Sisäinen tietoturva – tietovuodon vaikutukset pk-yrityksen toimintaan ja toimintatapojen muutosten vaikutus sisäiseen tietoturvallisuuteen
Case: BK-Automation Ky

Timo Nikkari

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Tietojenkäsittelyoppi
Pro gradu -tutkielma
Ohjaaja: Professori Pirkko Nykänen
Kesäkuu 2007

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Tietojenkäsittelyoppi
Timo Nikkari: Sisäinen tietoturva – tietovuodon vaikutukset pk-yrityksen toimintaan ja toimintatapojen muutosten vaikutus sisäiseen tietoturvaan
Case: BK-Automation Ky
Pro gradu -tutkielma, 66 sivua, 6 liitesivua
Kesäkuu 2007

Yleisissä keskusteluissa tietoturva on yhtä kuin viruksentorjunta ja palomuuriratkaisut. Varsinkin pk-yrityksissä tietoturvaratkaisut ovat enemmän tai vähemmän puutteellisia. Varsinkin yritysmaailmassa tietoturva on jaettavissa kahteen ryhmään: sisäiseen ja ulkoiseen tietoturvaan.

Tämän tutkimuksen tarkoituksena on ollut selvittää, mitä pk-yrityksen sisäiseen tietoturvaan kuuluu. Tässä tutkimuksessa sisäisellä tietoturvalla tarkoitetaan niitä tietoturvallisuuteen liittyviä asioita, jotka suoraan tai välillisesti liittyvät yrityksen työntekijöiden toimintaan ja toimintatapoihin. Koska pk-yrityksien taloudelliset resurssit ovat rajalliset, aihetta on tutkimuksessa käsitelty tämä huomioon ottaen, ja sisäiseen tietoturvaan liittyvät asiat on jäsennelty sen mukaan.

Tutkimus on suoritettu tapaustutkimuksena ja tietovuodon vaikutuksia on käsitelty juuri tutkimuksen kohteena olevan yrityksen tapahtumakulun kautta. Tapahtumia tutkimalla saadaan arvio siitä, kuinka paljon toimintatapoja muuttamalla pienennetään sisäisen tietoturvan riskejä ja mitkä ovat muutosten vaikutukset tulevaisuuden liiketoimintaan.

Avainsanat ja -sanonnat: sisäinen tietoturva, pk-yrityksen tietoturva, pk-yrityksen sisäiset tietoturvaratkaisut, tapaustutkimus

KIITOKSET

Kiitän BK-Automation Ky:tä ja erityisesti yrityksen toimitusjohtaja Asko Kuoppalaa.

And now, the end is near, and so I face, the final curtain.
My friend, I'll say it clear,
I'll state my case, of which I'm certain.
I've lived, a life that's full, I've traveled each and every highway.
And more, much more than this,
I did it my way.

(My Way – Frank Sinatra & Paul Anka)

1. Johdanto

Jokaisella tietokoneen käyttäjällä on jonkinlainen käsitys siitä, mitä tietoturva tarkoittaa. Useimmiten peruskäyttäjälle tulee käsitteestä mieleen virushyökkäykset ja niiden torjuntaohjelmistot ja palomuuriohjelmistot. Toinen asia, josta paljon puhutaan, on sähköpostin roskapostit ja niiden suodattaminen. Samoin luottamuksellisten tietojen, kuten pankkiyhteystietojen, joutuminen rikollisten käsiin koetaan vaaraksi, josta pankit kyllä hyvin tiedottavat [Kyselytutkimus, 2006]. Nämä kaikki edellä mainitut asiat kuuluvat kuitenkin pääsääntöisesti ulkoisen tietoturvan piiriin. Ne henkilöt, jotka työskentelevät jossakin suuressa yhtiössä, jolla on varaa panostaa kokonaisvaltaiseen tietoturvaan, tietävät ainakin jotakin myös sisäisestä tietoturvasta.

Pk-yritysten määrä on merkittävä, kun tarkastellaan yritystoimintaa yleisellä tasolla Suomessa. Käsitykseni onkin, että mitä pienempiä yrityksiä tarkastellaan, sitä suurempi vaara on, että tietoturvan taso ja osaaminen ovat lähellä edellä kerrotun yleisen tietämyksen tasoa. [Kyselytutkimus, 2006.]

Paitsi että tietoturvariskit lisääntyvät yrityskoon pienentyessä, ne korostuvat myös erityisesti niissä pk-yrityksissä, joissa tehdään merkittäviä innovaatioita, panostetaan vahvasti tuotekehitykseen ja joissa oma osaaminen on vankkaa ja sitä ylläpidetään jatkuvalla koulutuksella. Usein yrityksen keskeisin avainhenkilö on se yrittäjä, joka työskentelee liiketoiminnan kannalta tärkeissä tehtävissä, vaikka yrityksessä voi olla muitakin avainhenkilöitä.

Nykyään myös innovatiiviset pk-yritykset ovat melko riippuvaisia tietotekniikasta ja sen eri sovellutuksista. Tärkeät innovaatiot ja tuotekehityksen tulokset mallinnetaan esimerkiksi ohjelmakoodiksi, dokumentoinniksi, kaaviokuviksi, piirustuksiksi ja niin edelleen. Tällöin syntyy sisäisen tietoturvan kannalta uusi merkittävä riski: kyseiset tiedot voidaan myös

kopioida tai varastaa, varsinkin jos sisäinen tietoturva on puutteellinen tai sitä ei ole ollenkaan. Tätä aihealuetta on tässä tutkimuksessa tarkoitus käsitellä tarkemmin. [Kyselytutkimus, 2006.]

1.1 Aiheen esittely ja tutkimuksen kulku

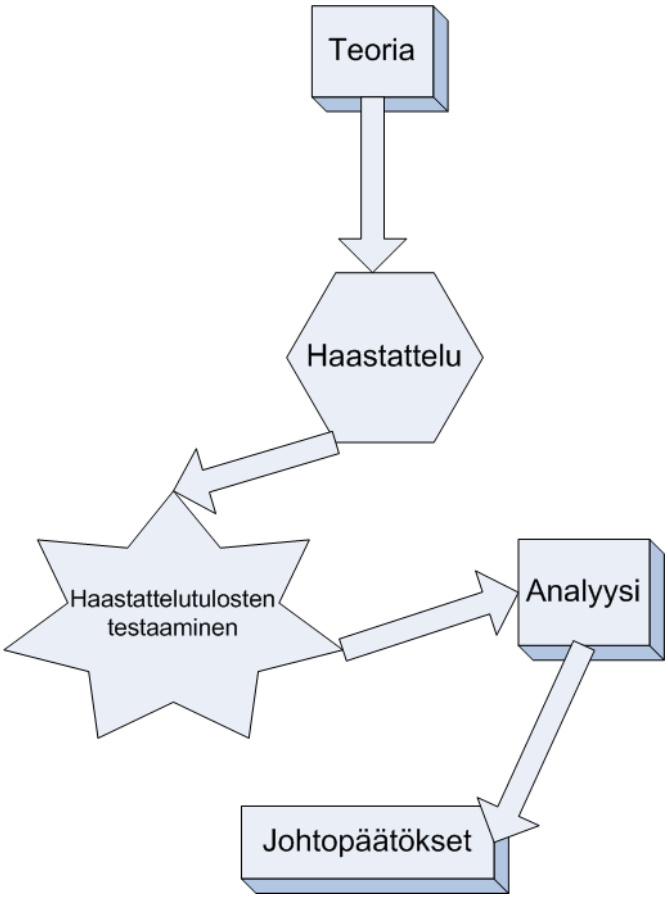
Aloittaessani tutkimuksen tekemistä, minulla oli selkeä näkemys, että haluan tehdä tutkimukseni sellaisesta aiheesta ja teoriasta, että tutkimustani pystytään vertaamaan käytännön toimiin oikeassa liiketoiminnassa. Tämän seurauksena aloin etsiä sellaisia ilmiöitä tai tapahtumia, jotka liittyvät yritystoiminnan tietoteknisiin ratkaisuihin. Löydettyäni monia mielenkiintoisia vaihtoehtoja tutkimukseni aiheeksi sain henkilökohtaisten kontaktieni kautta tietooni BK-Automation Ky:n tapauksen, joka yleisen tarkastelun perusteella osoittautui hyvin uniikiksi ja erikoiseksi. Kyseinen tapaus täytti kaikki ne kriteerit, joita olin asettanut tutkimuksen tekemiselle.

Tarkastellessani Pertti ja Annikki Järvisen [Järvinen ja Järvinen, 2004] teosta tutkimustyön tekemisestä minulle selvisi nopeasti, että tutkimuksestani tulee tapaustutkimus. Aloitin tutkimukseni tekemisen tutustumalla sisäiseen tietoturvaan liittyvään materiaaliin ja havaitsin, että tutkimukseeni sopivia tutkimuksia ja kirjallisuutta oli tarjolla hyvin niukasti ja että aiheen tutkiminen on toistaiseksi ollut melko yleisellä tasolla [Leiwo ja Kajava, 1994b]. Lisäksi löytämäni aineisto oli suurelta osin melko vanhaa, ja tämä vaikeutti työn tekemistä. Tässä tutkimusprosessin vaiheessa tein ratkaisun, että tutkimukseni tulisi pohjautumaan hyvin vahvasti BK-Automation Ky:n tapahtumiin ja niiden pohjalta tehtyihin johtopäätöksiin.

Rakensin tutkimukseni teoreettisen viitekehyksen kirjallisuuskatsauksen perusteella, jonka tein edellä mainitun suomalaisen pk-yrityksen tietoturvasta ja nimenomaan yrityksen sisäisistä ratkaisuista. Tähän katsaukseen nojautuen loin pohjan haastattelulle. Haastattelun tein helmikuussa 2007.

Haastateltavana oli yrityksen pääomistaja ja toimitusjohtaja Asko Kuoppala. Haastattelutilannetta varten haastateltavalle ei lähetetty valmista kysymyslomaketta, vaan häntä informoitiin aiheesta hyvin yleisellä tasolla. Näin menettelemällä halusin varmistua siitä, että haastattelutilanteessa vastaukset eivät olisi ennalta mietittyjä yksinkertaistettuja vastauksia, vaan että haastattelutilanne olisi pikemminkin vapaan keskustelun omainen. Tällä tavalla keskustelua johdattelemalla uskoin saavani autenttisemmat ja tarkemmat vastaukset vahingon sen hetkisestä tilanteesta, sen seurauksista ja toimintatapojen muutoksista. Haastattelun tarkkaa analysointia varten se tallennettiin nauhalle. Haastattelutilanteen runkona käytettiin mukaillen Ilvosen [Ilvonen, 2006] tekemää haastattelulomaketta[Liite 1].

Haastattelun jälkeen oli vuorossa sen tulosten vertaaminen teoriaan. Analyysin tarkoitus on kuvata sitä, mitä tapaus kertoo verrattaessa sitä luotuun teoreettiseen viitekehykseen. Tämä tutkimus seuraa siten perinteistä tutkimuskaavaa.



Kuva 1: Tutkimuksen eteneminen.

Analyysin jälkeen seuraava tutkimusvaihe oli johtopäätösten tekeminen. Tämän tutkimuksen johtopäätösten yhteydessä esitellään ne jatkotutkimuskohteet, jotka ovat tutkittuani aihetta syvällisemmin tulleet mieleeni ja jotka olisivat mielestäni hyviä aiheita tuleville tutkimuksille.

1.2 Tutkimusongelma

Pro gradu -tutkimukseni tarkoituksena on tutkia niitä tietoturvaan liittyviä asioita, joita pk-yrityksen tulisi ottaa huomioon sisäisessä tietoturvassaan. Sisäisen tietoturvan ongelmia kohdannut pk-yritys toimii tässä tutkimuksessa teorian kohteena, ja haastatteluna saatu aineisto on teoriaa testaava, kun pyritään etsimään vastauksia seuraavaan kysymykseen:

– Mitä tarkoitetaan pk-yrityksen sisäisellä tietoturvalla?

Tähän tutkimuskysymykseen pyritään vastaamaan luvussa 1.4 ja luvussa 2: luvussa 1.4 määritellään, mitä on sisäinen tietoturva ja luvussa 2 kuvataan, mitä sisäiseen tietoturvaan kuuluu tietoturvasta annettujen määritysten perusteella. Tämän tutkimuksen tutkimuskysymystä voidaan tarkentaa ja samalla täydentää kahdella lisäkysymyksellä:

– Mitkä ovat sisäisen tietoturvan pettämisen vaikutukset pk-yrityksen toimintaan?

– Onko toimintatapojen muutoksella vaikutusta sisäiseen tietoturvaan?

Näihin kysymyksiin pyritään vastaamaan osin luvussa 3 ja kokonaisuudessaan luvuissa 4 ja 5. Lisäksi yritetään löytää vastaus siihen, olisiko tapahtunut varsinkin case-yrityksen tapauksessa ollut mahdollista estää kokonaan, jos toimintatapoja olisi muutettu ennen tapahtumia. Toimintatapojen muutos saattaa aiheuttaa uusia ongelmia, joita tässä tutkimuksessa käsitellään niiden tärkeyden ja laajuuden puitteissa.

1.3 Tutkimuksen rajaukset

Yleisessä tiedossa on, että pk-yrityksellä on rajalliset taloudelliset mahdollisuudet kehittää yrityksen tietoturvaa. Yrityksille kohdennetuissa tietoturvakäsikirjoissa [Laaksonen et al., 2006] tietoturvan ratkaisut ja ohjeistukset ovat hyvin monimuotoisia ja yksityiskohtaisia. Niiden soveltaminen pk-yrityksen toimintaan on monessa tapauksessa hyvin vaikeaa, varsinkin kun yrityksen taitotieto on rajallista ja kokonaisuuden ymmärtäminen vaatii yleensä ammattilaisen toimenpiteitä. Pk-yritysten toiminnan laajuuden ja

taloudellisten resurssien johdosta ei ole mahdollista palkata erillistä henkilöä hoitamaan vain tietoturva-asioita.

Tutkimuksessa keskityn siis tarkastelemaan sisäisen tietoturvan kysymyksiä pk-yrityksessä, ja nämä kysymykset on linkitetty vahvasti tutkimuksessa käytetyn pk-yrityksen tapahtumiin, joita sovelletaan ja verrataan tutkimuksen teoreettiseen osaan. Yleisellä tasolla sisäisen tietoturvan osa-alueet pyritään jäsentämään taloudelliseen järjestykseen, ja näin pyritään luomaan kuva siitä, missä puitteissa sisäisen tietoturvan kehittäminen on järkevää. Tutkimuksessa ei kuitenkaan oteta kantaa siihen, missä järjestyksessä osa-alueita tulisi pk-yrityksessä rakentaa tai kehittää.

Vaikka kaikki tietoturvaan liittyvät ratkaisut ovat tavalla tai toisella liitettävissä aina johonkin henkilöön, tämän tutkimuksen kohteena ovat ne yrityksen ja työntekijän väliset suhteet, toiminnot ja ratkaisut, jotka liittyvät siihen, millä on suoranainen vaikutus yritykseen toimintaan. Ulkopuoliset uhat ovat tässä tutkimuksessa mukana siinä määrin, kun ne tulevat yrityksen ulkopuolelta ja niitä ei ole kohdennettu suoraan ja/tai tahallisesti yrityksen tietojärjestelmiin tai liiketoiminnan haittaamiseen. Tietoverkkoratkaisut, ohjelmistoratkaisut, virustorjunta, palomuurit, yleiset standardit, sähköpostiturvallisuus ja Internet-käyttäytyminen eivät siis sellaisenaan ole käsittelyn kohteena, koska niiden tärkeimpänä piirteenä ei ole työntekijän toiminnan vaikutus. Puhuttaessa valvonnasta näitä aiheita sivutaan vain hyvin yleisellä tasolla, koska ne ovat edellä mainitun lisäksi usein hyvin teknisiä ja niiden toiminnan kehittymisellä ei ole vaikutusta sellaisenaan työntekijän toimintaan tai käyttäytymiseen tai satunnaiseen tapaturmaan. Tämän tutkimuksen tarkoituksena on kuvata näiden osalta vain yleinen periaate, joka liittyy hyvään tietoturvajohtamiseen.

Työn edistyessä tutkimuksen rajaavana tekijänä on ollut empiriatutkimuksessa hankitun informaation niukkuus. Toisin sanoen tutkimukseen osallistunut yritys ei ole ollut halukas antamaan kaikkia

haluttuja, erityisesti taloudellisia tai henkisiä, tietoja tapauksen seurauksista, koska ne ovat hyvin henkilökohtaisia ja/tai arkaluonteisia. Osasyynä haluttomuuteen antaa tietoja on varmasti myös se, että tapahtuneesta on kulunut niin paljon aikaa, että luonnollinen yksityiskohtien unohtaminen on ymmärrettävää.

Tämän tutkimuksen kohdetoimialaa on yleisesti tutkittu sangen vähän ja muun muassa Tilastokeskuksen antamien tietojen mukaan prosessoitavaa tietoa tämän tutkimuksen tarkoituksiin ei ole saatavana, mikä puolestaan lisää tehdyn haastattelututkimuksen painoarvoa.

1.4 Keskeiset käsitteet

Tietoturvallisuudella tarkoitetaan tässä tutkimuksessa tietojen, järjestelmien ja palvelujen suojaamista sekä normaali- että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturvallisuus rakentuu tiedon kolmen ominaisuuden – luottamuksellisuuden, eheyden ja käytettävyyden – turvaamisesta. Tässä tutkimuksessa tietoturvallisuuden käsite on jaettu ulkoiseen ja sisäiseen tietoturvallisuuteen.

Sisäisellä tietoturvalla tarkoitetaan tässä tutkimuksessa ensisijaisesti yrityksen henkilökunnan tietoturvallisuuskäyttäytymistä yrityksen toimitiloissa tai etäkäyttönä yrityksen laitteilla ja ohjelmilla. Lisäksi ne henkilöt, joilla on perusteltu syy tai mahdollisuus päästä yrityksen tiloihin, kuuluvat sisäisen tietoturvan piiriin. Määritelmään kuuluu osana fyysinen turvallisuus ja sen suojaaminen. Fyysisen turvallisuuden suojaamisen osalta määritelmään kuuluvat tiedon luottamuksellisuus, eheys, käytettävyys, saatavuus, todennus, pääsynvalvonta ja kiistämättömyys. Ulkoisella tietoturvalla käsitetään tässä tutkimuksessa kaikki se muu, joka kuuluu yrityksen tietoturvaan ja jää edellisen, sisäisen tietoturvan, määritelmän ulkopuolelle.

EU:n komissio[EU] määrittelee pk-yritykset seuraavasti:

1. Mikroyritysten sekä pienten ja keskisuurten yritysten (pk-yritysten) luokka koostuu yrityksistä, joiden palveluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma on enintään 43 miljoonaa euroa.

2. Pk-yritysten luokassa pieni yritys määritellään yritykseksi, jonka palveluksessa on vähemmän kuin 50 työntekijää ja jonka vuosiliikevaihto tai taseen loppusumma on enintään 10 miljoonaa euroa.

3. Pk-yritysten luokassa mikroyritys määritellään yritykseksi, jonka palveluksessa on vähemmän kuin 10 työntekijää ja jonka vuosiliikevaihto tai taseen loppusumma on enintään 2 miljoonaa euroa.

Tutkittava case-yritys on siis pieni pk-yritys, ja tässä tutkimuksessa siitä käytetään termiä pk-yritys tai yritys.

Tietoturvajohtamisella tarkoitetaan tässä tutkimuksessa sisäisen tietoturvan ja siihen liittyvien asioiden kokonaisvaltaista hallitsemista. Samalla tarkoitetaan, että tietoturvajohtaminen on osa koko yrityksen johtamista.

1.5 Tutkimusmetodit

Tutkimus vaatii hyvin spesifioituja tietoja, koska sen aihe on tarkastellun kirjallisuuden perusteella melko harvinainen. Vastaavanlaisia tapauksia ei tietojeni mukaan ainakaan lähimenneisyydessä ole käsitelty julkisessa mediassa. Mahdollista on tietenkin se, että tällaista sisäisen tietoturvan

pettämistä tapahtuu laajasti, mutta siitä ei kehdata puhua julkisesti tai siitä ei yrityksissä edes tiedetä. Käytettävissä olevien resurssien puitteissa tämän tutkimuksen tutkimusmenetelmäksi on valittu case-tutkimus.

Tämän tutkimuksen tarkastelun kohteena on etelä-pohjanmaalainen kansainvälinen pk-yritys ja sen sisäisen tietoturvan kehitys vuosina 1996–2007. Tutkimuksen case-osan tarkoituksena on paitsi todentaa ja verrata teoreettista viitekehystä sekä pk-yrityksessä tapahtunutta sisäisen tietoturvan pettämistä, myös kuvata sen kehittämistä ja kehitystä tapahtuman jälkeen. Viitekehys on koottu pääsääntöisesti kotimaisesta kirjallisuudesta ja artikkeleista. Tämä kotimaisten lähteiden käyttäminen on ollut tietoinen valinta juuri siksi, että tutkielman tarkoituksena on osaksi ollut selvittää sitä, mitä asioita suomalaisessa tutkimuksessa on tiedostettu ja todennettu. Tällä on mielestäni merkittävä vaikutus juuri pk-yritysten toimintatapoihin verrattuna suomalaiseen kansainvälistä liiketoimintaa harjoittavaan suuryritykseen, koska taloudelliset resurssit ja monikansallisen tietotaidon hankkimisen edellytykset ovat suuryrityksissä aivan eri luokkaa.

1.5.1 Case-tutkimus

Case-tutkimus eli tapaustutkimus ei menetelmänä ole sidottu mihinkään tarkasti määriteltyihin tiedonkeruu-, analysointi- tai johtopäätöksentekomenetelmiin. Pääsääntöisesti tapaustutkimuksen tiedonkeruumenetelmät voidaan jakaa kliinisiin, ei-strukturoituihin ja analyyttisesti strukturoituihin menetelmiin. Tutkimustavan ongelmasta riippuu, mikä menetelmä valitaan ja usein on mahdollista käyttää useaa menetelmää rinnakkain. [Eriksson ja Koistinen, 2005; Luentomoniste, 2004.]

Kaikki yrityksen sisäisen tietoturvan pettämistapaukset ja niihin liittyvät tekijät ovat erilaisia tapahtumia riippuen yrityksen sisäisistä tekijöistä ja sen ulkopuolella vallitsevista ympäristötekijöistä. Tällöin tapaustutkimuksen

valitseminen tutkimusmenetelmäksi on perusteltua, koska sen avulla voidaan katsoa saatavan riittävän yksityiskohtaista informaatiota tapahtumien kulusta ja siihen vaikuttavista ympäristötekijöistä. [Eriksson ja Koistinen, 2005.]

Tässä tutkimuksessa tiedonkeruumenetelmiä ovat case-yritystä koskeva kirjallinen materiaali: lähinnä oikeudessa esitetty todistusaineisto, lehtileikkeet, nauhoitettu haastattelu ja suora havainnointi. Haastattelu on analyyttisesti strukturoitu, ja siihen on valittu henkilö, jolla on mahdollisimman hyvä kokonaiskuva ja strategista tietämystä yrityksen tietoturvasta.

Tapaustutkimuksessa eritellään usein tyyppejä, jotka määrittyvät sen mukaan, mitä tutkimuksella tavoitellaan tai mikä sen kontrastisuhde on case-yrityksen ja tutkimuksen välillä. Perren ja Ram [2004] ovat jakaneet tutkimustyypit neljään eri kategoriaan, ja ne ovat soveltuvia juuri pienyritysympäristöön:

- Itsessään arvokas, välillinen ja kollektiivinen tapaustutkimus
- Kuvaileva tapaustutkimus
- Selittävä tapaustutkimus
- Eksploratiivinen ja uutta teoriaa kehittävä tapaustutkimus.

Tämä kategorisointi perustuu tiedon ja tietämisen tapoihin eli epistemologiaan liittyvien oletusten perusteisiin [Perren, 2004].

Lisäksi tapaustutkimus on usein jaoteltu intensiiviseen ja ekstensiiviseen, jotka liittyvät hyvin vahvasti edellä mainittuihin kategorioihin. Kategorisointi korostaa kutakin kohtaa, etenkin klassisen ja uudemman tapaustutkimuksen suuntausten eroja. Klassisessa, intensiivisessä tapaustutkimuksessa on ideana ainutlaatuisen tapauksen selvittäminen hyvin tarkasti ja monipuolisesti. Siinä ei ole oleellista löytää tapausta koskevia yleistyksiä, vaan saada mahdollisimman tarkka kuvaus siitä, mitä juuri valitulla tapauksella halutaan kertoa. Ekstensiivinen, uudemman suuntauksen tapaustutkimus on monelta osin

vastakohtainen intensiivisen tapaustutkimuksen kanssa. Sen tarkoituksena on löytää uudenlaisia ilmiöitä ja tehdä tapauksista yhteneviä yleistyksiä. Teoriaa luovana tyylisuuntauksena siinä vertaillaan eri tapauksia aiempiin teorioihin yrittäen löytää uusia oletuksia ja yleistyksiä. [Eriksson ja Koistinen, 2005.]

Tässä tutkimuksessa tutkimustavaksi on valittu kuvaileva tapaustutkimus. Sen tarkoituksena on olla hyvin tarkka ja yksityiskohtainen case-yrityksen tapahtumien kuvaus. Sen ominaispiirteenä on ”hyvän tarinan” tuottaminen. Tässä tutkimuksessa on tapahtumien kulku, yrityksen sen hetkisen sisäisen tietoturvan tilanteen kuvaus, oikeusprosessien tuomiolauselmat ja nykypäivän tietoturvakäsikirjan kuvaus soveltuvin osin kuvattu mahdollisimman tarkasti ja yksityiskohtaisesti. Lisäksi yleisesti ajatellaan, että hyvän tarinan kertominen on itsessään teoriaa luovaa, mikä perustuu siihen näkemykseen, että inhimillisen toiminnan ominaisuus on etsiä asioille yhteyksiä, muodostaa palasista kokonaisuuksia ja tätä kautta ymmärtää maailmaa [Bruner, 1991]. Tämä tutkimus voidaan luokitella myös intensiiviseksi tapaustutkimukseksi, joka tutkimustyyppinä toimii lähinnä kuvailevaa tapaustutkimusta korostavana. Sen tarkoitus on ohjata, vahvistaa ja tukea tutkimusta juuri siihen suuntaan, että tutkimuksen tapahtumien kuvaus olisi mahdollisimman autenttinen ja validi.

1.5.2 Tutkimuksen luotettavuuden arviointi

Tutkimuksen luotettavuutta arvioitaessa keskeisiä käsitteitä ovat reliabiliteetti ja validiteetti. Reliabiliteetilla tarkoitetaan tutkimustulosten ja väitteiden luotettavuutta: johtuuko tutkimustulos vain sattumasta vai kyetäänkö tulokset toistamaan riippumattomasti toisistaan? Toistaminen voi tapahtua joko arvioitsijoiden välillä tai tutkimuskertojen välillä, toisin sanoen tutkimustarkkuus, luotettavuus. Jos esimerkiksi tutkittavilla yrityksillä on tuottojen ja menojen jaksottamisessa eri perusteet, epäluotettava

kannattavuusmittari antaa tuolloin yrityksille toisistaan poikkeavat kannattavuudet, eikä mittausperuste ei ole luottava. [Luentomoniste, 2004.]

Validiteetilla puolestaan tarkoitetaan tutkimuksen tai väitteen pätevyyttä eli sitä, oikeuttavatko käytetty aineisto tutkimusmenetelmät ja saadut tulokset esitetyt väitteet. Validiteetin arvioimiseksi on aina määriteltävä mittauksen kohde. Jos pyritään mittaamaan sisäisen tietoturvan luotettavuutta, on määriteltävä mitä sisäisellä tietoturvalla tarkoitetaan. [Luentomoniste, 2004.]

Yleisesti on esitetty, että tapaustutkimus ei anna yhtä valideja tutkimustuloksia kuin muut tutkimusmenetelmät. Keskeinen väittämä onkin, että yhdestä tapauksesta ei voi tehdä muita koskevia päätelmiä. Epäilemättä reliabiliteetti ja validiteetti ovat yksittäistapauksessa paljon heikompia kuin tilastollisia kontrollimenetelmiä käytettäessä. Mitä suurempi joukko tapauksia tilastollisessa tutkimuksessa on, sitä luotettavampana ja vähemmän sattumanvaraisempana sitä pidetään.

Tässä tutkimuksessa on sen reliabiliteettia pyritty parantamaan haastattelun tallentamisella nauhalle, josta sen purkaminen on pystytty suorittamaan tarkasti. Reliabiliteettia lisää myös se, että tutkitusta aiheesta on oikeusprosessien aikana kerätty kattava määrä erilaisia dokumentteja. Reliabiliteettia heikentävänä tekijänä voidaan pitää ajallista etäisyyttä tutkittavaan tapahtumaan.

Tässä tutkimuksessa on sen validiteettia pyritty parantamaan lähinnä haastattelukysymysten kytkemisellä mahdollisimman tiiviisti esitettyyn teoreettiseen viitekehykseen. Validiteettia lisää myös se, että samankaltaisia – vaikkakin edes vähän samankaltaisia – tapauksia on etsitty kotimaisesta mediasta ja tutkittu. Validiteettia puolestaan heikentää se, että tutkittava yritys lähti mukaan sillä varauksella, että kaikkiin sisäisen tietoturvan ratkaisuihin ei tarvitse yksityiskohtaisesti vastata.

2. Sisäinen tietoturva

Tässä luvussa määritellään ja jäsennetään ne asiat, jotka kuuluvat sisäiseen tietoturvaan. Asiaa tarkastellaan yritystoiminnan näkökulmasta ja yritetään löytää ne asiat, jotka yritystä perustettaessa tai sisäistä tietoturvaa kehitettäessä tulisi ottaa huomioon. Asioita ei ole tässä yhteydessä asetettu tärkeysjärjestykseen, vaan ne on esitetty yhtenevällä prioriteetilla: asioita on tarkasteltu suomalaisen lainsäädännön ja toimintatapojen näkökulmasta.

2.1 Tietoturvapolitiikka, -suunnitelma ja -ohjeistus

Yritystoimintaa perustettaessa olisi ensimmäisten toimien joukossa syytä luoda tietoturvasuunnitelma, joka on suunnitelma perusturvallisuuden toteuttamisesta ja ylläpitämisestä normaalioloissa. Suunnitelmassa esitetään organisaation tieto-turvallisuustoiminnan tavoitteet, hallinto, tehtävät ja menettelyt sekä osoitetaan elintärkeät tietojärjestelmät ja määritellään niiden toipumisen edellyttämät toimet [Vahti 4/2003].

Sisäinen tietoturvasuunnitelma on yrityksen ylimmän johdon ja muutaman avainhenkilön luettavissa. Sitä tulee säilyttää hyvin suojatussa tilassa, ja sen päivittäminen ajan tasalle säännöllisin väliajoin on tärkeää. Suunnitelmaa luotaessa on hyvä muistaa tietoturvan perusosa-alueet tai – tavoitteet, jotka ovat:

- luottamuksellisuus (C)
- eheys (I)
- saatavuus (A)
- todennus
- pääsynvalvonta
- kiistämättömyys.

Kolme ensimmäistä osa-aluetta muodostavat helpon muistisäännön CIA (englanniksi Confidentiality-Integrity-Availability), joka muodostaa suunnitelman peruskehyksen. Kolme muuta osa-aluetta ovat lisääviä tai edellisiä täydentäviä, mutta samalla hyvin tärkeitä osa-alueita. [Järvinen, 2002; Miettinen, 1999.]

Sisäistä tietoturvaa luotaessa luottamuksellisuudella tarkoitetaan sitä, että yrityksen tietoja pääsevät lukemaan vain ne työntekijät, joilla siihen on oikeus. Tämän oikeuden on usein määritellyt yrittäjä, ja hänellä on vastuu ja tietämys siitä, kuka tietoa työtehtävissään tarvitsee. Todennusta tarvitaan, koska muuten järjestelmän on mahdoton tunnistaa eri käyttäjät. Lisäksi tiedon tulee olla salattu siltä varalta, että esimerkiksi tietokone joutuu fyysisesti vääriin käsiin tai yrityksen työntekijä asentaa verkkoon vakoiluohjelman. Tällöin tietoa ei saa auki ilman oikeaa salasanaa. Eheydellä tässä yhteydessä tarkoitetaan sitä, että tiedostot ovat fyysisesti ehjiä. Tämän todentaminen ja varmistaminen on melko hankalaa, koska tiedosto ei rikkoonnuttuaan ilmoita mitään, vaan rikkoontumisen huomaa vasta silloin, kun tiedostoa tarvitaan. Varmuuskopiointi on hyvä keino löytää tiedostosta ehjä versio, mutta sen löytäminen voi vaatia varmuuskopioiden säilyttämistä pitkän ajan. Laadukkaiden komponenttien käyttäminen ja ohjeistus siitä, että kriittisimmät tiedot tulisi tallentaa aina kahteen eri paikkaan, ovat hyviä keinoja parantaa eheyttä. Tietojen saatavuudella sisäisessä tietoturvallisuudessa tarkoitetaan tietojärjestelmien ja ohjelmien toimivuutta. Tietojärjestelmät on hyvä ajoittaa niin, että ne toimivat työntekijöille työaikana. Muuten ne ovat pois käytöstä, ja aikaa hyödynnetään tiedostojen varmistukseen. Saatavuus tarkoittaa myös sitä, että työntekijällä on oikeanlaiset ohjelmat työnsä suorittamiseen. Ylimääräisten ohjelmien asentaminen on riski. Ongelmaksi voi muodostua tilanne, jossa työntekijä tarvitsee arkistoitua tietoa, joka on tuotettu 10–15 vuotta sitten. Ohjelmisto ja laitteisto eivät välttämättä enää kohtaa, tai tarvittavaa ohjelmaa ei enää ole yrityksessä olemassa. [Järvinen, 2002; Valtionvarainministeriö, 1992.]

Luottamuksellinen ja työntekijöiden oikeisiin tietoihin pääseminen edellyttää todentamista. Tämä tarkoittaa sitä, että jokaiselle työntekijälle on luotava henkilökohtainen käyttäjätunnus. Käyttäjätunnus on aina syytä suojata salasanalla. Todentaminen sisäisissä järjestelmissä on sinänsä haastavaa. Liikkuminen eri tiedostojen, hakemistojen, palvelimien tai ohjelmistojen välillä työpäivän aikana on hyvin arkipäiväinen ilmiö, ja pääsynvalvonta liittyy tähän hyvin olennaisesti. Yrityksen on tarkasti määriteltävä kenellä on oikeus liikkua mihinkin paikkaa. Pääsynvalvonta on hyvin usein ohjelma- tai tiedostokohtaista. Yleistä on myös se, että työntekijän pääsy sellaisiin palvelimiin, joista tämä ei tarvitse mitään tietoa, rajoitetaan kokonaan. Pääsynvalvontaa kuuluu oleellisesti myös käytön seuranta. Järjestelmä pitää kirjaa siitä, kuka ja koska käyttää tiedostoja tai ohjelmaa [Mäntylä ja Kajava, 1996]. Kiistettävyyteen ei sinänsä liity sisäisen tietoturvan kysymyksiä. Sen tarve tulee esiin lähinnä sähköisessä kaupankäynnissä. Näin ollen sitä ei käsitellä tarkemmin tässä tutkimuksessa. [Järvinen, 2002.]

Jokaisessa yrityksessä tulisi olla tietoturvapolitiikka-käsikirja, joka on jokaisen työntekijän saatavilla. Lisäksi siihen tutustuminen tulisi olla pakollista työsuhteen alkaessa. Tietoturvapolitiikan käsikirja on organisaation johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta. Tietoturvapolitiikka tai -strategia on kiinteä osa organisaation toiminta- ja tietohallintopolitiikkaa tai -strategiaa [Vahti 4/2003]. Tietoturvapolitiikan käsikirjassa käsitellään muun muassa, miksi sisäisissä ratkaisuissa on päädytty tiettyihin ratkaisuihin ja miksi se on yritykselle tärkeää. Käsikirjassa on selvitetty tietoturvallisuuteen liittyvät vastuut ja työntekijöiden valvontaan liittyvät keinot ja syyt. Tietoturvapolitiikkaan on myös monissa tapauksissa kirjattu työntekijöiden tietoturvallisuuden koulutustarpeet ja taitotiedon saattamisesta yrityksen vaatimalle tasolle. Yrityksen tietoturvan sopimuskäytäntö määritellään käsikirjassa. Tärkeää onkin, että käsikirja pidetään ajan tasalla. Sen jatkuva tarkistaminen ja sen

saattaminen nykypäivän säädösten ja asetusten tasalle on hyvin ratkaisevaa sen toimivuuden ja hyödyllisyyden kannalta. Käsikirjaa luotaessa on tärkeää kuitenkin muistaa, että sen tarkoitus on olla yrityksen toimintaa tukeva, ei sitä haittaava tai hidastava. [Laaksonen et al., 2006.]

2.2 Fyysinen suojaaminen

Fyysisellä turvallisuudella taataan organisaatiolle häiriötön ja turvallinen toimintaympäristö [Laaksonen et al., 2006]. Sillä tarkoitetaan niitä kaikkia toimintoja tai asioita, joihin ei järjestelmän teknisillä suojauksilla tai ratkaisulla ole vaikutusta. Fyysinen tietoturvallisuus määritellään valtiohallinnon tietoturvakäsitteistön [Vahti 4/2003] mukaan henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaamiseksi 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.

2.2.1 Palo-, vesi- ja ilmastointiturvallisuus

Tietokoneita ja tietojärjestelmiä on turha suojata monenlaisilla viruksentorjuntaohjelmilla ja palomuureilla ulkopuolisilta hyökkäyksiltä, jos fyysinen turvallisuus ei ole kunnossa. Fyysisen turvallisuuden uhkatekijät ovat usein sattumanvaraisia, yrityksestä itsestään riippumattomia ja mahdottomia ennustaa. Fyysisen turvallisuuden uhkien riskiä voidaan kuitenkin pienentää suojaamalla toimitilat mahdollisimman hyvin ainakin seuraavilta asioilta [Laaksonen et al., 2006; Järvinen, 2002; Paavilainen, 1998]:

- varkaus; sarjanumero ja turvamerkintä
- tulipalo tai lämpötilan liiallinen kohoaminen
- vesivahinko ja kosteus

- sähköhäiriö
- pöly
- työntekijän inhimillinen virhe.

Kaikille näille fyysisille uhille on yhteistä, että tieto voidaan säilyttää oikeanlaisella varmuuskopioinnilla (ks. luku 2.4). Tulipalo-, vesi-, sähkö- ja ilmastointivahinkojen mahdollisuudelta on järkevää suojautua vakuutuksella. Onnettomuuden sattuessa yrityksellä on mahdollisuus saada kohtuullinen korvaus menetetystä omaisuudesta tai toimitilojen uudelleen rakentamiskustannuksista. Ongelmana on kuitenkin se, että vaikka vakuutus ja varmuuskopio palauttaisivat kaiken menetetyn, niin usein tällaisen vahingon seurauksena on toimintojen hetkellinen keskeytyminen. Toiminnan palauttaminen voi kestää vahingon laajuudesta riippuen useita kuukausia. Tähänkin on vakuutusyhtiöillä vakuutuksia [If], mutta siinä tapauksessa vakuutusyhtiö vaatii suojaamiselta korkeaa tasoa. Sammutusjärjestelmä ja muut sammuttamistarvikkeet on oltava asianmukaisessa tilassa. Tietokoneiden ja palvelimien sijoittamisessa on otettava huomioon, että tila on hyvin eristetty ja ilmastoitu. Myös kattoon rakennettu välipohja on hyvä keino estää vesivahinkoja. Kaikki tämä rakentaminen ja hankkiminen aiheuttaa yritykselle huomattavia kuluja, minkä vuoksi aloittavalla tai pienellä yrityksellä voi olla vaikeuksia löytää taloudellisia resursseja näihin toimenpiteisiin. [Laaksonen et al., 2006; Kainomaa, 1984.]

Pölyn muodostuminen on estettävissä säännöllisellä siivouksella ja pitämällä kaikki tilat vapaana kaikesta työhön liittymättömästä tavarasta, joka tuottaa pölyä. Laitteiden oikeanlainen sijoittaminen estää pölyn muodostamista ja ehkäisee vesivahinkojen syntymistä. Sähköhäiriö on seurauksena verkkovirrassa tapahtuneesta ylijännitteestä, jonka voi aiheuttaa esimerkiksi ukkonen. Ukkonen voi pahimmassa tapauksessa aiheuttaa jopa laiterikon tai verkkovirheen koko yrityksessä. Ukkoselta suojautuminen on helpoin hoitaa

USP-laitteilla eli ylijännitesuojalla tai isoissa yrityksissä varageneraattorilla. [Laaksonen et al., 2006; Paavilainen, 1998.]

Varkauksia vastaan ja vakuutusyhtiötä varten on hyvä kirjata kaikkien koneiden sarjanumerot ylös ja säilyttää ne hyvin suojatussa paikassa. Koneeseen näkyvälle paikalle laitettu turvamerkintä heikentää sen laitonta jälleenmyyntiä. Turvamerkintä on hyvä sijoittaa niin, että sen poistaminen tai tuhoaminen herättää muiden huomion. [Järvinen, 2002.]

2.2.2 Kulunvalvonta

Työntekijöiden ja vierailijoiden kulunvalvonta on jo siksi keskeisessä roolissa, että oikeudellinen todistettavuus lisääntyy huomattavasti ja parantaa näin huomattavasti yrityksen tilannetta mahdollisessa kiistatilanteessa. Valvomaton kulkeminen yrityksen tiloissa on aina riskitekijä. Ilman asianmukaista kulunvalvontaa monelta muulta sisäisen tietoturvan osalta poistuu merkitys. Jos yrityksen tiloissa pystyy liikkumaan ns. jälkiä jättämättä, yrityksen on mahdoton selvittää, kuka on aiheuttanut tietovuodon tai tietoriskin, vaikka itse toiminto tai tietomurto havaittaisiinkin. Paavilainen [1998] onkin määritellyt ei-toivotulle tai ulkopuoliselle tunkeutumiselle kolme erilaista varautumismenetelmää, joilla voidaan kulunvalvonnassa varautua:

1. Valtuutus (authorization) määrää, kenellä on oikeus käyttää tiloja tai järjestelmiä.
2. Tunnistus (identification) on toimintaa, jossa tarkistetaan kontrollikohteen identiteetti.
3. Kulun- ja yhteydenvalvonta (access control) on toimintaa, jossa varmistetaan, että ainoastaan valtuutetut henkilöt pääsevät kontrolloidulle alueelle.

Kulunvalvonnan ei usein tarvitse olla yrityksessä huonekohtainen. Riippuen toki tietojen ja toimintojen arkaluontoisuudesta kulunvalvonta voi olla hyvinkin vyöhyke- eli aluekohtaista. Yrityksen tilat voidaan luokitella kuten tietoaineisto sen kriittisyyden mukaan. Näin pystytään rajaamaan esim. palvelinhuoneeseen pääsevien joukko niin, että vain siellä työskentelevillä on oikeus sinne. Kulunvalvonnan keskeinen konkreettinen keino on oikeanlainen lukitseminen. Perinteisen lukot ja lukitusmenetelmät ovat jäämässä pois, ja tilalle ovat tulleet sähköiset lukitusjärjestelmät. Sähköisten lukkojen turvallisuus on perinteisiä lukkoja huomattavasti parempi, ja niiden avulla kulunvalvontaa pystytään hallitsemaan tarvittaessa vaikka yhdeltä tietokoneelta.

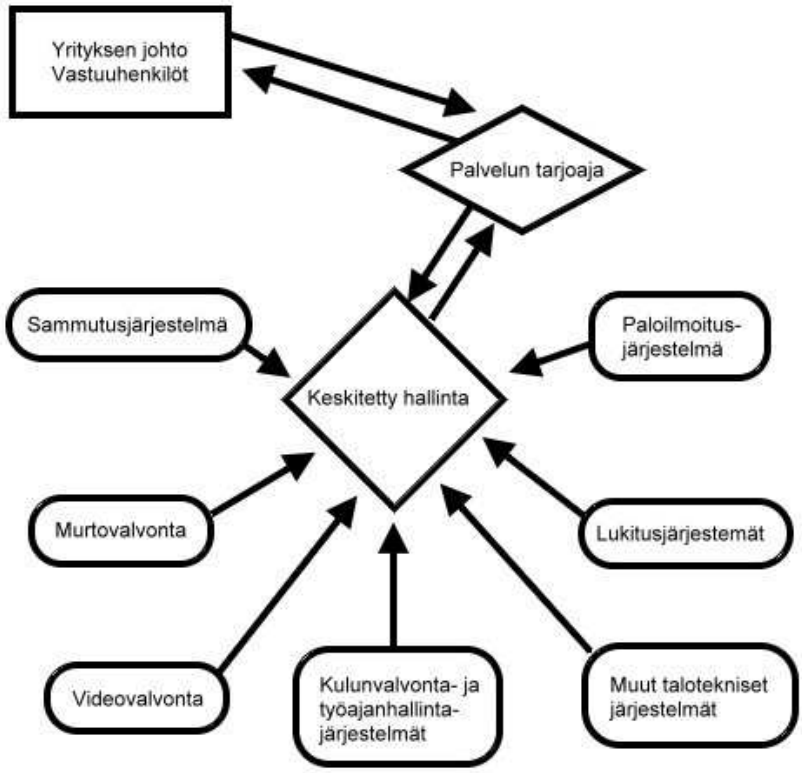
Henkilöiden tunnistamiseksi on useita eri vaihtoehtoisia ratkaisuja, joista varmin on biometriset tunnistuskeinot [Digitoday, 2007a]. Biometrinen tunnistus on ihmisen sähköistä tunnistusta jonkin fyysisen ominaisuuden perusteella. Tutuin esimerkki biometriasta on sormenjälkitunnistus, jossa tietokone tunnistaa ihmisen hänen sormenjälkensä perusteella. Muita biometrisen tunnistuksen menetelmiä ovat esimerkiksi kasvontunnistus, äänentunnistus ja silmän iiriksen tunnistus [Sisäasiainministeriö]. Perinteisempi tunnistamisen keino on henkilöiden välinen tunnistautuminen: esimerkiksi yrityksen eteisessä on vastaanottovirkailija, joka tuntee kaikki yrityksessä työskentelevät henkilöt ulkonäöltä. Jos tunnistautumista ei tapahdu, henkilön on todistettava henkilöllisyytensä virkailijalle. Sähköiset tunnistautumiset ovat nykypäivänä huomattavasti yleistyneet: toimikortit tai tunnusluvut tai niiden yhdistelmä ovat yleisimmin käytössä. Toimikortin suosiota on lisännyt siihen liitettävä ominaisuus, jolla yritys pystyy seuraamaan ja todentamaan työntekijän työajan esimerkiksi palkanmaksua varten. Toimikortin heikkoutena kuitenkin on, että se voi kadota tai se voidaan varastaa, jolloin kenellä tahansa on mahdollisuus liikkua yrityksen tiloissa toisen henkilön identiteetillä. Kuvalla ja/tai nimellä varustettu toimikortti on askel parempaan suuntaan, mutta se ei silti yllä

biometrisen tunnistamisen tasolle. Tunnusluvun yksi huono puoli on se, että sen voi unohtaa. Toinen tunnusluvun huono puoli on se, että jos se oman muistamisen helpottamiseksi kirjataan ylös sellaiseen paikkaan, jossa se on yleisesti luettavissa, se aiheuttaa tietoturvallisuusriskin. Tästä syystä turvallisin keino sähköisessä tunnistamissa on biometrisen tunnistautumisen ja salasanan yhdistelmä.

Kulunvalvonnan hyvänä apuna tai lisäominaisuutena toimii videovalvonta. Kaikki yrityksen kriittisissä paikoissa liikkuminen tallentuu videolle ja sen avulla henkilö voidaan tarvittaessa tunnistaa toimikortin väärinkäytöksen tai vastaavan sattuessa. Videolle tallentuvan kulunvalvonnan hoitaa hyvin usein ulkopuolinen vartiointiyritys, ja palveluun liittyy usein myös muita palveluja. [Paavilainen, 1998; Securitas; ISS.]

2.2.3 Kokonaisvaltaiset turvallisuuspalvelut

Nykypäivän vartiointiliikkeistä on tullut yhä enenevässä määrin kokonaisvaltaisia turvallisuuspalveluiden tarjoajia. Saatavilla on jopa myös ilmaista tietoturvallisuuskonsultointiapua [Digitoday, 2007d]. Yrityksen on mahdollista valita ja koota itselleen sopiva paketti melkeinpä kaikista mahdollisista fyysiseen tietoturvallisuuteen liittyvistä palveluista.



Kuva 2: Fyysisen tietoturvasuojaamisen palvelukokonaisuus.

Pakettiratkaisun suurimpana etuna onkin sen yhdenmukaisuus ja helppous. Yritystoiminnan arkaluontoisuuden, toiminnan suuruuden, henkilökunnan määrän ja toimitilojen sijainnin ja laajuuden perusteella yrityksen on mahdollista valita juuri sille sopiva kokonaisuus. Yrityksen on mahdollista keskittyä olennaisiin toimintoihin ja jättää suurin osa fyysisen tietoturvan päivittäisistä asioista alan ammattilaisille. [Securitas; ISS.]

2.3 Käyttäjätunnukset ja salasanat

Valtiohallinnon tietoturvakäsitteistön [Vahti 4/2003] mukaan käyttäjätunnus tarkoittaa käyttäjän sisäänkirjautumisen yhteydessä ilmoittamaa ja hänet yksilöivää tunnistetta. Käyttäjätunnus luodaan henkilölle tämän aloittaessa työnsä yrityksessä, ja se tuhotaan, kun työsuhde loppuu. Käyttäjätunnuksen

keskeisin tehtävä tunnistautumisen lisäksi on käyttöoikeuksien ja pääsynvalvonnan hallinta. Tämä on hyvin tärkeää, kun työntekijä liikkuu yrityksen sisäisessä verkossa ja osin sisäisen verkon kautta esimerkiksi Internetiin [Kajava ja Remes, 2000]. Käyttäjätunnuksen avulla yrityksen on siis mahdollisuus määritellä jokaiselle työntekijälle ne oikeudet, joita tämän työtehtävät vaativat.

Käyttäjätunnus toimii tarvittaessa tietojärjestelmissä sähköisenä sormenjälkenä. Yrityksellä on mahdollisuus vaikkapa dokumenttitasolla määritellä loki. Lokilla tarkoitetaan tiedostoa, johon tehdään aikajärjestyksessä merkinnät tapahtumista ja niiden aiheuttajista. Loki kerätään yleensä automaattisesti ja samaan järjestelmään liittyviä lokeja voi olla useita, esimerkiksi vikaloki ja laskutusloki [Vahti 4/2003]. Näin ollen tarpeen tullessa on mahdollista selvittää esimerkiksi, kuka on tehnyt järjestelmään muutoksia, ketkä ovat käyneet lukemassa ko. tiedoston, tai kuka on kopioinut ko. tiedostot omaan käyttöönsä. Lokitiedostot ovat melkein aina piilotettuja normaalikäyttäjiltä ja muutosten tekeminen tai niiden tuhoaminen on mahdotonta.

Käyttäjätunnukset voidaan karkeasti jakaa käyttöoikeuksien perusteella järjestelmän käyttöön tarkoitettuihin tunnuksiin ja ylläpitotunnuksiin. Järjestelmän käyttöön tarkoitetut tunnukset ovat melkeinpä yrityksen jokaisella työntekijällä ja johtajalla. Eri henkilöiden välillä toki on järjestelmä-, ohjelmisto- ja dokumenttikohtaisia eroja, jotka muuttuvat aina työtehtävien ja niiden vastuullisuuden mukaan, mutta käyttäjätunnuksen perusluonne on aina sama. Toinen käyttäjätunnusryhmä on ylläpitotunnukset. Ne ovat yrityksessä yleensä vain muutamalla avainhenkilöllä. Nämä henkilöt ovat yleensä tietohallinnon työntekijöitä tai yrityksen tietoturvasta vastaavia henkilöitä. Heillä on kokonaisvaltainen kuva yrityksen tietoteknisistä ja tietostrategisista ratkaisuista. Käyttäjätunnuksen luominen uudelle henkilölle on aina sellaisen henkilön tehtävä, jolla on ylläpitotunnus. Ilmoitus uuden tunnuksen luomisesta

tulee aina tehdä kirjallisesti, ja siinä on oltava esimerkiksi esimiehen allekirjoitus. Hyväksytty lomake on aina standardimuotoinen, ja se tulee säilyttää niin kauan kun työntekijä on yrityksen palveluksessa. Ylläpitotunnukset voivat olla myös ohjelmisto- tai järjestelmäkohtaisia. Varsinkin tässä tapauksessa ylläpitotunnuksen suojaaminen ja suojeleminen on ensiarvoista, sillä nämä tunnukset eivät ole kenenkään henkilön nimellä, ja tunnistaminen voi sen vuoksi olla mahdotonta. Yleensäkin ylläpitotunnukset ovat suuremman suojauksen ja salauksen tarpeessa, koska niiden joutuminen vääriin käsiin yleensä mahdollistaa vapaan liikkumisen yrityksen koko tietoverkossa.

Salasana on jokaiseen käyttäjätunnukseen liittyvä yksityinen, käyttäjän tiedossa oleva merkkijono. Tunnusta luotaessa se on ylläpidon kanssa ennalta sovittu sana tai numerosarja, mutta käyttäjän ensimmäisen sisäänkirjautumisen yhteydessä järjestelmä vaatii sen vaihtamista.

Salasanoja luotaessa on hyvä muistaa tiettyjä tietoturvallisuuteen liittyviä perussääntöjä. Salasanan yksityisyyden varmistamiseksi se on hyvä vaihtaa 3–4 kuukauden välein. Tämä on tärkeää siksi, että verkon vakoiluohjelmat voivat kerätä erilaisia kirjautumis- tai lokitietoja ja vaikka salasana näissä tiedoissa olisi suojattu, niin toistuvuus voi antaa salasanan selvittäjälle tarpeettoman edun. Vakoiluohjelmia voivat asentaa ulkopuoliset tahot, kuten siivousyrityksen työntekijät tai oman yrityksen epärehelliset työntekijät. Salasanan säilyttämistä työpisteessä tai missään muussa paikassa, jossa epärehellisellä tms. ihmisellä saattaa olla siihen pääsy, ei koskaan suositella. Salasanaa ei missään olosuhteessa tule luovuttaa kenellekään, vaikka kyseessä olisi esimerkiksi pitkäaikainen työkaveri. Salasanan luovuttaminen muodostaa tarpeettoman tietoturvariskin, jolla ei ole siihen rinnastettavaa hyötyä missään tilanteessa. Onkin suositeltavaa, että salasana olisi ainoastaan henkilön omassa päässä ja että sen kirjaamista minnekään vältetään. [Järvinen, 2002; Miettinen, 1999.]

Salasanan muodostaminen ei ole helppoa. Sen keksiminen sellaiseksi, että se olisi helppo muistaa, mutta samalla se olisi muille mahdollisimman vaikea arvattava, on haaste, johon työntekijät tarvitsevat apua ja ohjeistusta. Yrityksille salasanoja hallinnoivat ohjelmat ovat kehittyneet, ja ne itsessään tekevät perustarkistuksia ennen kuin ne hyväksyvät käyttäjän salasanan. Salasanoja muodostettaessa ja niitä käytettäessä onkin hyvä muistaa Juha E. Miettisen [1999] luoma tarkistuslista:

- Tietojärjestelmien salasanat ovat henkilökohtaisia. Pidä ne omana tietonasi, äläkä kerro niistä kenellekään ulkopuoliselle.

- Käytä riittävän pitkiä salasanoja. Salasanan on oltava vähintään kahdeksan merkkiä pitkä, jotta sitä ei ole helppo arvata tai muuten selvittää.

- Käytä vaikeasti arvattavia salasanoja. Salasanan tulee muodostua kirjaimista, numeroista ja erikoismerkeistä, mikäli tietojärjestelmä tämän hyväksyy.

- Vaihda salasana riittävän usein. Sopiva vaihtoväli on muutaman kerran vuodessa. Jos epäilet salasanasi joutuneen ulkopuolisen haltuun, vaihda se välittömästi.

- Vältä salasanan kirjoittamista paperille. Jos tämä on aivan välttämätöntä, varastoi paperille kirjoittamasi salasanat sellaiseen lukittuun paikkaan, johon ulkopuoliset eivät pääse.

- Kun kirjaudut ensimmäistä kertaa sisään uuteen järjestelmään, vaihda käyttöösi annettu oletussalasana välittömästi.

- Jos järjestelmä mahdollistaa käyttäjätunnuksen ja/tai salasanan varastoimisen järjestelmän muistiin, älä käytä tätä mahdollisuutta. Järjestelmän muistiin tallennetun käyttäjätunnuksen ja salasanan avulla kuka tahansa voi kirjautua sisään järjestelmään sinun käyttöoikeuksillasi.

- Jos käytät järjestelmää vieraan tietokonelaitteen kautta, varmistu, että kyseinen järjestelmä ei varastoi salasanaasi laitteen muistiin.

- Kun kirjoitat salasanaa, huolehdi siitä, että kukaan sivullinen ei näe sitä.

Muistilista on hyvä kirjata yrityksen tietoturvapolitiikkaan, josta se on kaikkien työntekijöiden luettavissa. Uudet työntekijät on aina hyvä velvoittaa lukemaan salasanaa koskeva ohjeistus tietoturvallisuuden takaamiseksi.

2.4 Varmuuskopiointi

Varmuuskopio on taltion, tiedoston tai ohjelman kopio, joka on tarkoitettu käytettäväksi, jos alkuperäinen menetetään vian tai vahingon takia [Vahti 4/2003]. Varmuuskopiointi on keino varmistaa, että varkauden, vahingon tai onnettomuuden sattuessa tiedoista ja ohjelmista on olemassa kopio. Sen tehtävänä on säilyttää tietoja ja ohjelmia useammassa kuin yhdessä paikassa ja useammalla kuin yhdellä tavalla. Varmuuskopiointiin ei ole olemassa

universaalia sääntöä, vaan se riippuu siitä, kuinka vitaalia tai arkaluontoista tieto on. Kun ollaan tekemisissä esimerkiksi ihmisten henkilötietojen kanssa, varmuuskopiointi on lainsäädännössä määriteltyä. Jo useammin kuin päivittäin tapahtuvaa varmuuskopiointia tarvitaan esimerkiksi pankkialalla, koska kyseessä on toisen omaisuuden säilyttäminen ja sen todentaminen ilman varmuuskopiota on mahdotonta. Toki tällaisissa tapauksissa rinnakkaisia järjestelmiä on olemassa, mutta kaikkein viimeisimpänä keinona pitää olla eri paikassa säilytetty ja ajan tasalla oleva varmuuskopiointi [Digitoday, 2007b]. [Miettinen, 1999.]

Varmuuskopiointi on hyvin usein automatisoitu. Se ei vaadi käyttäjän jatkuvia toimia, vaan se toimii annettujen speksien perusteella automaattisesti ja vaatii käyttäjän toimia vain virhetilanteissa. Jos varmuuskopiointi tapahtuu esimerkiksi CD-levylle, käyttäjän tehtäväksi jää vain levyn oikeanlainen säilyttäminen. Paavilaisen [1998] mukaan varmuuskopiointi voidaan jakaa kuuteen eri varmuusmenetelmään:

- täydellinen varmuuskopiointi
- kasvavan vedostuksen menetelmä
- useiden versioiden menetelmä
- varovaisen korvaamisen menetelmä
- differentiaali tiedostoista
- pelastusohjelma.

Täydellisessä varmuuskopioinnissa otetaan kaikista tiedostoista kokonaisuudessaan kopiot. Tämä menetelmä vaatii suurta tallennuskapasiteettia, ja sitä ei käytetä yrityksissä, joissa on monta erillistä tietokantaa tai kannat ovat itsessänsä suuria. Kasvavan vedosten menetelmässä toimitaan aluksi samoin kuin edellisessä, mutta sen jälkeen varmuuskopiosta poistetaan ne tiedostot, jotka eivät ole muuttuneet edelliseen versioon

verrattuna. Tämä on hyvä menetelmä juuri isoissa tietokannoissa. Useiden versioiden menetelmässä tietokannasta on useita yhtäaikaisia varmuuskopioita. Uutta kopiota ottaessaan se päivittyy ensin yhteen paikkaan täydellisesti ja siirtyy vasta onnistuneen kopioinnin jälkeen seuraavaan paikkaa. Periaatteessa tämä on sama asia kuin jatkuva varmuuskopiointi eli peilaus. Tämä on hyvä menetelmä muun muassa pankkialalla. Virhetilanteissa on tärkeä selvittää kopioiden virheettömyys. Varovaisen korvaamisen menetelmässä päivityksiä ei tehdä suoraan tietokantaan vaan tietokannan tai sen osan kopioon, ja kun kaikki tarvittavat päivitykset on tehty, kopio korvaa varsinaisen varmuuskopion. Differentiaalin ottaminen tiedostoista tarkoittaa sitä, että kopio tehdään työtiedostoihin ja ne yhdistetään aika ajoin varsinaiseen kantaan. Viimeisenä menetelmänä on pelastusohjelman toteuttaminen, ja sitä käytetään vasta silloin kun muut toipumiskeinot eivät auta. Toipumisohjelman käyttäminen vaatii tietokannan tai järjestelmävastaavan manuaalisia toimenpiteitä ja hyvää ammattitaitoa.

Monien vaihtoehtojen johdosta yrityksen on mahdollista valita itselleen sopiva ja toimintansa tarpeisiin suhteutettu järkevä varmuuskopiointimenetelmä. Kuten jo aiemmin on mainittu, varmuuskopio on ainoa keino palauttaa tiedot vakavan onnettomuuden tai muun vastaavan vahingon jälkeen. Varmuuskopiot sisältävät sellaista yrityksen tietoa, jonka arvo ei ole taloudellisesti mitattavissa, ja jonka menettämistä ei pystytä vakuutuksilla kattamaan.

2.5 Henkilöstöturvallisuus

Henkilöstöturvallisuuden ja henkilöstön tietoturvariskien hallintaa voidaan kehittää muun muassa toimenkuvien, käyttöoikeuksien ja koulutuksen avulla [Paavilainen, 1998]. Henkilöstöturvallisuus on yksi yritysturvallisuuden monista itsenäisistä osa-alueista. Sillä on kuitenkin monia yhtymäkohtia

tietoturvallisuuteen. Tässä yhteydessä henkilöstöturvallisuudella tarkoitetaan tietoturvallisuuden osa-aluetta, jossa tarkastellaan yrityksen tietojen ja tietojenkäsittelyn suojaamista ihmisten tahallisilta tai tahattomilta uhilta sekä ihmisten toimintaa tietoturvan varmistamiseksi. [Miettinen, 1999, Kajava ja Leiwo, 1994.]

2.5.1 Henkilöstön tietoturvakouluttaminen

Koulutuksen tavoitteena on tuoda henkilöstön tietoon se, millä tavalla yritys näkee tietoturvallisuuden ja miten se motivoi työntekijöitään työskentelemään tehokkaasti yrityksen toiminnan edistämiseksi. Tehokkaan koulutuksen tulee olla jatkuvaa ja laadullista siinä mielessä, kun se koskettaa työntekijän omaa työnkuvaa ja siihen liittyvää tietoturvaa. Koulutuksen tehokkuus riippuu siitä, kuinka hyvin henkilöstö on motivoitunut [ITviikko, 2007a]. Motivaatiota voi olla kahdenlaista: sisäistä ja ulkoista [Laaksonen et al., 2006]. Sisäisellä motivaatiolla tarkoitetaan sitä, että työntekijällä on aito innostus tietotekniikkaa kohtaan ja harrastuneisuus alaa kohtaan on opittu ennen työsuhdetta. Tämän kaltainen motivaatio on yrittäjälle tärkeää, koska se yleensä tarttuu muihin työntekijöihin. Ulkoisella motivaatiolla tarkoitetaan sitä, että työntekijällä on luonnostaan kova kilpailuvietti, joka ilmenee työnpaikalla siten, että työntekijöiden keskinäinen kilpailu lisää tehokkuutta. Ulkoinen motivaatio usein tukee voimakkaasti sisäistä motivaatiota. [Laaksonen et al., 2006.]

Onnistuneen koulutuksen pitää olla myös vaihtelevaa, ja kouluttajan tulee olla sellainen, että työntekijä kokee, että koulutuksen tarkoitus on tukea ja vahvistaa opittuja taitoja tai tuoda täysin uutta tietoa alalta. Koulutus ei siis saa olla sellaista, että työntekijä kokee koulutuksen saman kertaamiseksi ja jankuttamiseksi. Esimiehen tai yrittäjän tulee olla vahvasti mukana

koulutustilauksissa, ja koulutuksen tulee olla kaikille mahdollista. [Laaksonen et al., 2006.]

2.5.2 Uuden työntekijän taustojen tarkistus

Uuden työntekijän palkkaamiseen liittyy aina tietoturvallisuusriski. Uuden työntekijän tullessa yritykseen, työntekijän taustat on aina tarkistettava. Taustojen tarkistus on yrityksen koosta riippumatta usein liian kevyttä ja yleisesti ei tiedosteta, mitä taustojen tarkistukseen kuuluu. [Miettinen et al., 2006.]

Ilmaisia tarkistuskeinoja on yleisten taustatietojen etsiminen. Helpoin tapa on etsiä tietoa Internetistä, jossa henkilön aikaisemmista tekemisistä on merkintöjä. Ansioluettelon tarkistaminen on myös tärkeää. Sen oikeellisuuden ja kerrottujen referenssien tarkistaminen konkreettisesti esimerkiksi puhelimitse auttaa työnantajaa saamaan muun muassa tietoa siitä, miten työntekijän aikaisempi työsuhde on alkanut ja miten työntekijä on hoitanut työnsä. Maksullinen keino selvittää työntekijän taustoja on luottotietojen tarkistaminen. Luottotietojen tarkistaminen on tärkeää etenkin silloin, kun henkilön työtehtävät liittyvät taloudellisiin asioihin. Toinen maksullinen keino selvittää työntekijän tausta on teettää suojelupoliisilla turvallisuusselvitys, jonka tekeminen pk-yrityksen rekrytointitilanteessa on kuitenkin hyvin harvinaista. [Laaksonen et al., 2006; Miettinen et al., 2006.]

2.5.3 Työsopimus ja työsuhteen loppuminen

Yrityksen ja työntekijän välisen työsopimuksen tulee aina olla kirjallinen. Siitä tulee minimissään ilmetä yrityksen ja työntekijän tiedot, työsopimuksen laatu, lyhyt kuvaus työtehtävästä ja palkanmaksun perusteet. Tietoturvallisuuteen liittyvissä työtehtävissä on työsopimukseen hyvin usein lisätty myös salassapitosopimus ja tarkennus immateriaalisten oikeuksien omistuksesta.

Mitä tarkemmin työsopimuksessa asioita, tehtäviä, toimenkuvia ja oikeuksia on määritelty, sitä vahvemmalla työnantaja on, jos kiistatilanteita syntyy ja asioita joudutaan käsittelemään jopa oikeudessa. [Miettinen et al., 2006; ITviikko, 2007b.]

Työsuhteen loppumiseen liittyvät asiat on järkevää selvittää työsopimuksessa. Tällöin työntekijä tietää jo työsuhdetta aloittaessaan, miten hänen tulee toimia työsuhteen loppuessa ja mihin hänen tulee sitoutua. Tästä keskeisenä esimerkkinä on käyttäjätunnuksen ja salasanan luovuttaminen työnantajalle. Samalla työnantaja sitoutuu tuhoamaan kaikki työntekijän henkilökohtaiset tiedot ja henkilötiedot. [Laaksonen et al., 2006.]

2.5.4 Alihankkijoiden työntekijät

Alihankkijoiden työntekijöillä tarkoitetaan sellaisia yrityksen tiloissa liikkuvia henkilöitä, jotka eivät ole suorassa työsopimussuhteessa yritykseen. Näiden henkilöiden kohdalla on kuitenkin syytä noudattaa suurilta osin samoja ehtoja ja määräyksiä, joita noudatetaan yrityksen omien työntekijöiden kohdalla. Esimerkiksi siivoojalla, vartijalla, postinjakajalla tai tavarantoimittajalla on täysin sama vaitiolovelvollisuus kaikesta näkemästään yrityksen tiloissa kuin yrityksen omilla työntekijöillä.

2.5.5 Avainhenkilöriskit

Avainhenkilöllä tarkoitetaan pk-yrityksessä useimmiten yrittäjää itseään. Avainhenkilöllä tarkoitetaan myös muita henkilöitä, jotka hoitavat tehtäviä, jotka ovat elintärkeitä yrityksen liiketoiminnan laajuuden, kannattavuuden ja jatkuvuuden kannalta. [If; Vahti 3/2003.]

Avainhenkilöriskillä tarkoitetaan sitä, mitä yritykselle tulee maksamaan, jos avainhenkilön työpanos yllättäen menetetään, joko tilapäisesti tai pysyvästi. Suoranaisten katemenetysten lisäksi on huomioitava myös uuden henkilön

rekrytointikustannukset, perehdyttäminen, vajaa tuottavuus ja muun organisaation ajanmenetys sekä ylityökustannukset. [VTT; Kajava et al., 1996.]

Tärkeä osa avainhenkilöriskin hallintaa on varahenkilöjärjestelmä, jonka tulee olla harkittu ja jopa käytännössä testattu. Avainhenkilön vastuuseen kuuluu, että hän pitää varahenkilönsä ajan tasalla mahdollisen riskin toteutumisen varalta. Pk-yritysten ohuen organisaation takia varahenkilöjärjestelmä on niissä usein käytännössä hatara. [VTT; Kajava et al., 1996.]

Avainhenkilökatastrofilla puolestaan tarkoitetaan riskiä, jossa menetetään kahden tai useamman avainhenkilön työpanos samalla kertaa. Näin voi käydä esimerkiksi liikenne- tai lento-onnettomuudessa. Yrityksellä tulisikin olla matkustussääntö, jonka mukaan usea avainhenkilö tai hänen varahenkilönsä ei saa matkustaa samassa liikennevälineessä.

Avainhenkilökatastrofi on myös avainhenkilöiden joukkoirtisanoutuminen. Tämä mainittu riski toteutui case-yrityksessä. Avainhenkilöriski kääntyi tässä tapauksessa toisenlaiseen näkökulmaan, koska mainitut avainhenkilöt toimivat päinvastoin: he toimivat selkeästi työnantajansa etua vastaan. Samalla he varastivat työnantajansa omaisuutta ja perustivat sen varaan oman, kilpailevan yrityksen.

2.5.6 Sisäisen tietoturvan valvonta

Sisäisellä valvonnalla varmistutaan siitä, että tietoturvapolitiikkaa noudatetaan ja annettuja tietoturvaohjeita sovelletaan työnteossa. Tämän lisäksi valvonnalla ylläpidetään ja tarkkaillaan niitä uhkia, joiden tiedetään olevan yrityksen sisäisessä tietoturvassa ja jotka täyttävät tietoturvarikoksen tunnusmerkit [Leiwo ja Kajava, 1994]. Sisäinen valvonta pitää sisällään myös sen, että työntekijöiden toimintaa yrityksen järjestelmissä ja liikkumista sisäisessä tietoverkossa tarkkaillaan. Työntekijän normaalista poikkeavaan toimintaan

pystytään reagoimaan hyvin nopeasti, ja sen myötä tahalliset tai tahattomat tietovuodot pystytään estämään. [Pirnes et al., 2000.]

Tämän kaltaiseen tietoturvajohtamiseen on olemassa hyviä valvontatyökaluja. Niiden ei aina tarvitse olla kalliita suljettuja ratkaisuja, vaan esimerkiksi avoimen lähdekoodin ratkaisut ovat hyvin yleisiä. Valvonta tulee suorittaa aina niin, että se haittaa mahdollisimman vähän työntekijän päivittäisiä rutiineja, mutta on samalla tehokasta ja reagoivaa. Jos valvonnan vaikutus näkyy, on työntekijöille korostettava, että tarkoituksena ei ole turha ns. kyttääminen. [Laaksonen et al., 2006.]

3. Case: BK-Automation Ky

3.1 Yrityksen esittely

3.1.1 Nimi ja toimiala

BK-Automation Ky:n toimiala on vesitekniikan – niin puhtaan- kuin jätevesienkin – automaatio- ja kaukokäyttöjärjestelmien, samoin kuin siihen liittyvien mittauslaitteiden suunnittelu, toteutus, asennus ja yhteistyö- sekä huoltosopimukset. Uutena osaamisena yrityksen toimintaan kuuluvat patoturvallisuus ja tulvanhallintajärjestelmä. Nämä tuotteet ovat Suomessa ainutlaatuisia. [Ks. liite 2.]

Esimerkkiyritys on monestakin syystä hyvin mielenkiintoinen – erityisesti innovaatioiden suunnittelijana. Yrityksen toiminnan historiaa on jo vuodesta 1998 varjostanut sisäiseen tietoturvaan liittyvä teollisuusvakoiluvyyhti, joka lamautti yrityksen lähes täysin. Rikosvyyhti sai mediassa valtakunnallistakin huomiota. Muun muassa yrityksen liikevaihto ja henkilökunnan määrä ovat kriisin aikana puolittuneet. Tilanne on ollut yrittäjille niin henkisesti kuin taloudellisestikin äärimmäisen rasittava. Kummatkin osapuolet valittivat käräjäoikeuden päätöksestä hovioikeuteen, jossa se käsiteltiin alkuvuodesta 2005. Hovioikeus ei myöntänyt valitusoikeutta korkeimpaan oikeuteen. Huomattavaa oikeusprosessissa on se, ettei BK-Automation Ky ole asianomistajana yksin, vaan yritysvakoiluasiassa asianosaisina on myös kaksi muuta yritystä, joihin on kohdistunut samaa rikollisuutta, tosin vähäisemmässä määrin kuin BK-Automation Ky:hyn.

3.1.2 Omistaja ja omistusosuudet

Yrityksen yhtiömuoto on kommandiittiyhtiö, jonka vastuunalainen yhtiömies on yrityksen toimitusjohtaja Asko Kuoppala. Äänettömänä yhtiömiehenä on

Tarja Kuoppala. Aiemmin toisena vastuunalaisena yhtiömiehenä toimi Tarja Kuoppalan siskon mies Jorma Bärling (ks. jäljempänä). Bärling on terveydellisistä syistä vetäytynyt yrityksen toiminnasta, ja Asko Kuoppala on lunastanut hänen osuutensa.

3.1.3 Pääomistajan ura – miten hänestä tuli yrittäjä?

Asko Kuoppala on yrittäjäsukua monessa polvessa – muun muassa Kuoppalan vanhemmilla oli rakennusliike. Kuoppalalla on kokemusta myös vieraalla työskentelemisestä, ja hän on työn ohessa aikoinaan kouluttautunut sähkömestariksi. Koska myös Kuoppalan vaimo Tarja oli yrittäjähenkinen, syntyi perhepiirissä unelmia yrittämisestä. Näiden unelmien myötä perhe muutti maalle Ähtäriin, Askon kotiseudulle. Ähtärissä Asko Kuoppala perusti ensin yhden miehen yrityksensä T:mi Suomenselän LVIS-Automatiikan ähtäriläiseen autotalliin 1982. Yrityksen alkuaikoina Kuoppalan yritys keskittyi paikkakunnan ja maakunnan rakennus- ja saha-automaatioon. Tuolloin alueella ei ollut muita automaatiotekniikkayrityksiä.

Toiminta kasvoi hiljalleen, ja vuonna 1984 yritys muutettiin kommandiittiyhtiöksi. Asko Kuoppalan ohella vastuunalaiseksi yhtiömieheksi tuli Tarjan siskon mies Jorma Bärling, jolla oli prosessitekniikka- ja automaatiotausta. Yhtiön nimi johdettiin yhtiömiesten nimikirjaimista, ja Tarja Kuoppalasta tuli äänetön yhtiömies. Yhtiöön palkattiin ensimmäinen työntekijä vuonna 1985, ja vuonna 1987 yritys sai Ähtärissä vuoden yrittäjäpalkinnon. Kasvun myötä yritys muutti ensin Seinäjoelle ja myöhemmin Seinäjoen-Nurmon teollisuusalueelle, jossa se toimii edelleen.

Yrittäjällä oli 1980-luvun puolivälin jälkeen se näkemys, että valtava talouskasvu ja ns. investointiboomi loppuvat ennen pitkää ja täytyisi löytää uusia liiketoiminta-alueita. Yrityksen kannalta lähes merkittävin käännekohta oli vuonna 1989, jolloin Asko Kuoppala oli Ranskassa vesialan seminaarissa.

Seminaarissa käsiteltiin maapallon vesivarantoja ja niiden järkiperäistä käyttöä. Yhtäkkiä Asko oivalsi, että tuo on alue, jolle yritys voi laajentua. Lisäksi markkinapotentiaali oli silloin hyvin ajankohtaista Suomessa ympäristömääräysten kiristyessä.

Toinen, tekninen oivallus oli, että vesijärjestelmien automatisoinnissa voidaan soveltaa samantyyppistä teknologiaa kuin sähkönjakelujärjestelmissäkin, siis voimalaitosten, sähkölaitosten ja jakeluverkoston automatisoinnissa. Oli siis sovitettava yhteen kaksi hyvin erilaista osaamisen aluetta: vesihuollon prosessit ja automaatiotekniikka.

Laajan tutkimus- ja selvitystyön tuloksena selvisi Sveitsin ABB:lta tieto, että yhteistyökumppani löytyisi lähempää kuin arvattiinkaan. ABB-Strömberg Vaasassa oli erikoistunut juuri tähän tarvittavaan teknologiaan. Tiukkojen neuvotteluiden jälkeen Asko Kuoppala allekirjoitti ABB:n kanssa lisenssisopimuksen maaliskuussa 1990. Tuolloin alkoi edelläkävijyyden ja kasvun aika, jota jatkui aina vuoteen 1998 ja yritysvakoilutapaukseen asti.

Vakoilutapauksen jälkeenkin, ns. säästöliekillä toimiessaan, yritys on satsannut tuotekehitykseen ja innovaatioihin niin paljon kuin taloudellisesti on pystytty, ja uusi tuoteperhe valmistui keväällä 2004. Uusin tuotekehityksen tulos, tulvanhallintajärjestelmä, on valmistumassa kaupalliseksi tuotteeksi kuluvan vuoden aikana, ja tämä on ainoa alansa tuote markkinoilla.

3.1.4 Yrityksen liikevaihto ja sen kehitys

Seuraavassa on kerrottu yrityksen taloudellisista tunnusluvuista pyörein luvuin. Yrityksen liikevaihto oli vuonna 1996 noin 3.9 milj. markkaa, mutta parhaimmillaan, ennen vakoilutapausta, liikevaihto oli vuonna 1997 noin 5.7 milj. markkaa. Vuonna 2004, jolloin yritysvakoiluasia oli käräjäoikeuden ja hovioikeuden käsittelyjen välissä, liikevaihto oli noin 3 milj. markkaa. Edellä mainittu yritysvakoilijoiden perustama yritys alkoi ns. mellastaa markkinoilla

rikollisin keinoin hankkimansa sisäpiiritietonsa turvin. Heidän toimintansa onnistuikin hyvin, ja tulokset alkoivat näkyä vahvasti BK-Automationin toiminnassa. BK-Automationin työntekijämäärä on puolittunut, ja viennin osuus liikevaihdosta on supistunut noin 15 prosenttiin. Tämän mainitun vakoilutapauksen lisäksi syynä supistumiseen on ollut viennin osalta yleinen markkinatilanne ja euron nopea vahvistuminen.

3.1.5 Tuotteet, tavarat, palvelut ja resurssit

Yrityksen tuotteista, tavaroista, palveluista ja resursseista on tarkempaa tietoa yhtiön kotisivulla www.bk-automation.fi, ja tuotteet on lajiteltu seuraavanlaisesti:

- valvomotuotteet
- ympäristönseurantajärjestelmät
- vesihuollonseurantajärjestelmät
- instrumentointi
- UV-putket
- tulvanhallintajärjestelmä.

Yleensä BK-Automationin tuote on kokonaisjärjestelmä, joka näkyy asiakkaalle helppokäyttöisenä, turvallisena ja toimintavarmana kokonaisuutena. Niinpä asiakassuhteet ovatkin vuosia kestäviä ja luottamuksellisia yhteistoimintasopimuksia, joista asiakas saa aina uusimman ja tarkimman tiedon.

Yrityksellä on toimitilat Seinäjoen-Nurmon teollisuusalueella, ja tällä hetkellä toimintaa on laajennettu Euran lähellä sijaitsevaan Hauttuan alueelle, josta yritys saa merkittävän ja tasaisen tulovirran lisäyksen kuukausittain. Yrityksen taloushallinto sijaitsee Porissa. Yrityksessä työskentelee 11 henkilöä.

3.1.6 Yrittäjän ja henkilöstön erityisosaaminen

Yrittäjän ja henkilöstön erityisosaamista ovat erilaisten teknisten ratkaisujen kehittäminen ja ymmärtäminen sekä yhdistäminen erityisesti siten, että ne ovat käyttäjänsä kannalta luotettavia, varmoja ja helppokäyttöisiä. Tämä edellyttää tarkkaa ja laaja-alaista tuntemusta eri aloilta sekä ohjelmointitaitoja räätälöityihin ratkaisuihin. Tärkeätä on syvällinen ja ylivoimainen erikoistuminen omaan markkinarakoon. Erittäin tärkeitä ovat myös tuotteiden myyntitaito ja asiakassuhteiden aktiivinen hoitaminen ja hankkiminen.

Yrityksen tärkeimmät asiakkaat ja markkina-alueet ovat kunnat ja kuntayhtymät, vesi- ja jätevesilaitokset sekä yritykset, jotka käyttävät paljon vettä prosesseissaan. Tärkeitä asiakkaita ovat myös vastaavanlaiset ulkomaiset vesialan yhteisöt ja yritykset.

3.1.7 Mikä on yrityksen kilpailuetu?

Yksi yrityksen keskeisin kilpailuetu ovat pitkät ja luottamukselliset asiakassuhteet, jotka ovat vaikeuksista huolimatta pitäneet yrityksen markkinoilla. BK-Automation on jo vanha, yli 20 vuotta toiminut, yritys joka on alalla tunnettu. Toinen tärkeä kilpailuetu ovat tietenkin yrityksen innovaatiot ja vahva tuotekehitys. Tärkeä kilpailuetu on myös edelläkävijyys omalla toimialasektorilla: yritys toimittaa vesialaltaan, jonka prosesseja ja automaatiota se hallitsee. Tärkeätä on uskoa myös omaan toimintaan ja lisäksi kehittää toimintaa jatkuvasti. Henkilöstöstä huolehtiminen ja heidän osaamisensa lisääminen on myös keskeisessä roolissa. Loppujen lopuksi tärkeimpänä kilpailuvalttina on periksi antamaton yrittäjyys ja vankka visio siitä, mihin ollaan menossa.

3.1.8 Yrityksen tulevaisuuden näkymät

Rikostutkinta ja oikeusjuttu olivat vireillä vuosina 1998–2005, mikä on hankaloittanut yrityksen toimintaa monella tavalla. Yrittäjien elämä on ollut niin henkisesti, fyysisesti kuin taloudellisestikin rankkaa, mistä on toivuttu yrittäjän mukaan vasta viime vuosien aikana. Yrittäjät ovat joutuneet myymään lähes kaiken omaisuutensa (noin 300 000 euron arvosta) pitääkseen yrityksensä pystyssä. Oikeusjuttu sitoi valtavasti yrittäjien ja henkilökunnan aikaa, resursseja ja pääomia.

3.2 Sisäisen tietoturvan pettäminen

Vuonna 1997 yrittäjä havahtui pahemman kerran: eräs asiakas soitti yrittäjälle ja ihmetteli, kuinka yrittäjän työntekijä oli tarjoamassa hänelle samaa urakkaa oman yrityksensä nimissä. Tilanne aikoi tämän jälkeen selvitä todella nopeasti. Vaikka yrittäjä reagoi tilanteeseen nopeasti erottamalla työntekijän, sillä ei ollut enää minkäänlaista vaikutusta vahinkoihin, jotka yritys tulisi kokemaan. [Ks. liite 3.]

Samaan aikaan selvisi, että yrityksen monta muutakin työntekijää oli mukana toiminnassa, eli kyseessä olevat henkilöt olivat perustamassa omaa yritystä, joka toimisi täysin samalla alalla kuin Kuoppalan yritys ja alkaisi myös taistella sen kanssa samoista asiakkaista. Yrityksen viidestätoista työntekijästä seitsemän oli lähdössä pois uuden yrityksen palvelukseen. Kun aikaa kului muutama päivä asian esiin nousemisesta, myös loput työntekijät sanoivat joukolla itsensä irti. Tämä laittoi yrittäjän todella hankalaan asemaan, sillä kaikki nämä työntekijät olivat käytännössä päässeet töihin yritykseen lähes suoraan koulun penkiltä, ja he olivat nuoresta iästään huolimatta nousseet yrityksessä avainasemaan. Tilanne yrityksessä oli se, että muutama iso projekti oli juuri valmistumassa ja kaikki tarvittava tieto oli näiden henkilöiden takana. Vaikka työntekijöillä oli kuukauden irtisanomisaika, heitä oli todella vaikea

saada töihin lukuisten ”sairastumisten” takia. Koska laki oli tässä asiassa hyvin vahvasti yrittäjän puolella ja työntekijöillä oli pelko siitä, että olleessaan pois työstä ilman pätevää syytä, he voisivat korvausvelvollisuuteen, työntekijät suorittivat meneillään olevat projektit loppuun.

Näiden työntekijöiden lähdettyä yrityksestä alettiin selvittää, olivatko työntekijät vieneet yrityksen tietoja mukanaan. Tämän selvittäminen osoittautui melko hankalaksi, sillä toiminta yrityksessä oli perustunut vahvaan luottamukseen, eikä työntekijöiden käyttöoikeuksia oltu rajoitettu millään lailla. Jokaisella työntekijällä oli siis käytännössä pääsy kaikkiin yrityksen tietoihin. Totuus alkoi selvitä, kun kilpailevan yrityksen Syspoint Oy:n toiminta pääsi vauhtiin. Jokaisessa tarjouskilpailussa uusi yritys tarjosi asiakkaalle aina hieman halvemman ratkaisun kuin KB-Automation Ky, ja olemassa oleville asiakkaille uusi yritys oli jo tarjonnut KB-Automationia halvemman ratkaisun säännöllisesti toimitettavissa päivitystapauksissa.

Kävi ilmi, että yrityksestä lähteneet työntekijät olivat ajan kuluessa kopioineet kaikki yrityksen koneilla olevat tiedot. Lisäksi kopio oli otettu kaikista yrityksen käytössä olevista ohjelmista ja jopa henkilökohtaiseksi luokitellut tiedot, kuten sähköposti ja kalenterimerkinnät, olivat joko lähteneet työntekijöiden mukana tai tiedot oli kopioitu verkon yli ajan kuluessa. Tämän seurauksena yrittäjä teki poliisille tutkintapyynnön, ja tapauksen selvittäminen johti aina hovioikeuteen asti.

Poliisi teki asian vakavuuden johdosta kotietsinnän Syspoint Oy:n tiloihin ja muutamien avainhenkilöiden koteihin. Näistä paikoista löytyi selkeitä todisteita siitä, että kopiointi oli ollut järjestelmällistä ja systemaattista. Tämän seurauksena asia eteni Seinäjoen käräjäoikeuteen, jossa tekijät saivat syytteen muun muassa tekijänoikeusrikoksesta, yrityssalaisuuden rikkomisesta ja yritysvakoilusta. Tämä asia on kuvattu tarkemmin luvussa 3.4.1. Kummatkin osapuolet olivat tyytymättömiä käräjäoikeuden tuomioon ja valittivat Vaasan hovioikeuteen. Tätä on kuvattu tarkemmin luvussa 4.3.2. Hovioikeus ei

myöntänyt valituslupaa korkeimpaan oikeuteen, vaikka yrittäjä olisi sitä halunnut.

3.3 Sisäisen tietoturvan tilanne tietovuodon hetkellä

Sisäinen tietoturva oli melko heikolla pohjalla yrityksessä. Toiminta perustui lähes kokonaan henkilöiden keskinäiseen luottamukseen, ja esimerkiksi yrityksen tietoturvallisuuspolitiikkaa ei oltu dokumentoitu millään tavalla. Jokaisella työntekijällä oli toki salasanat omille koneilleen ja yrityksen sisäiseen verkkoon, mutta liikkumista verkon sisällä ei oltu rajoitettu mitenkään. Lisäksi kävi ilmi, että työntekijöillä oli tiedossa jopa toimitusjohtajan henkilökohtainen salasana. Salasanat ja muut sisäsäiset käyttöoikeuksien rajoitukset olisivat olleet suhteellisen turhia, koska samat henkilöt, jotka lähtivät yrityksestä, olivat olleet vastuussa tietoturvasta, sen ylläpitämisestä ja kehittämisestä. Tietoturvallisuus ei varsinaisesti ollut kenenkään vastuulla, ja sitä ylläpiti ja kehitti aina se henkilö, jolla satunnaisesti oli muilta työkiireiltä aikaa. Tämän vuoksi se vähäinen aika, joka tietoturvaan sijoitettiin, keskittyi pääsääntöisesti ulkoisen tietoturvan kysymyksiin. Uuden työntekijän tullessa taloon, tällä ei ollut mitään tietoa yrityksen tietoturvakäytännöstä, vaan asia tuli eteen vasta siinä vaiheessa, kun työntekijälle luotiin käyttäjätunnus ja salasana. Myös kaikenlainen muu tietoturvaohjeistus oli hyvin vähäistä.

Toimintatavat rekrytointitilanteissa olivat myös hyvin yleisellä tasolla. Huomiota kiinnitettiin pitkälti henkilön koulutukseen ja ammattitaitoon. Yleisenä toimintatapana oli valita yritykseen nuoria vastavalmistuneita henkilöitä tai henkilöitä, jotka olivat opintojen jälkeen hetken ehtineet tutustua työelämään. Työntekijöiden taustojen selvittäminen ja heidän aikaisempaan työhistoriaan perehtyminen oli hyvin vähäistä ja pintapuolista. Työntekijät olivat pääsääntöisesti ensimmäisessä koulutusta vastaavassa työssä, ja yrityksen toimintatapana oli antaa työntekijöille hyvin paljon vastuuta ja

vapauksia. Nämä työntekijät saivat siis itse luoda oman toimintamallinsa ja -ympäristönsä. Yrityksen koko toiminta perustui hyvin vahvaan luottamukseen, ja yrittäjän mukaan oli täysin mahdotonta arvata, että puolet henkilökunnasta käyttäisi annettuja valtuuksia ja vapautta niin törkeästi hyväkseen.

Työtilauksia oli tuolloin niin paljon kuin niitä vain ehdittiin tekemään, koska alueella, tai edes koko valtakunnassa, ei ollut juurikaan kilpailijoita. Ongelmaksi tämän myötä muodostui se, että tietoturvaan yleensä ei ollut nimetty varsinaista työntekijää, vaan tietoturva-asioita hoiti se, jolla oli työtilausten välillä aikaa. Koska toiminta perustui täysin luottamukseen, yrittäjä antoi työntekijöille valtuuden kehittää ja ylläpitää tietoturvaratkaisuja. Tämä taas johti siihen, että kun työntekijät lähtivät joukolla pois yrityksen palveluksesta, tietoturvan tilaa alettiin tarkastaa. Tällöin havaittiin, että sisäisen tietoturvan ratkaisut olivat hyvin yksinkertaiset. Sisäistä tietoturvaa ei juuri ollut olemassa – käyttäjätunnusten ja salasanojen näennäistä käyttöä lukuun ottamatta. Työntekijät olivat rakentaneet ratkaisun niin, että melkein jokaisella työntekijällä oli pääsy kaikkiin yrityksen palvelimiin talon ulkopuolelta. Toimialalle on tyypillistä, että yrityksellä on useiden asiakkaiden luona oma palvelin. Näihin kaikkiin palvelimiin työntekijät olivat rakentaneet itselleen pääsyn myös henkilökohtaisilta koneiltaan.

Koska toimintaa ei ollut rajoitettu juuri millään tavalla, kaikilla työntekijöillä oli mahdollisuus asentaa ohjelmia rajattomasti kaikille yrityksen koneille. Tämä mahdollisti sen, että yrityksen tietokoneilla ja palvelimilla oli ohjelmia, jotka automaattisesti kopioivat tiedostoja ja lähettivät ne ennalta määriteltyihin osoitteisiin. Ongelmaksi muodostui se, että varsinkaan palvelimilla ei ollut olemassa minkäänlaisia loki-tiedostojärjestelmiä ja ne olivat käytännössä kaikki samassa tilassa. Jälkeenpäin oli täysin mahdoton todistaa, mitä tietoa oli kadonnut ja/tai kopioitu. Siirrettävien medioiden, kuten USB-muistin, CD:n tai ulkoisen kovalevyn, käyttö oli täysin kiinni kulloisestakin

tietoturva-asiaa hoitavasta henkilöstöstä. Siirrettävien medioiden käyttäminen ilman minkäänlaista lupaa tai selitystä oli täysin normaalia.

Tietokoneiden ja palvelimien fyysinen suojaaminen oli korkeintaan keskinkertaisella tasolla. Yrityksen tilat oli suojattu ulkopuolisilta hälytysjärjestelmällä ja vartiointiliikkeen palvelulla. Myös useat työtilat ja palvelinhuone oli lukittu erikseen. Palohälytys- ja sammutusjärjestelmät olivat asianmutkaisesti järjestetty. Ongelma tässä tapauksessa oli kuitenkin se, että lähes kaikilla oli avaimet kaikkiin yrityksen tiloihin. Minkäänlaista kulunvalvontaa ja videokameroita ei ollut, ja näin ollen yrittäjällä ei ollut minkäänlaista tietoa siitä, kuinka yrityksessä liikuttiin esimerkiksi päiväsaikaan tai missä ja mihin aikaan työntekijät ylipäätään liikkuivat yrityksen tiloissa.

Avainhenkilöille ei ollut minkäänlaista varahenkilöjärjestelmää. Koska noin puolet henkilöstöstä lähti yrityksen palveluksesta samanaikaisesti, yrityksessä ei yksinkertaisesti ollut osaavaa henkilöstöä jäljellä hoitamaan tarvittavia tehtäviä. Juuri tästä syystä useista projekteista jouduttiin jättäytymään pois, ja tämä vaikutti liiketoimintaan niin paljon, että yritystoiminnan loppuminen oli todella lähellä. Vain yrittäjän henkilökohtainen taloudellinen panostaminen piti yrityksen toiminnassa vaikeimpana aikana.

3.4 Oikeudenkäynti

Tässä luvussa käsitellään kummassakin oikeusasteessa käydyt istunnot ja oikeuden päätökset. Kappaleen lopussa tuodaan esille päätösten eroavuudet ja yritetään löytää niille looginen selitys. Kummassakin kappaleessa on tekijöille langetetut tuomiot, mutta tuomionimikkeeseen liittyvää sisältöä ei tässä tutkimuksessa ole keskeistä käsitellä.

3.4.1 Käräjäoikeus

Käräjäoikeuden istunnot aloitettiin keväällä 2003. Tätä ennen poliisi ja kumpikin osapuoli oli tehnyt perusteellista tutkimustyötä. Todistusaineistona olivat muun muassa lukuisat tekniset pöytäkirjat, talousasiakirjat ja ohjelmisto/tiedostokuvaukset. Käräjäoikeudessa kuultiin kaikkia irtisanoutuneita, yrittäjää ja yrityksen palvelukseen jääneitä. Lisäksi kummatkin osapuolet käyttivät asiantuntijatodistajia todistaakseen oman kantansa. [Käräjäoikeus, 2003a.]

Käräjäoikeus tuli siihen lopputulokseen, että irtisanoutuneet työntekijät olivat toimineet rikollisesti ja lähtiessään ottaneet huomattavasti yrityksen omaisuutta mukaan, jonka pohjalta he olivat ryhtyneet perustamaan omaa liiketoimintaa. Lisäksi käräjäoikeus totesi, että työntekijöiden perustama yritys, sen toiminta ja sen käyttämät tuotteet olivat ”kopioita” BK-Automationin toiminnasta tai tuotteista. Kahdeksan henkilöä Syspoint Oy:stä saivat tuomion yhdestä tai useammasta seuraavista syytteistä:

- tekijänoikeusrikos
- yrityssalaisuuden väärinkäyttö
- yritysvakoilu.

Käräjäoikeus määräsi myös Syspoint Oy:n maksamaan yhteisvastuullisesti 40 000 euroa BK-Automation Ky:lle. Tekijöiden rangaistukset vaihtelivat sakoista aina ehdolliseen vankeuteen asti. [Käräjäoikeus, 2003b.]

3.4.2 Hovioikeus

Kummatkin osapuolet olivat tyytymättömiä käräjäoikeuden päätöksen ja hakivat valituslupaa hovioikeuteen. Yrityksen puolelta oltiin erityisen tyytymättömiä vahingonkorvausten suuruuteen ja siihen, että heidän

liiketoimintakieltovaatimuksensa hylättiin. Vastaajan puolella oltiin yleisesti tyytymättömiä tuomioon, ja he olivat valituksessaan sitä mieltä, että he olivat täysin syyttömiä ja vaativat kaikkien syytteiden kumoamista. Hovioikeudessa käsittely aloitettiin alkuvuodesta 2005. Hovioikeuden käsittelyssä pääosaan nousi näkökulma siitä, kuka oli tehnyt kyseiset ohjelmakoodit ja ohjelmistoihin liittyvät kuvat. Käytetty sovelluskehitin oli saatavilla yleisillä markkinoilla, ja sen tuottamat tiedostot eivät itsessään ylittäneet tekijänoikeusrikoksen kynnystä. Hovioikeus katsoi, että ko. tiedostot olivat ohjelmiston tuotteita ja että yksittäisinä ne eivät antaneet kenellekään mitään hyötyä. Tärkeäksi seikaksi nousi myös se, että eräs työntekijöistä oli tehnyt samanlaisesta aiheesta diplomityönsä. Hovioikeus totesikin, että jo silloin käytössä oli ollut samankaltaisia tiedostoja. Lisäksi Hovioikeus totesi, että käytetyt ohjelmat ja niihin liittyvät toimintatavat olivat hyvin yleisessä tiedossa. Monet kiistan alaiset tiedostot olivat ohjelman ominaispiirteitä, eli ne olivat siis yleisissä ”kirjastoissa”, jossa niihin oli kaikilla lisenssin omistajilla mahdollisuus päästä. Hovioikeus tuli siihen lopputulokseen, että BK-Automationissa tapahtuneet kirjastotiedostojen muutokset liittyivät lähinnä niiden yhteensopivuuteen yrityksen järjestelmiin ja toimintoihin, eivätkä ne siis vaikuttaneet toiminnallisuuteen ja omaperäisyyteen. Hovioikeus myös totesi, että yrityssalaisuuden väärinkäyttöä ei voida todistaa, sillä yritys ei ollut tehnyt minkäänlaisia suojauksia tai vaitiolosopimuksia, vaikka sillä olisi ollut siihen mahdollisuus monessa eri yhteydessä. [Hovioikeus, 2005a.]

Hovioikeus alensi tekijöiden tuomioita edelliseen, käräjäoikeuden tuomioon verraten huomattavasti. Ainoaksi syyksi luettavaksi kohdaksi jäi tarjouslaskenta-ohjelman väärinkäyttö. Yhtä henkilöä lukuun ottamatta rangaistukset muuttuivat sakkorangaistuiksi. Tämän seurauksena korvausvelvollisuus ja syyllisten korvattaviksi määrätyt oikeudenkäyntikulut alenivat huomattavasti tai siirtyivät valtion maksettavaksi. Käräjäoikeudessa langetettu yhteisösakko alennettiin 10 000 euroon. [Hovioikeus, 2005b.]

3.4.3 Yhteenveto tuomiolauselmista

Tuomiot ja vahingonkorvaukset vaihtelivat merkittävästi eri oikeusasteiden välillä. Ratkaisevaksi seikaksi nousi se, että hovioikeudessa päähuomio kiinnittyi ohjelmien ja toimintojen omaperäisyyteen. Käräjäoikeus taas katsoi asian kokonaisuutta ja katsoi yhtiöiden samanlaisuuden ja täysin samanlaisten tuotteiden ja toimintojen olevan riittävä näyttö siitä, että Syspointin toiminta perustui BK-Automationista saatujen tietojen ja tiedostojen varaan. Hovioikeuden käsittelyssä kopiointi ja muunlainen väärinkäytös olivat sinänsä toissijaisia asioita, ja sen todistelussa keskityttiinkin siihen olivatko BK-Automationin tuotteet ja ohjelmisto omaperäisiä vai osa yleisesti saatavilla olevan ohjelmiston perustoimintoja. Hovioikeudessa katsottiin myös, että annetut työtehtävät vaativat useiden tietojen saatavuutta. Koska tietoja ei ollut suojattu millään tavalla, niiden hallussapito ei sinänsä ole rikos. Muuhun kuin kehitysohjelmistoihin liittyvien asiakirjojen tai tiedostojen kopioinnista BK-Automationilla ei ollut esittää riittäviä todisteita. [Käräjäoikeus, 2003a; Hovioikeus, 2005a.]

Saman asian katsominen kahdelta eri kannalta voi saada aikaan hyvin erilaisen ratkaisun. Vaikka oikeudessa esitettiin todisteet siitä, minkälaista vahinkoa tietovuoto oli aiheuttanut yrityksen toimintaan [Laskelma, 2001], se ei tuomioistuimessa tai korvausvelvollisuudessa painanut. Vahingolla tässä tarkoitetaan siis sellaista kilpailutoimintaa, joka eroaa normaalista tilanteesta, jossa alueella tulee täysin erillinen kilpailija. Sanomattakin on selvää, että työntekijä voi koska tahansa halutessaan sanoa itsensä irti ja alkaa itsenäiseksi yrittäjäksi. Mutta tilanne, jossa yli puolet työntekijöistä irtisanoutuu joukolla yrityksen palveluksesta ja uudesta täysin saman alan yrityksestä löytyy edes vähänkin todisteita siitä, että työntekijät ovat hyödyntäneet aikaisemman työnantajansa omaisuutta tai taitotietoa, on omasta mielestäni ja myös yleisen käsityksen mukaan tuomittava ja moraaliton.

3.5 Sisäisen tietoturvan pettämisen seuraukset

Tässä luvussa yritetään saada käsitys siitä, mitä tämänkaltainen prosessi on aiheuttanut yritykselle ja ennen kaikkea yrittäjälle. Aihe on sinänsä arka ja useista näkökulmista katsoenkin vaikeasti mitattava, koska ihmiset käsittelevät asioita ja reagoivat niihin eri tavoin. Lisäksi osa seurauksista perustuu ammattilaisen tekemään tai yrittäjän omaan arvioon. Varmoja faktoja ei siis voida esittää, mutta uskon, että nämä arviot antavat ainakin oikeanlaisen suunnan tapahtuneille seurauksille.

3.5.1 Yrittäjän työajan menetys

Sanomattakin on selvää, että kahdessa oikeusasteessa käsitelty juttu vaatii jo lukemattomia tunteja oikeusistuntoja ja niihin liittyvää valmistautumista. Todistusaineiston kerääminen oli keskeisessä roolissa, ja se vei huomattavasti aikaa, sillä kukaan ei varmasti osannut sanoa, mitä yrityksestä oli oikeasti viety tai kopioitu. Yrittäjä kertoikin, että pahimpaan aikaan tämä prosessi vei jopa yli puolet hänen päivittäisestä työajastaan. Lisäksi osa työntekijöistä joutui keskittymään siihen, että sisäinen tietoturva rakennettaisiin uudestaan mahdollisimman nopeasti: yrityksessä haluttiin varmistua siitä, että jos talon järjestelmiin oli tehty mahdollisuus päästä käsiksi yrityksen ulkopuolelta, nämä aukot tukittaisiin mahdollisten lisävahinkojen estämiseksi.

3.5.2 Henkiset kärsimykset

Kaikesta materiaalista ja etenkin haastattelutilanteesta on aistittavissa, että tilanne oli yrittäjälle todella kova paikka ja että se tuli täysin yllättäen. Yrittäjä oli perustanut koko johtamisensa hyvin vahvaan luottamukseen. Hänen mukaansa työpaikalla töitä tehtiin tehokkaasti, mutta samalla työilmapiiri oli rento ja vapautunut. Vastuuta ja valtaa annettiin heti, kun työntekijän taidot ja

tiedot karttuivat. Tämän oli tarkoitus toimia kannustimena yhdessä taloudellisen hyödyn kasvamisen kanssa. Tapauksen selvittyä normaalin yksityisyrittäjän vähäinenkin vapaa-aika oli poissa, ja rentoutuminen oli silloin täysin mahdotonta. Tapaus vaikutti myös kaikkiin työntekijöihin, koska noin puolet henkilökunnasta oli yhtäkkiä poissa ja uutta henkilökuntaa osaavaa henkilökuntaa oli mahdotonta palkata nopealla aikataululla johtuen työn vaatimista erityisosaamisista. Työn lisääntyminen ja sen määrä aiheutti kaikille lisää henkisiä paineita, ilmapiiri oli epätoivoinen, ja kaikilla oli huoli työpaikkojen säilymisestä ja koko yrityksen toiminnan jatkuvuudesta.

Vaikka tänä päivänä yrittäjä katsookin jo tulevaisuuteen, tapaus on jättänyt häneen ikuiset jäljet. Enää yrittäjä ei pysty luottamaan kehenkään työntekijään niin paljon kuin aikaisemmin, ja eräänlainen kyynisyys ihmisiä kohtaan on lisääntynyt tapahtuneen seurauksena. Myös oikeuslaitoksen uskottavuus on kärsinyt merkittävän kolauksen yrittäjän mielessä.

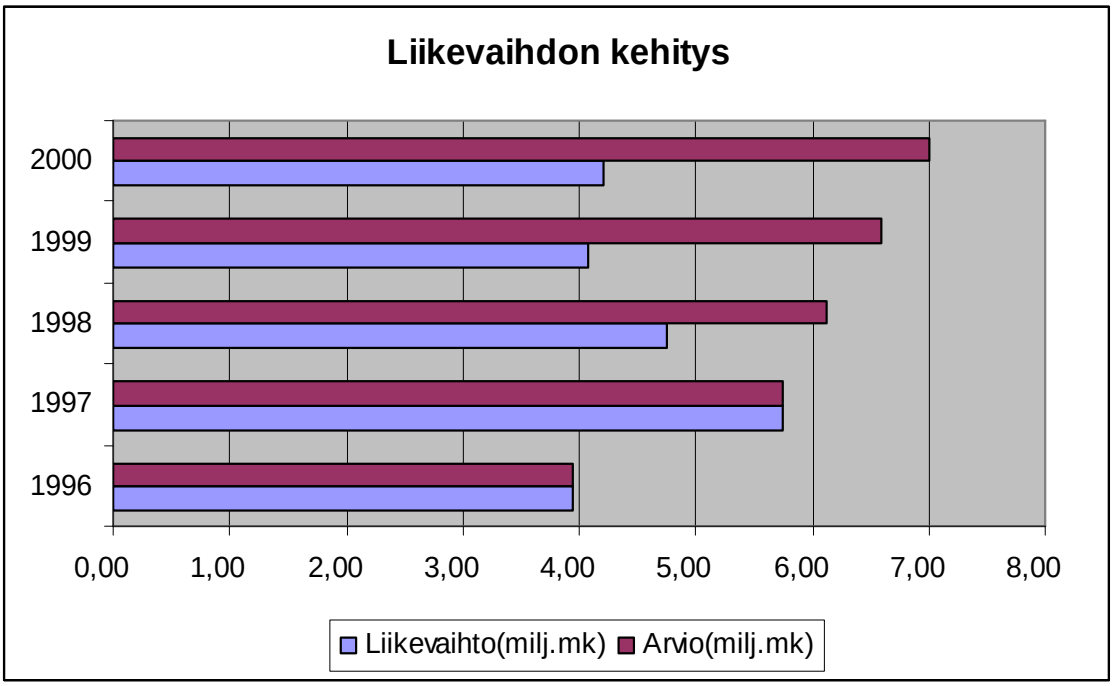
3.5.3 Taloudelliset menetykset

Oikeusprosessien aikana yrittäjä teetti laskelman, jossa käy ilmi se, minkälaiset vahingot tapauksesta olivat aiheutuneet. Laskelmassa on asiaa tarkastelu kolmesta eri näkökulmasta [Laskelma, 2001], jotka ovat:

1) liikevaihdon ja sitä kautta myyntikatteen menetys
2) kehittämispanoksen oikeudeton käyttöönotto
3) vaihto-omaisuuden vanhentumisena menetetty liiketoiminta.

Kohta kaksi oli siinä mielessä merkittävä, että yritys oli ottanut merkittävän lainan tuotekehitystä varten, ja nyt siitä saatuja tuloksia ei pystytty mitenkään taloudellisesti hyödyntämään. Lainat oli maksettava vanhempien tuotteiden kustannuksella tai uutta tuotekehitystä oli tehtävä päivittäisen työn ohella. Sitä,

miten tapaus vaikutti yrityksen toimintaan, on kuitenkin helpoin arvioida ensimmäisen kohdan perusteella.



Kuva 3: Liikevaihdon todellinen ja arvioitu kehitys 1996–2000.

Arvio liikevaihdon kehityksestä perustuu yrityksen vuonna 2001 teettämään laskelmaan [Laskelma, 2001]. Kuvioista on helppo huomata, että tietovuodolla oli selvä vaikutus yrityksen liikevaihdon kehittymiseen. Kriittisesti tarkasteltuna voidaan toki sanoa, että vaikka kilpailija olisi aloittanut ns. puhtaalta pöydältä, sillä olisi ollut vaikutusta liikevaihtoon. Alan ammattilaiset arvioivat kuitenkin, että vaikutus ei olisi ollut niin jyrkkää kuin mitä se nyt oli. Kuviota katsottaessa on otettava huomioon, että yrittäjä on, varovaisten arvioiden mukaan, laittanut omista henkilökohtaisista varoistaan noin 300 000 euroa (noin 1,8 Mmk) yrityksen toiminnan jatkamiseen, mikä on huomattava osuus esimerkiksi vuoden 1999 liikevaihdosta. Vaikeimpien vuosien aikana myös yrityksen työntekijät olivat valmiita joustamaan ja tekemään taloudellisia uhrauksia. Yrityksen vahva panostus tuotekehitykseen oli näistä syistä pakko lopettaa useiden vuosien ajaksi, millä arvellaan olleen vaikutus aina nykypäivään asti. [Laskelma, 2001.]

4. Pk-yrityksen sisäisen tietoturvan oikeanlainen kehittäminen

Yleisesti on tiedossa, että pk-yritysten taloudelliset resurssit ovat kohtuullisen niukat ja niille on monenlaisia käyttökohteita. Innovatiivisissa yrityksissä tämän merkitys korostuu, ja usein myös yrittäjän ja/tai avainhenkilöiden työaikaresurssit ovat rajalliset. Nämä resurssit ovat usein täydessä käytössä.

Se vähäinen panostus, joka tietoturvaan tehdään, kohdistetaan useimmiten ulkoiseen tietoturvaan. Tutkimuksen mukaan sisäisestä tietoturvasta ei ole edes keskusteltu tai ohjeistettu, eikä sitä ei ole dokumentoitu mitenkään, ja näistä asioista ei yrittäjälläkään ole tarvittavaa tietämystä. On ymmärrettävää, että liiketoiminnan jatkuva kehitys, suotuisa kilpailutilanne ja näennäinen rento työilmapiiri vaikuttivat siihen, että sisäisen tietoturvan ongelmista ei edes tiedetty ennen vahingon sattumista.

Tämä tutkimuksen ja erityisesti sen case-osan perusteella on seuraavassa esitetty vaiheittainen taulukko tietoturvan vaiheittaisesta jäsentelystä. Taulukon järjestys perustuu kustannustehokkuuteen, parhaaseen hinta-laatusuhteeseen ja toimintatapojen oikeanlaiseen rakentamiseen. Listassa, taulukossa 1, on kolme kategoriaa, jotka määrittyvät hankintahinnan mukaan:

Lähes ilmaiset	Kohtuuhintaiset	Hinnaltaan merkittävät
Tietoturvapolitiikka	Varmuuskopiointi järjestelmä	Henkilökunnan jatkuva kouluttaminen
Tietoturvaohjeistus	Käyttäjätunnusjärjestelmä	Palkankorotukset
Riskien ennakointi	Salasanajärjestelmä	Toiminnan keskeytysvakuutus
Taustojen tarkistus	Vahinkovakuutus	Henkilökunnan vapaaehtoiset vakuutukset
Työsopimuksen sisältö	Kulunvalvonta ja lukitukset	Muut sitouttamiskeinot
Toimenpiteet työsuhteen loppuessa	Turvallisuuspalvelut	
Käyttöoikeuksien rajoittaminen	Valvontatyökalut	

Taulukko 1: Sisäisen tietoturvan vaiheittainen jäsentely

Lähes ilmaiset -kategoriaan kuuluvat asiat ovat niitä asioita tai toimintoja, joiden toteuttaminen vaatii minimaalisen taloudellisen panostuksen, jollainen on

esimerkiksi työaika, ja/tai melko vähäisiä muita kuluja. *Kohtuuhintaiset*-kategoriaan kuuluvat ne toiminnot, joiden toteuttaminen vaati jonkin verran rahaa, mutta jotka ovat realistisesti pk-yrityksen toteutettavissa. Kyse on siis kertaluontoisista kustannuksista tai pienehköistä kuukausittaisista eristä. *Hinnaltaan merkittävät* -kategoriaan kuuluvat ne asiat, jotka ovat jo kertaluontoisesti kalliita ja joiden ylläpitäminen vaatii merkittäviä taloudellisia resursseja. Lisäksi nämä toiminnot eivät palvele pelkästään sisäistä tietoturvaa, vaan ne vaikuttavat myös yritykseen laajemmin. Tähän kategoriaan kuuluvien asioiden tai toimintojen hankkiminen ja/tai ylläpitäminen vaatii todella menestyvää liiketoimintaa.

4.1 BK-Automation Ky:n nykytila ja toimintatapojen muutos

Kymmenen vuotta tapahtuman jälkeen yritys on toipunut sille tasolle, jolla se oli ennen sisäisen tietoturvan pettämistä. Koska tuotekehitys on toimialalla ratkaisevassa osassa, BK-Automation on siihen panostamalla vaikeinakin aikoina saanut nykypäivänä kilpailukykynsä takaisin sille tasolle, että se on jälleen alkanut pärjätä tarjouskilpailuissa. Lisäksi vahva panostus kokonaan uusien tuotteiden kehittelyyn on aiheuttanut sen, että kilpailijoilla, ja etenkin Syspoint Oy:lla, ei ole mahdollisuutta vastata millään lailla niihin liittyviin tarjouskilpailuihin.

Vahingosta on viisastuttu ja sisäiseen tietoturvaan on tehty todella merkittäviä muutoksia. Nykypäivänä kenelläkään työntekijälle ei ole mahdollisuutta saada kaikkia yrityksen tietoja tai tietokantoja käsiinsä. Palvelimia on useita eri paikoissa ja eri paikkakunnilla, ja nämä kaikki on luonnollisesti suojattu asianmukaisella kulunvalvonnalla. Tieto on suojattu salasanoin ja käyttöoikeuksin siten, että jokaisella työntekijällä on pääsy vain tietoihin, jotka koskevat vain hänen työnkuvaansa.

Nykypäivänä yrityksen tietoturva on yhden ihmisen hallinnassa. Yrittäjän oma poika on nuoresta iästään huolimatta täysipäiväisesti mukana yrityksen toiminnassa ja huolehtii yrityksen sisäisistä ja ulkoisista tietoturvaratkaisuista. Yrittäjä ja hänen poikansa ovat suunnitelleet yritykselle uuden tietoturvaratkaisun, joka perustuu aiemman tapauksen virheistä oppimiseen. Tänä päivänä yrityksen tietoturvallisuus on dokumentoitu hyvin selvästi. Yritys on laatinut yksityiskohtaisen tietoturvallisuussuunnitelman, jossa kuvataan kaikki sen sisäiseen ja ulkoiseen tietoturvaan liittyvät asiat ja ratkaisut. Tietoturvallisuussuunnitelmaa säilytetään turvallisessa paikassa yrityksen ulkopuolella, ja sen lukuoikeus on vain muutamilla avainhenkilöillä. Suunnitelman tarkoituksena on toimia kahden avainhenkilön tallennuspaikkana, jonne kirjataan kaikki tehdyt muutokset ja lisäykset tietoturvaan. Suunnitelma palvelee yritystä ongelmatilanteissa, joissa esimerkiksi pitkän sairastumisen vuoksi toinen tai kummatkin avainhenkilöt ovat poissa. Tällöin toimintaa pystytään jatkamaan normaalisti ja yrityksessä ollaan tarkasti tietoisia siitä, miten tietoturva on hoidettu. Tietoturvallisuusohjeistuksen noudattamista seurataan hyvin tarkasti: muun muassa työntekijöiden Internet- ja sähköpostiliikennettä valvotaan sillä tasolla, jolla se lain puitteissa on sallittua. Tämä asia on tuotu hyvin selvästi työntekijöiden tietoon ja uusia työntekijöitä opastetaan ja perehdytetään yrityksen tietoturvapolitiikkaan.

Uutta työntekijää palkattaessa rekrytointiprosessin rakenne on aivan eri tasolla kuin aikaisemmin. Yrityksessä painotetaan kokemusta ja uuden työntekijän taustat ja aikaisempi työhistoria tarkistetaan huolellisesti. Työsuhdetta solmittaessa ei mitään asiaa jätetä sattuman varaan. Nykyään työsopimukseen kirjataan kaikki asiat, jotka liittyvät muun muassa työsuhteen lopettamiseen, työaikana syntyvien innovaatioiden omistusoikeuteen ja liiketoimintakieltoon. Työsopimus on teetetty yhteistyössä Urakoitsijaliiton lakimiehen kanssa. Muutamilla työntekijöillä on nykypäivänä mahdollisuus

etätyöskentelyyn, mutta etäyhteyden muodostaminen on rajoitettu vain yhteen palvelimeen, jonka liikennettä seurataan koko ajan, ja sen sisältö on hyvin rajoitettua. Työntekijöiden kanssa on myös kirjallisesti sovittu, että mitään yrityksen ohjelmia ja tiedostoja ei saa löytyä omalta tietokoneelta. Tämän vuoksi etätyötä tekevät henkilöt saavat yritykseltä käyttöönsä kannettavan tietokoneen, joka sisältää vain välttämättömimmät ohjelmat sen hetkiseen työntekoon, ja siitä muodostettavat yhteydet ovat hyvin suojattuja. Lisäksi tietokone on suojattu esimerkiksi varkauden varalta salasanalla, joka estää koko koneen luvatta käynnistämisen. Työsuhteen päättyessä työntekijän on allekirjoitettava paperi, jossa hän vakuuttaa palauttaneessa kaiken yrityksen omaisuuden, ja samalla hän sitoutuu olemaan vaiti kaikesta, mikä liittyy yritykseen tai sen liiketoimintaan. Tämä asia on tuotu henkilöstön tietoon työsuhdetta solmittaessa. Näillä keinoilla yritys varmistaa sen, että aiemman kaltaisen toiminnan mahdollisesti toistuessa, sillä on yksiselitteiset dokumentit mahdollista oikeuden käsittelyä varten.

Ohjelmistojen ja laitteistoiden käyttämiseen on muodostettu selkeä käytäntö. Usealla työntekijällä on USB-muistitikku, jolla on mahdollisuus siirtää tai varmentaa pieniä määriä tietoa. Vain palvelimissa on enää tallentavat CD-asemat, ja niiden käyttö rajoittuu vain yhteen henkilöön, joka ottaa varmuuskopioita. Lisäksi kaikenlaisten muiden massamuistien käyttäminen on yrityksessä nykypäivänä kiellettyä.

Fyysisessä suojauksessa on myös otettu selkeitä askeleita eteenpäin. Yritys on laajentunut kahdelle eri paikkakunnalle, ja kummassakin toimipisteessä kulunvalvontaan sekä tietokoneiden ja palvelimien suojaamiseen on kiinnitetty huomiota. Palvelimet ovat nykyään sellaisessa tilassa, johon avaimet ovat vain yrittäjällä ja hänen pojallaan. Lisäksi tiedon suojaaminen näissä koneissa on hoidettu todella hyvin. Varmuuskopioita otetaan säännöllisesti, ja lisäksi kummassakin paikassa olevat pääpalvelimet ”peilaavat” eli kopioivat toisensa päivittäin. Tällä varmistetaan se, että jos toinen toimipiste tuhoutuu esimerkiksi

tulipalon seurauksena, tärkeät ja päivitetyt tiedostot ovat heti saatavilla toisesta palvelimesta. Kulunvalvonta on järjestetty henkilökohtaisella seurannalla ja vierailijat ja muut yrityksen tiloissa kävijät on ennalta määritelty tai he liikkuvat yrityksen tiloissa aina jonkun työntekijän seurassa.

4.1.1 Tulevaisuuden näkymät

BK-Automation:ssa harjoitetaan hyvin määrätietoisesti ja systemaattisesti jatkuvaa tietoturvan kehittämistä. Sisäisen tietoturvan ratkaisuja tarkkaillaan ja tarvittaessa tarkistetaan jatkuvasti. Osoituksena jatkuvasta kehityksestä yrityksen toiminnassa voidaan pitää muun muassa täysin uuden salasanaohjelmiston käyttöönottoa lähitulevaisuudessa. Myös kriittisten tietojen luokitteleminen ja hallitseminen on noussut esiin niissä keskusteluissa, joissa on pohdittu sitä, miten tulevaisuudessa oman taitotiedon suojaaminen ja suojeleminen saataisiin vielä aiempaa paremmalle ja aukottomammalle tasolle. Avainhenkilökysymykseen on myös kiinnitetty huomiota. Yrityksessä mietitään kiivaasti ratkaisua sille, kuinka tietyille henkilöille saataisiin osaavat varahenkilöt esimerkiksi poislähdön tai pitkän sairastumisen sattuessa.

Pahimpien aikojen jälkeen yrittäjät ovat tulevaisuuden suhteen optimistisia, kuten pitääkin. Tilanne on pakottanut aina vain syventämään tuotekehitystä ja kohdentamaan taloudellisia resursseja yhä tarkemmin etsimällä uusia ja parempia ratkaisuja. Avainhenkilökatastrofin jälkeen on onnistuttu rekrytoimaan uutta ja oppimishaluista henkilökuntaa. Rakennettavien järjestelmien komponentit ja ominaisuudet muuttuvat ja kehittyvät. Toimiakseen ne vaativat laajaa ohjelmisto- ja ohjelmointityötä. Yrittäjät arvioivat, että kun kehitellyt tuoteuutuudet saadaan markkinoille, liikevaihto saadaan yhä selvempään nousuun, mistä on ollut viitteitä parin viimeisen vuoden aikana.

Yrittäjän tulevaisuuden näkymän kannalta erittäin tärkeä asia on, että hänen poikansa Ville Kuoppala on nuoresta iästään huolimatta jo vankasti mukana yritystoiminnassa. Atk-taitojensa avulla hän itse asiassa johtaa yrityksen tietohallintoa ja osallistuu itse sen päivittäiseen toimintaan.

5. Johtopäätöksiä

Sisäisen tietoturvan kehittäminen ja sen avulla riskien pienentäminen vaatii taloudellisten resurssien lisäksi huomattavaa asiaan perehtymistä ja yrityksen reagointikykyä. Sisäisen tietoturvan ongelmat ovat usein hyvin ennalta arvaamattomia ja niiden vaikutukset yrityksen liiketoimintaan todella vakavia. Kun joku sisäisen tietoturvan osa-alueista pettää totaalisesti, siitä seuraa merkittäviä taloudellisia menetyksiä tai yrityksen toimita saattaa keskeytyä joksikin aikaa tai kokonaan. Koska seuraukset ovat merkittävät, tällaisesta tilanteesta toipuminen on yleensä todellisten ponnistelujen tulos, ja onnistuminen vaatii jo sitä kuuluisaa tuuria. Tutkittavassa case-yrityksessä pelastava tekijä tilanteessa oli yrittäjän henkilökohtaisten sijoitusten realisointi.

Sisäisen tietoturvan riskejä pystytään merkittävästi pienentämään kiinnittämällä niihin huomiota. Hyvän sisäisen tietoturvan kivijalkana on siihen liittyvän suunnitelman tekeminen ja sen tarkoituksen avoin selvittäminen henkilöstölle. Hyvä sisäinen tietoturva vaatii todella valveutunutta näkökulmaa tietoturvaan yleensä. Se ei ole kuitenkaan niin helppoa kuin sen yleisesti mielletään olevan. Yrityksen tietoturvasta puhuttaessa päähuomio keskittyy liian usein ulkoisten tietoturvakysymysten tarkastelemiseen ja niiden ratkaisujen etsimiseen. Syy tähän on, että yrityksille suunnattua informaatiota sisäisen tietoturvan ei ole juurikaan saatavilla, minkä seurauksena yrittäjien taitotiedon puute tässä asiassa ei ole yllätys.

Tutkimuksen perusteella voidaan sanoa, että sisäisen tietoturvan kehittäminen ei ole niin kallista kuin kuvitellaan. Se pitää sisällään paljon sellaisia toimintoja, joiden toteuttaminen vaatii vain asiaan perehtymistä ja yrittäjän omaa aikaa sen toteuttamiseen: kustannukset ovat vuositasolla merkityksettömiä kuten esimerkiksi palovakuutus. Nämä toiminnot ovat jo laajuudeltaan sellaiset, että sisäisen tietoturvan taso nousee huomattavasti. Taloudellisesta panostuksesta riippumattomat toiminnot sisältävät

ennaltaehkäiseviä ja tilannetta kartoittavia toimintoja. Lisäksi sisäisen tietoturvan kehittäminen pitää sisällään paljon henkilöturvallisuuden toimintoja. Kuten tutkittavan case-yrityksen tapauksessa huomataan, henkilöturvallisuus on yksittäisenä osa-alueena se, josta seuraa vakavimmat ja tuhoisimmat vahingot niiden toteutuessa.

Taloudellisia resursseja vaativat toiminnot ovat yleensä seurausta kehittyneestä ja järjestelmällisestä sisäisen tietoturvan kehittämisestä. Vaikka kaikki toiminnot ovatkin keskeisiä ja niiden toimivuus on osaksi kiinni toisistaan, se ei ole esteenä toiminnan aloittamiselle. Taloudellisten resurssien merkitys lisääntyy samassa suhteessa kuin yrityksen toiminta laajenee sekä henkilöstön ja tiedon määrä kasvaa. Tässä tilanteessa taloudelliset resurssit ovatkin usein kasvaneet ja mahdollistaneet sisäisen tietoturvan kehittämisen. Tässä kohdassa avaintekijäksi nousee se, että liiketoiminnan kasvaessa muistetaan suunnitelmaan kirjatut tavoitteet. Vaikka toiminta onkin sillä hetkellä turvallista, on muistettava, että vahingon sattuessa menetykset nousevat samassa suhteessa.

Tutkimus on osoittanut myös sen, että sisäisen tietoturvan kehittämisessä ei ole yhtä mallia tai kaavaa, jolla kaikkien yritysten tulee toimia. Sisäisen tietoturvan ratkaisut ovat aina suhteessa yrityksen toimialaan. Innovatiivinen ja tietointensiivinen yritys on paljon riippuvaisempi sisäisen tietoturvan ratkaisuista kuin sellainen yritys, jossa yritystoiminnan keskeisintä on suorittava työ. Esimerkiksi tutkitun case-yrityksen ja autokorjaamon välillä sisäisen tietoturvan kehittämiseen on suhtauduttava eri intensiteetillä. Sisäisen tietoturvan ratkaisut eivät saa koskaan muodostua liian raskaiksi, jolloin niiden tuoma hyöty ylittää niihin sijoitetut resurssit. Sisäistä tietoturvaa ei saa myöskään kehittää niin, että henkilöstö kokee sen työtä haittaavaksi tai heidän toimintaansa rajoittavaksi.

Sisäisen tietoturvaohjeistuksen noudattamisen valvonta on myös keskeistä. Sen avulla pystytään ennakoimaan ja ennen kaikkea reagoimaan tuleviin ongelmiin. Hyvän ja organisoidun valvonnan avulla pystytään usein välttämään pahin mahdollinen. Valvonta on osa hyvää tietoturvajohtamista. Hyvä tietoturvajohtaminen näkyy jokapäiväisessä toiminnassa ja sen ratkaisujen tulee olla kaikille tasapuolisia: ratkaisuja ei tarvitse selittää henkilökunnalle, vaan ne tulee rakentaa ja ohjeistaa niin, että kaikki ymmärtävät, miksi ne ovat olemassa.

Yritystoiminnan kehittyessä tietyt työntekijät nousevat yrityksessä avainasemaan. Näiden avainhenkilöiden merkitys on tiedostettava hyvissä ajoin, ja toiminnan jatkuvuuden kannalta on tehtävä ratkaisuja sellaista tilannetta varten, jossa avainhenkilö ei ole enää yrityksen palveluksessa tai hän on joistain syystä estynyt tekemään työtään. Mitä tärkeämpi avainhenkilö on yritykselle, sitä vaikeampi hänelle on tehdä varahenkilöjärjestelyjä. On kuitenkin ehdotonta varmistua siitä, että kenenkään työntekijän asema yrityksessä ei ole sellainen, että tämän lähdettyä yrityksestä, sen toiminta häiriintyy vakavasti tai loppuu kokonaan. Fyysisiä riskejä vastaan pystytään aina ottamaan vakuutus, mutta avainhenkilön osaamiselle ei sellaista ole tarjolla.

Vaikka sisäinen tietoturva olisi ollut tutkittavassa yrityksessä niin kehittynyttä kuin se sen hetkisillä ratkaisuilla oli mahdollista, se ei kuitenkaan olisi poistanut riskiä kokonaan. Kun kyse on ihmisen tekemistä henkilökohtaisista ratkaisuista, niitä ei millään teknisellä ratkaisulla pystytä sulkemaan pois. On täysin selvää, että BK-Automationissa sisäisen tietoturvan tila oli vähintäänkin heikko. On ymmärrettävää, että yrittäjällä ei ollut mahdollisuutta saada siitä tietoa samassa määrin kuin ulkoisesta tietoturvasta, mutta näin jälkeenpäin asiaa tarkasteltuna voidaan sanoa, että tilaisuus teki varkaan. Koska kaikki yrityksen tieto oli tarjolla, niin niiden käyttäminen väärin henkilökohtaisen edun saavuttamiseksi oli liian helppoa. Ongelmaksi

tässä yrityksessä nousikin se, että tekijöiden saattaminen edesvastuuseen tapahtuneesta ei onnistunut, koska sisäisen tietoturvan ratkaisut juuri henkilöstöturvallisuudessa ja tiedon suojaamisessa olivat täysin olemattomat.

On täysin mahdoton sanoa, mikä oli lähteneiden työntekijöiden toimien todellinen syy ja olisiko tämä tapahtunut joka tapauksessa, mutta se on varmaa, että palkankorotukset, henkilöstön kouluttaminen ja kaikenlainen muu sitouttaminen olisi pienentänyt riskiä. Tässä tapauksessa työntekijät näkivät, että ruoho oli vihreämpää aidan toisella puolella. Yrittäjän harmiksi työntekijät ottivat niin sanotusti yrityksen ruohonleikkurin mukaan.

Koska tutkimuksessa on käytetty case-menetelmää, voidaan esimerkinomaisesti asettaa muutamia hypoteettisia mitä jos -ajatuksia. Mikä olisi BK-Automationin nykytilanne, jos sisäisen tietoturvan riskeihin olisi kiinnitetty huomiota jo yrityksen perustamisvaiheessa? Olisivatko työntekijät lähteneet yrityksestä perustamaan omaa liiketoimintaa, jos yrityksessä olisi ollut kannustavampi palkitsemisjärjestelmä kuin perinteinen kuukausipalkka, ja jos yritys olisi panostanut työntekijöiden kouluttamiseen? Mikä olisi ollut työntekijöiden rangaistus, jos henkilöturvallisuuteen liittyviin asioihin olisi kiinnitetty huomiota, ja yrityksen tietojärjestelmistä olisi ollut selvä merkintä niiden kopioimisesta? Sisäinen tietoturva ei ole sen tärkeämpi kuin ulkoinen, mutta siihen on keskittyvä samalla intensiteetillä kuin ulkoiseen. Sisäinen ja ulkoinen tietoturva muodostavat yhdessä yrityksen riskejä pienentävän tietoturvan, ja ne varmistavat toiminnan jatkuvuuden mahdollisen tietovuodon ja vahingon sattuessa.

6. Yhteenveto ja jatkotutkimuskohteet

On harvinaista, että näin laaja tietoturvaa ja tietovarkautta koskeva rikosvyyhti, ja erityisesti juuri pk-yrityksessä tulee median kautta yleiseen tietoisuuteen. Kuten tässä tutkimuksessa on todettu, kyseisiä rikoksia voidaan olettaa tapahtuvan paljon enemmänkin, mutta niistä ei puhuta tai tiedetä. Rikoksesta ei välttämättä tiedetä edes siinä yrityksessä, joka on joutunut kyseisen rikollisuuden kohteeksi.

Koska on kysymys hankalasti määriteltävistä asioista ja käsitteistä, kuten tietojen yksilöllisyys, persoonallisuus, tekijänoikeudet yms., tässä tutkimuksessa kuvattu oikeusprosessi oli sangen hankala, suuritöinen ja kallis. Vaikka kyseisen tietovarkauden vahingot yrityksen liiketoiminnalle ja yrittäjille pystyttiin talousasiantuntijan tekemien laskelmien perusteella osoittamaan, oikeusprosessin tulos oli täysin erilainen kuin mitä monet asiantuntijat, saati maallikko, tapaukseen tutustuttuaan voisi odottaa. Tämä nähtiin myös case-yrityksen tapauksessa. Käytännössä BK-Automationin oikeusprosessin päätyttyä saamat korvaukset olivat lähes olemattomat. Case-yrityksen tapaus osoitti myös, että työnantajalla, siis tässä tapauksessa BK-Automationilla, oli vastuu siitä, ettei se ollut työsopimuskeinoin tai muilla sopimuksilla, kuten kilpailukieltosopimuksilla, erityisesti kieltänyt työntekijöitään tekemästä rikoksia.

Mielenkiintoinen jatkotutkimusaihe olisikin selvittää, kuinka yleisiä sisäisen tietoturvan puutteet ja riskit ovat yleensä pk-yrityksissä, sillä on hyvin todennäköistä, ettei case-yritys tässä suhteessa ole varmaankaan uniikkitapaus. Samalla voitaisiin sisäisen tietoturvan pettämiseen kehitellä erityinen vakuutusturva. Kauppa- ja teollisuusministeriö on tänä keväänä teettänyt pk-yritysten tietoturvaa koskevan tutkimuksen, jossa sisäistä tietoturvaa kartoitetaan kuitenkin melko vähän [Kyselytutkimus, 2006]. Toinen jatkotutkimusaihe voisi olla vaikkapa tässä tutkimuksessa esitellyn casen

tarkastelu juridisesta näkökulmasta, ja tutkimuksen voisi suorittaa esimerkiksi oikeustieteen opiskelija pro gradu -tutkimuksenaan. Tutkimuksessa voitaisiin tarkastella juuri tekijänoikeuksia, kopiointioikeuksia, sopimusoikeutta ja sisäistä tietoturvaa muulla tavoin kuin ne tässä tutkimuksessa on esitetty. Kolmas jatkotutkimusaihe voisi olla tämän rikosasian psykologisten vaikuttimien tutkiminen, mikä olisi mielenkiintoista poliisinkin tekemän rikoksentekijän profiloinnin kannalta. Tärkeätä olisi saada tietoa siitä, voidaanko tällaiseen rikokseen motivoituvan ja ryhtyvän henkilön riskipitoisuus ainakin jollakin tasolla ennustaa esimerkiksi psykologisissa testeissä.

Lopuksi voidaan pähkinänkuoressa yhteenvetona kiteyttää, että tutkittu prosessi kaikkine kuluineen, katemenetyksineen ja hukattuine työaikoineen sekä henkisine kärsimyksineen oli valtava ns. oppirahan maksaminen. Tämän seurauksena yrityksen tietoturva, niin sisäinen kuin ulkoinenkin, ovat nyt mallikelpoisessa kunnossa. Monilla pk-yrityksillä olisikin tästä casesta varmasti opittavaa.

Lähdeluettelo

[Digitoday, 2007a] Digitoday-verkkolehti, *Sveitsiläispankki luottaa yksinomaan biometriaan tunnistuksessa*. 8.5.2007, http://www.digitoday.fi/page.php?page_id=9&news_id=200711117 (Luettu 15.5.2007).

[Digitoday, 2007b] Digitoday-verkkolehti, *Deferon pk-yrityksille: varokaa vanhoja nauhoja*, 2.4.2007, http://www.digitoday.fi/page.php?page_id=14&news_id=20078175 (Luettu 15.5.2007).

[Digitoday, 2007c] Digitoday-verkkolehti, *Tyytymätön työntekijä on vaaraksi yritykselle*. 27.4.2007, http://www.digitoday.fi/page.php?page_id=14&news_id=200710342 (Luettu 15.5.2007).

[Digitoday, 2007d] Digitoday-verkkolehti, *HP konsultoi pk-yrityksiä ilmaiseksi*, 14.3.2007, http://www.digitoday.fi/page.php?page_id=50&news_id=20076464 (Luettu 15.5.2007).

[Eriksson ja Koistinen, 2005] Päivi Eriksson ja Katri Koistinen, *Monenlainen tapaustutkimus*. Kuluttajatutkimuskeskus, Savion Kirjapaino Oy, Kerava, 2005.

[Haastattelu, 2007] Toimitusjohtaja Jukka Kuoppala, BK-Automationin kokoushuone. 1.2.2007, Nurmo (kesto n. 120 min).

[Hovioikeus, 2005a] Vaasan Hovioikeus, *Tuomio Nro 712; Diarinro R 03/1245*. Vaasa, 17.5.2005.

[Hovioikeus, 2005b] Vaasan Hovioikeus, *Tuomiolauselma Nro 712; Diarinro R 03/1245 TL: 1-9*. Vaasa, 17.5.2005.

[IBM] Oy International Business Machines, http://www-05.ibm.com/services/fi/cio/governance/ (Luettu 5.5.2007).

[If] If Vahinkovakuutusyhtiö Oy, 2007, http://www.if.fi/web/fi/commercial.nsf/noframes/0B68543550363CA1C1256CB7004A4AE4 (Luettu 27.4.2007).

[ISS] ISS palvelut Oy, 2007, http://www.fi.issworld.com/view.asp?ID=1381 (Luettu 15.5.2007).

[Ilvonen, 2006] Ilona Ilvonen, *Tietoturvallisuus Pirkanmaalaisissa Tietointensiivisissä pk-yrityksissä*. eBRC, CityoffsetOy, Tampere, 2006.

[ITviikko, 2007a] ITviikko verkkolehti, *IT-opetus jää työkaverin harteille*. 25.4.2007, http://www.itviikko.fi/page.php?page_id=46&news_id=200710046&rss=18 (Luettu 15.5.2007).

[ITviikko, 2007b] ITviikko verkkolehti, *Käräjäoikeus kielsi rekrytoinnin SysOpenista*. 11.4.2007, http://www.itviikko.fi/page.php?page_id=46&news_id=20078684&rss=18 (Luettu 15.5.2007).

[Järvinen, 2002] Petteri Järvinen, *Tietoturva & Yksityisyys*. WS Bookwell, Porvoo, 2002.

[Järvinen ja Järvinen, 2004] Pertti Järvinen ja Annikki Järvinen, *Tutkimustyön metodeista*. Opinpaja Oy, Tampere, 2004.

[Kainomaa, 1984] Seppo Kainomaa, *Tietoturva sekä Vahingot ja Väärinkäytökset ATK:ssa – Yleiskatsaus ja yhteenveto suoritetusta organisaatiokyselystä*. Tietotekniikan Kehittämiskeskus Ry, Helsinki, Helmikuu 1984.

[Kajava et al., 1996] Jorma Kajava, Sami Heikkinen, Paavo Jurvelin, Tero Viiru ja Päivi Parviainen, *Tietojenkäsittelyn ulkoistaminen ja tietoturva – Information Security Research from Information Processing Outsourcing*, s. 13–19, Working papers series B 42, Oulu, Toukokuu 1996.

[Kajava ja Leiwo, 1994] Jorma Kajava ja Jussipekka Leiwo, *Tietoturvahenkilöstö Organisaatiossa – Information Security Staff in Organizations*. Working papers series B 34, Oulu, Joulukuu 1994.

[Kajava ja Remes, 2000] Jorma Kajava ja Timo Remes, *Inranet Security from Organizational Point of View*, Working papers series B 59. Oulu, Maaliskuu 2000.

[Kyselytutkimus, 2006] Kauppa- ja Teollisuus Ministeriö, *Pk-yritysten tietoturvakysely 2006*. Tietoykkönen Oy, Jyväskylä/Vantaa, 2006, http://julkaisurekisteri.ktm.fi/ktm_jur/ktmjur.nsf/41bebb1e5a750661c2256b27004dbea3/e546d8a775141f0ac225727b003e0ae9/$FILE/Pk-yritystentietoturvakysely.pdf (Luettu 14.4.2007).

[Käräjäoikeus, 2003a] Seinäjoen Käräjäoikeus, *Tuomio Nro 03/526; Diarinro R 03/50*. Seinäjoki, 25.7.2003.

[Käräjäoikeus, 2003b] Seinäjoen Käräjäoikeus, *Tuomiolauselma Nro 526; Diarinro R 03/50 TL: 1–9*. Seinäjoki, 25.7.2003.

[Laaksonen et al., 2006] Mika Laaksonen, Terho Nevasalo ja Karri Tomula, *Yrityksen tietoturvakäsikirja – Ohjeistus, toteutus ja lainsäädäntö*. Oy Nordprint Ab, Helsinki, 2006.

[Laskelma, 2001] Kari Rantala, SVH PricewaterhouseCoopers Oy, *Laskelma BK-Automation Ky:lle aiheutuneista vaihingoista.* Seinäjoki, 12.3.2001 (suurelta osin salainen).

[Leiwo ja Kajava, 1994a] Jussipekka Leiwo ja Jorma Kajava, *Tietojenkäsittelyn Varmistaminen Yrityksen Turvallisuusjärjestelyjen Osana*. Working papers series B 31, Oulu, Syyskuu 1994.

[Leiwo ja Kajava, 1994b] Jussipekka Leiwo ja Jorma Kajava, *Erään Peinen Organisaation Tietorikosketjun Tarkastelua – An Analysis of a Typical Information Crime Series in a Small Organization*. Working papers series B 32, Oulu, Syyskuu 1994.

[Luentomoniste, 2004] Timo Tuomivaara, *Y125: Tieteellisen tutkimuksen perusteet*. Helsingin Yliopisto, Helsinki, 2004.

[Miettinen, 1999] Juha E. Miettinen, *Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan*. Kauppakaari Oy, Helsinki, 1999.

[Miettinen et al., 2006] Tarmo Miettinen, Anssi Keinänen ja Miia Laukkanen, *Pientyönantajan työoikeudelliset ongelmat ja neuvontapalvelu*. Hakapaino Oy, Helsinki, 2006.

[Mäntylä ja Kajava,1996] Vesa Mäntylä ja Jorma Kajava, *Järjestelmähallinnan tietoturva – Information Security in Systems Management*. Working papers series B 46, Oulu, Marraskuu 1996.

[Paavilainen, 1998] Juhani Paavilainen, *Tietoturva*. Gummerus Kirjapaino Oy, Jyväskylä, 1998.

[Perren ja Ram, 2004] L. Perren and M. Ram, *Case-Study Method in Small Business and Entrepreneurial Research: Mapping Boundaries and Perspectives*. International Small Business Journal, 22(1) 83–101.

[Pirnes et al., 2000] Jari Pirnes, Anssi Salmela ja Jorma Kajava, *Tietoturva ja Sisäinen Valvonta – Information Security and Internal Control*. Working papers series B 62, Oulu, Marraskuu 2000.

[Pk-yritys] Euroopan unionin virallinen lehti L 124/36, 20.5.2003, ec.europa.eu/enterprise/enterprise_policy/sme_definition/sme_user_guide fi.pdf. (Luettu 5.3.2007).

[Securitas] Securitas Oy Turvallisuuspalvelut, 2007, https://www.securitas.fi/pages/secwebfi.nsf/sp?open&cid=Home (Luettu 15.5.2007).

[Sisäasiainministeriö] Sisäasianministeriö, 2007, http://www.intermin.fi/intermin/hankkeet/biometria/home.nsf/pages/4BB93202E6BDC28AC225701C004319D4 (Luettu 15.5.2007).

[Vahti 4/2003] *Valtionhallinnon tietoturvakäsitteistö*. Valtionvarainministeriö, Helsinki, 2003 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf (Luettu 15.5.2007).

[Vahti 6/2006] *Tietoturvatavoitteiden asettaminen ja mittaaminen*. Valtionvarainministeriö, Edita Prima Oy, Helsinki, 2006.

[Valtionvarainministeriö, 6/1992] Kaarlo Korvola, Teemupekka Virtanen, Rauli Parmes, Aulis Gerlander, Heikki Hietanen, Erkki Leiviskä, Kari Suvila ja Matti Tenhunen, *Valtiohallinnon tietoturvallisuuspäätös 6/1992*, 1992.

[VTT] Pk-yrityksen henkilöriskit, 2000, VTT Automaatio, Turun kauppakorkeakoulu, Työterveyslaitos ja Tampereen teknillinen korkeakoulu(PK-RH hanke), http://www.pk-rh.fi/ftp/kalvot/kal-henkiloriskit.pdf (Luettu 15.5.2007).

Liitteet

LIITE 1: KYSYMYSLOMAKE [Ilvonen, 2006]

Haastattelu BK-automationissa 1.2.2007

Taustatietoa

1. Yrityksen toiminnan lyhyt kuvaus (toimiala, asiakkaat, toimittajat)

2. Tilojen kuvaus (mm. toimistoympäristö, tuotantolaiteet, onko jaettu muiden yritysten kanssa?)

3. Työntekijöiden määrä yrityksessä

4. Mitä tietoturvallisuus on?

5. Minkälaista tieto yrityksessä käsitellään?

6. Mitä toimintoja yrityksessänne on ulkoistettu (esim. siivous, vartiointi, IT-palveluja)?

7. Onko yrityksen arvot määritelty? Onko arvoissa tai niitä selittävissä dokumentaatioissa viittauksia tietoturvallisuuden arvoihin eli tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen?

Totaalisen tietovuodon kuvaus

– koska?
– miten?
– miksi?
– olisiko tämän voinut estää, miten?
– toipuminen
– selvät toimintatapamuutokset

Hallinnollinen turvallisuus

1. Kuvaile tieturvallisuuspolitiikkaanne (tavoitteet, laajuus, dokumentointi). Millaisia dokumenttikokonaisuudella tietoturvallisuutta hallitaan, ts. onko eri osa-alueille muodostettu omaa

tietoturvallisuuspolitiikkaa (esim. yleinen tietoturvapolitiikka, verkon tietoturvapolitiikka, sisäinen tietoturva)?

2. Miten vastuu tietoturvallisuudesta on jaettu eri organisaatiotasoille? Kuinka tietoturvallisuusvastuista viestitetään?

3. Valvotaanko tietoturvallisuuspolitiikan tai -ohjeistuksen noudattamista? Miten noudattamista valvotaan?

Henkilöstöturvallisuus

1. Miten yrityksessä kehitetään tietoturvallisuustietoisuutta eli henkilökunnan asenteita ja motivaatiota tietoturvallisuutta kohtaan?

2. Miten työntekijä koulutetaan tietoturvallisuuteen liittyvissä asioissa? Onko uusille työntekijöille olemassa valmista koulutuspakettia tai ohjeistusta? Jos ei, niin miksi?

3. Onko sisäisestä tietoturvasta erillistä ohjeistusta (esim. luotettaviksi/salaisiksi luokiteltujen tietojen kopiointi ja/tai vieminen pois yrityksen tiloista)?

4. Kuinka työntekijöiden tausta selvitetään rekrytointitilanteessa (rikosrekisteri, suosittelijan lausunnot yms.)?

5. Millaisia turvallisuusmääräyksiä ja ehtoja kirjataan työsopimuksiin (esim. kohtuullisuus)?

6. Onko työntekijöillä mahdollisuus etätyöskentelyyn? Miten etätyöskentely on hoidettu?

7. Onko yrityksessä dokumentoituja tai muuten vakiintuneita toimintatapoja työsuhteen päättyessä (pääsy/käyttöoikeuden hallinta, työhön liittyvän materiaalin hallinta)?

Ohjelmisto-, laitteisto- ja tietoliikenteen turvallisuus

1. Onko työntekijöillä oikeus asentaa ohjelmia tietokoneelleen? Miten käytössä olevien ohjelmien ylläpito on organisoitu?

2. Miten yrityksessä on lupa käyttää siirrettäviä medioita (esim. USB-muisti, CD, disketti)?

3. Onko kannettavien tietokoneiden kovalevyt salattu? Miksi ei?

4. Onko yrityksellä käytössä servereitä vai onko tieto yksittäisillä tietoasemilla? Jos servereitä on, onko niillä minkälainen logi-tiedostojärjestelmä tai tapahtumadokumentointi järjestelmä?

5. Kuka ottaa ja kuinka usein varmuuskopiot kriittisistä tiedoista? Missä varmuuskopioita säilytetään?

6. Kuinka eri työpisteiden autentikointi (oikeaksi tunnistaminen) on järjestetty?

7. Minkälainen varmuuskopiointipolitiikka yrityksessä on? Miten varmuuskopiointi on käytännössä organisoitu? Missä varmuuskopioita säilytetään?

8. Valvotaanko Internet- ja intranet liikennettä?

Fyysinen turvallisuus

1. Onko toimitiloissa kulunvalvontajärjestelmä? Minkälainen? Kuinka toimitilan kulkuoikeudet ja -säännöt on määritelty? Käytetäänkö videovalvontaa ja miten?

2. Miten vierailija tunnistetaan/kirjataan? Onko yrityksessä määritelty sääntöjä, jotka koskevat vierailijoita?

3. Kuinka pääsy tietoturvallisuuden kannalta merkittävimpiin paikkoihin on järjestetty (esim. palvelinhuoneet, arkistotilat)?

4. Kuinka tulipalon ja vesivahingon tunnistus, hälytys ja torjunta on järjestetty?

Tietoaineisto- ja käyttöturvallisuus

1. Onko yrityksessä määritelty politiikka tietojärjestelmiin pääsylle (esim. käytetäänkö henkilökohtaista käyttäjätunnusta ja salasanaa)?

2. Minkälainen salasanapolitiikka yrityksessä on? Miten sen noudattamista valvotaan?

3. Kuinka tieto on luokiteltu (luokittelutapa, kuinka käsitellään ja kuinka hävitetään)? Onko se dokumentoitu?

4. Onko työntekijöiden pääsyoikeuksia rajoitettu vain heidän työtehtävissään tarvitsemiin tietoihin? Onko henkilöstön tehtävien jaossa kiinnitetty huomiota turvattomiin/vaarallisiin työyhdistelmiin?

5. Onko kriittisiin tietoihin/tiedostoihin merkitty omistaja?

Liiketoiminnan jatkuvuus ja riskienhallinta

1. Millä tavalla yrityksessä arvioidaan tietoturvallisuuteen liittyviä riskejä? Kuka niitä arvioi? Kuinka usein niitä arvioidaan?

2. Kuvaile menettelytapoja liiketoiminnan jatkuvuuden varmistamiseksi ongelma/häiriötilanteissa (esim. liiketoiminnan jatkuvuussuunnitelma, suunnitelma onnettomuustilanteista selviämiseksi, mahdolliset varahenkilöt avainhenkilöiden tilalle).

3. Käytetäänkö agenttien, jällenmyyjien, alihankkijoiden tai yhteistyökumppaneiden kanssa salassapitosopimuksia?

4. Miten yrityksenne käsitystä tietoturvallisuudesta viestitään asiakkaille ja toimittajille?

LIITE 2: LEHDISTÖTIEDOITE

BK-automation ky

11.11.1998

LEHDISTÖTIEDOTE

BK-automation on korkean teknologian yritys, joka on urakkakilpailuissa voittanut ja menestyksellisesti toteuttanut lukuisia projekteja Suomessa ja ulkomailla. Projektien joukossa on hyvin vaativia, mm. Kiinassa yhdessä Lemminkäinen Oy:n kanssa toteutetut vesi- ja jätevesilaitoshankkeet.

Automaatio on yrityksen ydinosaamista. Toiminta-ajatuksena on tehdä systeemien hallitseminen helpommaksi ja tarkemmaksi. Yrityksen perusti tätä periaatetta toteuttamaan Asko Kuoppala Ähtärissä 1982. Yhtiössä työskentelee tällä hetkellä 12 teknikan erityisosaajaa, joista useimmat ovat insinöörejä. Yrityksen kotipaikka on vuodesta 1992 ollut Seinäjoki. Viimeisen kymmenen vuoden aikana yritys on keskittynyt vesitekniikan automaation ja kaukokäytön kehittämiseen. Asiakkaina on ollut kuntia, kaupunkeja, tuorantolaitoksia ja vesihuoltoyhtiöitä. Laajoja kaukokäyttöjärjestelmiä on toimitettu yhteensä yli 30.

Vuonna 1990 BK-automation solmi lisenssisopimuksen ABB:n kanssa, joka toi BK-automationin asiakkaille ison talon koulutusjärjestelmän edun ja laitteistojen huollon sekä takuun tuoman varmuuden.

Erikoistuminen

Aluksi yritys toimitti automatisointia ja kaukokäyttöjä hyvin monille aloille. Perusajatus oli kuitenkin alusta tuottaa asiakkaillemme etua kontrolloimalla ja kauko-ohjaamalla prosesseja entistä paremmin ja tarkemmin. Nykyisin keskitymme toimittamaan ja asentamaan laitteita vedenkäsittelyyn niin puhdasvesilaitoksiin kuin viemärilaitoksiin sekä ympäristön valvontaan, mikä aiheuttaa tänä päivänä eniten kysyntää. BK-automation on edelläkävijä vedenkäsittelyn valvonnan ohjauksen ja toimintojen dokumentoinnin kehittämisessä. Meillä on pitkä kokemus näiden toimintojen rakentamisesta ja yhdessä pysymme kehittämään taanusi hyviä ja kaikki lainsäädännön vaatimukset toteuttavia ratkaisuja.

Kunnioittavasti

Asko Kuoppala

osoite	puhelin	telephone	address
BK-automation Ky	06-2140 120	+358-6-2140 120	BK-automation
PL 901	fax	fax	P.O.Box 901
60101 SEINÄJOKI	06-2190 131	+358-6-2190 131	FIN-60101 SEINÄJOKI FINLAND

LIITE 3: LEHTIARTIKKELI

ILTALEHTI

15.5.2003

Entisiä työntekijöitä epäillään tietovarkauksista

Kahdeksaa Seinäjoella toimivan tietotekniikkayrityksen entista työntekijää epäillään tietovarkauksista. Laajan tietovarkausjutun valmisteluistunto pidettiin Seinäjoen käräjäoikeudessa eilen. Jutun pääkäsittely alkaa kesäkuun alkupuolella.

Tietovarkaudet tapahtuivat vuosina 1998–1999. Epäillyt olivat tallenteita jaljentämällä hankkineet salaa tietoa yritykselle kuuluneista yrityssalaisuuksista. Myöhemmin tietoja käytettiin hyväksi epäiltyjen perustaman oman yrityksen liiketoiminnassa.

Syyttäjä vaatii epäillyille rangaistuksia yritysvakoilusta, rekijänoikeusrikoksista ja yrityssalaisuuden väärinkäytöstä. Lisäksi epäillyiltä ja heidän perustamaltaan yritykseltä haetaan runsaan miljoonan euron vahingonkorvauksia.

Asianomistajien mukaan vohkituissa tiedostoissa oli yhdisteltynä suuri määrä yrityksen avaintietoja ja teosta koitui huomattavaa taloudellista vahinkoa. Entisiä työntekijöitä epäillään yksityiskohtaisten tietojen haltuunottamisesta ja käyttämisestä omassa liiketoiminnassa.

Tapauksen tutkinta aloitettiin loppuvuonna 1999, kun tietotekniikkayrityksen johto oli havainnut tietovarkaudet.