LAUREA

Kohti parempaa tietoturvaa pienyrityksessä

Kaukver, Hanna

2012 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Kohti parempaa tietoturvaa pienyrityksessä

Kaukver, Hanna
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Kaukver, Hanna

Kohti parempaa tietoturvaa pienyrityksessä

Vuosi 2012 Sivumäärä 42

Tämä opinnäytetyö käsittelee tietoturvaa yleisellä tasolla, ja pureutuu tietoturvallisuuden hallinnan, -johtamisen ja henkilöstön tietoturvan yleisimpiin uhkiin sekä niiden turvallisuusmenettelyihin. Yritys Oy:n johto ilmaisi tarpeen tälle opinnäytetyölle yrityksen tiloissa tapahtuneen kolmannen vesivahingon jälkeen. Päätettiin samalla tarkastella yrityksen tietoturvallisuuden tasoa laajemmassa mittakaavassa ja käsitellä eteentulevat mahdolliset tietoturvauhat.

Tämän opinnäytetyön tavoitteena oli sisäistää ja ymmärtää pääasiassa tietoturvallisuuden johtamisen ja henkilöstön tietoturvan tietoturvastandardit ja tehdä niiden pohjalta kohdeyritykselle kokonaisvaltainen suunnitelma tietoturvan hallinnasta, sekä laatia sen henkilöstölle oma tietoturvaohjeistus. Tarkoituksena oli hallita ja ohjata kohdeyrityksen tietoturvaa kokonaisvaltaisesti. Muutosta tai muita toimenpiteitä vaativat esiintulevat tehtävät toteutettiin, jolloin työn päättyessä toimeksiantajan tietoturvan hallinta on ajanmukaisella ja vaaditulla tasolla.

Asiasanat: tietoturva, BSI, konstruktiivinen tutkimus, henkilöstöturvallisuus, henkilöstön tietoturvaohjeistus

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Kaukver, Hanna

Towards better information security in a small business

Year 2012 Pages 42

This thesis focuses on information security in general and, more specifically, on information security management, leadership, and personnel security as well as the most common threats to their safety procedures. Company Ltd's management expressed the need for this thesis after the third water damage in their premises. It was decided at the same time to look into the company's level of information security on a larger scale and address potential security threats.

The purpose of this thesis was mainly to internalize and understand information security management and personnel security as well as information security standards. Based on the standards, the purpose was also to design a comprehensive plan for information security management for the target company, and to draw up its own security personnel manual. The objective was to manage and control the target company's data security as a whole. Tasks requiring alterations or other measures were carried out, and thus the company's information security management was on an up-to date and requisite level when the thesis project was finalized.

Key Words: Information Security, BSI, constructive research, personnel security, personnel security guide

Sisällys

1 Johdanto

Tietoturva on nykyaikaisessa yrityksessä laaja käsite. Käsite sisältää yrityksen fyysisen turvallisuuden lisäksi laaditut tietoturvasäännöt, ohjelmistojen valinnat ja käyttäjien tietoturvatietoisuuden.

Tietoturvahallinto sekä -organisaatio sisältää tietoturvan perusratkaisut, kuten: Miten yrityksessä käsitellään tietoturvaa? Onko sitä laisinkaan, tai pidetäänkö sitä yllä? Kuka on vastuussa ja kenelle?

Olen rakentanut työni niin, että ensin kerron mitä tietoturvallisuus on, mitä hyvä tietoturvallisuus vaatii, ja mitä se toteutuessaan antaa. Tämän jälkeen käyn läpi valitsemani teorian kautta kohdeyritykselleni kolme parhaiten soveltuvaa tietoturvallisuuden osa-aluetta. Kehitysehdotuksiin ja johtopäätöksiin päästään kohdeyrityksen nykytilakartoituksen kautta, minkä teen käyttämäni teorian pohjalta.

Olen valinnut tutkimukseni kohteeksi pienen yrityksen, jossa itse työskentelen. Yritys ei halua tulla tunnistetuksi näin arkaa aihetta käsiteltäessä ja siksi käytän siitä termiä Yritys Oy tai kohdeyritys. Ajatus tähän opinnäytetyöhön lähti, kun Yritys Oy:n toimitiloissa tapahtui kolmas vesivahinko vähän ajan sisään. Palvelinkoneen tietoturvan parantamista piti lähteä kartoittamaan, ja ajateltiin tehdä samalla tietoturvallisuuden kartoittaminen laajemmassa mittakaavassa. Tietoturvallisuus ja manuaalit, johon työni teoria pohjautuu on laaja ja siksi rajaan työni koskemaan vain kolmea tietoturvallisuuden osa-aluetta: tietoturvallisuuden hallintaa,-johtamista ja henkilöstön tietoturvaa. Tutkimuksessani keskityn erityisesti henkilöstöön tekemällä heille tietoturvaohjeistuksen.

Tavoitteenani on sisäistää ja ymmärtää pääasiassa tietoturvallisuuden johtamisen ja henkilöstön tietoturvan tietoturvastandardit ja tehdä niiden pohjalta kohdeyritykselleni kokonaisvaltainen suunnitelma tietoturvan hallinnasta, sekä laatia sen henkilöstölle oma tietoturvaohjeistus. Tarkoituksenani on hallita ja ohjata kohdeyrityksen tietoturvaa kokonaisvaltaisesti. Muutosta tai muita toimenpiteitä vaativat esiintulevat tehtävät on tarkoitus toteuttaa, jolloin työni päättyessä toimeksiantajan tietoturvan hallinta on ajanmukaisella ja vaaditulla tasolla.

2 Tutkimusongelma ja tutkimusmenetelmän valinta

Hakiessani työhöni parhaiten sopivaa tutkimusmenetelmää, tarkastelin asiaa ensin hyvin suppeasti: kahdelta kannalta, jotka olivat kvalitatiivinen (laadullinen) ja kvantitatiivinen (määrällinen). Lukiessani kvantitatiivisen ja kvalitatiivisen tutkimuksen erottelua Hirsjärven kirjasta Tutki ja Kirjoita (1997, 126), tulin siihen tulokseen, ettei työni kannalta paras ratkaisu olisi valita näistä jompaa kumpaa. Päätin laajentaa tietämystäni tutkimusmenetelmistä, jolloin löysin parhaiten tämän opinnäytetyön tarpeisiin sopivan menetelmän.

Tutkimusongelmani kasvoi työn myötä koko ajan, koska työn aikana haluttiin saada konkreettisia muutoksia aikaan. Tarkoituksena ei ollut pelkästään kartoittaa tarpeellisia toimia, vaan myös toteuttaa ne. Idea tähän opinnäytetyöhön saatiin kohdeyrityksessä tapahtuneiden vesivahinkojen kautta. Ajateltiin, että palvelinkoneen tietoturvaa tulisi parantaa vastaavanlaisten tapahtumien sattuessa uudestaan ja asiaa pohdittua päätettiin samalla tarkastella tietoturvallisuutta laaja-alaisemmin kohdeyrityksessä.

Ojasalon, Moilasen ja Ritalahden (2009, 65) mukaan konstruktiivisesta tutkimuksesta on kyse silloin, kun on tarkoitus luoda jonkinlainen konkreettinen tuotos tai suunnitelma, mittari tai malli. He jatkavat kirjassaan kehittämistyön menetelmät (2009,66) seuraavalla sivulla, että tässä tutkimusmenetelmässä pyritään ratkaisemaan jokin olemassa oleva käytännön ongelma. Konstruktiivinen tutkimus sopii parhaiten tämän opinnäytetyön tutkimusmenetelmäksi juurikin näistä syistä. Ongelma on selvillä ja siihen tarvitaan konkreettinen ratkaisu.

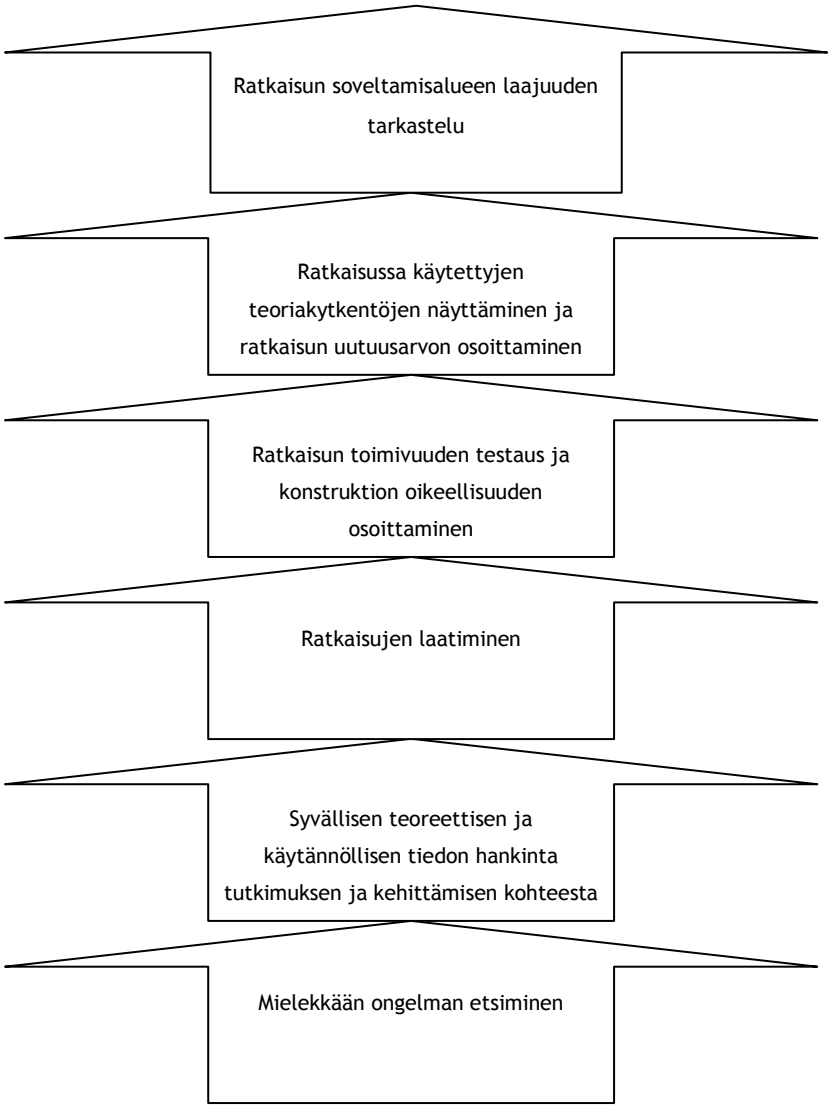
Kolmikko myös toteaa (2009, 65) konstruktiivisen tutkimuksen olevan hyvin lähellä innovaatioiden tuottamista, mutta esimerkiksi uusi kirja, budjetointijärjestelmä, yrityksen www-sivusto eivät ole innovaatioita, vaan kehitystyön tuloksena syntyneitä rakenteita. He varoittavat myös (2009, 66) sekoittamasta konsultaatiota ja konstruktiivista tutkimusta keskenään. Konsultaatiossa ei tukeuduta yhtä vahvasti aiempaan teoriaan, kun taas konstruktiivisessa tutkimuksessa se on välttämätöntä.

Konstruktiivinen tutkimus on suunnittelua ja käsitteellistä mallintamista sekä näiden mallien toteutusta ja testausta, sekä sen tavoitteena on saada ongelmaan uudenlainen ratkaisu. (Ojasalo, Moilanen, Ritalahti 2009, 65.)

Konstruktiivinen tutkimus voi kestää hyvin pitkäänkin, koska se perustuu myös uusiin ideoihin ja innovointiin. Uusia ideoita kannattaa testata esikokein ennen varsinaista testaamista. Tämän tutkimusmenetelmän eri vaiheiden dokumentointi on tärkeää. Tutkijan on kirjattava

kehittämishaaste selvästi näkyviin ja perustella työn tavoitteet selkeästi. (Ojasalo, Moilanen, Ritalahti 2009, 67.)

Konstruktiivisessa tutkimuksessa käytettäviä menetelmiä on paljon. Koska konstruktiivisen tutkimuksen tavoitteena on selkeästi kehittää yritykseen jotain uutta, tarvittava aineisto kannattaa kerätä monen eri menetelmän kautta. Tyypillisiä menetelmiä ovat havainnointi, ryhmäkeskustelu, kysely ja haastattelu. Konstruktiivisessa tutkimuksessa tutkijan rooli vaikuttaa voimakkaasti kohdeympäristössä. (Ojasalo, Moilanen, Ritalahti 2009, 68.)



Kuva 1: Konstruktiivisen tutkimuksen prosessi.

Havainnoinnin avulla on mahdollisuus saada tietoa siitä, miten ihmiset käyttäytyvät ja mitä tapahtuu heidän luonnollisessa toimintaympäristössä. Havainnointia voidaan käyttää itsenäisesti, mutta usein se tapahtuu haastattelun tai kyselyn lisänä ja tukena. Havainnoinnin

avulla voidaan täydentää haastatteluja, tai haastattelulla voidaan täydentää havainnointia. Havainnoinnin avulla saadaan helposti tietää esimerkiksi toimivatko ihmiset kuten sanovat toimivansa. (Ojasalo, Moilanen, Ritalahti 2009, 103.)

Havainnointi tässä tapauksessa osoittautui yllättävän haasteelliseksi. Kuvittelin sen olevan huomattavasti helpompaa pienyrityksessä, mutta toisin kävi. Sain toki paljon tarpeellista tietoa ihmisten käyttäytymisestä heidän luonnollisessa toimintaympäristössään, mutta tiedon jäsentely tuntui vaikealta. Tämä varmasti johtuu siitä, että olen itse tässä työssäni käyttämän kohdeyrityksen palveluksessa, jolloin oli vaikeaa asettaa itseään tavallaan ulkopuolisen tarkkailijan rooliin.

Kolmikko Ojasalo, Moilanen, Ritalahti (2009, 108) toteaa kyselytutkimusten etuna olevan, että niiden avulla voidaan kerätä laaja aineisto, jossa suurelta määrältä ihmisiä voidaan kysyä monia asioita. Tyypillisimpiä ovat postitse toimitettavat lomakkeet sekä internetissä täytettävät kyselyt. Useimmiten siis kyselytutkimusta kannattaa tehdä suurelle väkimäärälle, eli pienyrityksen tietoturvallisuuden kartoitusta ei ehkä kannata tehdä tällä menetelmällä.

Haastattelu on yksi yleisimmistä tiedonkeruumenetelmistä sekä tutkimus- että kehittämistyössä. Myös haastattelu, kuten havainnointikin kannattaa yhdistää myös toisiin menetelmiin, sillä useimmiten menetelmät tukevat hyvin toisiaan. Haastattelujen tehtävänä on useasti asioiden selventämminen tai syventäminen. Haastattelun muotoja on muun muassa teemahaastattelu, syvähaastattelu, ryhmähaastattelu ja strukturoitu eli standardoitu lomakehaastattelu. (Ojasalo, Moilanen, Ritalahti 2009, 95.)

Puolistrukturoidussa haastattelussa kysymykset laaditaan ennakkoon, mutta haastattelija voi haastattelun kulun mukaisesti vaihdella niiden järjestystä. Kysymysten tarkat sanamuodot voivat myös vaihdella ja haastattelun kuluessa voidaan kysyä uusia mieleen tulevia kysymyksiä. (Ojasalo, Moilanen, Ritalahti 2009, 97.)

Koska kyselytutkimuksen rajasimme jo pois tiedonkeruumenetelmistä, jää jäljelle ainakin havainnointi ja haastattelu. Haastattelumenetelmistä puolistrukturoitu haastattelu sopi parhaiten tutkimusongelman tarpeisiin, koska pyrin tiedonkeruullani enemmän keskustelua muistuttavaan lopputulokseen, kuin kysyjä/vastaaja –tapaan.

Kohdeyrityksen tietoturvallisuuden nykytilakartoituksen toteutan laatimalla aiheesta kysymyslistan, jonka tekisin mille tahansa yritykselle selvittäessäni asiaa. Vastaan ja avaan kysymykset keskustelujen, sekä haastattelujen pohjalta, joita olen käynyt yrityksen sisällä ja tietoliikennealan palveluita Yritys Oy:lle tarjoavan tahon kanssa.

3 Tietoturvallisuus pienyrityksessä

Tietoturva on iso osa yrityksen liiketoimintaa ja tärkeän tiedon turvaaminen on yksi menestymisen edellytys. Tieto on yrityksen liiketoiminnalle tärkeää silloin, kun sen puuttuminen, virheellisyys tai paljastuminen tuottaisivat taloudellisia tai muita vahinkoja. Tietoturvassa ei ole kyse ainoastaan tekniikasta, vaan myös ihmisten työskentelytavoista. Jokaisen tulee tietää, kuinka tietoturvasta voidaan huolehtia. Yrityksen liiketoiminnan kannalta tärkeä tieto ei usein ole vain sähköisessä muodossa, vaan kaikki tieto papereissa ja puhuttunakin on tärkeää. Hyvä tietoturva ei välttämättä vaadi suuria investointeja, vaan vähäisempikin panostus voi jo palvella yritystä hyödyllisesti. Tietoturvan ylläpito ei ole yksittäinen toimenpide, vaan se on jatkuvaa, suunnitelmallista toimintaa. (Tietoturvaopas, Yrityksen tietoturvaopas)

Yritykseen kohdistuvat uhat voivat olla tarkoituksellisia tai tahattomia. Tarkoitukselliset, laajat hyökkäykset ja tietojen kalastelut ovat nykypäivänä merkittävää teollisuusvakoilua ja menestyvissä yrityksissä onkin huolehdittu siitä, että tieto ei leviä yrityksen ulkopuolelle. Myös yrityksen sisällä piilee tietovuodon uhka.. Huolimattomuus, esimerkiksi tiedostojen salaamatta jättäminen tai arkaluontoisten yritysdokumenttien leviäminen henkilökohtaiselta koneelta voi pahimmassa tapauksessa aiheuttaa suurta taloudellista haittaa ja antaa kilpailijoille etulyöntiaseman. Tietoturvan ammattilaiset painottavat nykyään yhä enemmän yrityksen sisäisen verkon valvontaa, henkilöstön kouluttamista sekä sisäisten tietovuotojen proaktiivista torjuntaa. (It-Palvelut.org, Yrityksen tietoturva)

Suomen Internetopas –sivusto toteaa, että tietoturvalla halutaan suojata yritykselle tärkeät tiedot ulkopuolisilta. Tarvittavien toimenpiteiden kautta voidaan taata yhtiön tietojen koskemattomuus.

Klassinen tietoturvallisuuden määritelmä koostuu kolmesta perusominaisuudesta:

- luottamuksellisuus
- käytettävyys
- eheys

Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain niiden henkilöiden käytössä joille ne on tarkoitettu. Käytettävyydestä on kyse, kun tiedot ovat saatavissa riittävän nopeasti ja oikeassa muodossa. Eheydellä tarkoitetaan tiedon oikeellisuutta, eivätkä ne sisällä tahallisia tai tahattomia virheitä. (Laaksonen, Nevasalo, Tomula 2006,19.)

Näiden kolmen lisäksi tietoturvan ominaisuuksiin kuuluu myös

- pääsynvalvonta
- autentikointi
- kiistämättömyys
- tunnistaminen

Viestintäviraston internetsivuilla avataan hieman näitä neljää ominaisuutta: Pääsynvalvontaa on se, ettei tietoa tai tietojärjestelmää voida käyttää ilman lupaa. Autentikointi on osapuolten luotettavaa tunnistamista. Esimerkiksi henkilötietoja tarkasteltaessa voidaan käyttäjän tiedot tarkastaa ajokortista ja samalla käyttäjä tunnistetaan. Kiistämättömyys on todisteiden luomista varmistaakseen, ettei kukaan tietojen käsittelyn osapuoli voi jälkikäteen kiistää osuuttaan siihen. Tunnistamisella yksilöidään kohde, kuten käyttäjä tai järjestelmä. Kolmikko Laaksonen, Nevasalo ja Tomula (2006, 19) toteavat, että tietoturvallisuus on kiinteä ja keskeinen osa liiketoimintaa, ja liiketoiminta on nykyisin hyvin sidoksissa tietojärjestelmiin. Organisaation tehokkuus, toimivuus ja kehityskyky ovat yleensä osittain tai merkittävästi riippuvaisia tietojärjestelmistä ja niiden tietoturvallisuudesta.

3.1 Tietoturvallisuuden hallinta

Heiskanen, Marjokorpi, Nishio ja Nurminen (2009, 5-6) ovat käyttäneet BSI:tä pohjana tietoturvan hallinnan projektityössään ja toteavat BSI:n tulevan saksan kielen sanoista Bundesamt für Sicherheit in der Informationstechnik, ja se tarkoittaa Saksan tietoturvavirastoa. Kyseinen tietoturvavirasto on julkaissut metodologian perustason tietoturvallisuuden toteuttamisen tueksi, jonka pohjalta pääasiassa käsittelen kohdeyrityksen tietoturvauhkia ja menettelyjä. Enimmäkseen käsittelemäni teoria on alunperin paristakin englanninkielisestä manuaalista, jonka olen tarvittavilta osin vapaasti suomentanut tätä opinnäytetyötä varten.

Moni manuaali ohjaa käyttämään rakenneanalyysia, kun halutaan selvittää yrityksen tietoturvaosaamista, sekä sitä, millä tasolla tietoturva yrityksessä on. Nelikko kertoo (2009, 6) yrityksen rakenneanalyysin sisältävän kattavan ja kokonaisvaltaisen kohdeyrityksen analysoinnin aina fyysisestä infrastruktuurista organisaatiorakenteen, hierarkian ja henkilöstön roolien kautta teknisiin komponentteihin saakka.

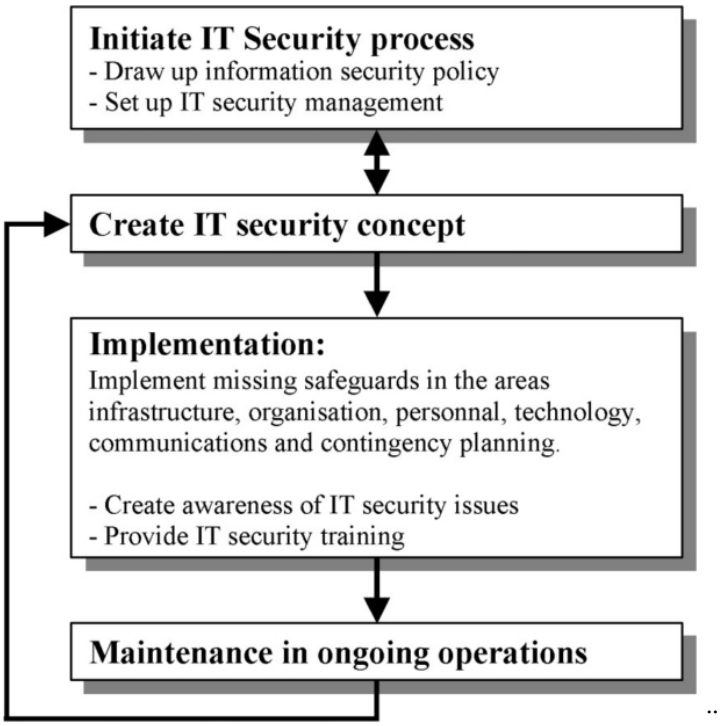
Nelikon mukaan (2009, 6) BSI:n mukainen rakenneanalyysi sisältää ainakin seuraavat asiat:

- Olemassaoleva infrastruktuuri järjestelmästä, palvelimista, koneista ja henkilöstöstä.
- Henkilöstöhallinto. Kuka johtaa? Ketkä ovat kenenkin alaisia IT ja turvallisuusasioissa? Kenellä on pääsy mihinkin tietojärjestelmiin, ja miten tietoturvapolitiikkaa toteutetaan.
- Käytössäolevat IT-järjestelmät, ja niiden käyttöjärjestelmät, niin verkossa kuin Stand-alonetkin.
- Käytössäolevat yhteydet IT-järjestelmistä ulkomaailmaan. Onko järjestelmillä internetyhteys ja miten se on toteutettu? WLAN, LAN ja niiden turvallisuus, sekä sisäverkot ja niiden turvallisuus.
- Ohjelmistotaso. Koneiden käytössä olevat ohjelmistot.

Rakenneanalyysiä käytetään tarjoamaan tarvittava tietopohja kattavan tietoturvapolitiikan ja konseptin luomiseksi. Analyysin on tarkoitus selvittää tietoturvapolitiikan tekijöille yrityksen tarpeet, sekä yritykseen kohdistuvia uhkia sekä sen heikkouksia. (BSI Standard 100-2, 30.) Tällä kerralla, kun tehtävänä on pienyrityksen tietoturvan kokonaisvaltainen hallinta, ja henkilöstön tietoturvaohjeistuksen laadinta, kohdeyrityksen IT-rakenneanalyysi laajuudessaan ja yksityiskohtien tarkkuudessa ei näyttele yhtä tärkeää osaa tehtävän toteuttamisessa, kuin se olisi esim. tietokantajärjestelmiä tai työasemia tarkastellessa. Myös kohdeyrityksen ollessa näin pieni, on turhaa paneutua sen tarkemmin tietoturvaorganisaation toimintaan.

3.2 Tietoturvallisuuden johtaminen

Tiedon turvallinen käsittely on oleellista jokaisessa yrityksessä. Tallennettua tietoa on paperilla, tietokoneissa ja ihmisten muistissa. Varsinkin suurissa organisaatioissa, tulisi tietoturvallisuus kokonaisuudessaan järjestää järjestelmällisesti ja suunnitellusti niin, että organisaation yksiköt ja sidoshenkilöt noudattaisivat integroidusti luotua tietoturvallisuuspolitiikkaa. Parhaiten tämä onnistuu, kun organisaatiolla on tietoturvallisuuteen erikoistunut vastuuyksikkö, joka koostuu yhdestä tai useammasta asiantuntijasta. Jokaisen organisaation ollessa yksilöllinen tulee puutteet analysoida ja tietoturvallisuusmenettelyt suunnitella kutakin organisaaiota varten erikseen. (Heiskanen, Marjokorpi, Nishio, Nurminen 2009, 7.)



Kuva 2: Tietoturvaprosessi BSI:n mukaan

Ensimmäisenä tulee laatia politiikka, tapa toimia tietoturvallisuuden varalle. Sen jälkeen luodaan tietoturvallisuuskonsepti, joka sisältää rakenneanalyysin, organisaation, teknologian, suojausmenettelyt sekä suunnitelman kommunikoinnista. Näiden tarkoituksena on lisätä tietoturvatietoisuutta yrityksessä, sekä tarjota tietoturvakoulutusta. Seuraavana tasona on tietoturvallisuuden ylläpito, josta palataan takaisin toiselle tasolle, jos huomataan puutteita tai virheitä.

Alla joitakin uhkia, jotka BSI:n mukaan (2005, 358) aiheutuvat puutteellisesta tietoturvallisuuden johtamisesta:

- Työntekijöillä ei ole henkilökohtaista vastuuta, jos tietoturvallisuuden johtoa ei ole nimitetty. Työntekijät olettavat, että yrityksen tai yksikön ylin johto on vastuussa tietoturvallisuudesta, jolloin tietoturvallisuus jää puolitiehen.
- Tietoturvastrategioita ja – konsepteja ei ole tarkkaan määritelty, jolloin niiden käyttöönotto ei onnistu tehokkaasti.
- Tietoturvamenetelmät ovat epäkäytännöllisiä, ja tietoturvallisuuden johto ei toimi yhteistyössä keskenään.
- Tietoturvallisuusprosessia ei päivitetä.

Jos tietoturvallisuus ei ole kunnossa, yritys saattaa rikkoa sen yhteistyökumppaneiden ja henkilöstön välisiä sopimuksia tai valtiollisia lakeja. Rikkomuksia tapahtuu, kun esimerkiksi luottamuksellista tietoa päästetään julkisesti luettavaksi. (IT-Grundschutz Catalogues 2005, 408.)

Yrityksen liiketoiminta saattaa kokea häiriöitä, kun tietojärjestelmät lakkaavat toimimasta oikein. Työntekijät eivät pysty työskentelemään, jos esimerkiksi tietojärjestelmät kaatuvat sähkökatkoksen takia. Ainakin Yhdysvalloissa on saatu kokea tällainen ongelma. Yksikään lentokone ei ollut saanut lähtölupaa yli kahteen tuntiin tietokannassa olleen virheen vuoksi, ja tuhansien ihmisten matka viivästyi. (IT-Grundschutz Catalogues 2005, 409.)

Katakrin (2011, 8-13) mukaan perustason saavuttamiseksi organisaatiolla pitää olla kirjattuna turvallisuutta koskevat perusasiat erillisenä dokumenttina, tai osana yleisiä tavoitteita. Turvallisuusdokumentaatio sisältää ainakin henkilöstö-, tieto-ja tilaturvallisuuden osa-alueet. Jotta tietoturvallisuuspolitiikasta tai muusta vastaavasta olisi hyötyä, on se käytävä koko organisaation henkilöstön kanssa läpi ja sen pitää olla helposti saatavilla kertausta varten. Tietoturvallisuuden keskeiset tavoitteet tulee olla kuvattuna kyseisessä dokumentaatiossa.

Pienissä yrityksissä yksi johdon jäsenistä ottaa vastuulleen tietoturvallisuuden johdon. Keskikokoisissa ja suuremmissa organisaatioissa tietoturvallisuuden tehtävä nimetään yhdelle vastuuhenkilölle eli tietoturvavastaavalle. Yrityskoon kasvaessa tietoturvavastaavan alle voidaan nimittää lisähenkilöstöä vastaamaan tietoturvallisuuden yksityisyiskohdista ja erikseen määritellyistä sektoreista, jolloin he voivat työkennellä niissä tehtävissä yksinomaan tai muiden tehtävien lisäksi. (IT-Grundschutz Catalogues 2005, 1642.) Sama lähde (2005, 1258) jatkaa, että tietoturvallisuuden organisaatiorakenne tulee määritellä, jotta eri tehtävät voidaan suorittaa yhtenäisesti. Organisaatioon tulee nimittää tietoturvavastaava, joka on erikoistunut alalle ja vastaa koko organisaation tietoturvallisuudesta.

Tietoturvallisuuskonsepti, joka kuvaa organisaation tietoturvarakenteen ja toimintaperiaatteet, on yrityksen tietoturvallisuudessa keskeisin dokumentti. Kaikki turvallisuusmenettelyt tulisi olla mainittuna tietoturvallisuuskonseptissa, ja dokumentti tulisi pitää aina ajan tasalla. (IT-Grundschutz Catalogues 2005, 1266.)

Etsiessäni artikkeleita nimenomaan tietoturvallisuuden johtamisesta, löysin yhden mielenkiintoisen lähteen. Pasi Yliluoma kirjoittaa Talouselämän minä väitän -osiossa tietoturvan olevan osa johtamista. Tietoturva ei hänen mielestään ole rakettitiedettä vaan se on tapa toimia oikein päivittäisessä työssä.

Tietoturva on pääosin varmistettavissa maalaisjärjellä ja pitkäjänteisellä työllä. Yliluoma on myös koonnut niinkutsutun tietoturvan kymmenen käskyä, joita noudattamalla saavuttaa perustason tietoturva-asioissa:

1. Näytä esimerkkiä
2. Tee selkeä vastuutus
3. Suojaa aineeton omaisuus
4. Anna riittävät resurssit
5. Tarkkaile poikkeamia
6. Tee ohjeista todellisuutta
7. Analysoi sisäiset uhat
8. Analysoi ulkoiset uhat
9. Hyödynnä uusia mahdollisuuksia
10. Muista aina ihminen

Tietoturvallisuuden vastuuhenkilön tulee raportoida tietoturvan tilasta säännöllisesti ja laatia vähintään vuosittain raportti, joka käsittelee, yrityksen tietoturvallisuuden nykytilannetta sekä tulevaisuutta. Raportin tulee sisältää nykyhetken kuvauksen lisäksi raportti aiempien toimenpiteiden tuloksista sekä kuvaus kaikista uudistuksista, jotka tullaan ottamaan käyttöön jatkossa. Raportin tulee lisäksi sisältää kuvaus tietoturvallisuusjohtamisesta, raportteja johdolle yksittäisistä merkittävistä tietoturvatapahtumista, yhteenvedon yrityksen tietohallinnon teknisestä tilasta ja tarvittaessa IT-ohjeita käyttäjille. (IT-Grundschutz Catalogues 2005, 1280.)

Yrityksen tietoturvan tulee tulee ottaa myös huomioon lait, jotka koskevat henkilökohtaisen tiedon suojaamista, salausmenetelmien käyttöä, luottamuksellisen tiedon suojaamista ja tietojärjestelmien toimivuutta. (Heiskanen, Marjokorpi, Nishio, Nurminen 2009, 10.)

3.2.1 Organisaation tietoturva

Tässä kappaleessa käydään läpi toimenpiteet, jotka pitäisi tehdä, jotta voidaan saavuttaa tietoturvallisuuden vähimmäisvaatimukset organisaatiotasolla.

3.2.2 Force Majeure

Tulipalo on suuri riski yrityksen liiketoiminnalle ja se on erityisesti otettava huomioon myös tietoturvallisuutta arvioitaessa osana tämän osa-alueen riskikartoitusta. Tulipalon sammutustöiden vuoksi kiinteistöön pääsevä vesi voi olla riskinä myös paloalueen läheisyydessä oleville yrityksille, asuinrakennuksille tai muulle vastaavalle omaisuudelle.

Palamisprosesseissa muodostuu usein haitallisia kaasuja, jotka saattavat päästä leviämään ilmastointikanavien kautta ja voivat näin aiheuttaa herkkien elektronisten laitteiden vioittumisen hyvinkin kaukana itse palopaikasta. (IT-Grundschutz Catalogues 2005, 270.)

Luonnonmullistukset kuten maanjäristykset ja tulvat aiheuttavat riskin, joka on huomioitava myös tietoturvaa arvioitaessa. Vesi tulviessaan aiheuttaa esimerkiksi elektronisten laitteiden oikosulkuja ja maa täristessään herkkien atk-laitteiden vaurioitumisia.

Ilmaolosuhteet, jossa laitteet toimivat ovat myös merkittävä osa-alue joka tulee huomioida tietoturvassa. Nelikon mukaan (2009, 10-11) jokaiselle laitteelle on määritetty optimilämpötila toimivuuden kannnalta. Suuret lämpötilan vaihtelut voivat pahimmassa tapauksessa aiheuttaa koko järjestelmän pettämisen ja samassa kategoriassa pitää ottaa huomioon myös kosteus ja mahdollisen kosteuden muodostuminen. Osa laitevalmistajista määrittelevät optimaalisiksi varastointiominaisuuksiksi +20-22 astetta ja kosteusprosentiksi 40%.

3.2.3 Organisaatiotason puutteet

Tietoturvariskejä yrityksen toiminnalle aiheuttaa sääntöjen puuttuminen tai se, että säännöt eivät ole ajan tasalla. Monesti tietoturvallisuudelle on laadittu sääntöjä ja toimintatapoja, mutta myös yhtä useasti niitä ei päivitetä, jolloin ne eivät ole ajan tasalla. Jokaisen teknisen muutoksen tapahtuessa pitää huomioida myös sääntöjen, ohjeistusten ja toimintatapojen päivittäminen. Pahimmassa tapauksessa sääntöjä tai toimintatapoja ei ole laadittu ollenkaan. (Heiskanen, Marjokorpi, Nishio, Nurminen 2009, 11.)

Vaikkakin säännöt löytyisivät, se ei takaa kaiken onnistuvan. Kaikkien työntekijöiden tulee olla tietoisia toimintatavoista, varsinkin niiden, jotka ovat johtavassa asemassa. Jos jotain tapahtuu, ei voida vain piiloutua ja sanoa etten tiennyt, tai etten tiennyt olevani vastuussa tästä. (IT-Grundschutz Catalogues 2005, 288.)

Huollon tarpeellisuuden laiminlyöminen voi aiheuttaa suuria ongelmia. Pahimmassa tapauksessa voidaan varmasti puhua tulipaloista ja muista elektronisissa laitteissa tapahtuvista syttymisistä. Huollon tarve, huoltaminen ja niin sanottu päällekatsominen on ensiluokkaisen tärkeää, jotta niiden laiminlyöminen ei aiheuttaisi suuriakin uhkia organisaatiolle. (IT-Grundschutz Catalogues 2005, 291.)

3.2.4 Inhimilliset virheet

Nelikko toteaa (2009, 12), että Inhimillisestä virheestä on kyse, kun asiasta ymmärtämätön tai tietämätön esimerkiksi irrottaa palvelimen, reitittimen, kytkimen tai UPSin johdon seinästä ja laittaa sen tilalle jonkun muun, jolloin verkko ei ole käytössä ja muilta koneilta ei pääse verkkolevyihin käsiksi jolloin tieto ei pääse liikkumaan. Näiden virheiden välttämiseksi on hyvä jättää pöytäpinnat ja laittiatasot siisteiksi, sekä sammuttaa koneet ja laitteet yöajaksi. Näin kenenkään ei tarvitse turhaan siirrellä tavaroita ja vahinkopainalluksia ei pääse tapahtumaan.

Virransyöttöhäiriöt voivat aiheutua myös inhimillisen virheen kautta. Esimerkiksi siivoajia tulee ohjeistaa tarkasti siitä, minkä johdon saa poistaa seinästä imurin pistoketta varten. Väärän johdon poistaminen seinästä saattaa aiheuttaa jonkin tärkeän tiedon katoamisen tai koneista voi hajota jotain komponentteja. Tästäkin syystä on tärkeää, että tiedostot varmuuskopioidaan ja varmuuskopiot löytyvät sellaiselta laitteelta, jolla on varavirta tarvittaessa käytössään. Tuolloin tiedot säilyvät tallessa vaikka häiriötilanne syntyisikin. (Heiskanen, Marjokorpi, Nishio, Nurminen 2009, 12.)

3.2.5 Tekniset häiriöt

Tekninen häiriö voi johtua esimerkiksi luonnonilmiöstä, inhimillisestä virheestä tai ihmisen tahallisesta toimesta. Ukkonen voi aiheuttaa sähkökatkon ja näin haitata yrityksen toimintaa, mutta onneksi nämä ovat useimmiten lyhyitä, eivätkä siksi aiheuta suurta vaaraa yrityksille. Sähkökatko saattaa myös johtua inhimillisestä virheestä, jolloin asiaa ajattelematon ihminen poistaa itselleen tarpeettoman pistokkeen seinästä ja korvaa sen jolloin toisella. Pistoke voi olla hyvinkin tärkeän komponentin pistoke, joka toimiakseen tarvitsee jatkuvasti virtaa.

3.2.6 Tahalliset teot

Nelikon mukaan (2009, 13) luvattomasti rakennukseen tulleet henkilöt saattavat aiheuttaa suurta vahinkoa laitteistoille ja ohjelmistoille, sekä mahdollisesti jopa yrityksen toiminnalle jos he pääsevät käsiksi koneilla ja papereilla oleviin tietoihin. Kriittisten tiedostojen ja tietokantojen varmuuskopiot tulee viedä aika ajoin toiseen rakennukseen esimerkiksi pankin turvasäilöön, mahdollisen käyttöympäristön tulipalon tai täydellisen laitteistojen varkauksien varalta.

Ilkivaltaa on monenlaista, vaikka niiden ehkäisemiseen ei välttämättä ole montaa eri keinoa. Ilkivaltaa voi olla koneiden ja laitteiden rikkominen, ohjelmistojen ja ohjelmien tuhoaminen, tietojen tuhoaminen ja manipulointi niin tietokoneilta kuin papereilta, huonekalujen

rikkominen sekä rakennukseen liittyvät tuhot, kuten seinien sotkeminen tai ikkunoiden rikkominen.

Hyökkäykset voivat olla fyysisiä, jotka kohdistuvat henkilöihin tai hyökkäykset voivat kohdistua tietoihin, joita yrityksessä säilytetään ja jotka vaikuttavat yrityksen päivittäiseen toimintaan. Tietoon voi myös liittyä kolmas osapuoli, jos varastoitu tieto onkin esimerkiksi potilastietoja tai sopimuksia eri osapuolten välillä. (IT-Grundschutz Catalogues 2005, 574.)

Puhelimien ja tiedonsiirron salakuuntelua saattaa pystyä työkaveri hyödyntämään käyttämällä puhelimen konferenssiominaisuutta. Työntekijät saattavat aiheuttaa vahinkoa, jos he puhelimitse puhuvat tärkeistä ja salaisista yritykseen ja sen toimintaan liittyvistä asioista. Tärkeiden tietoliikenneyhteyksien salaaminen esim. VPN-tunneleilla (Virtual Private Network) auttaa pitämään tiedonsiirrot salassa. (Heiskanen, Marjokorpi, Nishio, Nurminen 2009, 15)

Työhuoneiden salakuuntelulla voi olla samat syyt ja vaikutukset kuin puhelimien ja tiedonsiirron salakuuntelulla. (IT-Grundschutz Catalogues 2005, 581.) Toki työhuoneiden salakuuntelussa voisi olla syynä työntekijän vilppiepäily ja tietojen väärinkäyttö, mutta Suomessa salakuuntelu ei ole laillista, joten tässä tapauksessa sitä ei voida soveltaa. Työhuoneiden ja neuvottelutilojen äänieristyksellä saadaan keskustelut pidettyä salassa.

Nelikko käy läpi (2009, 16) myös ylläpitotehtäviä ja heidän mukaansa ylläpitotehtävät ovat todella tärkeässä osassa yritysten toiminnassa. Ilman ylläpitotehtäviä ei mikään toimi, tai ainakin toiminta alkaa tökkiä. Ylläpitohenkilöstö huolehtii siitä, että koneet, laitteet ja ohjelmat toimivat. Ongelmien ilmetessä, on heidän tehtävänsä korjata ja hoitaa ne kuntoon. Näiden ihmisten tulee olla luotettavia ja asiansa osaavia. Tämän tasoista valtaa ja vastuuta tulee jakaa harkiten, koska sitä voidaan helposti käyttää väärin. Väärinkäytös saattaa aiheuttaa mittavia vahinkoja, tai jopa koko yrityksen toiminnan pysähtymisen. Henkilökunnan turvallisuusselvityksillä, henkilökunnan asianmukaisella koulutuksella ja käyttöoikeuksien rajaamisella voidaan ainakin hieman turvata yrityksen tietoja.

Edellä todetut, yrityksen oman ylläpitohenkilökunnan tuomat riskit, ovat samoja myös ulkoisten palveluntarjoajan ylläpitohenkilöiden yritykselle suorittamissa tehtävissä. Usein ulkopuolisilla ylläpitohenkilöillä on lähes yhtä paljon, ellei jopa enemmän oikeuksia ohjelmiin tai laitteisiin kohdistuvissa töissä. Ulkopuolisen työntekijän työskentelyssä suurena uhkana on se, että he pystyvät helpommin viemään varastettua tietoa ulos talosta ja pystyvät hyödyntämään sitä helpommin, ilman että osataan edes epäillä, että jotain tärkeää tietoa on hävinnyt. Heidän toimiaan on myös vaikeampi seurata, koska he eivät kuulu henkilökuntaan ja he useimmiten tuntevat omaa henkilöstöä paremmin järjestelmät ja ohjelmat. (Heiskanen, Marjokorpi, Nishio, Nurminen 2009, 16.)

Henkilöt, joilla ei ole oikeuksia tiettyihin tietoverkon osiin, voivat onnistua saamaan käyttöönsä toisen henkilön käyttäjätunnukset (käyttöoikeudet) esimerkiksi tietokoneelle tai johonkin erityiseen järjelmäosioon ja näin päästä muuttamaan tai varastamaan tietoja. (IT-Grundschutz Catalogues 2005, 640.)

Käyttäjätunnukset ja salasanat tulisi säilyttää ainoastaan omassa muistissa. Useasti vaihtuvat salasanat (pakotettu salasananvaihto -ohjelma) auttavat myös pitämään luvattomasti tietoverkkoon pyrkiviä poissa verkosta. Luvaton tunkeutuminen tietojärjestelmiin eli hakkerointi voidaan yrittää estää toimivilla palomuureilla sekä virustorjuntaohjelmilla.

Sabotointia on kaikki toimet, joilla pyritään vaikeuttamaan yrityksen päivittäistä toimintaa ja jotka tehdään kiusallaan. Mahdollista sabotointia voidaan tehdä tuhoamalla laitteita, lataamalla viruksia koneille ja poistamalla tärkeitä tietoja. Sabotointia voidaan myös pyrkiä tekemään tuhoamalla ja varastamalla papereita, joissa on yrityksen toiminnan kannalta tärkeitä tietoja. (Heiskanen, Marjokorpi, Nishio, Nurminen 2009, 17.)

3.3 Henkilöstön tietoturva

Tässä kappaleessa käydään läpi turvamenettelyt, joihin pitäisi kiinnittää huomiota henkilöstötasolla jokaisen työntekijän koko työsuhteen ajan. Siten voidaan henkilöstötasolla saavuttaa paras mahdollinen tietoturva. (IT-Grundschutz Catalogues 2005, 53.)

3.3.1 Force Majeure

Force Majeure mukainen tapahtuma , eli ennalta arvaamaton merkittävä tapahtuma tai olosuhteen muutos kuten sairaus, onnettomuus, kuolema tai lakko voi aiheuttaa odottamattomia vähennyksiä tai muutoksia henkilöstössä. Fyysisen vähenemisen lisäksi henkilöstöresurssien yllättävä pieneneminen voi myös tarkoittaa menetystä asiantuntemuksessa kun jonkun asian erityisosaaja menetetään. (IT-Grundschutz Catalogues 2005, 267.)

Force Majeure tapahtuma, joka johtuu muusta kuin yrityksen omasta toiminnasta on myös otettava huomioon varauduttaessa riskeihin.

3.3.2 Organisaatiotason puutteet

Tietoturvastrategian ja sääntöjen luominen on yritykselle tärkeää, mutta ei sinällään riitä. Tämän lisäksi täytyy pitää huolta siitä, että henkilöstö tuntee säännöt ja noudattaa niitä. Tietoturvastrategian ja sääntöjen tunteminen on keskeistä varsinkin niille, jotka ovat

vastuussa tietoturvasta. Tietämättömyys voi aiheuttaa isojakin vahinkoja, ja kun henkilöstö valmennetaan tietoturvallisuuteen oikein-väärin toiminnan riski pienenee ja kukaan ei voi todeta: ”En tiennyt olevani vastuussa tästä,” tai ”en tiennyt mitä tehdä.” (IT-Grundschutz Catalogues 2005, 288.)

Toivottavaa olisi, että käyttöoikeuksia olisi rajattu kullekin henkilölle niihin toimintoihin, joita hän työnsä tekemiseen tarvitsee. Yksinkertaisena esimerkkinä voidaan pitää seuraavaa: Henkilö, jonka ei tarvitse työssään käyttää kuin tekstinkäsittelyä ja taulukkolaskentaa ei myöskään tarvitse koneelleen muita ohjelmia. Käyttöoikeuksien rajaamisella varmistetaan turvallinen ja asianmukainen IT-järjestelmien ja prosessien käyttö. (IT-Grundschutz Catalogues 2005, 293.)

3.3.3 Inhimilliset virheet

Käyttäjän tahattomat toimet voivat suhteellisen helpostikin aiheuttaa luottamuksellisen tiedon tai järjestelmän eheyden menettämisen. Vanhingon laajuus tai luonne riippuvat menetetystä tiedosta ja siitä, kuinka arkaluontoista se on. (IT-Grundschutz Catalogues 2005, 415.)

Huolimattomuus, mutta myös tietämättömyys voi johtaa tiedostojen tai laitteistojen tuhoutumiseen. Pahimmassa tapauksessa tämä vaikuttaa koko järjestelmään ja voi haitata yrityksen toimintaa. Perusteellisella henkilöstön perehdytyksellä ja keskeisten asioiden kertauksella minimoidaan tämän kaltaiset riskit. (IT-Grundschutz Catalogues 2005, 416.)

IT-järjestelmän väärinkäyttöä voi ilmetä, jos esimerkiksi käyttöoikeuksia on myönnetty liian laajalti, salasanat ovat liian yksinkertaisia ja täten helppoja arvata tai varmuuskopioita ei ole tehty riittävästi. Henkilöstö kannattaa opettaa ja velvoittaa laittamaan tietokone aina lukkoon, kun poistuu paikalta. Näin varmistetaan, ettei tietoa katoa tai sitä ei muuteta jonkun sattumanvaraisen ohikulkijan toimesta. (IT-Grundschutz Catalogues 2005, 422.)

Yksi tavallisimmista ongelmista syntyy, kun sellaisia käyttäjätilejä, joissa on enemmän käyttöoikeuksia kuin mitä työn tekemiseen tarvitaan käytetään työskentelyyn. Monikäyttö kasvattaa myös virusten ja troijalaisten saastuttamisriskiä. Käyttäjätilit, joita ei tarvita tai jotka ovat vanhentuneita, ei saa säilyttää järjestelmässä, vaan ne tulisi poistaa välittömästi tarpeettomina. (IT-Grundschutz Catalogues 2005, 423.)

Internet tarjoaa miljoonia sivuja, dokumentteja ja tiedostoja. Tietoa haettaessa hakusanat ovat usein liian laajoja tai haettavasta asiasta käytetään väärää kuvausta. Tämä voi johtaa tiedon tuottamattomaan hakuun. Tuottamaton haku aiheuttaa liian suppean tai laajan

hakutuloksen, mutta useimmiten kuitenkin kyseessä on liian paljon toissijaista tietoa. Tämän toissijaisen tiedon analysointiin menee aikaa, eikä se tuota sitä tietoa ja lopputulosta mitä haulla on etsitty. On arvioitu, että turha sivujen välinen surffaus sekä tarpeettomat ja liian laajat haut internetissä aiheuttavat monen miljoonan kulut, jotka voitaisiin tarkemmalla haulla välttää. (IT-Grundschutz Catalogues 2005, 452.)

Salasanojen tulee olla sellaisia, ettei niitä voida järkeillen arvata. On myös tärkeää, että yhtä salasanaa käytetään vain yhdessä kohteessa, vaikkakin liian monen salasanan käyttö aiheuttaa usein muistiongelmia. Kun käyttäjä unohtaa salasanansa, aiheutuu siitä turhaa lisätyötä, mikä ei ole tehokasta yritykselle. Usein käyttäjät kirjoittavat salasanojaan itselleen muistiin, jotta niitä ei unohtaisi. Ongelmaa tästä ei synny, jos kukaan muu ei pääse näkemään muistilappua, mutta helposti näitä säilytetään esimerkiksi näppäimistön alla tai se saattaa olla jopa kiinnitettynä tietokoneen näyttöön. (IT-Grundschutz Catalogues 2005, 460.)

Hyvän salasanan ominaisuuksiin kuuluu riittävä pituus, sekä erilaisten merkkien käyttö. Hyvä salasana on esimerkiksi vähintään kahdeksan (8) merkkiä pitkä ja se sisältää sekä pieniä että isoja kirjaimia sekä numeroita ja numerot sijaitsevat keskellä sanaa. Hyvä salasana ei ole suomen- tai englanninkielinen sana, eikä ainakaan käyttäjälleen tutusta kohteesta, kuten esimerkiksi, ystävän tai lemmikin nimi. (Jyväskylän yliopisto, Tietohallintokeskus)

Hakumedia tarjoaa sivuston salasana.fi. Palvelu antaa mahdollisuuden luoda turvallisen, ainutlaatuisen sekä satunnaisen salasanalistan, jossa käyttäjä itse voi valita salasanojen pituuden sekä turvallisuustason. Valittavia turvallisuustasoja on kaksi, joista toinen sisältää helpommin muistettavia salasanoja, jotka ovat näinollen myös suojaustasoltaan matalampia.

Tärkeää myös on, että samaa salasanaa käytetään enintään puoli vuotta. Salasanoja ei tule koskaan kirjoittaa muistiin, vaan ne tulisi opetella ulkoa. Salasanaa ei myöskään saa koskaan luovuttaa ulkopuoliselle, eikä niitä tulisi tallentaa tietokantoihin sellaisenaan.

Tiedon huolimaton käsittely voi aiheuttaa yritykselle mittavia vahinkoja. Voi olla että jokin tieto tai asia vuotaa kilpailijoille ja aiheuttaa näin vahinkoa yritykselle ja sen toiminnalle. Voi myös olla, että jotkin tahot käyttävät hyväkseen tietoja ja näin pystyvät parantamaan omaa asemaansa tai käyttämään niitä oman etunsa tavoitteluun. (IT-Grundschutz Catalogues 2005, 461.)

Edelleen kannattaa myös huomioida työntekijöiden vahingossa aiheuttamat tietoturvariskit. Näitä voi yksinkertaisuudessaan olla muistitikun käyttäminen niin koti- kuin työkoneellakin tai sen unohtaminen esimerkiksi asiakastiloihin jonne on vapaa pääsy. Kaikkeen tulee olla salasanat ja virustentorjunnan tulee olla ajantasaista.

3.3.4 Tahalliset teot

Yrityksen tulee periaatteessa varautua siihen, että kuka tahansa henkilökuntaan kuuluva tai ulkopuolinen henkilö voi syyllistyä laitteiden, lisävarusteiden tai tiedon muunteluun tai tuhoamiseen. Syitä kyseiseen käytökseen voi olla monia, kuten esimerkiksi kosto, turhautuneisuus tai ilkeys. Tällöin lähes aina tavoitteena on aiheuttaa yritykselle jonkinasteita harmia tai suurempaa ja pitkäaikaisempaa ongelmaa. (IT-Grundschutz Catalogues 2005, 569.)

Tämän saavuttaakseen tekijällä on käytössään useita tapoja, joilla tietoja tai ohjelmistoja voidaan luvattomasti muuttaa, kuten väärän tiedon syöttäminen, tietojen tai järjestelmäosien tuhoaminen, muutokset käyttöoikeuksissa tai käyttöjärjestelmissä jne. Nämä toimenpiteet tosin ovat mahdollisia vain jos järjestelmään pääsee sisään. Tämän johdosta käyttöoikeuksien tarkka määrittäminen ja salasanojen valvonta on erittäin tärkeää. (IT-Grundschutz Catalogues 2005, 570.)

Pääkäyttäjän oikeudet omaava tai oikeutetusti tai laittomasti ne hankkinut henkilö, joka aikoo vahingoittaa järjestelmää tai sen käyttäjiä, voi aiheuttaa yritykselle ja sen järjestelmille todella suuria vahinkoja. (IT-Grundschutz Catalogues 2005, 588.) Järjestelmänvalvojan oikeuksien väärinkäyttö on kuitenkin harvinaista, mutta sitäkin voi tapahtua. Yritys voi vähentää tätä riskiä tarkastamalla nämä valtuudet saavan henkilön taustat erityisen tarkasti ja ohjeistamalla hänet toimintamallien ja salasanojen säilyttämisen osalta täsmällisesti.

Tietokonevirukset ovat ohjelmia, joiden ainoa tarkoitus on aiheuttaa järjestelmissä vahinkoa. Sähköpostihuijaus on viesti, jossa on varoitus tietynlaisesta viruksesta ja viestissä kehotetaan lähettämään tämä varoitus kaikkiin vastaanottajan sähköpostilistalla oleviin osoitteisiin. Tämä ei ole virus, ja sillä pyritään aiheuttamaan vastaanottajalle epävarmuutta ja ärsytystä. (IT-Grundschutz Catalogues 2005, 591.)

Iso osa viruksista on siinä mielessä harmittomia, etteivät ne aiheuta pysyvää tai peruuttamatonta vahinkoa. Ne aiheuttavat kuitenkin tarpeetonta työtä ja niiden aiheuttamien vahinkojen korjaamiseen kuluu turhaa aikaa, mikä on pois yrityksen varsinaisesta liiketoiminnasta. Yleisimpiä tapoja virusten leviämiselle on ohjelmoida se levittämään itse itseään sähköpostin kautta. Useimmiten virus sijaitsee sähköpostin liitetiedostossa, joka avattaessa aktivoi viruksen.

Olemassa on myös erilaisia tekniikoita, (IT-Grundschutz Catalogues 2005, 613) joiden avulla pyritään saavuttamaan luvaton pääsy tietoihin tai tietojärjestelmiin. Tällä tavalla käytetään

hyväksi ihmisten avuliaisuutta, luottamusta ja pelkoa. Henkilökuntaa voidaan manipuloida ulkopuolisen tahon toimesta niin, että heidän tekemisistään tulee luvattomia. Tyypillisiä esimerkkejä tällaisista manipuloinneista on soittaa henkilökunnan jäsenelle ja esittää olevansa:

- assistentti, jonka esimies tarvitsee nopeasti jotain tietoa tai toimenpidettä järjestelmässä, mutta on unohtanut salasanan ja tätä pyydetään,
- järjestelmänvalvoja, joka soittaa koska järjestelmässä on ongelma, jonka ratkaisemiseksi hän tarvitsee käyttäjän salasanan.

Tällaisista yrityksistä on informoitu mediassa aina silloin tällöin. Useimmiten kuvatun kaltaisen manipuloinnin kohteena ovat olleet verkkopankkien asiakkaat, joilta kysellään heidän verkkopankkitunnuksiaan.

Vakoilu on edellistä vaikeampi tapa saada tietoonsa yrityksen liiketoiminnan kannalta kriittisiä asioita. Vakoiluun yhdistetään usein tietoteknisiä laitteita, kuten puheluiden tai neuvotteluiden kaukokuuntelun mahdollistavat laitteet. (IT-Grundschutz Catalogues 2005, 679.)

4 Tietoturvallisuuden nykytilakartoitus Yritys Oy:ssä

Yritys Oy on henkilömäärältään pieni yritys, joka toimii kiinteistöalalla neuvonantajana ja järjestelijänä. Työntekijät ovat asiantuntijoita kiinteistöjen myynti-ja ostotransaktioissa sekä suurissa vuokrausjärjestelyissä. Heillä on kokemusta myös sale and leaseback -hankkeiden menestyksekkäästä toteuttamisesta. Yritys Oy:n toimintatapaan kuuluu yhtiön oman organisaation pitäminen kevyenä ja täten he hankkivat ympärilleen luodusta vahvasta ja osaavasta verkostosta projekteihinsa tarvittavat palvelut, kuten veroasiantuntemuksen, auktorisoidut arvioinnit ja tekniset palvelut.

Tietoturvaopas –sivustolla todetaan jokaisella yrityksellä olevan suojattavaa tietoa. Tämä tulee oivaltaa, jotta voidaan pyrkiä toimivaan tietoturvaan. Samaiselta sivustolta löytyy myös kysymysrunko tietoturvan nykytilan kartoittamiseksi, sekä malli tietoturvaohjeista joita käytin apunani pohtiessani omaa kysymyslistaani.

Selvittääkseni kohdeyrityksen tietoturvallisuuden tasoa, olisin voinut tehdä kysymyslomakkeen aiheesta, tai haastatella jotakuta yrityksen henkilökuntaan kuuluvaa. Kumpikin tapa tässä kyseisessä yrityksessä tuntui oudolta. Miksi tekisin kyselylomakkeen, kun suunnilleen tiedän itsekin vastauksen jokaiseen kysymykseen? Tai miksi haastattelisin ketään, kun minä itse olisin paras haastateltava koskien näitä asioita? Tulin siihen tulokseen, että

parhaiten selvitän kohdeyrityksen tämän hetkisen tietoturvallisuuden tason laatimalla kysymysrungon tietoturvan osa-alueiden pohjalta. Liite 1.

Tietojesiturvaksi.fi –sivuston mukaan tietoturva jaetaan kahdeksaan osa-alueeseen, jotka ovat:

1. Hallinnollinen tietoturva
2. Fyysinen tietoturva
3. Laitteistoturvallisuus
4. Ohjelmistoturvallisuus
5. Tietoaineiston turvallisuus
6. Tietoliikenneturvallisuus
7. Henkilöstöturvallisuus
8. Käyttöturvallisuus

Kohdeyrityksen kannalta minun ei ole järkevää tarkastella tietoturvan nykytilaa jokaisen edellämainitun osalta, joten olen valinnut niistä viisi (5) tähän opinnäytetyöhön ja tälle kohdeyritykselle parhaiten sopivaa osa-aluetta.

Yritys Oy:n tietoturvaa käsittelen seuraavien osa-alueiden kautta:

- Fyysinen tietoturva
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Henkilöstöturvallisuus

Tietojesiturvaksi.fi kertoo fyysisen tietoturvan sisältävän yrityksen toimitilojen sekä niissä sijaitsevien laitteiden suojaamisen. Valtiovarainministeriön VAHTI-julkaisu avaa tähän osa-alueeseen kuuluvaksi mm. kulunvalvonnan, kameravalvonnan, muun teknisen valvonnan ja vartioinnin sekä palo-, vesi- sähkö-, ilmastointi- ja murtovahinkojen torjunnan.

Laitteistoturvallisuuteen kuuluu kaikkien yrityksen teknisten laitteiden suojaaminen. Tietoturvan näkökulmasta tärkeimpiä kohteita ovat kannettavat tietokoneet, palvelimet, tulostimet ja matkapuhelimet. (Tietojesiturvaksi.fi, Laitteistoturvallisuus) VAHTI-julkaisun (2007, 63) mukaan laitteistoturvallisuuteen kuuluu itse suojaamisen lisäksi myös asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia. Laitteistoturvallisuudella pyritään turvaamaan minkä tahansa laitteen koko elinkaari.

Tietojärjestelmissä käytettävien lisenssien ja ohjelmistojen hallinnasta on kyse kun puhutaan ohjelmistoturvallisuudesta. Tähän kuuluu niin työpöytä kuin palvelinkäytössä olevat ohjelmistot. (Tietojesiturvaksi.fi, Ohjelmistoturvallisuus)

Olennaisia toimenpiteitä liittyen tietoaineistoturvallisuuteen on käyttöoikeuksien määrittäminen, tiedostojen varmuuskopiointi ja palautus sekä tiedon turvallinen säilyttäminen ja tuhoaminen. (Tietojesiturvaksi.fi, Tietoaineiston turvallisuus) VAHTI-julkaisun (2007, 83) mukaan tietoaineisto voidaan jakaa julkiseen tai salassapidettävään tietoon. Salassapidettävälle tiedolle on luokitusvastaavuuksia, mitkä näkyvät alla olevassa taulukossa

Luokitus	Perinteinen luokka	Perinteinen luokitus	EU:n englanninkielinen luokitus
Erittäin salainen	I turvaluokka	Erittäin salainen	EU Top Secret
Salainen	II turvaluokka	Salainen	EU Secret
Luottamuksellinen	III turvaluokka	Luottamuksellinen	EU Confidential
Käyttö rajoitettu	IV turvaluokka	Viranomaiskäyttö	EU Restricted

Kuva 3: Salassapidettävien tietoaineistojen luokitusvastaavuudet VAHTI-julkaisun mukaan.
Henkilöstöturvallisuus on riskien hallintaa ja siihen keskeisesti kuuluvat asiat ovat työhönotto, toimenkuvien olennaiset muutokset sekä palvelussuhteen päättymiseen liittyvät prosessit. Henkilöstön motivaatiolla, työtyytyväisyydellä sekä heidän riittävällä määrällä on suora yhteys siihen, millaisena tietoturvallisuus toteutuu. (VAHTI 2007, 57).

4.1 Fyysinen turvallisuus

Nelikon mukaan (2009, 12) kulkukorttijärjestelmää pidetään hyvänä jo siitä syystä, että se ei ainakaan helpota tunkeilijoiden asemaa. Jonkinasteinen kulkukortti, avainlätkä tai erityisavain onkin laajasti käytössä ensisijaisesti estäen vapaan kulun, mutta kehittyneessä muodossaan myös rekisteröiden henkilöiden liikkeet kiinteistössä myöhempää tarkastelua varten. Näin henkilökunnan ja ulkopuolisten liikkumisesta kiinteistössä aiheutuvaa tietoturvariskiä voidaan pienentää. Aivan kuten henkilökunnan pääsy yrityksen fyysisiin toimitiloihin myös pääsy yrityksen tietojärjestelmiin tulee olla rajattu. Tehokas rajaus pienentää tietoturvariskiä merkittävästi.

Yritys Oy:n toimisto sijaitsee Helsingin keskustassa, kiinteistön kuudennessa (6) kerroksessa, jonka rappukäytävään pääsyyn tarvitaan avain. Yritys Oy:n toimitiloihin rappukäytävään pääsyn jälkeen vaaditaan myös kulku lukitusta ovesta. Vaikkakin yrityksen tilat sijatsevat kahden lukitun oven takana on silti yrityksellä käytössä murtohälytysjärjestelmä, joka kytketään päälle aina kun toimisto jää tyhjäksi. Lisäksi murtohälytysjärjestelmä on

yhteydessä vartiointiliikkeeseen, missä on ympärivuorokautinen päivystys. Kohdeyrityksessä ei ole varsinaista kulunvalvontaa, niin että kustakin kulkijasta jäisi jälki tietokantaan. Toistaiseksi tähän ei ole nähty tarvetta.

Yritys Oy:ssä on kerran jouduttu miettimään mahdollista yritysvakoilun uhriksi joutumista. Edellisistä toimitiloista oltiin lähdössä ja vuokranantaja halusi esitellä tiloja mahdolliselle seuraavalle vuokralaiselle. Huoltomies päästi ihmiset toimitiloihin toimistoajan ulkopuolella sen enempää kyselemättä. Henkilökunnan työpöydillä oli tapauksen sattuessa papereita, joissa oli kriittisiä tietoja koskien yrityksen toimialaa, liiketoimintaa, kohderyhmiä ja asiakkaita. Tapauksesta käynnistettiin poliisitutkinta.

Vieraita Yritys Oy:ssä käy muutaman kerran viikossa ja he ohjataan eteistiloista suoraan neuvotteluhuoneisiin. Vierailijat eivät saa liikkua toimitiloissa valvomatta.

Kaikilla, paitsi yhdellä Yritys Oy:n työntekijöistä on vain kannettava tietokone käytössään. Tietokoneissa on määriteltynä käyttäjäprofiilit, joten konetta ei pysty käynnistämään kuin salasanan tunteva taho. Näin rajataan se, että ulkopuoliset eivät pääse koneen tai yrityksen tiedostoihin käsiksi. Tietokoneiden automaattisesta lukituksesta ei kuitenkaan ole ollut aiemmin puhetta. Kysyessäni asiaa työntekijöiltä, he sanoivat etteivät lukitse koneitaan poistuessaan hetkeksi tai edes hieman pidemmäksikin ajaksi koneeltaan. Kannettavien tietokoneiden ollessa kyseessä, tietokoneen lukitus CTRL+ALT+DELETE –toiminnon avulla voisi olla suotavaa hyvän tietoturvallisuuden varmistamiseksi.

Yritys Oy:n tiloista löytyy tietoliikennekaappi, joka sisältää tietotekniset kytkennät. Kaappi ei ole lukittu, joten siihen pääsee käsiksi kuka tahansa yrityksen työntekijä. Aikoinaan toimistotalossa, jossa Yritys Oy toimii on kaksi toimitilaa olleet yhtä yhtenäistä tilaa, ja ne on myöhemmin erotettu omikseen väliseinällä. Kun Yritys Oy muutti toiseen näistä tiloista, huomattiin ettei heidän puoleltaan löytynyt ollenkaan tietoliikennekaappia, josta näitä kytkentöjä voitaisiin hallita. Tilan jakamisessa kahdeksi, oli ilmeisesti joltakulta unohtunut tämä kaapin jakaminen, jolloin yksi yhteinen kaappi löytyi naapuritilasta. Tätähän ei voitu sallia, ja Yritys Oy sai oman kaapin omiin tiloihinsa.

Salasanat ovat käyttäjien itsensä määrittämiä, eikä järjestelmä pakota tietyin väliajoin uusimaan salasanaa. Tämän sisällytän varmasti kehitysehdotuksiini.

Useimmissa internetselaimissa on nykyään mahdollista tallentaa käyttäjätunnus ja salasana selaimen muistiin. Henkilön avatessa uuden sivun, joka vaatii kirjautumista, selain kysyy kirjautumistietojen antamisen jälkeen, halutaanko tiedot tallentaa. Tätä ominaisuutta ei pidä käyttää työkoneissa ja se kannattaa työnantajan kieltää.

4.2 Laitteistoturvallisuus

Yrityksessä käytössäolevan järjestelmän mukaisesti vain järjestelmänvalvoja voi antaa ja muuttaa käytössäolevia käyttäjätunnuksia tai salasanoja. Hänellä on varamies ja oletamme että hänen tunnuksensa eivät ole vuotaneet ulkopuolisille. Nykyiset salasanat ovat kohtuullisen turvassa, sillä järjestelmävalvoja ei pysty selvittämään tällä hetkellä käytössäolevia salasanoja, mutta pystyy kuitenkin luomaan uuden, jolloin nykyinen ei ole enää voimassa. Kuten jo aiemmin mainitsin, salasanoja ei yrityksessä tällä hetkellä uusita säännöllisesti. Säännöllisen uusintajärjestelmän käynnistäminen olisi perusteltua. Salasanat eivät ole listattuna tai kirjattuna mihinkään, vaan jokainen pitää ne muistissaan ja näin salasanojen ja niiden kautta tietojen joutuminen ulkopuolisille on mahdollista vain vilpillisin keinoin.

Yritys Oy:llä on yksi palvelinkone joka ylläpitää niin kutsuttua public –kovalevyä, jonne kaikki yrityksen toiminnan kannalta tärkeät tiedostot tulee tallentaa. Jokainen työntekijä pääsee käsiksi omalta koneeltaan siihen, pystyy tallentamaan sekä muokkaamaan siellä olevaa tietoa. Tälläkin koneella on oma virustentorjuntaohjelmansa.
Palvelinkone toimii myös varmuuskopioijana. Varmuuskopiointi tehdään kaksi kertaa viikossa public -kovalevystä, ja se tehdään nauhatallenteena.

Koska suurimmalla osalla työntekijöistä on käytössään kannettavat tietokoneet, ei sähkökatko vaikuta suuresti liiketoimintaan. Sähkökatkon ollessa pitempiaikainen, tulisi se vaikuttamaan liiketoimintaan todennäköisesti ratkaisevasti, koska palvelinkone sammuisi.

Nykyisissä toimitiloissaan yritys on ollut kolmisen vuotta. Toimitilojen sijaitessa vanhan rakennuksen ylimmässä kerroksessa, on vesi aiheuttanut jo kaksi kertaa yritykselle ongelmia. Talvella lumi kasautuu katolle ja keväällä lumen sulaessa vettä on päässyt katon läpi yrityksen tiloihin. Kummallakaan kerralla vesi ei ole tullut siihen huoneeseen, missä varmuuskopioinnin suorittava palvelinkone sijaitsee, mutta siihen on varauduttava viimeistään nyt.

Matkapuhelimet ovat nykyään lähes tietokoneita ja tämän johdosta myös ne on suojattava mahdollisilta tietovarkauksilta. Yritys Oy:ssä edellytetään työntekijä pitämään matkapuhelimestaan hyvää huolta, niin että se ei joudu ulkopuolisille, sekä pitämään niin kutsuttu suojakoodi päällä. Puhelimet, jotka yrityksen työntekijöillä on käytössä, tarjoavat mahdollisuuden automaattiseen lukkiutumiseen, kun puhelinta ei ennalta määritettyyn aikaan käytetä. Aika voi olla esimerkiksi 30 sekunttia tai 60 sekunttia. Lukituksen purkamiseksi ja siinä olevien tietojen selaamiseksi tarvitaan salasana, jolla puhelin aukeaa. Tämä lukitussuojaus toimii hyvin, mutta koetaan välillä hankalaksi, koska koodi pitää näppäillä

laitteeseen varsin usein. Suojaus on kuitenkin oleellista, koska puhelimissa on nähtävissä myös puhelimen haltijan sähköpostiliikenne, joka saattaa sisältää luottamuksellista tietoa.

Yritys käyttää sähköpostiliikenteessä ja yhteysosoitteissa Microsoftin Outlook –järjestelmää. Puhelimessa olevat tiedot sykronoidaan automaattisesti ja näin puhelimien tiedoista pitäisi olla palvelimella kopio, joka varmuuskopioidaan muiden tietojen ohella. Eräillä työntekijoillä ei kuitenkaan puhelinyhteystietojen tallennusmuoto vastaa Outlookin vaatimaa tapaa ja tämän johdosta heidät pitää velvoittaa ottamaan varmuuskopioita puhelimiensa osoitekirjoista säännöllisin väliajoin, esimerkiksi kerran kuussa.

4.3 Ohjelmistoturvallisuus

Jokaisella laitteella on oma F-Securen tarjoama virustentorjuntaohjelma. Kunkin tietokoneen käyttäjä on opastettu huolehtimaan itse kyseisen ohjelman päivittämisestä, mikä käytännössä tapahtuu automaattisesti aina kun kone avataan. Virustentorjuntaohjelma on myös ohjelmoitu tekemään virustarkistusta tietyin väliajoin, joten käyttäjän ei itse tarvitse huolehtia siitä. Toistaiseksi virukset ovat aiheuttaneet vaaran Yritys Oy:lle vain yhden kerran varsin kauan sitten. Tuolloin avattiin epähuomiossa sähköpostin liitetiedosto, joka saastutti yhden koneen.

Kaikkien Yritys Oy:n työntekijöiden matkapuhelimiin on asennettu Small Business Serverin kautta yhteys sähköpostiin. Vaikkakin virusten määrä matkapuhelinten käyttöjärjestelmiin on vielä vähäistä ja sitä kautta tietovarkauksien tapahtuminen erittäin harvinaista, ollaan Yritys Oy:ssä kokeiltu F-Securen tarjoamaa virustentorjuntaohjelmaa. Tämä on toiminut hyvin, mutta lisenssin uudistamisessa on joskus ollut vaikeuksia.

Tiedostojen salaus ei ole käytössä Yritys Oy:ssä, eikä sitä koeta tällä hetkellä tarpeelliseksi.

Yritys Oy:n internetsivuja eivät ulkopuoliset pysty muuttamaan, elleivät he hanki vilpillisin keinoin käyttäjätunnusta ja salasanaa jolla hallinnoidaan YritysOy.fi -domainin alta löytyviä tiedostoja.

4.4 Tietoaineistoturvallisuus

Tietojen kuljetuksesta, kopioinnista, hävittämisestä tai jakelusta ei Yritys Oy:ssä ole erikseen ohjeita, mutta työntekijöiden työsopimuksen liitteeksi allekirjoittama salassapitovelvollisuus kattaa nämä asiat. Tästä huolimatta minusta olisi kuitenkin suotavaa laittaa tästä aiheesta tietoturvaohjeistukseen oma osansa.

Yritys Oy:ssä ei ole tiedon luokitusjärjestelmää käytössä. Yleisohjeena voidaan pitää sitä, että kaikki tieto mikä on julkista, ei ole salassapidettävää tietoa, mutta kaikki muu on. Jos ei ole varma tiedon julkisuudesta, on parempi pitää sitä salassa välttääkseen sopimuksen rikkomisen.

Kaikilla työntekijöillä lukuunottamatta toimitusjohtajaa on samat luku-, kirjoitus- ja muutosoikeudet, eikä niitä ole jaoteltu heidän kesken. Koska kaikki työntekijät työskentelevät enemmän tai vähemmän toistensa tueksi, ei ole tarpeellista jaotella näitä oikeuksia työntekijöiden kesken. Toimitusjohtajalla on edellisen lisäksi palvelimella oma sektorinsa, jonne hän voi tallentaa ja hallita tietoja, joihin vain hänellä on pääsy.

Valtaosa yrityksen tiedosta ja tiedostoista tallennetaan verkkokovalevylle, jonne kaikilla on pääsyoikeudet. Yleisohjeena on, että kaikki liiketoiminnan kannalta tarpeellinen ja tärkeä tieto tallennetaan sinne, koska se on ainoa kovalevy, josta suoritetaan varmuuskopiointi. Tarvittaessa työntekijät tallentavat tietoa omille kannettaville tietokoneilleen esimerkiksi silloin, kun tietoa tarvitaan yrityksen ulkopuolella (presentaatiot). Yrityksessä käytetään erittäin vähän muistitikkuja ja niillä ei siirretä tietoa. Tietoa, joka on vain sähköisessä muodossa, hävitetään tavallisesti deletoimalla tiedostot, sekä tyhjentämällä tietokoneen roskakori. Papereita, joissa on salaiseksi luokiteltavaa tietoa ei saa koskaan heittää tavallisen paperijätteen sekaan, vaan se pitää hävittää silppuamalla. Yritys Oy:ssä jokaisessa työhuoneessa on paperisilppuri.

Järvinen kirjoittaa tiedon oikeanlaisesta tuhoamisesta kirjassaan Paranna tietoturvaasi (2006, 254). Hän toteaa, ettei pelkkä tiedoston poistaminen riitä, koska oikeanlaisilla välineillä tiedon palauttaminen on ainakin osittain mahdollista. Järvinen neuvoo käyttämään erillistä silppuamisohjelmaa, joka kirjoittaa niin kutsuttua roskaa sille kohtaa levyä, missä tiedosto aiemmin sijaitsi, jolloin tiedoston palauttaminen on mahdotonta.

Yritys Oy:ssä suurin osa tärkeästä tiedosta sijaitsee verkkokovalevyllä, josta varmuuskopionti suoritetaan. Osa yrityksen tiedosta on kuitenkin myös paperimuodossa, ja ne sijaitsevat erillisessä holvissa, joka on lukittu. Verkkokovalevyn tietoturvaa tulisi parantaa mahdollisia tulipaloja tai tulvia silmällä pitäen.

4.5 Henkilöstöturvallisuus

Henkilöstövalintaprosessissaan Yritys Oy tarkastaa työnhakijan koulutuksen ja muun soveltuvuuden lisäksi myös tämän muut taustat. Työnhakijalta pyydetään oikeus tarkastaa tämän taustat ja edelliset toiminnat. Samalla pyydetään myös mahdollisuuksien mukaan muutamien henkilöiden yhteystietoja, joilta voidaan varmentaa hakijan kertomusten

todenperäisyys. Ilman tätä tarkastusta yritykseen ei voi päästä töihin, koska yritys käsittelee työssään huomattavan määrän luottamuksellista tietoa ja on usein tietojen osalta salassapitosopimuksen alainen.

Yritys Oy:ssä työskentely edellyttää myös työsopimuksen liitteeksi tulevan salassapitovelvollisuussitoumuksen allekirjoitusta. Tällä sitoumuksella ja edellisessä kappaleessa kuvatulla tarkastuksella Yritys Oy:ssä pyritään minimoimaan riski, mikä voi aiheutua sellaisen ihmisen palkkaamisesta, joka ei syystä tai toisesta sovikaan työntekijäksi yritykseen. Luonnollisesti tämä koskee myös pitemmässä työsuhteessa olevia henkilöitä. Yritys Oy:n salassapitositoumus sisältää lausekkeen kilpailevasta toiminnasta, immateriaalioikeuksista sekä salassapitovelvollisuudesta.

Yritys Oy:ssä työntekijä sitoutuu työsuhteen aikana ja 12 kuukauden ajan työsuhteen päättymisestä lukien olemaan kilpailematta työnantajan kanssa omaan lukuunsa tai jonkun muun hyväksi ja olemaan menemättä työnantajan kanssa kilpailevan yrityksen palvelukseen sekä olemaan muutoinkaan millään tavoin tukematta tai avustamatta missään ominaisuudessa sellaista toimintaa, joka kilpailee työnantajan harjoittaman toiminnan kanssa. Mikäli työntekijä rikkoo kilpailukieltositoumusta vastaan, on työntekijä velvollinen maksamaan työnantajalle 12 kuukauden palkkaa vastaavan sopimussakon. (Yritys Oy, Salassapitovelvollisuus).

Kaikki työntekijän työn tuloksena tai sen sivutuotteena syntyvät immateriaalioikeudet siirtyvät ilman eri korvausta työnantajalle, sikäli kuin niiden ei jo suoraan lain nojalla katsota kuuluvan työnantajalle, ellei pakottavasta lainsäädännöstä muuta johdu. Mikäli oikeuksien siirtyminen edellyttää siirto-tai muun vastaavan asiakirjan allekirjoittamista, sitoutuu toimihenkilö allekirjoittamaan ko. asiakirjat. (Yritys Oy, Salassapitovelvollisuus).

Työnantajan liikesalaisuudella tarkoitetaan kaikkea työantajan ja työnantajan asiakkaiden ja yhteistyökumppaneiden taloudellista, teknistä ja/tai kaupallista aineistoa ja tietoa, joka ei ole yleisesti ulkopuolisten tiedossa ja/tai julkista ja jonka työntekijä työsuhteensa kestäessä saa tietoonsa siitä riippumatta, missä muodossa (kirjallisessa, suullisessa, analogisessa, digitaalisessa, mallina, teknisenä esikuvana tai muussa muodossa) liikesalaisuus on ja siitä riippumatta, onko työntekijä muodollisesti itse ollut osallinen liikesalaisuuden syntymiseen. (Yritys Oy, Salassapitovelvollisuus).

Yritys Oy:n työntekijöitä ei olla tähän mennessä informoitu sen kummallisemmin tietoturvallisuuteen liittyvistä asioista. Ollaan luotettu siihen, että kukin ymmärtää tiedon turvaamisen jo salassapitovelvollisuuden kautta, mutta myös osaa käyttää omaa harkintaansa

käyttäessään tietoa. Tämä tulee konkreettisesti muuttumaan tämän työn ansiosta, koska yritys saa käyttöönsä henkilöstön tietoturvaohjeistuksen.

4.6 Yleistä henkilöstön tietoturvaohjeistuksesta

Laatimani henkilöstön tietoturvaohjeistus on räätälöity kyseessä olevan kohdeyrityksen käyttöön. Koska aiempaa tietoturvaohjeistusta ei ole yrityksessä ollut, on tämä ohjeistus tarkoitettu jokaiselle yrityksen henkilökuntaan kuuluvalle ja se tullaan jakamaan heille lähitulevaisuudessa. Olen laatinut tietoturvaohjeistuksen tässä opinnäytetyössä tekemäni nykytilakartoituksen sekä yrityksen johdon kanssa käymäni keskustelun pohjalta.

5 Kehitysehdotukset, työn eteneminen ja arviointi

Olen kirjannut kehitysehdotukset erilliseen luetteloon, joka löytyy tämän työn lopusta liitteenä. Liite 3.

Suurin osa kehitysehdotuksistani olivat sellaisia, joissa jouduin olemaan yhteydessä tietoliikennealan palveluita Yritys Oy:lle tarjoavaan tahoon. He ovat asentaneet yrityksen nykyisen tietoliikennejärjestelmän, ja tarvitsin useasti heidän ammatillista osaamistaan selvittäessäni järjestelmän toimintaa ja asioiden hoitomahdollisuuksia.

Kuten jo aiemmin olen todennut, salasanoja ei säännöllisesti uusita yrityksessä. Selvitin palveluntarjoajalta, mahdollistaako nykyinen järjestelmämme salasanojen uusimisen säännöllisin väliajoin automaattisesti. Valitettavasti nykyinen järjestelmämme ei tällaisenaan sisällä kyseistä ominaisuutta. Tiedustelin palveluntarjoajan mielipidettä, tämän palvelun tarpeellisuudesta ja siitä, jos ottaisimme sen muulla tavoin käyttöömme. Hei eivät pitäneet sitä tarpeellisena. Heidän mukaansa salasanojen säännöllinen uusiminen pääsääntöisesti on toivottavaa, mutta ei ehkä tällä kerralla oleellista, koska kyseessä on pieni organisaatio, missä kaikki tuntevat toisensa. Heidän mielipiteensä oli, että ainoastaan isommissa organisaatioissa (esim. oppilaitokset), joissa käyttäjiä on oikeasti paljon, on suotavaa käyttää järjestelmää, joka itsestään tasaisin väliajoin vaatii salasanan uusimista. Ehdotan kuitenkin, että tietoturvaohjeistuksessa vaaditaan salasana uusimaan puolen vuoden välein.

Laatimani tietoturvaohjeistus otetaan yrityksessä käyttöön heti. Tällöin vaaditaan myös työntekijöiltä entistä tarkempaa kiinnostusta tietoturva-asioihin. Vieläkään heitä ei vaadita lukitsemaan tietokoneitaan heidän poistuessaan niiltä hetkeksi tai pitemmäksikin ajaksi yrityksen toimitiloissa ollessaan. Muualla heidän käyttäessään tietokoneitaan, tulee tietokone lukita aina poistuessa sen luota. Tämän toteutumista ei yrityksessä pystytä luonnollisesti

valvomaan, mutta työntekijät ovat pitkään olleet työsuhteessa ja ymmärtävät toimenpiteen tärkeyden, minkä johdosta tämän uskotaan toteutuvan varsin hyvin.

Tulvan, tulipalon tai muun niin kutsutun luonnonilmiön vuoksi on yrityksessä suhtauduttava vakavammin varmuuskopiointiin. Tällä hetkellä tulipalon sattuessa voi kaikki varmuuskopioitu tieto hävitä, kun sitä ei varmenneta muualle kuin yrityksen tiloissa olevalle nauhatallentimelle.

Yritys Oy:ssä on selvitetty ulkopuolisen palveluntarjoajan tarjoamaa varmuuskopiointia verkon yli. Etävarmistuspalvelu ostettiin samalta taholta, mistä kaikki muukin tietoliikenneosaaminen on hankittu ja se on otettu käyttöön. Etävarmistus tapahtuu jokaisena arkipäivänä ja alkaa iltakahdeksalta. Tämän palvelun myötä yrityksessä joudutaan seuraavaksi miettimään tietoliikenneyhteyden nopeuden nostoa. Nopeuden nostolla varmistettaisiin, etteivät yhteydet ole turhan hitaita etävarmistuksen aikaan. Tällä palvelulla varmistetaan tiedon säilyminen, jos jotain odottamatonta tapahtuu. Työntekijöitä ohjeistetaan myös tallentamaan tiedostot sekä palvelimen kovalevytilaan että oman koneen tiedostoihin.

Matkapuhelinten osalta työntekijöitä vaaditaan synkronoimaan yhteystietonsa sekä kalenterimerkintänsä tietokoneen kanssa, jolloin matkapuhelimen hävitessä tai tietojen kadotessa nämä tiedot olisivat helposti palautettavissa. Tämä on onneksi pystytty automatisoimaan, jolloin tieto löytyy varmemmin tarvittaessa.

Tiedon oikeanlaista tuhoamista ei tässä tapauksessa mielestäni tarvita otettavaksi päivittäiseen käyttöön. Ehdotan kuitenkin, että jos tietokone poistetaan käytöstä tai sen käyttäjä vaihtuu, tulee tässä vaiheessa kaikki tieto tuhota oikealla tavalla ennen koneen arkistointia, tuhoamista, hävittämistä tai käyttäjän vaihtumista.

Sivulla kahdeksan olen esittänyt konstruktiivisen tutkimuksen eri vaiheet. Tutkimusongelmaa ei niinkään tarvinnut tässä tapauksessa etsiä, vaan tavallaan etsittiin ongelmanratkaisijaa. Tapahtuneiden vesivahinkojen takia koettiin tarpeelliseksi kartoittaa palvelinkoneen parempi suojaaminen. Tämän lisäksi todettiin, että kiinnostus tietoturvan hallinnasta oli tarpeellista niin johdon kuin työntekijöidenkin keskuudessa. Kun tutkin lähdemateriaalia, oli sitä aivan liikaa ja suurin osa vielä englanninkielistä. Totesin, että aihetta on rajattava huomattavasti, joten otin vain toimeksiantajalleni parhaiten soveltuvat aihealueet. Tein yrityksen tietoturvan nykytilakartoituksen (liite 2) kysymyslistan avulla, jolloin pääsin lähemmäksi itse ongelmaa ja ongelmanratkaisu helpottui. Esitin kysymykset kullekin työntekijälle ja toimitusjohtajalle. Toimitusjohtajalle annoin vapaammat kädet vastaamisessa kuin työntekijöille, koska halusin kuulla hänen näkemyksensä vaaditusta tietoturvan tasosta. Vastauksesta olivat hyvinkin

yksiselitteisiä ja näin pystyin helposti selvittämään, missä kaikkialla on parantamisen varaa ja mitä voitaisiin tehdä toisin.

Kun olin kartoittanut nykytilanteen jaoin toimenpiteitä vaativat kohdat kahteen eri luokkaan, toinen oli toimenpiteet, jotka vaadin toteutettavaksi ja toinen oli toimenpiteet, jotka suosittelin toteutettavaksi.

Vaaditaan toteutettaviksi	Suositellaan toteutettaviksi
Henkilöstön tietoturvaoppaan käyttöönotto	Tiedon oikeanlainen tuhoaminen tietyissä tilanteissa.
Varmuuskopiointia / sähköisessä muodossa olevan tiedon varastointia tehostettava	Matkapuhelinten synkrointi kunkin käyttäjän tietokoneen kanssa
Internetyhteyden nopeuden nosto	Salasanojen säännöllinen uusiminen
Palvelinkoneelle tulisi varmistaa varavirta mahdollisten sähkökatkojen varalle	

Sisällytin henkilöstön tietoturvaohjeistuksen laatimisen ja käyttöönoton tähän opinnäytetyöhön ja se on otettu yrityksessä käyttöön. Varmuuskopiointia muutettiin niin, että vanhasta nauhatallenninjärjestelmästä luovuttiin ja ostettiin ulkopuoliselta palveluntarjoajalta etävarmistuspalvelu. Etävarmistuspalvelun käyttöönotto toi esille internetyhteyden riittämättömyyden ja se nostettiin tarvittavalle nopeudelle. Salasanojen säännöllisen uusinta ja matkapuhelinten synkronointi muutettiin vaadituiksi toimenpiteiksi yrityksen johdon kanssa käydyn keskustelun perusteella, ja ne sisällytettiin tietoturvaoppaaseen. Varavirtaa palvelinkoneelle ei olla vielä toteutettu, mutta sekin aiotaan tehdä mahdollisimman pian. Tiedon oikeanlainen tuhoaminen tulee aiheelliseksi, kun tarpeellinen tilanne tulee eteen (esimerkiksi tietokoneen käyttäjä vaihtuu).

Yritys Oy:n tietoturva on nyt saatettu vaaditulle tasolle. Työ oli verrattain jopa haastavaa, minkä koen johtuvan siitä, että tietoturva käsitteenä on niin laaja. Tarkka aiheen ja teorian rajaus auttoi paljon, ja niin alkoi kokonaisuus helpommin hahmottua. Monesti myös huomasin, kun jokin epäkohta korjattiin, aiheutti se uuden ongelman. Esimerkiksi kun varmuuskopiointipalvelu ostettiin, huomattiin tietoliikenneyhteyden olevan vähän turhan hidas. Tästäkin huomaa sen, kuinka tietoturvan hallinta vaatii päivittäistä työtä, ja päivitystä, eikä sitä voi vain saattaa jollekin tasolle ja olla sitten tyytyväinen.

Yritys Oy:n johto on kiitellyt työtäni ja he toivovat, että jatkan tietoturva-asioiden hoitamista oman työni ohella. He ovat tyytyväisiä myös siihen, että tämän asian hoitamiseen ei tarvinnut palkata väkeä talon ulkopuolelta, vaan osaaminen saatiin olemassaolevalta työntekijältä. Tärkein jatkotoimenpide tietoturvallisuuden hallinnassa on seuranta. Ei voida liikaa korostaa seurannan tärkeyttä tässä yhteydessä, koska tietoturvallisuus ei koskaan pysy vaaditulla tasolla itsestään. Järjestelmiin tulee muutoksia, ihmiset vaihtuvat tai otetaan täysin uusia menetelmiä käyttöön. Tästä syystä tietoturvallisuutta tulee koko ajan tarkkailla ja tehdä töitä hyvän tietoturvallisuuden ylläpitämiseksi.

Lähteet

Hirsjärvi, S., Remes, P. & Sajavaara,P. 1997. Tutki ja Kirjoita. Jyväskylä: Gummerus Kirjapaino Oy.

Järvinen, P. 2006. Paranna tietoturvaasi. Porvoo: WS Bookwell.

Järvinen, P. 2002.Tietoturva & yksityisyys. Porvoo: WS Bookwell.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing Oy.

Moilanen, T., Ojasalo, K. & Ritalahti, J. 2009. Kehittämistyön menetelmä. Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro Oy.

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Helsinki Edita Prima Oy.

Yritys Oy, Salassapitovelvollisuus

https://www.bsi.bund.de/cae/servlet/contentblob/479604/publicationFile/28020/it-grundschutz-kataloge_2005_pdf_en_zip.zip haettu 28.1.2010

http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/toimiva_tietoturva.html haettu 13.3.2010

http://www.yritysX.fi haettu 15.1.2010

https://www.jyu.fi/thk/ohjeet/faq/millainen-on-hyva-salasana haettu 17.11.2011

http://salasana.fi/ haettu 17.11.2011

http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html haettu 17.11.2011

http://www.tietojesiturvaksi.fi/content/tietoturvan-osa-alueet haettu 17.11.2011

http://www.tietojesiturvaksi.fi/content/fyysinen-tietoturva haettu 18.11.2011

http://www.tietojesiturvaksi.fi/content/laitteistoturvallisuus haettu 18.11.2011

http://www.tietojesiturvaksi.fi/content/ohjelmistoturvallisuus haettu 18.11.2011

http://www.tietojesiturvaksi.fi/content/tietoaineiston-turvallisuus haettu 18.11.2011

http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/index.html haettu 21.11.2011

http://www.internetopas.com/yleistietoa/tietoturva/ haettu 21.11.2011

http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvakartoitus_kysymyslista.pdf haettu 21.11.2011

http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvaohjeet.pdf haettu 21.11.2011

www.defmin.fi/files/1870/KATAKRI_versio_II.pdf haettu 23.5.2012
http://it-palvelut.org/yrityksen-tietoturva/ haettu 23.5.2012
http://www.talouselama.fi/minavaitan/tietoturva+on+osa+johtamista/a2019729 haettu 23.5.2012

Julkaisemattomat lähteet

Heiskanen, K., Marjokorpi, S., Nishio, E. & Nurminen, H. 2009. Tietoturvallisuuden hallinta, kehittäminen ja tietoturvaorganisaatio. Espoo: Laurea-ammattikorkeakoulu.

Kuvat ja kuviot

Liitteet

Liite 1

Yritys Oy:n tietoturvallisuuden nykytilakartoituksen kysymykset

Fyysinen turvallisuus

1. Onko yrityksessä kulunvalvontaa? -> ovien lukitus?
2. Onko yrityksellä hälytysjärjestelmää mahdollisten murtojen varalta?
3. Miten vieraiden annetaan liikkua yrityksen tiloissa?
4. Vaatiiko jokainen tietokone käyttäjän kirjautumisen järjestelmään ennen käyttöä?
5. Missä lähiverkon palvelimet sijaitsevat? -> lukittuna?
6. Kuinka usein salasanoja vaihdetaan? -> valvonta?

Laitteistoturvallisuus

1. Voiko kukaan muu muokata esim. käyttäjätunnuksia kuin järjestelmänvalvoja?
2. Vaihdetaanko salasanoja säännöllisesti?
3. Onko tietojen joutuminen ulkopuolisille mahdollista?
4. Miten energian jakelu on hoidettu sähkökatkon aikana?
5. Miten matkapuhelimet on suojattu mahdollisen varkauden varalta?

Ohjelmistoturvallisuus

1. Onko laitteisiin asennettu virustentorjuntaohjelma?
2. Kuka vastaa ko. ohjelmien päivittämisestä?
3. Kuinka usein virustarkistus tehdään?
4. Onko virukset koskaan aiheuttaneet vaaraa yritykselle?
5. Onko tiedostojen salaus käytössä?
6. Voiko ulkopuoliset muuttaa yrityksen nettisivuja?
7. Matkapuhelimet

Tietoaineistoturvallisuus

1. Miten henkilökuntaa on ohjeistettu tietojen kuljetuksesta?
2. Miten henkilökuntaa on ohjeistettu tietojen kopioinnista?
3. Miten henkilökuntaa on ohjeistettu tietojen hävittämisestä?
4. Miten henkilökuntaa on ohjeistettu tietojen jakelusta?
5. Onko yrityksessä luokitusjärjestelmää tiedolle?
6. Onko luku-, kirjoitus- ja muutosoikeuksia jaoteltu työntekijöiden kesken?
7. Miten yrityksessä tallennetaan tietoa?
8. Onko sähköposti suojattu? Miten?
9. Miten tietoa tai tallenteita hävitetään?
10. Miten varmuuskopiointi on suoritettu?
11. Miten tietoa on varastoitu?

Henkilöstöturvallisuus

1. Allekirjoittaako työntekijät salassapitosopimusta?
2. Tarkastetaanko työntekijöiden taustatietoja?
3. Informoidaanko työntekijöitä tietoturvallisuuteen liittyvistä asioista?

Henkilöstön tietoturvaohjeistus

Tiedon turvallinen käsittely on toimeentulon kannalta oleellista jokaisessa yrityksessä. Tietoa on tallennettu paperille, tietokoneisiin ja ihmisten muistiin, mutta tietokoneiden kanssa tiedon turvallista säilyttämistä ei voida hoitaa täysin tietoteknillisin menetelmin. Yrityksen tietoturva on hyvin laaja ja moninainen käsite. Useimmiten tietoturvasta puhuttaessa ihmiset kokevat sen koskevan vain internettiä, mutta yrityksen tietoturvaan kuuluu mm. kaikki johtoportaan laatimista tietoturvasäännöistä, työasemien ohjelmistojen valintoihin, sekä näiden käyttäjien tietoturvatietoisuuteen. Tämän lisäksi käsite sisältää myös yrityksen fyysisen turvallisuuden.

Fyysinen turvallisuus

- Ovet on aina lukittava.
- Hälytysjärjestelmä on kytkettävä päälle aina kun toimisto jää tyhjilleen. Ei koske kuitenkaan virka-aikaa.
- Vieraiden ei saa antaa liikkua toimitiloissa itsenäisesti, vaan heidät ohjataan esimerkiksi neuvotteluhuoneeseen.
- Tietokoneelta poistuttaessa pitää se lukita CTRL + ALT + DELETE –toiminnon avulla.
- Salasanoja ei saa kertoa kenellekään.
- Salasanoja ei saa kirjoittaa muistilapulle.
- Salasana uusitaan puolen vuoden välein.
- Salasanan pitää olla ainakin kahdeksan merkkiä pitkä ja siinä on oltava sekä kirjaimia, että numeroita.

Laitteistoturvallisuus

- Matkapuhelimissa on oltava lukituskoodi käytössä.
- Laitteen rikkoutuessa on siitä ilmoitettava viipymättä IT-tukeemme.
- Tietokoneisiin ei saa asentaa omatoimisesti mitään ohjelmistoja. Tarvittavista ohjelmistoista pitää ensin keskustella IT-tukemme kanssa.
- Tietokonetta ei saa käyttää yrityksen ulkopuoliset henkilöt. (Esimerkiksi perheenjäsenet)

Ohjelmistoturvallisuus

- Kunkin käyttäjän omalla vastuulla on ilmoittaa IT-tukeemme, kun virustorjunta vaatii uusimista.
- Virustarkistus pidetään päällä automaattisena.
- Matkapuhelinten kalenterimerkinnät sekä yhteystiedot synkronoidaan kunkin käyttäjän oman tietokoneen kanssa.

Tietoaineistoturvallisuus

- Tietojen kuljetuksessa vaaditaan tarkkuutta, eikä tietoa saa koskaan kuljetuksen aikana altistaa kenenkään nähtäväksi.
- Tietoa saa kopioida jos tarve vaatii.
- Paperidokumentit arkistoidaan vaadittuun kohteeseen.
- Paperidokumentit, joita ei tarvita, tulee silppuroida.
- Työpöytä ei ole papereiden säilytyspaikka.
- Tietoa ei jaeta turhaan.
- Tieto tallennetaan sekä oman koneen tiedostoihin, että public -kovalevylle.
- Varmuuskopiointi tapahtuu joka arkipäivä public –kovalevystä.
- Paperidokumentit varastoidaan yrityksen tiloissa olevaan holviin.
- Tietokoneelle ei saa tallentaa henkilökohtaisia tiedostoja.
- Sähköposti on tarkoitettu vain työasioiden hoitoon.

Tietoliikenneturvallisuus

- Internettiä käytetään ensisijaisesti työtehtävien hoitamiseen.
- Virusepäilyistä välittömästi ilmoitus IT-tukeen.
- Salasanoja ei saa tallentaa selaimen muistiin.

Henkilöstöturvallisuus

- Jokainen työntekijä allekirjoittaa salassapitovelvollisuuden.

Kehitysehdotukset

- Salasanojen säännöllinen uusiminen
- Henkilöstön tietoturvaohjeistuksen laadinta ja käyttöönotto
- Varmuuskopiointia / sähköisessä muodossa olevan tiedon varastointia tehostettava
    - Internetyhteyden nopeuden nosto
- Matkapuhelinten synkrointi kunkin käyttäjän tietokoneen kanssa
- Palvelinkoneelle tulisi varmistaa varavirta mahdollisten sähkökatkojen varalle
- Tiedon oikeanlainen tuhoaminen tietyissä tilanteissa.