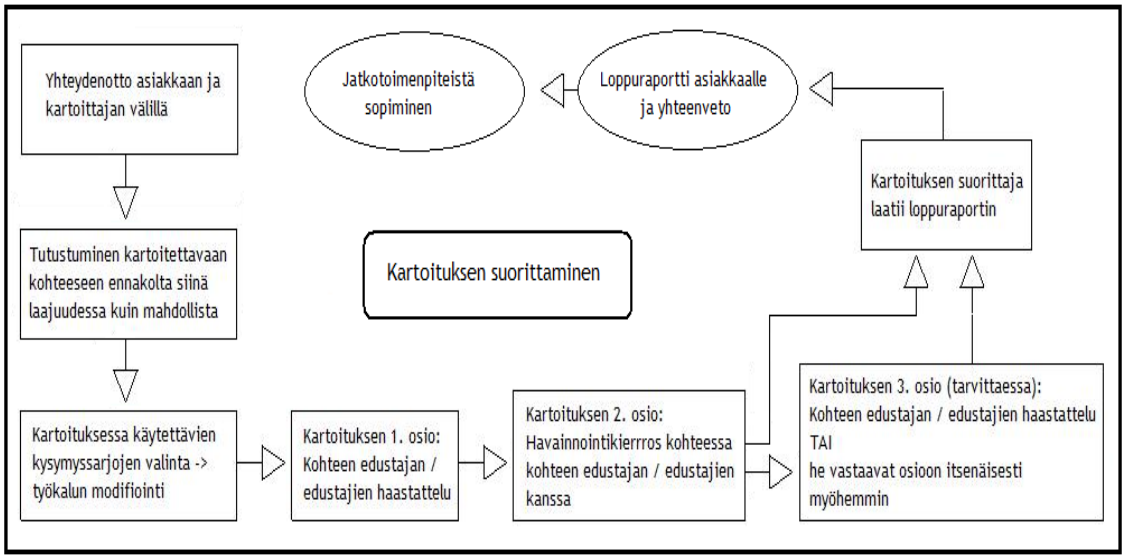
Lopputuotoksena syntyi kolmesta osiosta kysymyssarjoineen koostuva kartoitustyökalu olemassa olevien teknisten turvallisuusratkaisujen kartoittamiseen. Tätä kirjoittaessa työkalu on periaatteessa valmis käytettäväksi, mutta työkalua ei kuitenkaan vielä ole päästy käytännössä kokeilemaan. Työkalun kehitys on kuitenkin nyt viety siihen pisteeseen, mihin se ns. paperilla on vietävissä. Ennen työkalun käytöstä saatavia kokemuksia, työkalua on tarkoitus viimeistellä vielä ulkoasuun yms. liittyvien seikkojen suhteen.

11.4 Kartoitustyökalun soveltaminen käytännössä

Kartoituksen suorittaminen käynnistyy asiakkaan edustajan ja Niscayah Oy:n asiantuntijan välisellä yhteydenotolla. Tämän jälkeen ennen varsinaisen kartoituksen aloittamista, kartoituksen suorittaja tutustuu etukäteen kartoitettavaan kohteeseen ns. paperilla siinä laajuudessa kuin se on mahdollista ja nähdään tarpeelliseksi. Tarkoituksena on kiinnittää huomiota mm. kartoitettavan kohteen eli asiakkaan toimialan luonteeseen ja oletettavissa oleviin turvallisuustarpeisiin, jotka vaikuttavat kartoitustyökalun muokkaukseen asiakkaan tarpeisiin sopivaksi. Mikäli kyseinen kohde on jo ns. olemassa oleva asiakkuus, voidaan kohteeseen ja sen nykyisiin turvallisuusratkaisuihin perehtyä käytettävissä ja saatavilla olevien aikaisempien tietojen perusteella. Päätös kartoituksessa käytettävistä kysymyssarjoista voidaan tehdä jo tämän vaiheen perusteella.

Kartoitustyökalun soveltaminen käytännössä, itse kartoituksen suorittaminen, tapahtuu vaiheittain. Varsinainen kartoitusprosessi käynnistyy yrityksen tai organisaation turvallisuuteen ja varautumiseen keskittyvällä osiolla, joka toteutetaan haastattelemalla kartoitettavan kohteen edustajaa tai edustajia. Ensimmäisen osion kysymyssarjaan vastataan kyllä ja ei vaihtoehdoin, jota voidaan tarvittaessa täydentää ja kommentoida sanallisesti. Toinen osio, joka käsittelee suojaus- ja valvontaratkaisuja, suoritetaan tekemällä ns. havainnointikierros kohteessa. Havainnointikierros tehdään siinä laajuudessa, kuin kartoitukseen valitut kysymyssarjat edellyttävät. Tämän osion kysymyssarjoihin vastataan kyllä tai ei vaihtoehdoin sekä numeerisella arviolla välillä 1-3. Myös sanalliset huomautukset ja kommentit ovat mahdollisia. Kartoituksen viimeinen ja kolmas osio suoritetaan vain silloin, kun Niscayah Oy on toteuttanut kartoitettavan kohteen nykyiset tekniset turvallisuusratkaisut. Kyseessä voivat olla juuri hil-

jattain tai kauemman aikaa sitten toteutetut tekniset turvallisuusratkaisut. Kolmas osio suoritetaan myös haastattelulla, samoin kuin ensimmäisessä osiossa. Vaihtoehtoisesti kolmas osio voidaan toteuttaa myös siten, että kysymyssarja jätetään asiakkaan edustajalle myöhempää vastaamista varten, tällöin asiakkaan edustaja vastaa ja palauttaa kartoituksen viimeisen osion kartoituksen suorittajalle myöhemmin. Kolmanteen ja viimeiseen osioon vastataan numeerisella arviolla, jota voidaan tarvittaessa täydentää sanallisesti. Kartoitusprosessissa olisi hyvä olla kartoitettavan kohteen puolelta mukana useampi edustaja, esimerkiksi turvallisuuspäällikkö tai -asiantuntija sekä päivittäin kohteessa oleva henkilö, esimerkiksi vahtimestari tmv.



Kuva 15: Kartoitustyökalun soveltaminen käytännössä

Kartoituksen jälkeen kartoituksen suorittaja laatii loppuraportin, yhteenvedon kartoituksen tuloksista. Yhteenvedossa esitellään asiakkaalle kartoituksen tuloksia ja heidän toimitilaturvallisuutensa ja teknisten turvallisuusratkaisujen sen hetkistä tilaa. Raportissa peilataan turvallisuusratkaisujen nykytilaa asiakkaan kuvaamiin turvallisuustarpeisiin ja tavoitteisiin, kerrotaan kartoituksessa havaituista puutteista, esitetään ja ehdotetaan parannusehdotuksia sekä kehitysideoita turvallisuusratkaisujen edelleen kehittämiseksi sekä puuteiden korjaamiseksi. Yhteenvedon tarkoituksena on puutteiden ja kehitysehdotusten esittämisen lisäksi auttaa oikeiden toimenpiteiden kohdistamisessa oikeisiin kehityskohteisiin.

12 Yhteenveto

Lopputuotoksena syntyi siis kolmesta osiosta koostuva työkalu olemassa olevien teknisten turvallisuusratkaisujen kartoittamiseen. Työkalun kukin osio sisältää omat kysymyssarjansa, koko kysymyspatteriston koostuessa hieman yli sadasta kysymyksestä. Työkalua ei vielä ole

kuitenkaan päästy kokeilemaan käytännössä, joten yhteenveto ja johtopäätökset työkalun todellisen toimivuuden ja kartoitusten varsinaisen suorittamisen suhteen joudutaan tekemään vasta myöhemmin. Työkalun käytöstä saatujen kokemusten puutteen vuoksi on myös hyvin vaikeaa vielä yksilöidä työkalun mahdollisia kehitystarpeita. Alkuperäisenä tarkoituksena oli, että työkalua olisi jo tätä kirjoittaessa päästy kokeilemaan käytännössä, mutta työkalun kehitysprosessi venyi kuitenkin suunniteltua pidemmäksi. Tekoprosessin venymisen voidaan katsoa johtuneen ainakin osittain siitä, että koska työkalua kehitettiin muiden työtehtävien ohessa.

Kaiken kaikkiaan lopputuotosta voidaan kuitenkin pitää sekä tekijän, että toimeksiantajan tämän hetkisen näkemyksen mukaisesti onnistuneena ja tavoitteensa täyttävänä työkaluna, vaikka kartoitusten suorittaminen käytännössä oletettavasti tuokin vielä esiin kehitystarpeita sekä sisällöllisesti, että rakenteellisesti. Työkalua voidaan pitää myös objektiivisena, vaikka se toteutettiin varta vasten teknisiä turvallisuusratkaisuja tuottavan yrityksen toimeksiannosta. Työkalu ei kuitenkaan ota kantaa esimerkiksi turvallisuusjärjestelmien malleihin tai valmistajiin ja kartoitusten arvioinnin pohjana on käytetty kolmansien osapuolien tuottamia turvallisuuteen ja teknisiin turvallisuusjärjestelmiin liittyviä ohjeita sekä suosituksia. Lisäksi, kuten aiemmin on jo todettu, työkalu on enemmän tiedon keruun väline ja kartoitusten tarjoaman tiedon pohjalta kehitystarpeisiin voisi vastata periaatteessa mikä tahansa vastaava teknisiä turvallisuusratkaisuja tarjoava yritys, joten työkalun ei voida katsoa suosivan ainoastaan toimeksiantajana toiminutta yritystä. Kartoitustyökalu tuleekin nähdä ennen kaikkea etua ja hyötyä tuottavana menetelmänä ja mallina, mutta sisällöllisesti objektiivisena työkaluna.

Työkalun tekemistä prosessina voidaan myös pitää onnistuneena, vaikka se ajallisesti venyikin suunniteltua pidemmäksi. Yhteistyö toteutukseen osallistuneiden tahojen kanssa sujui kuitenkin ongelmitta ja ohjausta oli aina saatavilla. Kartoitustyökalun luomisessa ei käytetty ulkopuolisia tahoja eikä ulkopuolisten asiantuntijoiden konsultointi välttämättä olisi ollut edes perusteltua yrityksen sisäiseen käyttöön tulevan työkalun toteuttamisessa. Suunnittelu- ja kehitysprosessiin kuuluvat kuitenkin aina myös haasteet. Suurimmat haasteet sisällöllisesti liittyivät työkalun eri osioiden kysymyssarjojen laadintaan. Haasteita kysymyssarjojen laadintaan asettivat työkalun kohderyhmän laajuus sekä erilaisten turvallisuustarpeiden suuri kirjo aina hyvin korkean turvallisuustason kohteisiin asti.

Kysymyksiä laadittaessa oli pohdittava hyvin tarkkaan mm. kysymyssarjojen kattavuutta, että työkalu olisi sovellettavissa kohteeseen kuin kohteeseen, esimerkiksi kartoitettavan kohteen toimialasta ja turvallisuustarpeista riippumatta. Itse kartoitusten suorittamisen tulisi myös onnistua jouhevasti ja kohtuullisessa ajassa, joten työkalusta ei saanut tulla liian massiivista, mutta sen oli kuitenkin oltava riittävän perusteellinen ja kattava. Tähän löydettiin ratkaisu osittain tasoarvioiden sekä työkalun muokattavuuden avulla. Toinen työkalun sisällöllinen

suuri haaste liittyi juuri työkalun toisessa osiossa käytettäviin tasoarvioihin ja tasopohjien laatimiseen, että tasot kattaisivat mm. erilaisia vaihtoehtoisia suojaus- ja valvontaratkaisuja ja toteutustapoja. Tässä kohdin sovellettiinkin asiantuntemuksen ja kokemuksen perusteella hyväksi havaittuja käytäntöjä. Työkalun toinen osio asetti haasteita myös työkalun rakenteelliselle toteutukselle kartoitusten sujuvan suorittamisen suhteen. Kartoitusten suorittamisen sujuvuuden vuoksi havainnointiin pohjautuvassa toisessa osiossa jouduttiin pohtimaan kysymysten asettelua ja asiakokonaisuuksien järjestystä tarkkaan. Vyöhykemäinen rakenne osoittautui tässä kuitenkin eduksi.

On oletettavaa, jopa selvää, että työkalun pilotointi tuo oletettavasti vielä esiin kehitystarpeita. Suurimpien kehitystarpeiden voidaan, käyttökokemusten osoittaman tiedon puutteesta huolimatta, olettaa kohdistuvan kysymyssarjojen kysymysten asetteluihin ja muotoiluihin. Kehitystarpeita saattaa ilmaantua myös työkalun käytettävyyteen liittyen. Käyttökokemuksen puutteesta huolimatta tämän hetkisen työkalun voidaan kuitenkin sanoa tarjoavan hyvän pohjan kehitystoimenpiteille.

Lähteet

Access Basic. Idesco Oy. Viitattu 15.5.2009.
http://www.idesco.fi/products/pdf/access_basic_eng.pdf

Access 8 CM Pin. Idesco Oy. Viitattu 15.5.2009.
http://www.idesco.fi/products/pdf/Access_8_CMpin_Datasheet_English.pdf

Axis Phtoto Archive. Axis Communications Ab. Viitattu 18.5.2009.
http://www.axis.com/techsup/cam_servers/cam_211w/index.htm?tab=photos

Bosch Product Catalog. Bosch Security Systems. Viitattu 18.5.2009.
http://products.boschsecurity.fi/en/FI/products/bxp/CATM70e3f0fbe6342193142e608551935f28

EV669 kattoilmaisin. GE Security Oy. Viitattu 26.3.2009.
http://www.gesecurityproducts.eu/FI/products_single.php?product=EV669

EV1012AMZ liikeilmaisin. GE Security Oy. Viitattu 26.3.2009.
http://www.gesecurityproducts.eu/FI/products_single.php?product=EV1012AMZ

Garcia, M. L. 2001. The design and evaluation of physical protection systems. Boston: Butterworth-Heinemann.

Gill, M. 2003. CCTV. Leicester: Perpetuity Press Ltd.

Gruber, R. 2006. Physical and technical security: an introduction. Clifton Park: Thomson Delmar Learning.

Kameravalvonnan K-menetelmä 2006. Vakuutusyhtiöiden keskusliitto. Viitattu 16.4.2009.
http://www.vahingontorjunta.fi/asp/ida/download.asp?prm1=wwwuser_fkl&docid=163&sec=&ext=.pdf

Kulunvalvonta- ja rikosilmoitinjärjestelmät. 2007. ST-käsikirja 11. 4. painos. Espoo: Sähköinfo.

Laki yksityisistä turvallisuuspalveluista 12.4.2002/282.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Leppänen, J. 2006. Yritysturvallisuus käytännössä: turvallisuusjohtamisen portfolio. Helsinki: Talentum.

Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät: opas tilojen omistajille ja käyttäjille. 2004. Suomen toimitila- ja rakennuttajaliitto RAKLI ry & Turva-alan yrittäjät ry. Viitattu 21.1.2009. http://www.turva-alanyrittajat.fi/ajankohtaista/toimitilaturvallisuus.pdf

Miettinen, J. 2002. Yritysturvallisuuden käsikirja. Helsinki: Kauppakaari.

Murtohälytysjärjestelmät ja –palvelut ohje 2008. 2008. Finanssialan Keskusliitto. Viitattu 5.3.2009. http://www.vahingontorjunta.fi/asp/ida/download.asp?prm1=wwwuser_fkl&docid=24502&sec=&ext=.pdf

Rikosilmoitussanasto. 1993. Helsinki: Suomen vakuutusalan koulutus ja kustannus.

Takala, H. 1998. Videovalvonta ja rikollisuuden ehkäisy. Rikoksentorjunnan neuvottelukunta. Viitattu 7.4.2009. http://www.rikoksentorjunta.fi/uploads/igzauzw.pdf

Tietosuoja ja tekniset valvontajärjestelmät. 2005. Turva-alan yrittäjät ry. Viitattu 20.4.2009. http://turva-alanyrittajat.fi/doc/tietosuoja.pdf

Tikkanen, S., Aapio, L., Kaarnalehto, A., Kammonen, L., Laitinen, J., Mikkonen, J. & Pisto, M. 2008. Ammattina turvallisuus. Helsinki: WSOY.

Tolonen, P. 2009. Ip-kameroiden uusin tekniikka. Turvallisuus 1/2009, 31-32.

Tolonen, P. 2009. Analoginen valvontakamera pitää pintansa. Turvallisuus 2/2009, 22-24.

Turvallisuusalan valvontayksikkö. Viitattu 21.1.2009. http://www.intermin.fi/intermin/hankkeet/yksityinenturva/home.nsf/pages/911CA3E6C539AE07C2256E840029A29B?opendocument

Videotec S.p.A. Viitattu 18.5.2009. http://www.videotec.com/en/page_180.html

Videovalvontajärjestelmät. 2003. ST-käsikirja 13. 3. painos. Espoo: Sähköinfo.

Yritysten rikosturvallisuus 2008: Riskit ja niiden hallinta. 2008. Keskuskauppakamari. Viitattu 23.3.2009.http://www.keskuskauppakamari.fi/kkk/media/tiedotteet/2008_lehdistotiedotteet/fi_FI/yritysturvallisuus24042008/_files/79234154033787158/default/yritysturvallisuusselvitys%202008.pdf

Älykkäät ip-kamerat yläkastiin - analogiakameroista keskiluokka. 2009. Turvallisuus 1/2009, 33.

Kuvat