YRITYKSEN FYYSINEN TIETOTURVA

LAHDEN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma
Yritysviestintäjärjestelmät
Yrityksen fyysinen tietoturva
Kevät 2007
Juha Vedenoja

Lahden ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

VEDENOJA, JUHA: Yrityksen fyysinen tietoturva

Yritysviestintäjärjestelmien opinnäytetyö, 31 sivua

Kevät 2007

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli selvittää millainen on hyvä yrityksen fyysinen tietoturva, ja mistä eri elementeistä se koostuu. Tietoturvan toinen puoli, eli virustorjunta ynnä rajataan työstä pois. Fyysinen turvallisuus koostuu ulkopuolisista uhkista, kuten tulesta ja pölystä, sekä laitteiston kunnosta. Myös työntekijöiden ja vierailijoiden aiheuttamat uhkat ovat osa fyysisen tietoturvan suunnittelua. Teoreettisessa osuudessa perehdytään erilaisiin ongelmiin ja haasteisiin, mitä fyysinen tietoturva voi aiheuttaa, ja SIIHEN , miten niitä voidaan välttää. Yksinkertaisilla asioilla ja maalaisjärjen käytöllä päästään pitkälle, mutta lopulta on hyvä kysyä apua alan ammattilaisilta.

Opinnäytetyön case - osuudessa mielikuvitusyritykselle luodaan mahdollisimman täydellinen ja turvallinen ympäristö fyysisen tietoturvan kannalta, käyttäen tässä opinnäytetyössä esiteltyjä teorioita ja faktoja. Suurin panostus tapahtuu arkaluontoisen tiedon suojaamiseen ja siihen suoraan liittyviin fyysiseen ongelmiin ja niiden ratkaisuihin.

Fyysinen tietoturva on vaikeasti rajattava kokonaisuus, mutta sitäkin mielenkiintoisempi ja vähän käsitelty aihe, jota ei missään nimessä pitäisi väheksyä nykyajan tietoyhteiskunnassa.

Avainsanat: fyysinen, tietoturva, tietosuoja

Lahti University of Applied Sciences
Faculty of Business Studies

VEDENOJA, JUHA: The Physical Environment of Data Security In a Company

Bachelor's Thesis in Business Information Systems, 31 pages

Spring 2007

ABSTRACT

This bachelor's thesis deals with the physical environment of data security in a small or medium-sized company. This thesis is all about the physical side, so the virus-protection side of data security is left undiscussed. Physical data security consists of outside threats such as fire and dust and the physical condition of the computer parts and storage devices. The security threats caused by people working and visiting the premises are also included in the planning of a data security scheme of a company. The thesis discusses what elements are needed and what solution could cover all the previously mentioned risks. The theory part mainly deals with different kinds of problems that physical data security can cause and how one can avoid them. Keeping things simple may carry the company far, but in the end, advice from specialists is much appreciated.

The empirical part of this thesis is set up to find a nearly perfect and ideal physical data security solution for a made-up company. The study uses theories and facts presented in this thesis. The most crucial point is the protection of highly sensitive information and the physical problems concerning it.

Physical data security is a vast and elusive subject. But on the other hand, it is very interesting to study and not so well-known yet. The importance of physical data security should not be underestimated in our modern information society.

Keywords: physical, data security, information security

SISÄLLYS

1 JOHDANTO

Tietoturva voidaan jakaa armottomasti kahteen osa-alueeseen; fyysiseen ja ohjelmalliseen. Jälkimmäinen on kaikille tuttua virustorjuntaa**,** ja tiedostojen salasanalla suojaamista. Tämä opinnäyte työ käsittelee kuitenkin harvemmin puheeksi otettua fyysistä tietoturvaa. Tällä tarkoitetaan henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaamista tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan**,** sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden. Tämä koostuu pääasiallisesti yrityksen fyysisestä ympäristöstä ja sen aiheuttamista vaaratilanteista tietoturvaan. Keskeisimpiä elementtejä fyysisessä tietoturvassa ovat ulkopuolisiin ja kolmannen osapuolen aiheuttamiin uhkiin varautuminen**,** ennen kuin tuho on jo tapahtunut. Hyvä suunnittelu on kaiken takana.

Tämän työn case - osuudessa rakennetaan mahdollisimman tarkka, mutta silti käytännöllisesti järkevä tietoturvaratkaisu yritykselle. Olen itse ollut toteuttamassa vastaavia projekteja yrityksille, mutta tietoturvan kannalta nimet ja viittaukset oikeisiin yrityksiin on jätetty mainitsematta. Tämän kyseisen esimerkkiyrityksen fyysiset tietoturvaratkaisut rakennetaan täysin tyhjästä, käyttäen tässä työssä esiteltyjä menetelmiä, ja ottaen huomioon esille tuodut ongelmakohdat niin ulkopuolisten tekijöiden, kuten vesivahinkojen osalta, kuin myös henkilötasolla tapahtuvien riskien kannalta. Esimerkiksi huonosti työhön soveltuvien ihmisten välttämisellä. Työn tavoitteena on antaa kattava yleiskuvaus fyysisen tietoturvan tärkeydestä yrityksissä, jota ikävä kyllä vähätellään niin sanotun normaalin tietoturvan kustannuksella. Panostus esimerkiksi virustorjuntaan on aivan kohtuuttoman suuri**,** verrattuna fyysisten laitteiden

kunnossapitoon ja huolehtimiseen. Tutkimusongelmana tässä työssä on**,** miten fyysinen tietoturva tulisi toteuttaa, jotta se olisi mahdollisimman turvallinen.

2 OHJEISTUS JA STANDARDIT

Suomessa ei ole olemassa erityistä tietoturvaa koskevaa erillislakia, jossa olisi tyhjentävästi säädelty yhteisöjen ja yksittäisten tietokoneenkäyttäjien tietoturvavelvoitteita tai – oikeuksia. (Laaksonen, Nevasalo & Tomula 2006, 21.)

Julkisuudessa on usein ollut keskustelua sellaisen säätämisestä, mutta ainakin tähän asti on todettu sellaisen olevan tarpeeton. Lisäksi yrityksille on tehty kyselyjä, joissa on kartoitettu tarvetta säätää erillinen tietoturvalaki. Vastaanotto yritysten ja lainsäätäjien piirissä on ollut vaisua, ja kohtuullisen yhtenäisenä kantana on ollut, että lisää lainsäädäntöjä ei tarvita.

Yritykset haluavat enemmänkin ohjeistusta**,** sekä selviä kannanottoja viranomaisilta siitä, mitä tulisi tai saisi tehdä, jotta tietoturvan ylläpitämistä ja parantamista koskevat toimenpiteet olisivat lainmukaisia ja parhaiten palvelisivat osapuolten eri intressejä.

Suurimmat ongelmat yrityksissä on koettu siinä, että tekniikka kehittyy valtavalla vauhdilla kiihdyttäen osaltaan kilpailua markkinoilla ja mahdollistaen samalla aivan uuden tavan käsitellä tietoa ja informaatiota yhteisössä. (Laaksonen ym. 2006, 22.)

Samaan aikaan on kuitenkin säädetty uusia yksilön yksityisyyden suojaa koskevia lakeja, jotka toisessa päässä ovat rajaamassa käytettävissä olevia teknisiä keinoja tietojärjestelmien tehokkaaseen hyödyntämiseen.

Kansain välinen standardi ISO 27001 määrittelee tietoturvallisuuden hallintajärjestelmien vaatimukset ja toimii siten tietoturvallisuuden hallintajärjestelmien perusteena. Lisäksi Suomessa on käytössä valtionvarainministeriön kokoama valtionhallinnon tietoturva ohjeistus VAHTI, joka koostuu erilaisista ratkaisuista tietoturvariskeihin. (Laaksonen ym. 2006, 125)

3 FYYSINEN YMPÄRISTÖ

Fyysinen turvallisuus sisältää organisaation tuotanto- ja toimitilojen fyysiseen suojaamiseen liittyvät asiat, joilla pyritään estämään organisaation tarvitsemien tietojen tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin.

Fyysisellä turvallisuudella taataan organisaatiolle häiriötön ja turvallinen toimintaympäristö. Jokainen organisaatio tarvitsee fyysiset tilat toimintansa harjoittamiseen. Toimitilojen suojaaminen luo perustan kaikille muille suojaustoimille, joita tietoturvallisuuden ylläpitämiseen käytetään. Ilman turvallista toimintaympäristöä ei tiedon luotettavuutta voida aukottomasti varmistaa. Tietojenkäsittelyn fyysisen turvallisuuden suunnitteluun tarvitaan usein koko toimintaympäristön kattavaa turvallisuustarpeiden- ja ratkaisujen arviointia.

Kaikki organisaation tilat eivät ole fyysisen turvallisuuden kannalta samanarvoisia. Yleensä korkeaa suojausta vaativia kohteita ovat organisaation omaan vahvuusalueisiin liittyvät tilat, esimerkiksi tuotekehitystilat, atk-laitetilat sekä hallinnolliset tilat. Yleensä ottaen fyysisen turvallisuuden piiriin kuuluvat kaikki tilat, joissa käsitellään organisaation toiminnalle merkityksellistä tietoa.

Fyysinen toimintaympäristö tulisi arvioida säännöllisesti riskikartoitusten yhteydessä. Korjaus- ja kehitysehdotukset tulee kirjata ylös ja toteuttaa yleisten rakennus- ja korjaushankkeiden yhteydessä mahdollisimman nopeasti.

Toimitilojen tärkeysluokitus on hyvä apuväline tilojen suojaustarpeita suunniteltaessa. Luokituksen avulla tunnistetaan tilojen merkitys tietoturvan

kannalta. Mikäli luokitus ei ole käytössä, vaarana ovat virhearvioinnit ja resurssien hukkaaminen, sillä osa tiloista saatetaan turvata tarpeettoman hyvin ja osa puolestaan liian heikosti.

3.1 Tilojen suojaus

Fyysisen turvallisuuden asianmukainen järjestäminen on periaatteessa helppoa ja siihen on saatavissa lisäohjeita monilta tahoilta. Esimerkiksi tietojenkäsittelytilojen suojaamiseen on laadittu useita erilaisia tarkistuslistoja. (Laaksonen ym. 2006, 125.)

ISO 27001 –standardi sisältää omat vaatimuksensa, ja esimerkiksi Suomen puolustusvoimat määrittelee turvalliset tilat hyvinkin tarkasti. Samoin VAHTI –ohjeissa**,** sekä Viestintäviraston ja Rahoitustarkastuksen dokumenteissa**,** otetaan kantaa tilojen suojaukseen.

Toimitilat tulisi suojata ainakin seuraavilta asioilta:

- varkaus
- tulipalo ja lämpötilan liiallinen kohoaminen (kesällä)
- vesi ja kosteus
- sähköhäiriöt
- pöly

(Laaksonen ym. 2006, 126.)

Kannettavien tietokoneiden varkaudet ovat kasvava ongelma. ATK-laitteisiin kohdistuneet varkaudet eivät nykyään koske pelkästään itse laitetta**,** vaan myös sen muistissa olevaa dataa ja tietoa. Varkaudet tapahtuvat yleensä keskellä päivää hälytysjärjestelmien ollessa pois päältä.

3.2 Laitetilojen fyysiset uhkat

Tietoturvan kannalta tulisi pohtia, onko pääsy laitetilaan valvottua sekä varsinaisena työaikana, että toimitilojen ollessa suljetut. Laitetilaan tulisi asentaa hälytyksen siirrolla varustettu valvontalaitteisto, jolla seurataan liikkumista kyseisessä tilassa. Nykytekniikalla on helppo seurata milloin mikäkin ovi on rakennuksessa avattu**,** ja kuka sen on avannut. Näin mahdolliset väärinkäytökset saadaan kitkettyä minimiin tehokkaasti.

Tulipalon voivat aiheuttaa hyvinkin erilaiset syyt, joten organisaation on syytä varautua sekä tulipaloon että lämpötilan nousuun laitetiloissa. Laitetilaa suunniteltaessa on otettava huomioon tilan eristäminen muista tiloista paloturvallisesti. Tilaan ei saa päästä savua, joka voi vahingoittaa tallennusmediaa tai tallennuslaitteita. Lämpötilojen kohoamista tulee valvoa antureilla, jotka hälyttävät ennen kriittisen lämpötilan ylittymistä (esimerkiksi kiintolevyissä noin 80 astetta). Toisaalta laitetilassa on oltava tehokas ilmastointi, jolla tilan lämpö saadaan pysymään sopivien raja-arvojen sisällä. Ilmastoinnin suhteen tulee varmistua myös siitä, että kapasiteetti riittää myös mahdollisiin tuleviin laitteistoinvestointeihin.

Vesivahinko on tulipalon osalla toinen varsin yleinen organisaatioiden kohtaama vahinko. Laitetilojen suhteen on syytä varmistua siitä, että laitetilassa ei ole vesiputkia, jotka voivat aiheuttaa vuodon, joko itse tilassa**,** tai sen yläpuolella. Esimerkiksi isoissa palvelintiloissa on välipohja, joka suojaa mahdollisilta vesivahingoilta. (Laaksonen ym. 2006, 127.)

Pölyn muodostuminen voidaan estää säännöllisellä siivouksella ja laitetilan käytön rajoittamisella. Tilaa ei tule käyttää muussa toiminnassa, esimerkiksi varastona tai työskentelytilana. Laitteet tulee nostaa pois lattiatasosta, jotta pöly ei pääse kerääntymään laitteistojen sisälle. Tämä auttaa myös mahdollisissa vesivahinkotilanteissa. (Laaksonen ym. 2006, 127.)

Sähköhäiriö voi aiheuttaa käyttökatkoksia**,** ja jopa laiterikkoja. Laitteistot tulee suojata ylijännitesuojilla virtapiikeiltä, joita voi aiheutua muun muassa ukkosesta. Varsinaisiin sähkökatkoihin voidaan varautua UPS - laitteilla**,** jotka suojaavat myös virtapiikeiltä, ja isoissa organisaatioissa jopa varavirtageneraattoreilla. Näiden laitteiden toimivuus tulee testata säännöllisesti**.** (Laaksonen ym. 2006, 127.)

Lisäksi ongelmia saattavat aiheuttaa hyönteiset ja pienet jyrsijät. Tietojenkäsittelyssä usein käytettävä slangisana bugi onkin alun perin tarkoittanut englanninkielistä sanaa bug, hyönteinen. Suurten koneiden aikana muun muassa muurahaiset aiheuttivat suurimman osan laiteongelmista. Vielä nykyaikanakin hyvin ilmastoidussa tilassa hyönteiset hakeutuvat koneen sisuksiin lämmittelemään**,** ja näin aiheuttavat toimintahäiriöitä. Hyönteisiä suuremman riskin aiheuttavat pienjyrsijät**,** kuten hiiret ja rotat. Ne ovat erittäin kiinnostuneita tele- ja verkkokaapeleissa notkistusaineena käytettävästä rasvasta. Laitetilat tuleekin suojata erittäin huolellisesti kyseisiä otuksia vastaan. (Hakala, Vainio & Vuorinen 2006, 306.)

3.3 Valvontajärjestelmät

3.3.1 Kamerat

Tietokoneeseen liitettävät ip-kamerat ovat helppo ja halpa tapa pienen yrittäjän tilojen suojaukseen. Malleja on sekä langallisia (ethernet, bnc) että langattomia (wlan). Kamerat voidaan asentaa myös ulos (säänkestävyys) sekä myös kosteisiin tai muihin hankaliin oloihin. Säänkestävät kamerat vaativat yleensä oman erillisen, lisävarusteena saatavan kotelon ympärilleen. Kotelo estää muunmuassa kosteuden pääsyn herkkään kameraan ja tuulettaa kameraa kesähelteillä. Kamera tallentaa digitaalista kuvaa esimerkiksi suoraan yrityksen palvelimelle. Kuvamateriaali on siis helposti saatavissa ja nopeasti kelattavissa haluttuun kohtaan.

3.3.2 Kulunvalvonta

Edellä mainitun laitteistotilan yhteyteen tulisi ehdottomasti asentaa kulunvalvontajärjestelmä. Digitaalinen kirjautumistunnus**,** jolla pääsee ovesta, tai esimerkiksi sensori**,** joka rekisteröi jokaisen oven avauksen. Todella tiukan turvallisuuden omaaviin paikkoihin voidaan asentaa myös sormenjälkitunnistimia. (Laaksonen ym. 2006, 139-160.)

3.3.3 Hälytysjärjestelmä

Kun edellä mainitut laitteet yhdistetään, saadaan aikaiseksi varsin toimiva hälytysjärjestelmä, jonka voi ohjelmoida soittamaan esimerkiksi vartiointiliikkeelle. Hälytysjärjestelmän laajuus ja tehokkuus ovat yrityksen tai organisaation itse omassa turvallisuusstrategiassaan määrittelemiä.

3.4 Henkilöturvallisuus

Henkilöturvallisuus on yksi tärkeimmistä tietoturvallisuuden osa-alueista. Sillä tarkoitetaan henkilöstön toimista aiheutuvien ja heihin kohdistuvien tietoturvauhkien hallintaa. Tietojenkäsittely tulee suojata henkilöstön aiheuttamilta väärinkäytöksiltä ja virheiltä, jotta yrityksen toiminnalle ei aiheudu haittaa. (Miettinen 2002, 103-104.)

Tietoturvariskejä henkilöturvallisuuden osalta aiheuttavat muun muassa muutokset yhteiskunnassa, organisaation kilpailutilanteen kiristyminen sekä tietojenkäsittelyn osallistuvan henkilökunnan suuri määrä yrityksen sisällä ja sen ulkopuolella. Työntekijän on sovelluttava tehtävään, jotta organisaatio voi varmistua tietojenkäsittelyn turvallisuudesta.

Yrityksen on syytä laatia tietoturvaohjelma, jonka noudattamisesta tulee mainita esimerkiksi työsopimuksessa. Tällä tarkoitetaan niitä toimenpiteitä, joilla määrätään noudatettavia tietoturvallisuuteen liittyviä periaatteita ja toimintalinjoja

yleensä, sekä tietoturvallisuuden organisointia. Tietoturvaohjelman tavoitteena on suojata tiedon luottamuksellisuus, eheys ja käytettävyys. (Laaksonen ym. 2006, 128.)

3.4.1 Vaaralliset yhdistelmät

Työtehtävien kannalta oleellisia asioita ovat tehtävien eriyttäminen siten, että toimenkuvat ovat selkeitä**,** ja vastuut on rajattu esimerkiksi niin, että vaarallisia työyhdistelmiä ei pääse syntymään.

Vaarallisia yhdistelmiä ovat muun muassa tilauksen tekeminen, vastaanottaminen ja hyväksyminen**,** tai muutoksen suunnittelu, testaaminen ja tuotantoon siirto. (Laaksonen ym. 2006, 138.)

3.4.2 Rekrytointi ja palkkaaminen

Kauppakamarin vuonna 2005 tekemän tutkimuksen mukaan taustatarkastusten tekeminen ei ole yleistä minkään kokoisissa yrityksissä. Kaikista suomalaisyrityksistä hieman yli kolmannes tekee taustaselvityksiä rekrytointitilanteissa. Tästä huolimatta taustatarkastusten tekeminen koetaan hyödylliseksi, sillä väärän henkilön palkkaamisesta voi aiheutua suuriakin tietoturvauhkia muun muassa varkauksien ja sabotaasin muodossa. Joka tapauksessa väärän henkilön palkkaamisesta aiheutuu yritykselle merkittäviä kuluja ja vaivaa, vaikka työntekijä ei syyllistyisikään mihinkään rikolliseen toimintaan. (Miettinen 2002, 103-104.)

3.4.3 Taustatarkistukset

Taustatarkistusten tekemiseen on nykyään monia eri keinoja. Suosituimpana ja nopeimpana lienee internetin käyttö. Hakukoneet löytävät yllättävän paljon tietoa ihmisistä ja heidän eri elämänvaiheistaan. Internetistä saatuihin tietoihin on kuitenkin suhtauduttava kriittisesti ja esimerkiksi tarkistettava ne ansioluettelossa mainituilta yrityksiltä ja suosittelijoilta. (Miettinen 2002, 106-107.)

Maksullisia taustaselvityspalveluja on luottotietojen ja rikostaustan selvittäminen. Mikäli työnantaja haluaa, se voi teettää suojelupoliisilla turvallisuusselvityksen. Selvitys on mahdollista tehdä vain sellaisten työtehtävien osalta, johon liittyy esimerkiksi erityisen arvokkaita liike- ja ammattisalaisuuksia tai muuta tähän rinnastettavaa yksityistä omaisuutta. (Miettinen 2002, 104.)

Selvityksiä on kolmea eri laajuutta**,** joista suppea sopii tavallisen yrityksen tarpeisiin. Tämän selvityksen tarkoituksena on selvittää, voiko kyseiselle henkilölle myöntää oikeuden luottamuksellisen tiedon käsittelyyn ja pääsyn tietojenkäsittelytiloihin. Tällaisia tiloja tai tietoja ovat sellaiset kohteet, joilla on huomattavaa merkitystä valtion turvallisuudelle tai julkiselle taloudelle. Eli kioskin kesämyyjästä selvityspyyntöä on turha tehdä. (Miettinen 2002, 104-107.)

3.4.4 Sopimukset

Työsopimus tulee laatia kirjallisena ja siihen tulee kirjata vähintään työnantajan ja työntekijän tiedot, työsopimuksen laatu, lyhyt kuvaus työstä sekä henkilön palkanmaksun perusteet. Muilta osilta voidaan viitata lakiin ja työehtosopimuksiin. (Miettinen 2002, 108-109.) Edellisillä on hyvä turvata yrityksen immateriaaliset oikeudet, kuten ohjelmistojen lähdekoodi.

Tietoturvan kannalta on oleellista kirjata ylös, mitä henkilö tulee organisaatiossa tekemään, kuka on hänen esimiehensä ja kenellä on vastuu muun muassa henkilön koulutuksesta ja perehdyttämisestä. Näitä asioita ei tarvitse kirjata itse sopimukseen, mutta ne on hyvä käydä läpi työsopimuksen allekirjoittamisen yhteydessä.

Salaiset tiedot eivät saa paljastua asiattomalle tai muutoin sitoutumattomalle taholle. Lupa tietojenkäsittelyyn annetaan vasta mahdollisen salassapitosopimuksen allekirjoittamisen jälkeen. Sen tarkoituksena on suojata organisaation kannalta kriittistä tietoa siten, että luottamuksellinen materiaali ei kulkeudu väärille ihmisille. Sopimus voi olla voimassa myös työsuhteen päätyttyä tietyn aikaa. Salassapitosopimus ei ole tehokas ilman merkittäviä sopimuksessa määriteltyjä seuraamuksia rikkomistilanteissa. Seuraus on tavallisesti rahamääräinen vahingonkorvaus. (Laaksonen ym. 2006, 142.)

Kun työsuhde mahdollisesti päättyy, on hyvä olla olemassa niin sanottu vaitiolosopimus. Näin työntekijä ei saa kertoa muille kilpailijoille yrityksen toiminnasta.

4 TIETOJEN SÄILYTYS

Käyttäjien ja yritysten muisti on siirtymässä yhä enemmän tietotekniikan varaan; puhelinnumerot on tallennettu kännykkään, hoidettavat asiat ja tapaamiset sähköiseen kalenteriin ja kirjeenvaihto löytyy sähköpostista. Jos laitteet varastetaan tai tallennusmedia hajoaa, jää käyttäjä täysin tyhjän päälle.

4.1 Kiintolevyt

Tietokoneella työstettävä data tallennetaan kiintolevylle. Levyjen kapasiteetti on kasvanut 1990-luvun sadoista megatavuista satoihin gigatavuihin hinnan pysyessä samana. Käyttäjää kehitys tietysti ilahduttaa.

Muhkealla kapasiteetillä on kuitenkin varjopuolensa (Järvinen 2006, 324). Kun tilaa on paljon, tietoa ei tarvitse enää poistaa kiintolevyä siivoamalla. Ylenpalttinen kapasiteetti ei pakota kurinalaisuuteen eikä järjestelmällisyyteen. Se kostautuu, kun tiedostoja pitäisi löytää tai luottamuksellisia tietoja tuhota. (Järvinen 2006, 324.)

Levyjen tekninen kestävyys on vuosien saatossa heikentynyt. Syynä tähän ovat pakkaustiheyden valtava kasvu ja vallitseva hintakilpailu. Nykyiset kiintolevyt on mitoitettu kestämään niiden takuuaika. (Järvinen 2006, 324.)

Kiintolevyjen kestävyyttä mitataan MTBF ja Service Life arvoilla. MTBF on lyhenne sanoista Mean Time Between Failures. MTBF-arvo on tilastollinen keskiarvo, joka lasketaan yksinkertaisella kaavalla. Saatu arvo kertoo jotain levyn

luotettavuudesta sen elinkaaren alussa, mutta ei oikeastaan mitään sen pitkäaikaisesta kestävyydestä.

Service life tarkoittaa valmistajan antamaa odotettua elinikää. Tämä on hyvin usein kolmesta viiteen vuotta. Service lifen umpeuduttua vikaantumisen todennäköisyys kasvaa huomattavasti. (Järvinen 2006, 324-325.)

4.2 USB-asemat

Liikuteltavat USB-asemat ovat erinomaisia kodissa, pienessä yrityksessä tai matkamikroja varmistettaessa. Yhtä asemaa on helppo siirtää koneesta toiseen, niin että kaikkien tiedot voidaan kopioida samalle levylle.

Eduistaan huolimatta USB-asemat on tarkoitettu lähinnä tilapäiseen käyttöön. Ne eivät välttämättä kestä pitkäaikaista, yhtämittaista kuormitusta. Tästä kertoo sekin että asemille luvattuja MTBF- tai service life –arvoja on lähes mahdotonta löytää (Järvinen 2006, 335.)

USB-aseman kokoaminen itse halutusta kiintolevystä ei myöskään ole mahdottomuus. Markkinoilla on olemassa valmiita ”kuoria” joihin käyttäjä itse asentaa haluamansa kiintolevyn. Näin käyttövarmuutta saadaan lisää.

4.2.1 USB-muistit

USB-muisteissa data tallennetaan flash-tyylisille piirilevylle. Muisteissa ei ole liikkuvia osia, kuten kiintolevyissä**,** esimerkiksi lukupää. Näin muistien fyysinen kestävyys on hyvä. Valmistajat lupaavat tietyille muisteille jopa elinikäisen takuun toimivuuden kannalta. Tosiasia kuitenkin on, että myös muistitikkuihin mahtuu niin sanottuja maanantaikappaleita, jotka voivat hajota aivan yllättäen.

4.3 Optiset mediat

Kaikilla cd-levyillä yläpuoli on alapuolta haavoittuvampi (Järvinen 2006, 341**).** Varsinainen datakerros on heti ohuen suojalakan alla. Siksi levyn yläpintaan tulevat naarmut voivat olla kohtalokkaita. Tiedetään tapauksia, joissa pelkkä levyn päälle kiinnitetty nimiötarra on tuhonnut levyn tiedot. (Järvinen 2006, 341.)

Levyn yläpinnalle ei pitäisi kirjoittaa muulla kuin pehmeällä cd-r käyttöön tarkoitetulla tussilla. Valmistajien testaamat erilaiset materiaalit, kuten ftalosyaani ja tavallinen syaani antavat levyille kestävyyttä 75-100 vuotta. Esimerkiksi suurimpiin valmistajiin kuuluva TDK lupaa parhaiden cd-r levyjensä säilyvän 100 vuoden ajan. Muiden valmistajien arviot vaihtelevat 30-200 vuoden välillä.

Arkistointikäyttöä varten kannattaa ostaa vain tunnettujen valmistajien levyjä. Halvimmat marketeissa tai netissä myytävät levypakkaukset saattavat pilaantua muutemassa vuodessa**.** (Järvinen 2006, 342.)

Useaan kertaan kirjoitettavien cd-rw –levyjen tallennus tapahtuu metallikalvoon, johon laserin jättämä merkki voidaan ”sulattaa” takaisin ja kirjoittaa uudelleen. Menetelmä ei ole erityisen luotettava; TDK:n oma arvio datan säilyvyydestä on 20-30 vuotta. Lisäksi levyjen luotettavuus pienenee mitä useammin tieto on uudelleen kirjoitettu ja datapinta ”sulatettu”. (Järvinen 2006, 342.)

4.4 Tulevaisuuden mediat

Lähitulevaisuudessa on tulossa markkinoille muun muassa blu-ray ja hd-dvd asemia ja medioita. Näiden**,** periaatteessa dvd- levyjen**,** tallennuskapasiteetti mitataan kuitenkin kymmenissä gigatavuissa. Tarkemmilla lasereilla ja tiiviimmällä pakkaustekniikalla saavutettu lisätila tulee olemaan tervetullut lisä tietojen tallentamiseen.

Lapsenkengissä oleva ja vasta kehitetty teknologia ei välttämättä ole kuitenkaan niin varmaa ja säilyväistä kuin parikymmentä vuotta käytössä olleet cd-levyt.

Näin ollen datan säilyvyydestä ei voi vielä sanoa mitään. Kannattaa siis miettiä uskaltaako elintärkeitä tietoja tallentaa kyseisiin medioihin.

4.5 Nauha-asemat

Erityisesti palvelinkäytössä suuressa suosiossa olevat kapasiteetiltaan valtavat asemat kätkevät sisäänsä kuitenkin melkoisen riskin. Tutkimusten mukaan datan säilyvyys nauhoilla on jopa heikompi kuin optisilla levyillä. Nauha-asemat soveltuvat siis parhaiten jatkuvasti muuttuvan tiedon säilyttämiseen, mutta eivät pitkäaikaiseen varastointiin.

5 TIEDON TUHOAMINEN

Tietoturva nähdään usein vain pyrkimyksenä tiedon säilyttämiseen eli varmuuskopiointina. Näin turvataan tiedon saatavuus, joka on yksi kolmesta tietoturvan tukipilarista. Toinen pilari, tiedon luottamuksellisuus, on aivan yhtä tärkeä. Kun luottamuksellisen tiedon elinkaari päättyy, tiedon tuhoamisesta tulee osa tietoturvaa. Tiedot eivät saa käytön jälkeenkään päätyä vääriin käsiin**.** (Järvinen 2006, 251-252.)

Tiedon säilymisen suurimpina uhkina ovat laiteviat, käyttövirheet, haittaohjelmat sekä erilaiset yllättävät katastrofitilanteet, kuten vesivahingot ja tulipalot. Nämä ovat helppoja uhkia mieltää, joten niihin osataan varautua poikkeuksetta.

Yleensä tiedon tuhoamiseen ei kuitenkaan käytetä yhtä paljoa huomiota. Ja mikä kaikkein yllättävintä: kaikkihan tietävät, että tiedon säilyttäminen ja varmuuskopiointi on työlästä ja aikaa vievää puuhaa. Ei tiedon täydellinen tuhoaminen todellakaan ole yhtään sen helpompaa. (Järvinen 2006, 251-252.)

Kaikkihan tietävät, että papereita ja piirtoheitinkalvoja ei pidä jättää lojumaan ympäriinsä työpaikan pöydille. Paperia osataan käsitellä oikein, koska siitä on ihmisillä pitkä kokemus ja sen sisältämä tieto näkyy paljain silmin. Yrityksillä on paperien tuhoamista varten erityisiä lukittuja roskalaatikkoja ja silppureita.

Sähköisten tallennusvälineiden kohdalla tilanne on aivan erilainen. Poistoon lähtevän tietokoneen sisällä olevaa kiintolevyä kukaan ei joko yleensä edes muista, tai sen sisällön uskotaan olevan tuhottua. Kuitenkin yhdellä tavallisella kiintolevyllä voi olla tietoa enemmän kuin yrityksen kymmenen vuoden aikana keräämissä paperimapeissa yhteensä sillä paljon tietoa mahtuu hyvinkin pieneen tilaan.

Tietotekniikka on paperiin verrattuna abstraktia ja siksi erittäin petollista. Kun käyttäjä laittaa firman tärkeät paperit silppuriin, hän näkee omilla silmillänsä kuinka tieto tuhoutuu. Lisäksi paperisilppua on lähes mahdoton liimata kokoon, paitsi television rikossarjoissa.

Kiintolevyjen kanssa tilanne on aivan toinen. Kun käyttäjä on innoissan formatoinut kiintolevynsä, hän luulee, että levy on todellakin tyhjä, näyttäähän windowssin resurssienhallinta niin. Mistä tavallinen ihminen voisikaan tietää,että formatointi ei tuhoakaan levyllä olevaa dataa?

5.1 Tiedon palautus

Tietoa voidaan poistaa joko yksi tiedosto kerrallaan tai sitten tyhjentämällä koko kiintolevy. Poistettujen tiedostojen palautus on yleensä naurettavan helppoa, sillä delete-komento poistaa vain tiedostosta kertovan merkinnän kiintolevyltä, ei itse tiedostoa. Tiedon palauttamiseen on internetistä saatavilla satoja erilaisia ohjelmia. (Järvinen 2006, 253.)

Mitä kauemmin aikaa poiston ja palautuksen välille syntyy, sitä epätodennäköisemmin palautus onnistuu. Toinen tiedostojen palauttamiseen vaikuttava tekijä on tiedoston pirstoutuminen. Isot tiedostot ovat yleensä hajallaan ympäri kiintolevyä, kun taas pienet ovat sievässä jonossa samassa paikassa, joten näiden palautus on huomattavasti todennäköisempää. Ajan myötä vanhojen tietojen päälle kirjoitetaan uutta tietoa, joten niiden palautuksesta tulee hankalampaa, ellei jopa mahdotonta.

5.2 Turvallinen poistaminen

Tiedoston turvallinen poistaminen ja tuhoaminen edellyttävät uudelleenkirjoittamista. Levykohtiin, joissa tiedosto on aiemmin sijainnut, kirjoitetaan siis nollaa eli tyhjää tietoa tai jotain roskaa, jolloin palauttaminen käy

mahdottomaksi. Turvallista poistamista varten on saatavilla useita eri apuohjelmia. (Järvinen 2006, 254-258.)

Pelkkä poistamiskäsky tai formatointi vain poistaa koneen rekisteristä merkinnän tiedoston olemassaolosta, eli sen luontipäivän, koon ja niin edelleen, mutta ei itse tiedostoa.

5.2.1 Aputiedostot

Monet sovellukset luovat käytön aikana aputiedostoja, joissa on osa käsiteltävän tiedoston sisällöstä. Esimerkiksi Microsoft Word tekee kyseisen tiedoston joka kerta kun painaa tallenna nappia. Kun saat dokumentin valmiiksi ja tiedoston käsittely loppuu, aputiedostot poistetaan kiintolevyltä automaattisesti. Virhetilanteita voi luoda esimerkiksi tietokoneen kaatuminen kesken kaiken, jolloin aputiedostot voivat jäädä kiintolevylle kummittelemaan. Aputiedostojen vaarallisuutta lisää se, että ne ovat yleensä täysin salaamattomia, vaikka itse dokumentti olisikin salattu. Näin ollen palautetusta aputiedostosta saattaa löytyä täysin selkokielisiä lauseita. (Järvinen 2006, 303-309.)

5.2.2 Päällekirjoittaminen

Tiedostot poistuvat levyltä vasta, kun niiden päälle kirjoitetaan uutta tietoa. Tämä tarjoaa helpon keinon tietojen tuhoamiseen: kirjoittamalla levy täyteen soopaa voidaan varmistua siitä, että vanhojen tietojen päälle on mennyt uutta tietoa, eikä niitä voida enää onkia takaisin käyttöön.

Yksinkertainen ohje onkin siis seuraava: formatoi levy, täytä se aivan täyteen turhilla tiedostoilla ja formatoi se toisen kerran. Riippuen kiintolevyn koosta, operaatio voi viedä useitakin tunteja. Siksi pelkkä formatointi houkuttelee**;** se on nopea**,** koska se ei poista oikeasti yhtään mitään.

Montako päällekirjoituskertaa todella riittää? Yhdysvaltojen puolustusvoimien standardi DoD 5220.22-M velvoittaa pyyhkimään luottamuksellisen tiedon vähintään kolmeen kertaan. Useat tiedontuhoamiseen kehitetyt ohjelmat hoitavat homman kirjoittamalla vuorotellen ykkösiä ja nollia kolme kertaa. (Järvinen 2006, 257-258.)

5.2.3 Fyysinen tuhoaminen

Jos ei ole tarvetta säästää kyseistä kiintolevyä, sen voi huoletta hajottaa vaikka vasaralla. Tai jos haluaa olla hienovarainen, repiä pihdeillä siitä kannen auki. Näin sisään pääsevä pöly ja ilma pilaavat herkän magneettipinnan. Tuhoa voi edesauttaa naarmuttamalla levyn sisäosia. (Järvinen 2006, 254.)

5.2.4 Demagnetointi

Viimeisin vaihtoehto levyn tietojen täysin varmaan tuhoamiseen on käyttää voimakkaan magneettikentän synnyttävää pyyhintälaitetta. Koska demagnetointi tuhoaa levyn pinnalle valmistusvaiheessa luodut urat ja sektorimerkinnät, levystä tulee romurautaa käsittelyn jälkeen. Demagnetisointi vastaa levyn fyysistä tuhoamista. (Järvinen 2006, 259-260.)

6 TIETOJEN SUOJAUS

Kaikki meistä ovat tietoisia internetin virus- ja haittaohjelmien vaaroista. Hyvin viattomilta vaikuttavat ohjelmat yrittävät iskeä kyntensä läpi palomuurin, esiintymällä esimerkiksi Windowsin suojauspäivityksinä, tai ironista kyllä, haittaohjelmien poistotyökaluina. Jälkimmäiset poistavat kyllä jotain haittaohjelmia koneesta näön vuoksi, mutta asentavat omansa tilalle. Terve järki on tässä tapauksessa tarpeen, ja yksikin väärä hiirenklikkaus voi altistaa yrityksen tai organisaation koko verkon haittaohjelmille. Mieti mitä teet, ja jos et ole varma, kysy apua ammattilaiselta.

6.1 Käyttäjäoikeudet

Tehokas keino tietoturvan parantamiseksi on Windows-käyttäjien oikeuksien rajoittaminen. Windows on ainoa käyttöjärjestelmä, jossa oletusasetuksena annetaan käyttäjälle täydet oikeudet kaikkiin koneen toimintoihin. Tämä altistaa suurelle tietoturvariskille**,** varsinkin jos käyttäjä on kokematon tietoturva-asioissa. (Järvinen 2006, 195-196.)

Windowsissa oikeuksien rajoittaminen on mahdollista, ja varsin helppoakin, mutta se vaatii suunnitelmallisuutta ja harkintakykyä. Tulos maksaa kuitenkin vaivan**;** kun käyttäjä ei pääse kirjoittamaan tietoa Windowsin omiin hakemistoihin**,** eikä muuttamaan järjestelmän asetuksia**,** monet virheet jäävät pois**,** ja haittaohjelmien leviämisestä tulee vaikeaa**,** ellei jopa mahdotonta. (Järvinen 2006, 195-196.)

Valitettava tosiasia on, että käyttäjätilien hallinta on lisätty Windowsiin matkan varrella**,** eikä sitä ole suunniteltu siihen alusta alkaen. Näin ollen oikeuksien rajoittamisesta voi ilmetä ongelmia ja virheilmoituksia.

Yritysverkoissa käyttäjäoikeudet määritellään Windows-toimialueen palvelimella. Näin käyttäjät saavat rajoitetut oikeudet tarpeellisiin lähiverkon palveluihin. Omaan koneeseensa käyttäjällä on yleensä vain perusoikeudet. Verkkoa ja sen koneita valvomaan on hyvä palkata tai nimetä asiansa osaava ammattihenkilö.

6.2 Ohjelmat

Tietoturvan parantamiseen on olemassa jos jonkinlaista ohjelmaa. Tärkeimpinä voidaan pitää palomuuria ja viruksentorjuntaa. Nämä kyseiset ohjelmat on syytä olla käyttäjillä jopa kotikoneissa, yrityksistä puhumattakaan.

6.2.1 Palomuurit

Pitkän aikaa internet-käytön tietoturva perustui palomuureihin ja niiden antamaan turvaan. Ne ovat edelleen tarpeellisia, mutta niiden kokonaismerkitys tietoturvassa on vähentynyt. Palomuureja voi olla kahdenlaisia**;** fyysisiä ja ohjelmallisia.

Fyysiset palomuurit ovat yleensä integroitu jo adsl-reitittimeen omille piirilevyilleen ja niiden käyttö on verrattain vaikeaa, mutta turva on parempi. On myös saatavilla erillisiä ohjelmistoja, jotka tekevät muuten vanhaksi käyneestä tietokoneesta pelkän palomuurin. Tälläinen on muunmuassa Smoothwall. (www.smoothwall.org)

Ohjelmalliset palomuurit toimivat samalla tavalla kuin muutkin ohjelmat käyttöjärjestelmässä ja ne vievät koneen resursseja. Nykypäivän suurimmat ongelmat palomuurien heikkoon suojaustasoon on yritysten käyttämä tekniikka. Asiakkaat ja oma henkilökunta tuovat tiloihin kannettavia tietokoneita ja

muistitikkuja, joista yrityksen sisäverkkoon voi levitä haittaohjelmia ja viruksia. Jotkin suuret yritykset kieltävät omien medioiden käyttämisen yrityksen tiloissa. Myös Wlan-tukiasemat saattavat päästää liikennettä ulos ja sisään palomuurin ohi. Palomuurin toimintaperiaate on ip-osoitteiden ja porttinumeroiden kontrollointi. Suurimpana murheena nykyään on portti 80, jota tarvitaan internetissä surffausta varten. Siksi useat ohjelmat ovatkin alkaneet käyttää sitä. Esimerkiksi juuri vakoiluohjelmat välittävät tietoa yleensä juuri kyseisen portin kautta, koska näin niiden aiheuttama tietoliikenne hukkuu muuhun surffauksessa käytettävään, ja palomuurit eivät osaa reagoida tilanteeseen. (Järvinen 2006, 105-112.)

6.2.2 Virustorjuntaohjelmat

Virustorjuntaohjelmat toimivat ohjelmistoperiaatteella käyttäjän koneella, jollei esimerkiksi lähiverkon palvelimelle ole erikseen asennettu ohjelmaa, jonka läpi kaikki verkkoon tuleva tieto kulkee.

Virustorjuntaohjelmistoja on saatavilla maksullisia ja maksuttomia, myös yrityskäyttöön. Eroina on yleensä esimerkiksi ruudulle pomppaava mainos kerran päivässä tai tuotetuen puuttuminen. Eli ongelmatapauksissa käyttäjä joutuu itse selvittämään mitä on vialla.

Ohjelmat perustuvat liikenteen suodattamiseen tai tietyin aikavälein suoritettavaan valittujen tiedostojen tutkimiseen. Esimerkiksi tunnetun suomalaisen yrityksen F-Securen tuotteet tutkivat jatkuvasti koneelle tulevaa verkkoliikennettä ja näin pystyvät estämään virusten pääsyn koneelle jo ennen kuin tuhoa on ehtinyt syntyä.

Viruksen löydettyä ohjelmat voivat laittaa sen karanteeniin, jolloin tarttunutta tiedostoa valvotaan**,** ja näin virus ei pääse leviämään Muita mahdollisia tapoja ovat muun muassa tiedoston poistaminen. (F-Secure Oyj 2006)

Poistamisessa piilee kuitenkin riski, että saastunut tiedosto on osa käyttöjärjestelmää, näin ollen kyseisen tiedoston poistaminen voi sekoittaa koko

käyttöjärjestelmän ja näin aiheuttaa vielä suurempia murheita. (F-Secure Oyj 2006)

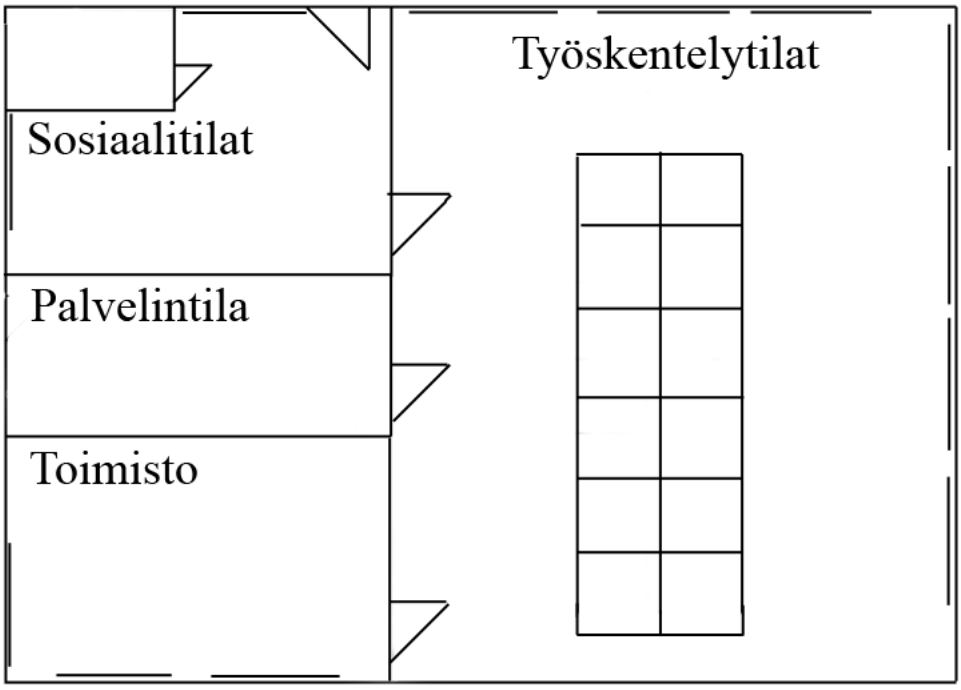
7 FYYSINEN TIETOTURVAMALLI

Tämän opinnäytetyön tutkimuksen aiheena on kuvitteellinen pienyritys, jonka toimiala on kilpailukykyinen**,** ja näin ollen vaatii tarkkaa fyysistä tietoturvaa.

Yritys sijaitsee omassa rakennuksessaan, joka on varta vasten rakennettu yrityksen tarpeiden mukaiseksi. Fyysisesti tila on noin 300 neliömetriä ja se sijaitsee niin sanotussa teollisuuspuistossa kaupungin ulkolaidalla.

Yritys suunnittelee 3D-malleja toisille yrityksille korkeatasoisilla tietokoneilla. Tämän takia jo fyysisissä laitteissa kiinnitettynä oleva raha vaatii tarkkaa turvaa, puhumattakaan liikesalaisuuksista ja informaatiosta koneiden sisällä ja palvelimilla.

Alla yrityksen fyysisen rakennuksen pohjapiirustus (KUVIO1). Kuva on viitteellinen, ei mittakaavassa.



KUVIO1. Yrityksen pohjapiirustus

Yritys koostuu neljästä erillisestä tilasta, jotka ovat sosiaalitila, palvelintila, toimisto sekä työskentelytila.

7.1 Fyysisen tietoturvan priorisointi

Kuten pohjapiirustus näyttää, yritys koostuu neljästä eri tilasta, joilla on erilaiset tietoturvalliset prioriteetit. Nämä on hyvä suunnitella etukäteen, jotta resurssit tulee sijoitettua oikein.

Tärkeimpänä tilana tässä yrityksessä on palvelintila, jonne työasemilla tuotettava tieto siirretään päivän päätteeksi. Toisena on työskentelytilat kalliiden laitteidensa ja jatkuvasti kehitettävän tiedon takia. Kolmantena yrityksen toimistotilat, joista löytyy muunmuassa kirjanpitoa ja rekistereitä tehdyistä töistä, mutta ei kuitenkaan yrityksessä suunniteltua tietoa. Viimeiseksi jää sosiaalitilat, joissa ei mitään

tietoturvan kannalta tärkeää edes ole. Tärkeimmäksi priorisoitu tila vaatii siis tarkimmat turvatoimenpiteet.

7.2 Pohjapiirustus

Kun aletaan rakentaa fyysisesti tietoturvallista yritystä kivijalasta ylöspäin**,** on hyvä huomioida muutama seikka. Tässä yrityksessä on palvelintila sijoitettu rakennuksen keskelle, ikkunattomaan huoneeseen. Tilaan on yksi sisäänkäynti toisesta hyvin tarkasti suojatusta tilasta, työskentelytilasta. Työaikaan ovelle on esteetön näkyvyys usealta työpisteeltä. Yrityksen ollessa suljettuna ovea vahtivat elektroniset valvontalaitteet, joilla ei ole katvealueita.

Palvelintilan välittömässä läheisyydessä ei ole myöskään vesiputkia, vaan talon ainoat vettä käyttävät tilat on sijoitettu mahdollisimman kauas. Näin mahdolliset vesivahingot on minimoitu. Tilan alle on rakennettu välipohja, mikä kerää vedet mahdollisten vahinkojen sattuessa. Myös tulipaloja sammutettaessa sammutukseen käytetty vesi ohjautuu ensiksi välipohjaan**,** eikä palvelintilan lattialle. Seinissä on käytetty palamatonta materiaalia, joka palon sattuessa eristää tilan muista tiloista**,** ja näin data saattaa säilyä jopa tulipalosta.

Yrityksen ovet on suunniteltu poikkeuksellisesti avautumaan niin sanotusti ”väärään” suuntaan, jotta esimerkiksi toimistoon murtautunut henkilö joutuu avaamaan fyysisesti ison oven suoraan työskentelytilassa oleviin sensoreihin. Iso ovi aiheuttaa huomattavasti herkemmin hälytyksen kuin pieni ihminen, joka saattaisi pahimmassa tapauksessa päästä livahtamaan sensorien ohi.

Työskentelytila on jätetty tarkoituksella avonaiseksi**,** eikä sitä ole lohkottu pieniin huoneisiin. Työpisteitä erottaa toisistaan vain kevyet sermit**,** jotka eivät ole tilan kattoon saakka. Sensoreille ja valvontakameroille ei näin tule katvealueita.

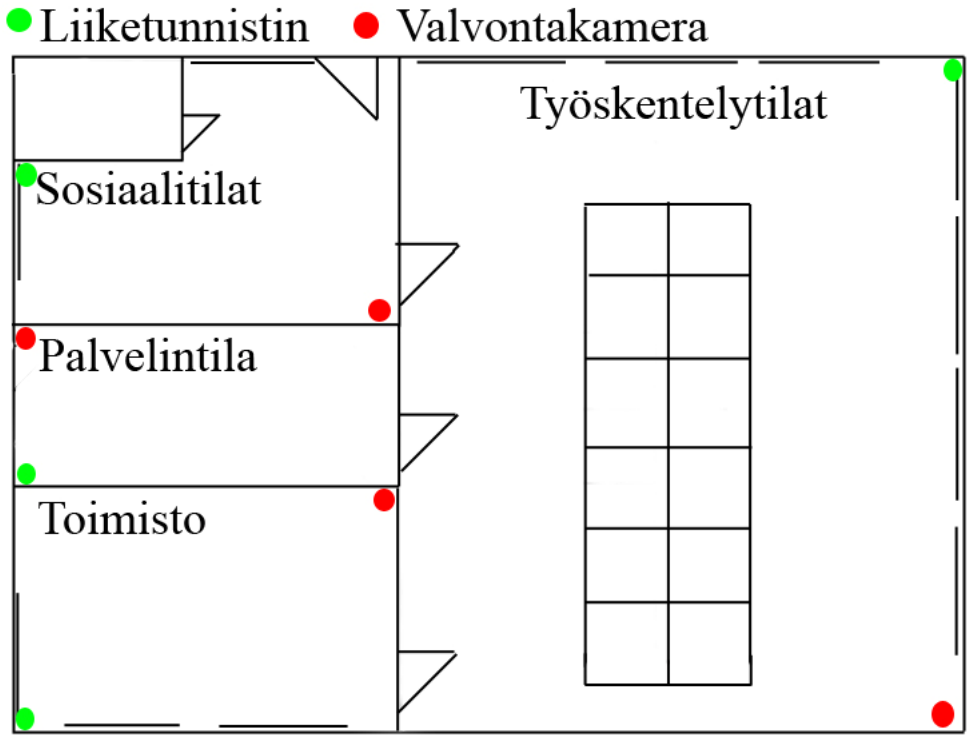
7.3 Valvontakamerat ja sensorit

Nykyisten kameroiden ollessa sen verran monipuolisia laitteita, ei pieneen yritykseen periaatteessa edes tarvitse vanhanaikaisia liiketunnistimia. Tässä tapauksessa ne kuitenkin asennetaan maksimaalisen turvan saamiseksi.

Kameroina käytetään D-Link DCS-3420 päivä- ja yökäyttöön soveltuvaa internet-kameraa. Kamerat toimivat joko RJ-45 verkkokaapelilla, langattomasti tai jos haluaa yhdistää kameran vanhanaikaiseen valvontakamerajärjestelmään, siinä on myös BNC-liitäntä. Malli toimii myös ulkokäytössä lisävarusteena saatavan ilmastoidun ja lämmitettävän kotelon avulla.

Liiketunnistinsensoreina toimivat perusmalliset, valoataittavat, mitkä saa hankittua muun muassa Securitas Direct Oy:ltä. Nämä ovat niitä punaista led-valoa vilkuttavia valkoisia laatikoita huoneiden nurkissa, joita näet kaikkialla.

Valvontakamerat toimivat sisäänrakennetun liiketunnistimensa avulla, jotta palvelintilaa ei hukkaantuisi ja mahdolliset murtautumiset ynnä muut on helppo löytää. Normaalit liiketunnistimet ovat käytössä kokoajan. Tunnistimet ja kamerat on sijoitettu seuraavan (KUVIO2) kuvan mukaisesti.



KUVIO2. Yrityksen pohjapiirustus, liiketunnistimet ja valvontakamerat

Valvontakamerat eivät ole kytkettynä itse hälytykseen niiden sijoittelun takia. Kamera voi vahingossa ottaa ikkunan läpi ulkopuolella näkyvää liikettä ja näin syntyisi aiheeton hälytys. Yksi kamera kuvaa ulko-ovea, josta ihmiset saapuvat työpaikalleen. Yksi kuvaa toimistossa, yksi työskentelytilassa**,** sekä tärkeimpänä jatkuvasti palvelintilassa päällä oleva kamera. Kamerat on kytketty palvelinkoneeseen RJ-45 verkkokaapeleilla, langattomien signaalien mahdollisten kaappauksien vuoksi.

Liiketunnistimet on sijoitettu siten, että ne eivät ole suoraan ikkunoita kohti. Näin kaikki hälytykset tulevat varmasti talon sisältä.

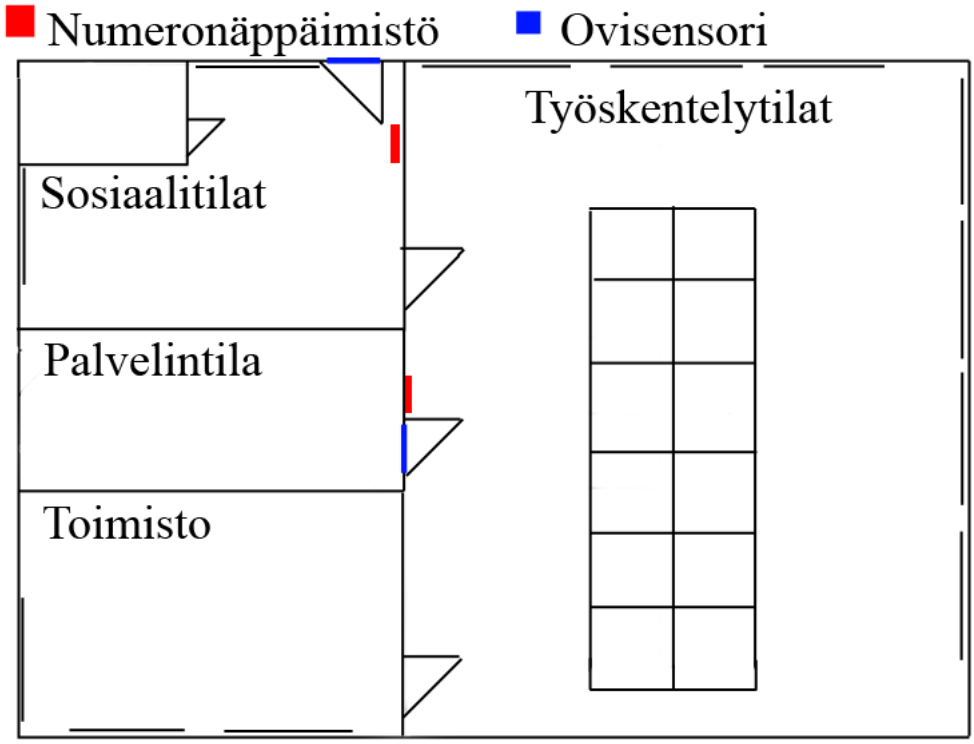
7.4 Käyttönäppäimistöt ja ovisensorit

Ulko-oven välittömään läheisyyteen sijoitetaan numerokoodilla toimiva käyttönäppäimistö, joka ohjaa koko yrityksen hälytysjärjestelmää (KUVIO3).

Pois lukien palvelintilan ovea, jolle on oma numerokoodinsa, tämä maksimaalisen tietoturvan saavuttamiseksi.

Kun ulko-oven avaa, kytkeytyy puolen minuutin ajastin, jonka aikana oikea koodi on näppäiltävä näppäimistöön tai hälytys laukeaa automaattisesti. Turvaa lisää se seikka, että koodia ei tarvitse antaa jokaisella työntekijälle**,** vaan esimerkiksi sihteerille ja esimiehelle, jotka tulevat toimipaikalle hiukan muita aikaisemmin avaamaan ovet ja kytkemään hälytyksen pois päältä.

Palvelintilan oven numerosarja on visusti varjeltu salaisuus, jonka tietävät esimerkiksi vain yrityksen esimies, omistaja ja atk-tukihenkilö. Näin saadaan tehokkaasti pidettyä ulkopuoliset muuttujat pois herkästä ja erittäin tärkeästä palvelintilasta, jossa pelkkä ihmisten mukana tuoma pöly voi aiheuttaa ongelmia.



KUVIO3. Yrityksen pohjapiirustus, numeronäppäimistöt ja ovisensorit

7.5 Palvelimet ja työpisteet

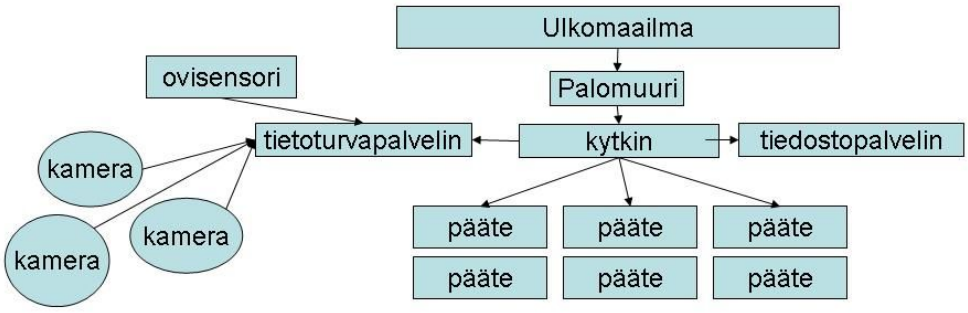
Palvelimiksi kyseiseen yritykseen valittiin HP:n valikoimista peruspalvelimet RAID- ominaisuuksilla. Yrityksessä päädyttiin käyttämään RAID1- eli peilausmenetelmää (*mirroring*)**;** sama data tallennetaan kahdelle (tai useammalle) erilliselle levylle, jolloin toisen levyn hajotessa kaikki data säästyy. Näin vahinkojen sattuessa pystytään toiminta pitämään käynnissä.

Raid- ohjaimet ovat hyvin herkkiä eri levyille, joten eri valmistajien tekemät kiintolevyt eivät ole hyvä ratkaisu, eivätkä myöskään samasta valmistuserästä tulleet samanlaiset levyt. Ideaalitilanteessa palvelimessa käytetään samanmerkkisiä ja -mallisia levyjä, mutta eri valmistuserästä. Näin levyrikon tapahtuessa todennäköisyys, että toinenkin levy rikkoontuu samalla hetkellä**,** on merkittävästi pienempi. Palvelimessa on lisäksi Hotswap - ominaisuus, eli kiintolevyjä voi vaihtaa palvelinta sammuttamatta. Tämä sen takia, että työskentely voi jatkua**,** vaikka palvelimiin vaihdeittaisiin uusia kiintolevyjä rikki menneiden tilalle.

Käytössä on kaksi eri palvelinta, joista toinen on pelkästään tietoturvaan**,** ja toinen tiedostopalvelimeksi suunniteltu. Lisäksi on erillinen palomuurikone.

Dedikoitu palomuurikone parantaa tietoturvaa erittäin paljon, sekä säästää resursseja työpisteiden koneissa. Kaikki yrityksen internetliikenne kulkee tämän lävitse**,** ja sitä voidaan säätää tarpeisiin sopivaksi, niin tiukaksi kuin halutaan. Esimerkksi sulkemaan kaikki arveluttavat portit ja päästämään läpi vain html-portin (portti 80) vaatima tieto.(KUVIO4) Tarkoitukseen sopivia ohjelmistoja on saatavilla ilmaiseksi internetistä, myös yrityskäyttöön.

Kaikki verkotus yrityksen tiloissa on tehty asennuskouruja pitkin RJ-45 verkkokaapeleilla ulkoisten häiriöiden minimoimiseksi. Asennuskourut estävät esimerkiksi pienjyrsijöiden pääsyn kaapeleiden kimppuun, sekä ovat luotettavempia kuin langattomasti toteuteutettu lähiverkko.



KUVIO4.Yrityksen sisäverkko

7.6 Kustannusarvio

Edellä mainittujen valvontalaitteistojen karkea kustannusarvio internetistä saaduilla hinnoilla on seuraava. (TAULUKKO1) Mukaan on laskettu valvontakamerat, valvontasensorit, kaksi palvelinta ja arvio johdotustyöstä sekä ammattilaisen tekemästä asennuksesta. Ovinäppäimistöt ja –sensorit ovat sisällytetty tarvikkeisiin. Asennuksen hinta-arvioksi on käytetty paikallisen Akusolvers Oy:n internet-sivuillaan julkaisemaa tuntihintaa asennustöille. Hinnat ovat silti suuntaa antavia ja niihin pitää suhtautua varauksella, sillä kilpailuttamalla saatava säästö voi olla merkittävä. Kaikki tuotteiden hinnat ovat www.verkkokauppa.com nettisivustolta. Hinnat sisältävät alv-22%.

Tuote	a-hinta	määrä	yhteensä
D-Link DCS-3420	781,90 €	4	3 127,60 €
Valvontasensorit	80,00 €	4	320,00 €
HP ML350 G5 tornipalvelin	1 767,90 €	2	3 535,80 €
ViewSonic VX712 17" TFT LCD-näyttö	189,90 €	2	379,80 €
D-LINK DES-1228 kytkin	201,90 €	2	403,80 €
Kiintolevyt palvelimiin			
HP 146GB, 15krpm, 3.5", SAS	675,90 €	4	2 703,60 €
Johdot,kaapelit ja tarvikkeet	1 500,00 €	1	1 500,00 €
Asennustyö	40,00 €	40	1 600,00 €
		yhteensä	**13 570,60 €**

TAULUKKO1. Kustannusarvio

8 YHTEENVETO

Tavoitteena tässä opinnäytetyössä oli tutkia yrityksen fyysistä tietoturvaa; miten se toteutetaan ja mitä se oikeasti tarkoittaa. Yleisesti ottaen tietoturvalla käsitetään juuri ne perusasiat eli palomuurit ja virustorjuntaohjelmat, mutta fyysinen osio jätetään heitteille. Olin aikaisemmin koulun ohella töissä atk-alan yrityksessä, joka toteutti muunmuassa erilaisia turvallisuuspalveluita yrityksille. Myös itse olin rakentamassa varsin perusteellista fyysisen tietoturvan pakettia eräälle Päijät-Hämeessä sijaitsevalla yritykselle. Mielenkiinto aiheeseen ja jonkinasteinen alustus sekä pohjaosaaminen olivat siis valmiina, ennen kuin työtä aloitin edes tekemään.

Aloitin työn tekimisen tutustumalla fyysiseen tietoturvaan ja yritysten fyysiseen turvallisuuteen lukemalla siitä eri kirjallisista lähteistä**,** sekä selaamalla asiaan viittaavia artikkeleita internetistä. Pikkuhiljaa aloin kirjoittamaan ja kasaamaan opinnäytetyön teoreettista osuutta, josta tuli omasta mielestäni varsin kattava yleissilmäys fyysisen tietoturvan maailmaan.

Tämän työn fyysisen tietoturva mallin toteuttaminen oli varsin mielenkiintoista puuhaa. Pyrin ottamaan huomioon kaiken työn teoreettisessa osuudessa läpikäydyistä aihepiireistä. Varmasti monen asiantuntijan mielestä jotkin asiat voisi tehdä eritavalla, mutta omasta, sekä muutaman alalla työskentelevän ihmisen mielestä mallissa on otettu huomioon erilaisia piirteitä eri osa-alueilta.

Fyysistä tietoturvaa rakennettaessa tulisi huomioida yrityksen koko ja sen tarpeet. Tässä tapauksessa kyseessä oli pieni yritys, jonka tarpeet ovat kohtalaisen helpohkot toteuttaa. Isoissa yrityksissä ongelma kasvaa huomattavasti, sillä mukaan tulee paljon enemmän työntekijöitä ja enemmän itse fyysistä tilaa. Perusajatus pysyy kuitenkin kokoajan samana, vain mittakaava muuttuu. Mahdollisimman hyvä fyysinen tietoturva koostuu siis luotettavista ja koulutetuista työntekijöistä, suunnitellusta tilan käytöstä ja suojauksesta**,** sekä sopivasta laitteistosta.

LÄHTEET

Järvinen Petteri. 2006. Paranna tietoturvaasi. 1. Painos. WS Bookwell, Porvoo.

Kauppakaari & Miettinen Juha E.. 2002. Yritysturvallisuuden Käsikirja. Gummerus Kirjapaino Oy, Jyväskylä.

Laaksonen Mika, Terho Nevasalo & Karri Tomula. 2006. Yrityksen tietoturvakäsikirja. Oy Nordprint Ab, Helsinki.

Mika Hakala, Mika Vainio & Olli Vuorinen. 2006. Tietoturvallisuuden käsikirja. WS Bookwell, Porvoo.

F-Secure Oyj . 2006. http://www.f-secure.fi/

Verkkokauppa.com Oy. 2006. http://www.verkkokauppa.com

Akusolvers Oy. 2006. http://www.akusolvers.fi