Aalto-yliopiston teknillinen korkeakoulu

Koulutuskeskus Dipoli

10. PÄÄSUUNNITTELUKOULUTUS 2010

KÄYTÄNNÖN TIETOTURVA RAKENNUSHANKKEESSA

Kari Koistinen

Sisällysluettelo

1. JOHDANTO

Tietoturvassa on kyse yrityksen tai yhdistyksen toiminnan turvaamisesta niin tahallisilta kuin tahattomiltakin riskeiltä. Tietoturvan tehtävänä on minimoida sekä aineelliset, että aineettomatkin tuhot ja häiriöt.

Alati muuttuva sähköinen tiedonvälitys on helpottanut tiedonsiirtoa, tämä on kuitenkin samalla lisännyt riskejä tiedon päätymisestä vääriin käsiin. Tietoa säilytetään ja siirretään hyvin erilaisilla tavoilla, mutta mikään tapa ei ole täysin turvallinen hyökkäyksiä vastaan. Erilaiset haittaohjelmat (virukset, madot, Troijalaiset yms.) ja tietomurrot ovat kaikille tietokoneohjelmien käyttäjille tuttuja jollain tasolla. Erilaisiin uhkiin, ja fyysiseen ja aineettomaankin turvallisuuteen voidaan varautua ennalta ja ehkäistä huolellisella suunnittelulla. Tätä suunnittelua kutsutaan tietoturvasuunnitelmaksi.

Tietoturva vaatii jatkuvaa kehittämistä ja sitoutumista toiminnan ylläpitämiseen. Mikäli tietoturvaa ei kehitetä, eikä toimintaan panosteta riittävällä tasolla jatkuvasti, menevät investoinnit täysin hukkaan. Päivittämätön tietoturva on sama kuin sitä ei olisikaan. On ensiarvoisen tärkeää viedä ajatus organisaation johtotasolle asti siitä, että kehittyvä ympäristö on toimiva ympäristö, joka heijastuu perinteisestä yritystoiminnasta aina käytännön työtehtäviin ja tietoturvalliseen käyttäytymiseen.

2. YLEISTÄ

Tietoturva rakennushankkeessa pääsuunnittelijan kannalta sisältää tietoturva- asiat siinä toimintaympäristössä missä hän työskentelee, ja tietoturva- asioiden käsittelyn niissä hankkeissa joissa hän toimii pääsuunnittelijana. Esimiesasemassa ollessaan pääsuunnittelijan tehtäviin kuuluu seurata alaistensa käyttäytymistä myös tietoturvallisuuden kannalta ja tarvittaessa puuttua siihen. Esimiehenä pääsuunnittelija vastaa alaistensa tietoturvakoulutuksen riittävyydestä sekä valvoo sen noudattamista

Tietoturvasta huolehtiminen ja kehittäminen on osa yrityksen toimintaa siinä missä liiketoiminnan kehittäminenkin. Yritysturvallisuuden osa-alueet eivät ole toisistaan erillisiä, yhden osa-alueen kehittäminen vaikuttaa usein ainakin yhteen toiseen, ellei useaan muuhun osa-alueeseen. Tästä johtuu, ettei tehokasta uhkilta suojautumista aina voi saavuttaa vain yhtä osa-aluetta kehittämällä. Lukituksen ja avainhallinnan parantamisella voi olla suuri merkitys tietoturvallisuuden parantamiseen, vaikkei tätä tulisi heti ajatelleeksi.

Jokainen yritys on oman näköisensä, ja siksi turvallisuusmalleja ei voi kopioida muilta. Hyviä käytäntöjä löytyy ja niitä voidaan hyödyntää, mutta yrityksen tulee itse kantaa vastuu siitä miten turvallisuutta kehitetään ja miten sitä tehdään yritykselle järkevällä tavalla. Turvallisuuden suunnittelua ja kehittämistä ei kannata ulkoistaa ainakaan kokonaan, turvallisuuden toteutus taas voidaan osittain ulkoistaa. Ostopalveluja voidaan käyttää esimerkiksi vartioinnissa, kuitenkin oma henkilökunta on usein ratkaisevassa asemassa siinä, miten yrityksen turvallisuus eri tilanteissa toteutuu. Henkilökunnan on oltava mukana johtoa myöten turvallisuuden kehittämisessä ja ylläpitämisessä. Toimiva tietoturvapolitiikka edellyttää henkilökunnan kouluttamista ja opastamista kyseisiin asioihin ja ohjeet tulee olla kaikkien helposti saatavilla. Mikäli nämä asiat laiminlyödään, on turha vaatia henkilökuntaa hallitsemaan turvallisuusasioita.

3. TIETOTURVA

3.1 Osa-alueet

Yrityksen tietoturvallisuus voidaan jakaa kahteen eri osa-alueeseen

- hallinnolliseen tietoturvallisuuteen
- tekniseen tietoturvallisuuteen

Hallinnollinen tietoturvallisuus koostuu toimitilaturvallisuudesta ja henkilökunnan ohjeistuksesta ja koulutuksesta.
Tänä päivänä olemme hyvin riippuvaisia tietokoneiden ja tietoverkkojen toimivuudesta. Tietokoneisiin on tallennettuna hyvin suuri määrä tietoa, mutta onko tieto saatavilla silloin kun sitä tarvitaan.
Tärkeä osa tietoturvaa on jokaisen ihmisen oma maalaisjärki, jonka avulla useimmista asioista selvitään myös tietoturvan osalta. [1]

[1] Vesterinen, P et al (2008): Helsingin seudun kauppakamari: Yrityksen Turvallisuusopas

3.2 Riskien arviointi

Yrityksessä tulee tehdä turvallisuusasioiden riskianalyysi. Yritys arvioi, mitkä asiat ovat tietoturvan kannalta tärkeitä. Tämän jälkeen voidaan arvioida sitä, millaisia uhkia toiminnalle tärkeisiin asioihin kohdistuu. Turvallisuusasioihin perehdyttäessä tulee huolehtia siitä, että turvallisuustoiminta on oman toiminnan näköistä. Suojautumista ei tule ylimitoittaa, muutoin turvallisuusasiat voivat painottua vääriin asioihin. Turvallisuuden tasoa määriteltäessä yritys voi käyttää apunaan asiantuntijoita, käytännössä kuitenkin yrityksen sisällä on riittävä tieto siitä, mitä tarvitsee suojata ja millainen uhka niihin kohdistuu. Suojausta arvioitaessa ei kannata arvioida pelkästään sitä, minkä arvoinen jokin asia on taloudellisessa mielessä. Tärkeää on myös se, mitä jonkin asian vahingoittuminen, toiminnan keskeytys tai jopa tuhoutuminen aiheuttaa yrityksen toiminnalle. Suojattavia arvoja voivat olla ihmiset, tieto, omaisuus, ympäristö ja maine. Suojautumisen tasoon vaikuttaa myös uhan todennäköisyys.

Yksinkertaisin ja yleisin tapa arvioida riskejä on tehdä taulukko, johon arvoihin kohdistuvat riskit sijoitetaan sen mukaan, miten todennäköiseksi ne arvioidaan ja miten suurta vahinkoa yritykselle voisi koitua riskin toteutuessa.

Taulukko Riskianalyysitaulukko, kuvitteellinen yritys

Uhka	Esiintyminen	Kustannus	Hallinta
Tietomurto / hakkerointi	Mahdollinen	Korkea - Erittäin korkea	Ajantasaiset ja oikein konfiguroidut palomuurit, tietoturvapäivitykset, virustorjunta sekä käyttäjien koulutus.
Vesivahinko	Mahdollinen	Korkea	Ei vesisammuttimia laitehuoneisiin, verkon aktiivilaitteet suojataan kaapeilla. Lattiatasossa ei mitään laitteita.
Laitevika	Mahdollinen	Matala - Korkea	Säännöllinen huolto ja tarkistukset, UPS varmennus
Laitevarkaus	Epätodennäköinen	Matala - Korkea	Ei vaadittuja toimenpiteitä.
Virukset / Madot	Todennäköinen	Matala - Keskitaso	Ajantasaiset virustorjunnat sekä palomuurit. Käyttäjien kouluttaminen
Social engineering	Todennäköinen	Matala - Erittäin korkea	Käyttäjien kouluttaminen.
Vakoilu	Epätodennäköinen	Matala - Erittäin korkea	Käyttäjien kouluttaminen. Ajantasaiset palomuurit, pääsynvalvonta
Tietojen luvaton kopiointi omaan käyttöön	Mahdollinen	Korkea	Käyttäjien kouluttaminen, pääsyn valvonta
Yrityssalaisuuksien paljastaminen	Mahdollinen	Korkea - Erittäin korkea	käyttäjien kouluttaminen
Sähkökatko	Mahdollinen	Matala	UPS varmennus kriittisille laitteille
Tietoverkko-hyökkäykset	Mahdollinen	Matala - Keskitaso	Ajantasaiset palomuurit, verkon toiminnan seuraaminen, automaattiset tietoturvapäivitykset

Malli riskien arviointi taulukosta[2]

Pääsuunnittelijan tulee olla selvillä kulloisenkin rakennushankkeen turvallisuusriskeistä, nämä tiedot ovat yleensä saatavissa tilaajalta. Tietoturvariskit ovat hyvin erityyppisiä ja – laajuisia, riippuen kulloinkin kohteena olevasta rakennusprojektista.

[2] Kortelainen, J (2010): Tietoturvasuunnitelmatyökalu.

4. UHKAT

4.1 Ihmiset

Henkilöt ovat yrityksen suurin tietoturvauhka, koska he pääsevät käsiksi monenlaisiin tietoihin, heidän kautta tulevat uhat voivat olla ulkoisia tai sisäisiä. Sisäiset uhat toteutuvat omien työntekijöiden kautta ja ulkoiset yrityksen ulkopuolisten tahojen kautta. Työntekijät tietävät aina eniten toimitilajärjestelyistä ja siitä mitä missäkin säilytetään. He tietävät myös pääpiirteissään, miten tiloja valvotaan. Samaan ryhmään voidaan laskea turvalaitteiden asentajat ja siivoojat.

Monikaan ihminen ei kuitenkaan ajattele käsittelevänsä luottamuksellista tietoa, toisaalta epälojaali henkilö voi tehdä tietoturvaponnistukset täysi turhiksi. Henkilö- ja palkkatiedot mielletään salassa pidettäviksi, mutta muun tiedon salaus yritysympäristössä ei liene yhtä selvää. Alihankkijat, kuten kiinteistöhuolto ja siivous, saavat myös haltuunsa tietoa ja usein heillä on pääsy toimitiloihin, kun siellä ei ole normaalia toimintaa.

Tietokoneiden vaihtuessa on pidettävä huolta vanhoista laitteista. Tavallisesti joku työntekijöistä joko saa tai ostaa vanhan koneen itselleen. Tällöin pitää ehdottomasti muistaa poistaa vanhasta koneesta kaikki yrityksen omistamat tiedot, ohjelmat ja ohjelmistot.

4.2 Haittaohjelmat

Haittaohjelmat ovat tänä päivänä sähköisessä tiedonvälityksessä arkipäivää. Ei pidä puhua pelkästään tietokoneviruksista vaan parempi termi koko ongelmavyyhdelle on haittaohjelma. Erilaiset madot, troijalaiset, rootkitit eli piilohaittaohjelmat sekä vakoilu –ja mainosohjelmat. Kaikissa tapauksissa kyse on tietokoneen käyttöä tai käyttäjää haittaavista erilaisista ohjelmista, joita nykyään on olemassa jo noin miljoona erilaista. Näiden avulla voidaan tehdä aivan mitä haittaohjelman tekijä vaan haluaa.[3]

Internettiä käytettäessä tulee muistaa koneen suojaus, jotta vältytään saastuttamasta konetta erilaisilla haittaohjelmilla. Kannattaa pysyä poissa sopimattomilta www-sivuilta, mikäli vähänkään epäilee sivun turvallisuutta. Tosin vaarallisten sivujen erottaminen vaarattomista pelkän ulkonäön perusteella on usein hankalaa asiantuntijallekin.

4.3 Muut uhkat

Muita uhkia ovat tietomurto, palo- ja vesivahinko, tekniset viat sekä asiakirjojen huolimaton säilytys. Työpaikalla tietosuojan haavoittuvin käsittelyvaihe on silloin, kun tuhottavaksi tarkoitettu asiakirja odottaa työpöydän alla olevassa pahvilaatikossa tyhjennystä. Hylätyt asiapaperit saattavat lojua viikkoja työpöydän alla kaikkien liikkuvien saatavilla, ennen niiden tuhoamista tai siirtoa turvallisempaan paikkaan.

[3] Vesterinen, P et al (2008): Helsingin seudun kauppakamari: Yrityksen Turvallisuusopas

5. SUOJAUTUMINEN

Suojautumisesta puhuttaessa pääsuunnittelijan kannalta olisi tärkeää päästä vaikuttamaan asiaan jo esisuunnitteluvaiheessa. Tietoturvan kannalta pääsuunnittelijan tulisi yhdessä rakennuttajan kanssa voida vaikuttaa suunnittelusopimuksiin siten, että niissä sovittaisiin yhteisistä pelisäännöistä tiedonsiirrossa ja korostettaisiin niiden tärkeyttä.

Pääsuunnittelijan tehtäväluettelossa [4]annetaan mahdollisuus osallistua suunnitteluryhmän kokoamiseen yhdessä rakennushankkeeseen ryhtyvän kanssa. Tässä vaiheessa olisi pääsuunnittelijalla mahdollisuutta kontrolloida sitä, että muilla suunnitteluryhmän jäsenillä on edellytykset toimia projektissa halutulla tavalla. Valitettavasti tämä ei useinkaan toteudu, vaan ainakin osasta muita suunnittelijoita on päätetty ja sopimukset tehty kysymättä asiaa pääsuunnittelijalta.

Tämän päivän tietomallipohjaisessa suunnittelussa vastuut ja tiedonsiirron pelisäännöt tuntuvat hämäriltä. Pääsuunnittelijan tulisi olla se henkilö joka hallinnoi tietomallia ainakin niin kauan kuin rakentaminen kestää, koska hänellä on parhaiten kokonaisnäkemys hankkeesta. Loppukädessä tietomalli on rakennuttajan omaisuutta, mutta kuka huolehtii sen hallinnasta ja päivityksestä? Pystyykö rakennuttaja hyödyntämään saamaansa mallia riittävästi, onko hänellä siihen kykeneviä henkilöitä ja laitteita?[5]

[4] RT 10-10764 (2001): Pääsuunnittelun tehtäväluettelo PS 01; Tehtävät 1.5

[5] RT 10-10992 (2010); Tietomallinnettava rakennushanke. Ohjeita rakennuttajalle

5.1 Sähköinen suojautuminen

Sähköisellä suojautumisella tarkoitetaan kaikkea turvallisuuteen ja toimivuuden jatkuvuuteen vaikuttavia tekijöitä, jotka johtuvat laitteista tai käytetyistä tekniikoista. Tähän sisältyy mm. viruksilta ja hyökkäyksiltä suojautumista, varmuuskopiointi ja palomuuri.

5.1.1 Varmuuskopiointi

Varmuuskopiointi on yksi tärkeimmistä toiminnan jatkuvuuden turvaavista tekijöistä ja sen toteuttaminen luotettavasti takaa yrityksen toiminnan jatkumisen, tekniikan tai turvallisuuden pettäessä. Mitään yrityksen toiminnan kannalta olennaista tietoa ei tulisi säilyttää työasemilla tai kannettavilla laitteilla, vaan kaikki tieto tulisi varastoida palvelimille, joiden toiminta on suojattu sähköverkon vikatilanteilta ja jotka on asianmukaisesti varmuuskopioitu. Kaikki olennainen tieto pitää varmuuskopioida ja kaikkia varmuuskopioita tulee säilyttää paloturvallisessa tilassa riittävän kauan, esimerkiksi vuosi varmuuskopion ottamisesta. Kaikkien otettujen varmuuskopioiden toimivuus tulee testata välittömästi, jotta vikatilanteen sattuessa saadaan palautettua viimeisin tieto. Yleisimpiä tallennusmuotoja ovat nauhatallennus, kovalevytallennus ja optiset levyt. Tulevaisuudessa tekniikoiden kehittyessä on muistettava pitää huoli siitä, että tarvittaessa myös vanhoja varmuuskopioita pystytään lukemaan.

5.1.2 Palomuuri

Palomuuri on säännöstön sisältävä järjestelmä, jonka avulla voidaan ohjata ja rajoittaa liikennettä kahden tai useamman verkon välillä. Palomuuri sijoittuu kahden eri verkon väliseen reitittimeen. Ohjelmistopohjaiset palomuurit on tarkoitettu yksittäisten työasemien suojaamiseen ja lisäävät näin henkilökohtaista tietoturvaa. Palomuuriohjelmistot valvovat käyttäjän verkon liikennettä ja varoittavat heti, mikäli epäilyttävää liikennettä havaitaan ja suodattaa suoraan jo tunnettua haitallista tai kiellettyä liikennettä. Myös mikäli palomuuri havaitsee, että uusi prosessi tai ohjelma pyrkii koneelta verkkoon, antaa se hälytyksen ja pyytää käyttäjää selvittämään tilanteen. Ohjelmallisissa palomuureissa on versioita, joita pystyy hallitsemaan suurissakin verkoissa keskitetysti vähentäen verkonhallinnan työtä ja tehostaen toimintaa. Keskitetysti hallinnoimalla kaikkien työasemien ohjelmia voidaan varmistua siitä, että kaikkiin on asennettu viimeisimmät päivitykset ja kaikissa on samanlaiset pääsy ja esto säännöt.

5.1.3 Tiedon salaaminen

Tiedon salaamiseen on olemassa monia ohjelmistoja joiden käyttö on hyvinkin helppoa. Esimerkiksi kannettavaan tietokoneeseen asennetaan ohjelmisto, joka automaattisesti salakirjoittaa koko kovalevyn sisällön siten, ettei sitä pystytä tulkitsemaan ilman asianmukaista käyttäjätunnusta tai tokenia. Token on erillinen laite, joka voidaan liittää vaikka USB-porttiin ja toimii näin käyttäjän tunnistamiseen tai sitä voidaan käyttää erillisen salasana suojauksen tukemiseenkin. Kovalevyn salaamisella vältytään laitevarkauden aiheuttamalta tietoturvariskiltä, sillä ilman käyttäjätunnusta ja/tai tokenia ei tietoihin pääse mitenkään käsiksi.[6]

[6] Kortelainen, J (2010): Tietoturvasuunnitelmatyökalu.

Joissain käyttökohteissa on otettava käyttöön kryptaus. Kryptaamisella tarkoitetaan tiedon salakirjoittamista siten, että sen lukeminen ja käyttö vaatii esimerkiksi salasanan ja käyttäjätunnuksen. Tämä tekniikka on erityisen hyödyllinen kannettavien laitteiden yhteydessä, sillä kannettavan tietokoneen varastaminen fyysisesti on kuitenkin hyvin helppoa, mikäli kyseessä on liikkuva työntekijä.

Pääsuunnittelijan kannalta esimerkiksi piirustusten, kokousmuistioiden ja visualisointien siirto muiden suunnittelijoiden, rakennuttajan ja urakoitsijan välillä tapahtuu kätevimmin käyttämällä projektipankkia. Projektipankkiin pääsy on varmistettu salasanoin vain tietyille projektissa toimiville henkilöille. Mikäli kuvia toimitetaan verkon kautta suoraan muille suunnittelijoille, on hyvä lähettää kuvat IFC-muodossa (Industry Foundation Classes). Tällöin siirretään ainoastaan oliotietoa eli 3D-geometriaa ja parametrejä, tässä piirustusmuotoinen tieto ei siirry.

5.2 Lojaliteetti

Lojaliteetti tarkoittaa työyhteisön arvoihin perustuvaa sitoutumista. Sitoutumiseen liittyy useita sitouttavia tekijöitä eli sidoksia. Työnantajan ja työntekijän välille syntyy sidoksia mm. yhteisistä arvoista, pitkästä ja haastavasta työsuhteesta, mahdollisuudesta kehittää ammattitaitoa, molempien työn arvostuksesta, tasavertaisuudesta ja hyvästä työnteon hengestä

Työsopimuslain mukaan työntekijän on oltava lojaali työnantajaa kohtaan. Lojaliteetti ei ole juridinen ongelma, vaan työnjohdollinen ongelma. Juridiikka ei voi näin ollen ratkaista ongelmaa. Perinteisesti on ajateltu, että esimiehen tehtävä on varmistaa alaistensa työnteon edellytykset ja ylläpitää alaistensa työmotivaatiota. Johtamisjärjestelmät sisältävät kuitenkin intressejä, jossa työntekijöihin liitetyt arvot ovat toissijaisia aineellisiin arvoihin verrattuna.
Tietoturvallisuus ei ole yksinomaan juridiikkaa, matematiikkaa, tietotekniikkaa, mittareita, koulutusta ja ohjeistusta. Tietoturvallisuus on viimekädessä henkilöstöön kulminoituva ongelma. Inhimillisillä tekijöillä on ratkaiseva rooli tietoturvallisuuden toteutumiselle. Epälojaali henkilö voi tehdä yhteiset tietoturvaponnistukset täysin turhiksi.

Tieto voi kävellä hetkessä kilpailevaan organisaatioon tai levitä globaalisti Internetin välityksellä koko toimialan hyödynnettäväksi. Lojaliteettisidosten murruttua henkilö voi aiheuttaa nykyiselle tai aikaisemmalle työnantajalleen monenlaista vahinkoa kopioimalla tai luovuttamalla yrityssalaisuuksia kilpailijan käyttöön tai hyödyntämällä yrityssalaisuuden piiriin kuuluvia tietoja uudessa työpaikassa työnantajan tietämättä.

On verrattain tavanomaista, että työntekijät kopioivat itselleen sen tiedon, jonka he ovat työtehtävissään saaneet haltuunsa ja jonka katsovat parantavan omaa kilpailukykyään työmarkkinoilla. Kopiointi tehdään yleensä jo hyvissä ajoin niin, että irtisanoutumisilmoituksen yhteydessä toimeenpantavalla käyttövaltuusrajoituksella tai välittömällä työntekovelvollisuuden päättämisellä ei ole tässä vaiheessa enää käytännön merkitystä. Työntekijän normaalia työntekoa irtisanoutumisaikana tulee rajoitta vain, jos on konkreettisia syitä odottaa uhkaavaa yrityssalaisuusrikosta.
Useimmat työntekijät arvostavat työpaikkaa, joka voi tarjota toimeentulon eläkeikään asti. Työyhteisön jäsenen lojaliteetti työnantajaa kohtaan voi päällisin puolin näyttää hyvältä, mutta käsitys asioiden oikeasta tilasta saattaa osoittautua kuitenkin vääräksi. Järkevän vaihtoehdon ilmaannuttua henkilö onkin valmis katkaisemaan sidoksensa työnantajaan ja valmis vaihtamaan työpaikkaa.

Turvallisuus muodostuu ja toteutuu työn suorituspaikalla. Hyviä tuloksia voidaan odottaa vain, jos työilmapiiri on hyvä. Hyvälle työilmapiirille on keskeistä mm. työyhteisössä vallitseva luottamus ja avoimuus. Henkilöstöllä voi olla monenlaisia työyhteisön ilmapiiriä kuormittavia ongelmia. Tavanomaisia ongelmia ovat esimerkiksi:

Työuupumus.
Sairaus.
Lähiomaisen kuolema, sairaus tai vammautuminen.
Perheongelmat.
Katkeruus työyhteisöä kohtaan.
Turhautuminen jne.

5.3 Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöiden toiminnasta organisaatiolle aiheutuvien riskien hallintaa. Henkilöstöturvallisuuden tavoitteena on rekrytoida organisaation eri työtehtäviin soveltuvia, työkykyisiä, lojaaleja ja rehellisiä ihmisiä. Henkilöstöturvallisuuden riskienhallintatoimenpiteet keskittyvät rekrytointiin, sen yhteydessä tehtäviin taustaselvityksiin ja testeihin, työsuhteen aikana suoritettaviin testeihin, sisäiseen valvontaan ja ohjeistuksiin.

Organisaation on rekrytointiprosessissaan erotettava tavanomaiset tehtävät selkeästi luottamuksellisuutta edellyttävistä tehtävistä. Poikkeukselliset selvittelytoimenpiteet eivät ole osa normaalia rekrytointiprosessia. Turvallisuusselvityksiin tai muihin poikkeuksellisiin taustaselvityksiin suostumista ei voida edellyttää tavanomaisiin työtehtäviin hakeutuvilta henkilöiltä. Peruslähtökohta työnantaja/työntekijä suhteessa on molemminpuolinen luottamus.

Rekrytoivan esimiehen käytössä on mm. henkilön CV, haastattelutiedot, soveltuvuustestin tulos ja oma intuitiivinen arvio rekrytoitavasta henkilöstä.

Vuonna 2001 henkilöstöturvallisuuden varmistamiseksi tehtävää selvitysmenettelyä selkeytettiin uudella lailla. Lain myötä luotettavuuslausunto muuttui turvallisuusselvitykseksi, joita on laajuudeltaan kolme eri tasoa, suppea turvallisuusselvitys (LIITE 1), perusmuotoinen turvallisuusselvitys, sekä laaja turvallisuusselvitys. Suppean turvallisuusselvityksen antaa pääsääntöisesti sijaintipaikkakunnan kihlakunnan poliisilaitos. Supo antaa perusmuotoisen ja laajan turvallisuusselvityksen.

Turvallisuusselvityksessä poraudutaan yksilön kannalta ehkä kaikkein arimmalle yksityisyyden alueelle. Turvallisuuslausunnon tuloksen merkityksen arviointi valintaprosessissa jää rekrytoijan vastuulle. Supon lausunnon taustalla olevia tietoja ei voi tarkistaa eikä oikaista.

Erityisasemassa ovat niin sanotut avainhenkilöt. Avainhenkilöllä tarkoitetaan organisaation palvelu- ja liiketoiminnan kannalta vaikeasti korvattavaa henkilöä. Avainhenkilön tunnusmerkkejä ovat mm. seuraavat piirteet:

- Henkilö hallitsee kriittisten ydinjärjestelmien toimintaan liittyvät tekniset yksityiskohdat.
- Henkilö omaa luottamukselliset suhteet palvelu- tai liiketoiminnan kannalta tärkeimpiin yhteistyökumppaneihin.
- Henkilö omaa toimialalta sellaista kriittistä tietoa, jota muilla ei ole.

Työnaikaista sitoutumista voidaan vahvistaa luottamuksellisuussitoumuksella, joka voi olla työnantajan ja tilaajan- tai työntekijän ja tilaajan välinen (LIITE 2).

Työsuhteen päättyessä rikoslain mukainen salassapitovelvollisuus työntekijän kohdalla päättyy kahden vuoden kuluttua. Tämän jälkeen yrityssalaisuus ei nauti rikosoikeudellista suojaa. Mikäli tieto on saatu haltuun oikeudettomasti, jatkuu salassapitovelvollisuus ilman aikarajoitusta.

Salassapitoaikaa voidaan jatkaa salassapitosopimuksella, kun on kulunut kaksi vuotta palvelussuhteen päättymisestä. Salassapitosopimus ei estä kokemusperäisen tai muistinvaraisen tiedon hyväksikäyttöä, ellei asianomainen ole ilmaissut tai käyttänyt hyväksi sellaista tietoa, joka on ollut vain edelliselle työnantajalle ominainen toimintaperiaate, ohje tai ratkaisu.

Mikä tieto on yrityssalaisuus ja mikä työntekijän yleistä ammattitaitoa?
Tämä asia on vaikeasti määriteltävissä. Työnantajan on hyväksyttävä, että entisen työntekijän on usein helppo käyttää luottamuksellista tietoa uudessa tehtävässään uuden työnantajan hyväksi ja vanhan työnantajan on erittäin vaikea näyttää tätä toteen. Ainoa tapa minimoida tällä tavalla mahdollisesti aiheutuvat vahingot on rajata työsuhteen aikana työntekijän pääsy vain hänelle tarpeelliseen tietoon. Tämä on vaikeaa ja vaatii työnantajalta paljon turvallisuuteen liittyvää työtä.

Työtekijöille on syytä korostaa, että kaikista toimistossa tehtävistä töistä ei ole syytä lörpötellä niin sanotusti ’ympäri kylää’, ainakaan ennen kuin ne ovat julkisia. Tämänkin jälkeen tulee harkita mitkä hankkeet ovat sellaisia, että niistä ulkopuolisille puhuminen on jätettävä mahdollisimman vähälle.

5.4 Toimitilaturvallisuus

Toimitilan olemassa olevat rakenteelliset ratkaisut muodostavat turvallisuussuunnittelulle lähtökohdan.
Vanhoissa kiinteistöissä lähtötilanne on aina hankalampi, kuin uudisrakennuksissa, joiden turvaratkaisuihin voidaan vaikuttaa jo rakentamisvaiheessa. Kaikissa olosuhteissa voidaan kuitenkin ohjeistuksin, katselmuksin ja käytännön harjoituksin lisätä merkittävästi toimitilojen turvatasoa.
Vastuu työpaikan turvallisuudesta kuuluu organisaation johdolle. Tätä vastuuta ei voi delegoida esimerkiksi vartiointiliikkeelle.

Toimitilaturvallisuutta käsitellään rikollisen toiminnan ehkäisemisen näkökulmasta eikä siinä oteta huomioon palotuvallisuuteen tai rakenteiden kestävyyteen liittyviä seikkoja. Tässä pyritään rikollisen toiminnan vaikeuttamiseen yrityksen toimitiloihin liittyvillä turvallisuustoimilla, kohdistui se yritykseen sitten ulkopuolisen tai sisäpuolisen henkilön toimesta.

Toimitilaturvallisuus muodostuu useasta pienestä osa-alueesta, joita pyritään kuvaamaan vyöhykeajattelumallin kautta (ks. 6.1.4 Toimitilojen sijoittelu). Kyseisessä mallissa toimitilat jaetaan eri vyöhykkeisiin ja pyritään löytämään ne osa-alueet, jotka vaikuttavat kyseisen vyöhykkeen turvallisuuteen. Käymällä järjestelmällisesti vyöhyke kerrallaan läpi saadaan nostettua yrityksen ja toimitilan turvallisuustasoa.

Osa-aluejako ei sinänsä estä rikollista toimintaa, kuten luvatonta tunkeutumista tilaan, mutta sen tarkoituksena on saada tehtyä tilasta rikollisen kannalta niin hankala, että tunkeutuja mieluummin luopuu yrityksestä kuin lähtee yrittämään tunkeutumista aiheuttaen jo yrityksellään vahinkoa rakenteille. Usein tällaisessa tunkeutumisessa menetetynomaisuuden arvo on vain murto-osa siitä, mitkä kokonaiskustannukset tällaisesta luvattomasta tunkeutumisesta aiheutuu.[7]

[7] Vesterinen, P et al (2008): Helsingin seudun kauppakamari: Yrityksen Turvallisuusopas

5.4.1 Ympäristö

Ympäristö, jossa yritys sijaitsee, merkitsee yllättävän paljon toimitilaturvallisuuteen. Kun aktiivista siistiä ympäristöä, verrataan ympäristöön, jossa on vähän liikennettä ja alueen ilmeeseen ei kiinnitetä huomiota eikä kiinteistöistä huolehdita, niin jälkimmäisellä on suurempi riski joutua murron, ilkivallan tai muun rikollisen toiminnan kohteeksi.

5.4.2 Aidat ja portit

Aidattu alue viestii siitä, missä kulkee alueen raja. Fyysisten ominaisuuksien lisäksi aita antaa symbolisen viestin siitä, että jollei sisäpuolelle ole asiaa, niin sinne ei mennä. Aidalla on myös merkitystä itse rakennusta koskevan ilkivallan vähenemisellä. Vaikka piha-aluetta ei ympäröisikään aita, olisi kiinteistön alueelle johtavalla tieosuudella oltava portti. Aidan ja portin yhdistelmässä olisi portin ja aidan oltava yhtä vahvaa tekoa. Ajoesteillä pyritään estämään ajoneuvolla ajaminen sisään toimitiloihin.

5.4.3 Piha-alue

Piha-alueen järjestelyt tulisi olla sellaiset, että ne eivät anna suojaa tunkeutumista tai ilkivaltaa aikovalle. Rakenteet ja muut rakennukset tulisi sijoittaa niin, etteivät ne helpota alueelle tunkeutumista, kuten esimerkiksi kiipeämistä aitojen yli.

5.4.4 Valaistus

Kiinteistö valaistuksella on suuri vaikutus turvallisuuteen, varsinkin pimeänä aikana. Pimeät sopet ja rappusyvennykset tulee valaista silloinkin kun kiinteistössä ei ole käyttäjiä. Valaistuksen riittävyyteen tulee kiinnittää erityistä huomiota, mikäli rakennukseen hankitaan tallentava kameravalvonta. Kattavakaan kameravalvonta ei toimi pimeän aikana mikäli valaistus ei ole riittävä, tämä koskee niin ulko- kuin sisätilojakin.

5.4.5 Liikenne

Liikkuminen kiinteistön alueella tulisi olla mahdollisimman helppoa ja selkeää. Liikkumista tulee ohjata ennalta suunniteltua reittiä pitkin, tämä mahdollistaa kameravalvonnan oikean mitoittamisen ja poikkeavista reiteistä saadaan teknisillä apuvälineillä havainto mahdollisimman aikaisessa vaiheessa.

Pysäköintipaikoilla henkilökunnan pysäköintipaikat on syytä pitää erillään vieraspaikoista ja merkitä nämä erikseen.

6. KIINTEISTÖN TURVALLISUUS

Rakenteiden turvallisuutta mietittäessä perusasia on, että mitä vahvempi materiaali on ja mitä enempi sitä on, sitä turvallisempi rakennus on. Rakennusmateriaalit määritellään rakennuslupa vaiheessa, mutta niihin voidaan vielä vaikuttaa rakentamisen alkuvaiheessa. Yleensä myös palamattomat rakenteet antavat hyvän suojan tunkeutumista vastaan.

Finanssialan keskusliitto on määritellyt rakennusmateriaaleja, ovia, lukkoja, rakenteita, kaltereita sekä sitä, millaiset ovat käyntivälykset ovissa, ikkunoissa ja luukuissa. Ohjeessa käsitellään myös sitä, mitä kaikkia suojaustoimia tulee hankkia, jotta vapaaehtoisen vakuutuksen ehdot täyttyvät.[8] Tällaiset määritteet ovat käyttökelpoisia pohdittaessa, millaisia teknisiä tai rakenteellisia suojauksia toimitiloissa tarvitaan. Sidosryhmävelvoitteet, kuten turvallisuussopimukset, voivat velvoittaa yritystä suojaamaan kiinteistöjään myös rakenteellisesti. Tällöin suojaustarpeet koskevat yleensä niitä tiloja, joissa tehdään esimerkiksi alihankintana toiselle yritykselle tuotteita tai palveluja.

Suoraan seinän läpi tapahtuvia murtoja tehdään suomessa vähän ja tällöinkin ne ovat tapahtuneet pääasiassa väliseinien läpi. Kevytrakenteiset ulkoseinät eivät tarjoa kunnon suojaa tunkeutumista vastaan. Tällaisessa tapauksessa seinärakenteita voidaan vahvistaa kriittisistä kohdista tai niihin voidaan liittää hälytysjärjestelmiin liitettäviä ilmaisimia.

Katto on paikka rakennuksessa jossa sijaitsee jo valmiiksi välikatolle tai suoraan rakennukseen johtavia akkoja, esimerkiksi katoikkunoita, savupoisto- ja huoltoluukkuja. Tällaiset aukot tulee suojata kaltereilla ja hälytysjärjestelmillä.

[8] Finanssialan Keskusliitto (2005) : Rakenteellinen murtosuojeluohje 1, 2, 3

Ikkunat muodostavat houkuttelevan ja helpohkon reitin rakennukseen tunkeutumisessa. Ikkunan saa rikottua helposti ja nopeasti varsinkin, jos ne sijaitsevat alle 3-4 metrin korkeudessa. Ulkoikkunat tulee liittää murtohälytysjärjestelmään ja ikkuna-aukon murtosuojausta voidaan parantaa esimerkiksi kiinteärakenteisella teräsristikolla, alaslaskettavalla metallirulolla, panssarilasilla tai polykarbonaattilevyllä.

Ovien kohdalla huomiota tulee kiinnittää itse ovien kestävyyteen, karmien kestävyyteen, karmin kiinnitykseen ympäröiviin rakenteisiin sekä karmin kiinnityksiin varsinkin lukon ja saranoiden kohdalta. Lähtökohta on, että ovea ei pystytä rikkomatta avaamaan ulkoapäin ilman avainta. Ulkovaipan ovet tulee liittää murtohälytysjärjestelmään ja ovien lasiosien kohdalla pätee se mitä edellä on kerrottu ikkunoista. Kotimaiset ovet ja karmit on lähes poikkeuksetta varustettu luokituskyltillä, joka löytyy oven saranapuolelta ovesta ja samalta puolelta karmista. Mikäli ovi ja karmi on murtotestattu, niistä löytyvät luokituskyltit, joissa on merkintä SFS 4487, SS 817345, tai DIN 18103.

Lukitus tulee toteuttaa tehdastasona, esimerkiksi Abloy Exec. Tämä takaa käytön helppouden ja seurannan, sekä avainten kopioimissuojan. Avainten sarjoituksessa tulee kiinnittää huomiota eri alueille pääsemiseen ja pääsyn estämiseen niille alueille, joihin toimenkuvan tai aseman vuoksi ei ole oikeutta.

Avainturvallisuus pitää sisällään avainhallintaprosessin joka kuvaa, dokumentoi ja ohjeistaa mahdollisten henkilömuutosten vuoksi. Avaimia käyttävien henkilöiden tulee olla tietoisia kuittaamisen ja avainten henkilökohtaisuudesta. Mekaanisten avaimien lisäksi tarkoitetaan elektronisia avaimia, kulkukortteja sekä liikkumiseen käytettäviä koodeja.

Kiinteistössä liikkuminen tulee järjestää niin, että kaikki vieraat, asiakkaat, tilapäiset huoltoon -, korjaukseen – ja ylläpitoon liittyvät tilapäiset henkilöt ilmoittautuvat vastaanottopisteeseen. Vastaanottopisteestä heidät noutaa vierailun isäntä tai huollon yhteydessä he kuittaavat itselleen tarvittavat avaimet. On myös tiloja joihin ei koskaan saa päästää ketään ilman saattajaa.

6.1 Tekninen valvonta

9

Toimitilojen tekninen valvonta on tänä päivänä perusasioita ja kehittyy koko ajan. Tekninen valvonta pitää sisällään rikosilmoitin-, kulunvalvonta-, kameravalvonta- ja kiinteistön ylläpitojärjestelmät tai jopa kaikkien edellä mainittujen järjestelmien yhdistelmät. Huomioitavaa on, että yrityksessä jossa harkitaan edellä mainittuja valvontamenetelmiä, asia tulee käydä läpi ja esitellä työntekijöiden kanssa yhteistoimintamenettelyssä (Yhteistoimintalaki 30.03.2007/ 334).

[9] Sanomalehti Kaleva (2010) :Juba Tuomola; Sarjakuva Viivi ja Wagner

6.1.1 Rikosilmoitinjärjestelmä

Rikosilmoitusjärjestelmä paljastaa ja osoittaa murtautujan tulon tai yrityksen tulla valvottuihin tiloihin. (CEA; European insurance and reinsurance federation 4039:2002-08 fi)[10]. Rikosilmoitinkeskukset tulee sijoittaa hyvin suojattuun lukittuun tilaan, jota voidaan valvoa järjestelmän ilmaisimilla.

6.1.2 Kulunvalvonta

Kulunvalvonta voidaan jakaa henkilöliikenteen-, vierailijoiden- ja tavaraliikenteen kulinvalvontaan.

Henkilöliikenteen kulunvalvonnassa kuvalliset henkilökortit ovat kulunvalvonnan ja turvallisuuden kannalta ensiarvoisen tärkeitä asioita. Kuvallinen henkilökortti soveltuu kaiken kokoisille organisaatioille, jopa yhden hengen konsulttiyritykset käyttävät henkilökortteja. Kuvallinen henkilökortti voi nykyisin olla pelkkä ID-kortti, varustettu kulunvalvontaominaisuudella tai varustettu kulunvalvonta- ja käyttövaltuusominaisuuksilla. Henkilökunnan kulku toimitiloihin sallitaan "virallisista" kulunvalvontapäätteillä varustetuista ovista. Henkilökunnan tulee rekisteröidä kulku henkilökohtaisella tunnisteellaan kulunvalvontapäätteellä jokaisen kulkukerran yhteydessä (sisään/ulos).

Vierailijoiden kulku tapahtuu aina pääoven kautta. Vierailijan tulosta ilmoitetaan etukäteen erikseen sovittavan käytännön mukaisesti pääsisäänkäynnin vahtimestarille. Vierailijan ilmoittaminen tapahtuu valitun käytännön mukaisesti esimerkiksi sähköiseen vieraskirjaan, sisäisellä sähköpostilomakkeella, puhelimitse tai jättämällä ilmoitus henkilökohtaisesti. Vierailijoiden kohdalla tulee erottaa kulunvalvonnalliset prosessit muista yhteistyöprosesseista.

[10] Vesterinen, P et al (2008): Helsingin seudun kauppakamari: Yrityksen Turvallisuusopas

Vahtimestarille ilmoittautuminen liittyy kulunvalvontaprosessiin, eikä prosessin yhteyteen tule kytkeä sitoumusten tai luottamuksellisten henkilötietojen keruuta. Vierailijan isäntä ilmoittaa vieraansa nimen ja organisaation sekä joissakin erityistapauksissa myös vierailun syyn. Sosiaaliturvatunnusta, vaitiolositoumusta tai muita tietoja ei vierailijalta edellytetä. Vierailijan ilmoittautuessa vahtimestarille, hänelle luovutetaan suoraan vierailijakortti. Vieraskortin voimassaoloaika on yksi työpäivä. Erityistilanteissa voimassaoloaikaa voidaan pidentää. Vierailun päätyttyä isäntä tai hänen edustajansa saattaa vierailijan vastaanottopisteeseen ja varmistaa, että vierailijakortti luovutetaan takaisin.

Tavaraliikenteen kulunvalvonnassa tavaran haltijalla tulee olla tavaran kuljetukseen oikeuttava osaston/yksikön antama lupa. Kuljetukseen oikeuttava lupa on esitettävä pyynnöstä vahtimestarille tai vartijalle. Myös tavaraliikenteen henkilöt voivat käyttää ID-korttia tai muuta tunnistusjärjestelmää sisään - ja ulospääsyyn.

6.1.3 Kameravalvonta

Tunnistettavia henkilöitä tallentavan kameravalvonnan tallenteet muodostavat henkilörekisterin, jonka käsittelystä on säädetty henkilötietolaissa (523/1999). Henkilörekisterinpitäjä on se osapuoli, joka harjoittaa kameravalvontaa. Mikäli valvontakameroiden kuvainformaatiota ei tallenneta eikä henkilötietoja muutoinkaan kerätä valvontakameroiden avulla, henkilötietolakia ei sovelleta. Rikosvalvontakamera on käyttöolosuhteiden mukaisesti valittu still- tai videokamera. Rikosvalvonnassa tulee aina käyttää tallentavia kamerajärjestelmiä. Digitaalisuus mahdollistaa usean valvontakuvan esittämisen monitorin kuvaruudulla. Aluevalvonnassa on tärkeätä noudattaa ristivalvonnan periaatetta.

Kameroihin on saatavana valvonta-automatiikkaa lisääviä laitteita, kuten pimeänäkölaitteita, kääntömoottoreita ja erityyppisiä liikeilmaisimia. Käyttötarkoituksensa mukaan rikosvalvontakamerat jaetaan seuraavasti:

- Piilokamera.
- Kohdevalvontakamera.
- Aluevalvontakamera.

Rikosvalvontakameroiden sijoittelu

Rikosvalvontakameroiden kuvasektorit tulee kattaa kaikki keskeiset asiakaspalvelualueet. Paras tulos saavutetaan ristivalvonnalla. Ristivalvonnalla eliminoidaan normaalisti kameravalvonnan ulkopuolelle jäävät kuvakulmat. Ristivalvonnalla saadaan koko alueesta yksi tai useampia valvontakuvia. Vikaantumistilanteissa kamerat myös varmistavat toisiaan. Mikäli kameraa yritetään kääntää, vahingoittaa tai varastaa, tallentaa toinen kamera tapahtuman.

Suljetut alueet

Alueet, joihin yleisöllä ei ole vapaata pääsyä, mutta joissa esimerkiksi työskennellään jatkuvasti. Kameravalvonta on sallittua, mutta edellyttää ilmoittamista henkilökunnalle ja niiden osalta suostumusta, jotka altistuvat valvonnan kohteeksi pidempään tai toistuvasti.

Rajatut alueet

Työpisteet, joissa suoritetaan asiakaspalvelua esimerkiksi kassapisteet ja hotellin vastaanotto. Kameravalvonta edellyttää työpisteissä toimivien henkilöiden suostumusta.

Piha-alueet

Aidatulla piha-alueella kameravalvonta on sallittua, mutta edellyttää ilmoitusta. Valvonnasta ei tarvitse ilmoittaa, jos ulkopuolisilla on mahdollisuus oleskella pihalla. Jos piha-alueiden kameravalvonta aloitetaan työajan päätyttyä ja porttien sulkemisen jälkeen, ei kameravalvonnasta tarvitse ilmoittaa.

6.1.4 Toimitilojen sijoittelu

Toimitilojen sijoittelu tulee tehdä yhteistyössä kulunvalvonnan ja avainhallinnan kanssa, miettien kenen tulee päästä millekin alueelle ja milloin. Toimitilat tulee jakaa omiksi tiloiksi käyttöoikeuksien mukaan. Myös palo-osastointi tulisi huomioida siten, että jokainen toiminto olisi itsenäinen palo-osasto. Toimitilat voidaan pääsääntöisesti jakaa kolmeen tärkeysluokkaan.

- A-luokka: tilat, joissa säilytetään asiakirjoja kootusti. Luokkaan kuuluvat myös tilat, joissa säilytetään asiakkaiden omaisuutta, arkistoa, kiinteistön avaimia sekä puhelinjakamot ja serverihuone.
- B-luokka: työntekijöiden työhuoneet ja työtilat
- C-luokka: kaikkien käytössä olevat tilat

6.1.5 Vartiointi

Vartioinnin pääfunktio liittyy toimitilaturvallisuuden lieventävien kontrollien toiminnalliseen osaan. Vartioinnin turvallisuustoiminnot riippuvat kuitenkin oleellisesti vartiointipalveluiden toteuttamistavasta ja kattavuudesta, joten vartioinnin kontrollivaikutus voi sisältää tapahtumaa ehkäiseviä, ilmaisevia ja lieventäviä ominaisuuksia. Yleensä vartiointi toteutetaan piiri-, paikallis- tai hälytysvartiointina. Vartiointi voi tapahtua ympärivuorokautisesti tai ainoastaan erikseen sovittavina ajankohtina.

Porttivartioinnilla tarkoitetaan paikallisvartioinnin muotoa, jossa vartijan tehtävät sijoittuvat toimipaikan portille. Tehtäviin voi liittyä myös teknisten vartiointijärjestelmien seuranta. Vartiokierroksella tarkoitetaan vartijan toimipaikassa kulkemaa reittiä, jonka aikana hän suorittaa ennalta sovitut tarkistukset.

Piirivartioinnilla tarkoitetaan tietyllä alueella erillään sijaitsevien kohteiden vartiointia. Piirivartioinnin muotoja ovat:

- Avaamis- ja sulkemiskierros
- Tarkastuskierros
- Vartiokierros

Hälytysvalvonnassa vartija saapuu tarkistamaan kohteen, mikäli sen jokin järjestelmä antaa hälytyksen.

Vartiointitoimiala kuuluu Suomessa luvanvaraiseen elinkeinotoimintaan. Vuonna 1983 voimaan tulleen vartioimisliikelain (237/1983) yleisperustelun mukaan vartiointiliiketoiminta on poliisin toimintaa täydentävää toimintaa. Vuonna 1995 lakiin tehtiin Euroopan unionin jäsenyyden edellyttämät muutokset.

6.1.6 Kalusteet

Kalusteilla pyritään täydentämään tai korvaamaan puutteita, joita ilmenee muussa suojauksessa. Kalusteiden merkitys kasvaa pohdittaessa toimitilojen tietoturvallisuutta tiedon suojaajana sekä tiedon säilyttäjänä. Turvakaapeista käytetään yleensä nimitystä kassakaappi, vaikka moni käytössä olevista kaapeista on jokin muu kuin kassakaappi. Kassakaappiin samaistetaan myös paloturvakaappi, aikaviivekaappi ja datakaappi. Muita kalusteita ovat työpöydän lukittavat laatikostot, lukittavat pukukaapit ja erilaiset rakenteilla toteutetut holvit ja tallelokerot. Ennen kalusteiden hankintaa tulee varmistaa

mitä käyttötarkoitusta varten kalusteet hankitaan ja mitä niissä säilytetään sekä kuinka paljon säilytettävää ja suojattavaa omaisuutta on.

Kassakaappi on tarkoitettu arvo-omaisuuden suojaamiseen murtautumista vastaan ja se on murtotestattu, testauksesta on sisäpuolella valmistajan kilpi, jossa kerrotaan testausluokka. Murtosuojauksesta kertovat koodisarjat ovat SFS-murtostandardin tai EN- standardin mukaisesti testatut ja hyväksytyt kaapit (esimerkiksi EN-1143, INSTA 610, SFS 3529). Mikäli kassakaapissa aiotaan säilyttää papereita tai rahaa, tulisi sillä olla paloluokitus. Paloluokitustiedot löytyvät samasta kyltistä, paloluokitusstandardeja ovat esimerkiksi NT-Fire 017 sekä EN 1047-1. Luokitukset palonkestävyydeksi ovat 6oP (palonkestävyys 60 minuuttia), 90P(palonkestävyys 90 minuuttia), 120P(palonkestävyys 120 minuuttia). Mikäli kaapissa säilytetään sähköisiä tallenteita, muistitikkuja, ulkoisia kovalevyjä, varmuuskopioita, mg-nauhoja, diskettejä kannettavia tietokoneita, tulisi kaapissa olla dataturvaominaisuus. Dataturvaominaisuudesta löytyy kaapin sisältä luokituskyltti, jossa maininta 60 dis tai 120 dis. Tämä tarkoittaa vastaavaa minuuttiajan suojausta sähköisille tallenteille palotilanteessa.

Turvakaapit tulisi sijoittaa vyöhykemallin suojatuimpaan tilaan ja niihin voidaan liittää hälytysjärjestelmän ilmaisimia. Hankittaessa tai siirrettäessä kaappia tulee huomioida rakenteiden kantavuus. Kaappi tulee aina kiinnittää tukevasti rakenteisiin siten, että sitä ei saa irti rakenteista ilman kaapin avaamista. Turvakaapin avainta tai numeroyhdistelmää ei saa säilyttää koskaan samassa tilassa turvakaapin kanssa.

7. YHTEENVETO

Tietoturvan kannalta yrityksissä ja rakennushankkeissa olennaista on, että mahdolliset riskit on kartoitettu ja niiden vakavuusaste tiedostettu. Suojausten; niin lukituksen, kulunvalvonnan kuin tietoturvankin osalta on oltava riittäviä ja päivitykset pidettävä jatkuvasti ajan tasalla. Tietoturvakonsultin käyttö on suotavaa.

Tietoturvallisuus ei ole kertainvestointi vaan jatkuvasti seurattava ja kehitettävä prosessi. Ensiarvoisen tärkeää on henkilökunnan ja johdon sitouttaminen tietoturvan vaalimiseen ja kehittämiseen. Koska jokainen yritys on omannäköisensä, on tietoturva-asiat räätälöitävä jokaiselle yritykselle erikseen.

Varmuuskopioinnista huolehdittava tarvittavan usein ja niiden uudelleenluettavuus on myös varmistettava. Yrityksessä on oltava tietoturva-asiat hallitseva avainhenkilö ja tällä varamies huolehtimassa tietoturvajärjestelmän ylläpidosta.

LÄHTEET JA KIRJALLISUUS

Finanssialan Keskusliitto (2005): Rakenteellinen murtosuojeluohje 1, 2 ja 3.

Heljaste J; Korkiamäki, J; Laukkala, J-M; Mustonen,J; Peltonen,J; Vesterinen P (2008): Yrityksen Turvallisuusopas. Helsingin seudun kauppakamari / Helsingin Kamari Oy

Elinkeinoelämän keskusliitto; Sisäasiainministeriö; Puolustusministeriö (KATAKRI 2009): Kansallinen turvallisuusauditointikriteeristö

Kortelainen, J (2010): Tietoturvasuunnitelmatyökalu. Opinnäytetyö; Tietoverkkotekniikka. Jyväskylän Ammattikorkeakoulu.

RT 10-10764 (2001): Pääsuunnittelun tehtäväluettelo PS 01; Tehtävät 1.5
RT 10-10992 (2010); Tietomallinnettava rakennushanke. Ohjeita rakennuttajalle

SecMeter (2008): Suomalainen yritysturvallisuudesta kertova tietopalvelu www.secmeter.com.

LIITTEET

LIITE 1

HAKEMUS Arkistonumero ▪ _____

SUPPEA TURVALLISUUSSELVITYS

Laki turvallisuusselvityksistä (177/2002)

Selvityksen hakijan tiedot:

▪ Hakija	▪ Yritys- ja yhteisötunnus
Yhteystiedot, yhteyshenkilö, puhelinnumero	

Selvitys turvallisuus- ja ennalta estävistä toimenpiteistä liitteenä
x Aiemmin toimitetun selvityksen numero _____ (numero/vuosi)

Tehtävään liittyvät tiedot:

Tehtävänimike	Osasto tai yksikkö	
Suojattava etu		☐ Liite
Tarkka tehtäväkuvaus (mitä tekee, missä tekee)		☐ Liite
Arkaluontoisen tilan tai paikan kuvaus		☐ Liite

Selvityksen kohteena olevan henkilön tiedot:

▪ Sukunimi	▪ Etunimet
▪ Henkilötunnus tai syntymäaika (ppkkvv) ☐ Nainen ☐ Mies	Syntymäkotikunta
Osoite	Postinumero ja –toimipaikka
Kansalaisuus	Ammatti

☐ Ansioluettelo liitteenä ☐ Ulkomaalaisen henkilön passin tietosivu liitteenä

TIEDOKSIANNOT JA SUOSTUMUS

Minulle on selvitetty seuraavat asiat (kohteena oleva henkilö täyttää):

☐ Turvallisuusselvitys ei sido selvityksen hakijaa;
☐ Turvallisuusselvityksen tarkoitus ja että sitä käytetään vain kyseistä tehtävää varten;
☐ Minulla on oikeus tietää, onko minusta tehty turvallisuusselvitys kyseistä tehtävää varten;
☐ Minulla on oikeus saada kihlakunnan poliisilta turvallisuusselvitykseni sisältämät tiedot;
☐ Hakijan säilyttämis-, salassapito- ja vaitiolovelvollisuus.

Vakuutan, että antamani tiedot ovat oikeita.
Suostun siihen, että minusta tehdään suppea turvallisuusselvitys.
(Laki turvallisuusselvityksistä (177/2002) 4. luku)

Paikka ja päiväys	Allekirjoitus

Poliisilaitoksen merkinnät:

▪ Poliisilaitoksen koodi	Atk-rekisterit ☐ Ei merkintöjä ☐ Merkintöjä, tuloste liitteenä	Käsittelijä	Pvm
Selvityksen tulos ☐ Ei merkityksellistä tietoa ☐ Merkityksellistä tietoa	▪ Muistion nro	Laatija	Pvm
Ilmoitettu hakijalle ☐ Puhelimitse ☐ Kirjeitse saantitodistuksella yhteyshenkilölle		Ilmoittaja	▪ Pvm
Maksuperustelain (150/1992) mukainen maksu	Selvityksen rekisteröinti	▪ Syöttäjän P-tunnus	▪ Pvm

Poliisilomake Poliisin arkisto, säilytysaika 10 vuotta

LIITE 2

LUOTTAMUKSELLISUUSSITOUMUS

_____ (jäljempänä "Yhtiö"), jonka osoite on

_____, ja Y-tunnus _____,

sekä Oyj, jonka osoite on

, ja ,

ryhtyvät neuvotteluihin tarkoituksenaan selvittää mahdollisuudet yhteistyöhön, joka

koskee

_____

_____ _____ tai

ovat jo ryhtyneet mainittuun yhteistyöhön (jäljempänä ”Yhteistyö”).

Yhteistyön ehdot määritellään erillisissä Oyj:n tilausasiakirjoissa, Yhteistyöstä

erikseen solmittavassa sopimuksessa tai erillisessä toimeksiannossa (jäljempänä

"Toimeksianto"), eikä tämä sitoumus tai Tietojen luovuttaminen tai vastaanottaminen

velvoita Oyj:tä tai Yhtiötä ryhtymään Toimeksiantoon.

Neuvottelujen, Yhteistyön tai Toimeksiannon yhteydessä Oyj mahdollisesti luovuttaa

Yhtiölle luottamuksellisia, esimerkiksi kaupallisia, teknisiä, turvallisuuteen tai laitos- tai

muihin järjestelmiin liittyviä tietoja, jotka eivät saa tulla muiden tietoon, tai Yhtiö

saa niitä muutoin tietoonsa suorittaessaan Toimeksiannon mukaista tehtäväänsä.

Tämän vuoksi Yhtiö on tänään sitoutunut seuraavaan:

1.

"Tiedoilla" tässä sitoumuksessa tarkoitetaan kaikkia Oyj:n tai sen

yhteistyökumppaneiden toimintaan liittyviä tai vaikuttavia, esimerkiksi kaupallisia,

teknisiä, turvallisuuteen tai laitos- tai muihin järjestelmiin liittyviä seikkoja, (mukaan

lukien esimerkiksi ATK-tiedostot, salasanat ja ATK-järjestelmän yksityiskohdat), jotka

ovat luottamuksellisia riippumatta siitä, millä tavoin tai missä muodossa tiedot Yhtiölle

ilmaistaan tai miten Yhtiö muuten saa ne tietoonsa tai siitä, onko tiedon luovuttamisen

yhteydessä erityisesti ilmaistu tai osoitettu tiedon olevan luottamuksellista.

2.

Yhtiö sitoutuu olemaan ilmaisematta ja luovuttamatta Tietoja kolmansille osapuolille

(mukaan lukien sen emo-, tytär- ja sisaryhtiöt) ja noudattamaan tarpeellista

huolellisuutta Tietojen luottamuksellisuuden säilyttämiseksi.

Yhtiö sitoutuu käyttämää Yhteistyön ja Toimeksiannon toteuttamisessa vain Yhtiön

omaa henkilökuntaa.

3.

Oyj pidättää kaikki oikeudet luovuttamiinsa Tietoihin sekä Yhteistyön tai

Toimeksiannon tuloksena syntyvään materiaaliin, raportteihin ja tiedostoihin

(jäljempänä "Tulosaineisto"), eikä Yhtiöllä ole oikeutta Tietojen tai Tulosaineiston

hyödyntämiseen muuhun kuin vain ja ainoastaan Yhteistyön toteuttamiseen

Toimeksiannon mukaisesti. Yhtiöllä ei siten ole oikeutta myöskään hyödyntää Tietoa

eikä Tulosaineistoa muussa toiminnassaan.

Tiedon luovuttaminen Yhtiölle ei tarkoita, että Yhtiölle samalla tai muutoin

myönnettäisiin mitään lisenssiä tai Oyj:n tai kolmannen omistamaa muuta

immateriaalioikeutta.

4.

Yhtiöllä on oikeus antaa Tietoja henkilökuntaansa kuuluvien käyttöön vain siinä

laajuudessa, kuin se Oyj:n ja Yhtiön kesken sovittujen tehtävien suorittamiseksi on

tarpeen. Yhtiö sitoutuu tiedottamaan Tietoja vastaanottaville henkilökunnan jäsenille

tästä sitoumuksesta heille ja Yhtiölle aiheutuvista velvoitteista.

Yhtiö sitoutuu ilmoittamaan kirjallisesti Oy:lle niiden henkilökuntaansa kuuluvien

henkilöiden nimet ja henkilötiedot, joille se aikoo ilmaista kokonaan tai osittain tässä

sitoumuksessa tarkoitettuja Tietoja.

Edellä tarkoitettujen henkilöiden tulee

- allekirjoittaa **liitteenä** oleva henkilökohtainen salassapitositoumus
- allekirjoittaa suostumus suppean turvallisuusselvityksen tekemiseen käyttäen

  tarkoitusta varten vahvistettua Oyj:n esitäyttämää lomaketta
- sitoutua noudattamaan Oyj:n kulloinkin voimassa olevia turvallisuus- ja muita

  ohjeita ja määräyksiä työskennellessään Oyj:n tiloissa tai alueella.

Oyj:llä on oikeus kieltää Tietojen ilmaiseminen jollekin tai joillekin Yhtiön

palveluksessa olevalle henkilölle tarvitsematta perustella kieltoa.

5.

Luottamuksellisuusvelvoite ei koske Tietoja,

a: jotka ovat olleet yleisesti tiedossa ennen neuvottelujen alkua tai tulevat

myöhemmin tietoon muutoin kuin Yhtiön tai sen henkilökunnan

huolimattomuuden tai laiminlyönnin vuoksi;

b: joiden Yhtiö voi osoittaa olleen sen hallussa ennen Tietojen saamista Oyj:ltä;

c: jotka on saatu kolmansilta osapuolilta ja joiden ilmaisemiseen näillä on ollut

oikeus eikä kolmas osapuoli ole saanut tietoja välittömästi tai välillisesti Oyj:ltä;

d: joiden ilmaisemiseen Yhtiö on saanut Oyj:n kirjallisen suostumuksen.

Tässä kohdassa 5 tarkoitettuja Tietoja eivät ole yksittäiset Tiedot pelkästään sillä perusteella, että ne sisältyvät johonkin yleisluontoisempaan tietoon, joka on yleisesti tiedossa tai Yhtiön hallussa, eivätkä tiettyä kokonaisuutta kuvaavat tiedot pelkästään sillä perusteella, että jotkin osat tästä kokonaisuudesta ovat yleisesti tiedossa tai Yhtiön hallussa.

6.

Tämän luottamuksellisuussitoumuksen mukaiset velvoitteet ovat voimassa kunnes Oyj

kirjallisesti ilmoittaa Yhtiölle luottamuksellisuusvelvoitteen lakkaamisesta. Tällöinkin

luottamuksellisuusvelvoitteen lakkaaminen koskee vain Oyj:n sanotun ilmoituksen

jälkeen antamia tietoja.

7.

Yhtiö sitoutuu palauttamaan saamansa Tiedon ja Tulosaineiston kunkin projektin,

Toimeksiannon tai Yhteistyön päätyttyä tai Oyj:n pyynnöstä muulloinkin sekä

vahvistamaan kirjallisesti, että kaikki aineisto on palautettu. Palautusvelvollisuus

sisältää mm. dokumentit, ohjelmat, disketit ja muut sähköiset alustat, sekä kaikki niistä

mahdollisesti otetut kopiot.

8.

Yhtiö toteaa ymmärtävänsä olevansa vahingonkorvausvelvollinen Oyj:lle, mikäli

Yhtiö rikkoo tätä sitoumusta.

_____

(aika ja paikka)

_____

(yhtiö)

_____

(allekirjoitus)

_____

(nimen selvennys)

_____

(aika ja paikka)

_____

(yhtiö)

_____

(allekirjoitus)

_____

(nimen selvennys)

LIITE LUOTTAMUKSELLISUUSSITOUMUKSEEN

Me allekirjoittaneet _____:n (jäljempänä "Yhtiö")

henkilökuntaan kuuluvat henkilöt olemme tutustuneet Yhtiön

Oyj:lle antamaan luottamuksellisuussitoumukseen, ja sitoudumme

noudattamaan sen ehtoja.

Sitoudumme noudattamaan Oyj:n kulloinkin voimassa olevia turvallisuus- ja muita

ohjeita ja määräyksiä työskennellessämme Oyj:n tiloissa tai alueella.

Suostumme siihen, että Yhtiö saa luovuttaa Oyj:n luottamukselliseen käyttöön

työsuhdettamme ja meitä koskevia tietoja.

Lisäksi annamme kukin erikseen suostumuksen suppean turvallisuusselvityksen

tekemiseen (Laki turvallisuusselvityksistä 177/2002) käyttäen tarkoitusta varten

vahvistettua, Oyj:n esitäyttämää lomaketta.

Paikka ja aika:

_____

Nimi	Henkilötunnus	Allekirjoitus
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____