Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2012

Eetu Salmi

TIETOTURVAOHJEISTUS FUJITSU FINLAND OY:N KÄYTTÖTUKEEN

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Marraskuu 2012 | 38 sivua

Esko Vainikka

Eetu Salmi

TIETOTURVAOHJEISTUS FUJITSU FINLAND OY:N KÄYTTÖTUKEEN

Opinnäytetyön aiheena oli tehdä tietoturvaohjeistus Fujitsu Finland Oy:n käyttötuessa työskenteleville henkilöille, yrityksen yleisten tietoturvaohjeiden tueksi. Tietoturvaohjeistuksen tarkoitus on tukea käyttötukihenkilöitä päivittäisessä työssä ja toimia uuden henkilön perehdytysmateriaalin lisänä. Käyttötukea koskevaa ohjeistusta ei vielä ollut olemassa.

Työn teoreettisessa osuudessa käsiteltiin tietoturvan teoriaa, joka toimii pohjana tietoturvaohjeistukselle. Osuudessa käytiin läpi tietoturvan osa-alueet. Osuus nojautui alan kirjallisuuteen ja sähköiseen materiaaliin.

Empiirisessä osuudessa on koostettu tiiviis tietoturvaohjeistus käyttötukihenkilöitä varten. Tietoturvaohjeistus itsessään on salainen, joten sitä ei työn raportissa ole.

ASIASANAT:

Tietoturva, tietoturvaohjeistus, tietoturvallisuus

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data communications

November 2012 | 38 Pages

Esko Vainikka

Eetu Salmi

INFORMATION SECURITY GUIDANCE FOR FUJITSU FINLAND OY SERVICE DESK

The objective of this study was to make an information security guide for those who work at the service desk and to support a company's general guidance. The purpose of security guidance is to support the service desk worker in daily work and in addition to assist new personnel's orientation. Service Desk information security guidance does not yet exist.

The theoretical part of the thesis is based on information security theory. This part was based on relevant literature and electronic materials.

In the empirical part I edited tight information security guidelines for the use of service desk staff. Security Guide itself is a secret, so it is not included.

Key words:

Information security, information security guidance

SISÄLTÖ

1 Johdanto

Tietoturva on tämän päivän puhutuimpia aiheita niin IT-alan yrityksissä kuin lehdissäkin. Tietoturva koskettaa kaikkia ihmisiä nyky-yhteiskunnan sähköistymisen myötä, vaikkakin tietoturva pitää sisällään myös ei-sähköisen tiedon turvaamisen. Tietoturvalla tarkoitetaan tiedon, palvelujen ja tietoliikenteen turvaamista. Tietoturva koostuu organisaation pienistä teoista sen toiminnassa, pääasiassa henkilöstön toimista ja tekniikasta. Tietoturva perustuu Suomen lakiin ja sen asetuksiin.

Opinnäytetyöni aiheeksi valitsin tietoturvaohjeistuksen laatimisen Fujitsu Finland Oy:n käyttötuelle. Aiheen idea tuli työnjohtajaltani, jonka mielestä tietoturvaohjeistus pitäisi päivittää tai tehdä täysin uusi. Käyttötukea koskevaa tietoturvaohjeistusta ei vielä ollut, joten katsoimme sen olevan tarpeellinen. Ohjeistus tulee olemaan yleisohje tietoturvasta käyttötuelle ja sitä tullaan käyttämään uusien ja vanhojen työntekijöiden kouluttamisessa. Opinnäytetyön perimmäinen tarkoitus on edistää käyttötuessa toimivan henkilöstön tietoturvatietoisuutta, joka suoranaisesti vaikuttaa Fujitsun ja asiakkaiden tietoturvaan. Tutkimuksessa keskitytään tietoturvaan käyttötuen ja asiakkaan näkökulmasta. Ohjeistus tulee sisältämään tietoturvakoulutukseen tarkoitetun materiaalin, jota ei voida julkistaa salassapitosyistä.

Työssäni tulen hyödyntämään tietoturvaan liittyvää kirjallisuutta, lehtiä, internetiä, Fujitsun tietoturvamateriaaleja ja standardeja, joista Fujitsu Finlandilla on ISO/IEC 27001 sertifikaatti. Päälähteenä käytän Esko Vainikan tietoturvakurssin luentomateriaalia, joka ei yleisesti ole saatavilla. Minun tulee ottaa huomioon Fujitsun tietoturvapolitiikka ja asiakkaiden tietoturva. Asiakkaiden tietoturva koostuu heidän omasta politiikastaan ja pääasiassa Fujitsun tietoturvapolitiikasta, koska Fujitsulle on annettu vastuu tietyistä osa-alueista, ellei kaikesta. Tarkastelen asiakkaiden tietoturvaa yleisesti, enkä ota yksityiskohtaisesti mitään asiakasta tarkasteluun, koska kaikilla on erilaiset sopimukset ja eri käyttötuilla omat asiakkuudet.

2 Fujitsu Finland Oy

Yritysesittely

Fujitsu on Suomen johtava tietotekniikan palvelu- ja laitetoimittaja. Tavoitteena on helpottaa yritysten ja yhteisöjen toimintaa edistyksellisten ict-toimintamallien ja teknologioiden avulla.

Fujitsun Patja- ja Sohva-palvelut huolehtivat asiakkaiden tieto- ja viestintätekniikasta sekä sovellusten tukipalveluista, toiminnasta ja kehittämisestä. Teknologiatuotteiden valikoima kattaa tietokoneiden koko kirjon, kannettavista päätelaitteista aina konesaliratkaisuihin saakka.

Patja- ja Sohva -palveluiden piirissä on 130 asiakkaan yli 130 000 työasemaa ja 7 000 palvelinta.

Muita vahvoja osaamisalueita ovat muun muassa liikkuvan työn palvelut, sähköinen asiointi sekä Microsoft, SAP- ja EMC Documentum -pohjaiset ratkaisut.

Maaliskuussa 2009 päättyneellä tilikaudella Suomessa toimivan palveluyhtiö Fujitsun liikevaihto oli 395 miljoonaa euroa. Suomessa ja Baltiassa Fujitsu työllistää lähes 2 800 ihmistä neljässä yhtiössä, jotka ovat Fujitsu Finland Oy, Fujitsu Technology Solutions Oy, Isoworks Oy ja Nice-business Solutions Finland Oy.

Suomen Fujitsu on osa maailmanlaajuista Fujitsu-ryhmää. Fujitsu Limited on yksi maailman suurimmista ict-palveluyrityksistä. Fujitsun osaajaverkostoon kuluu 186 000 työntekijää 70 maassa. Fujitsu-konsernin liikevaihto oli maaliskuussa 2009 päättyneellä tilikaudella 4,6 triljoonaa jeniä eli 35,3 miljardia euroa. (Fujitsu Finland Oy 2010.)

Historia

1960–1990

Nokia-aika: tuotteet, työryhmäohjelmistot: Mikko, MikroMikko ja Tiimi.

Yhtiön juuret ovat 1960-luvulla Suomen Kaapelitehtaan Elektroniikka-osastossa, josta myöhemmin tuli osa Nokiaa.

1980-ja 90-luvuilla yhtiö valmisti edelläkävijä-pc:itä MikroMikkoja sekä ToimistoTiimiä, joka on menestynein suomalainen valmisohjelmisto.

1990–1999

ICL-aika: perustietotekniikan ulkoistus ja Patja-toimintamalli.

1995 Patja-toimintamallin kehitystyö alkoi. Ensimmäinen asiakas oli Helvar Merca.

1997 perustettiin e-bisnes-yksikkö ja sovellusliiketoiminnassa keskityttiin maailmanluokan valmisohjelmistoihin.

1999 perustettiin mobiiliteknologian kehityskeskus Helsinkiin. Samana vuonna perustettiin huoltotoimintaan keskittyvä yhteisyritys Isoworks Oy Soneran kanssa. Vuoden 2006 alussa Fujitsu osti Isoworksin kokonaan itselleen.

2000

Fujitsu-aika: sovellusulkoistus, Sohva-toimintamalli ja sähköinen asiointi.

2000 perustettiin e-bisnes-yhteisyritys Nice-business Solutions Finland Oy Nokian kanssa.

2000 ostettiin Pohjoismaiden it-palveluliiketoiminnat ICL Plc:ltä ja Suomen tuotemyyntitoiminnot myytiin ICL Plc:lle.

1.4.2002 nimi muuttui ICL Inviasta Fujitsu Inviaksi ja 1.10.2003 Fujitsu Finland Oy:ksi

Vuonna 2004 Fujitsu julkisti Sohva-kumppanuusmallin, joka tarjoaa uuden toimintamallin liiketoiminnan operatiivisten sovellusten hankintaan ja kehittämiseen.

Patja-toimintamalli täytti 10 vuotta ja jatkoi voittokulkuaan. Sadas Patja-asiakas oli Ramboll Finland. (Fujitsu Finland Oy 2010.)

Laatu

Fujitsun toiminta perustuu visiota, arvoja ja strategiaa tukeviin toimintaprosesseihin. Ydinprosesseja ovat asiakkuuden hallinta (sisältää myynnin ja palvelun hallinnan ydinprosessit), projektiprosessi ja palveluprosessi. Mahdollistajaprosessit ovat johtaminen, palvelukehitys ja osaamisen johtaminen.

Prosessien kehittymistä, oppimista, tehokkuutta ja kannattavuutta seurataan systemaattisesti prosessimittareilla. Tavoitteena on hyvä asiakastyytyväisyys. Hyvä asiakastyytyväisyys tarkoittaa sitä, että asiakas on valmis suosittelemaan Fujitsua palvelutoimittajana muille yrityksille.

Fujitsu kerää asiakaspalautetta kaikista mahdollisista lähteistä. Yhtenä tietolähteenä ovat asiakastyytyväisyystutkimukset, joita tehdään eri kohderyhmille. Tavoitteena on muodostaa kokonaisnäkemys asiakastyytyväisyydestä. Palautteet analysoidaan systemaattisesti ja hyödynnetään toiminnan kehittämisessä.

Fujitsulle myönnettiin 2.4.2008 ISO/IEC 20000-1:2005 -sertifikaatti. Se on kansainvälinen standardi tietotekniikkapalvelujen johtamiseen ja hallintaan. Fujitsu on sertifikaatin ensimmäinen haltija Suomessa ja tiettävästi myös Pohjoismaissa. Fujitsulla on Suomessa palveluyrityksen toimintaa tukeva ISO9001:2000-standardin mukainen sertifikaatti.

Fujitsu palvelutuotannolle on myönnetty standardin ISO/IEC 27001:2005 vaatimusten mukainen tietoturvasertifikaatti. Sertifikaatti kertoo, että palvelutuotannon toiminnassa on analysoitu keskeiset riskit, niihin on varauduttu ja turvallisuus on hyvällä tasolla.

Fujitsun Logistiikka ja esiasennuskeskuksella on ISO 14001-ympäristösertifikaatti, joka takaa asiakkaalle ympäristöystävällisen laitetoimituksen ja -kierrätyksen.

Fujitsu ottaa ympäristökysymykset huomioon esiasennus- ja logistiikkakeskuksen toiminnassa. Yksikön johto ja henkilöstö ovat sitoutuneet ympäristön pilaantumisen ehkäisemiseen sekä ympäristönsuojelun tason jatkuvaan parantamiseen. Tämän varmistamiseksi huolehdimme henkilöstön ympäristötiedon tasosta ja organisaation toiminta auditoidaan säännöllisesti.

Tavoitteena on sähköisten asiakirjojen käytön lisääminen ja jätteiden lajittelun lisääminen. Nämä yrityksen ympäristönäkökohdat tarkistetaan ja päivitetään vuosittain. Tavoitteiden saavuttamista seurataan mittarein. Fujitsu noudattaa toiminnassaan lainsäädäntöä, kaikkia ympäristönsuojeluun liittyviä lakeja, määräyksiä ja asetuksia sekä seuraa niissä tapahtuvia muutoksia. (Fujitsu Finland Oy 2010.)

Asiakkaat

Fujitsun asiakkaat edustavat laajasti koko elinkeinoelämää. Fujitsun monipuolinen osaaminen ja vuosikymmenien aikana kertynyt kokemus eri toimialoilta koituvat

asiakkaan eduksi. Fujitsulla on asiakkaita julkishallinnosta, terveydenhuollosta, kauppa- elintarviketeollisuudesta, kuluttajapalveluista, finanssialalta ja teollisuudesta. (Fujitsu Finland Oy 2010.)

Yhteistyökumppanit

Fujitsulla ja Microsoftilla on merkittävää kansainvälistä yhteistyötä, jota laajennettiin kesällä 2002 solmitulla sopimuksella. Fujitsu on Microsoftin Gold Certified Partner Collaborative-ratkaisuissa ja Support-palveluissa (Gold Certified for Support Services).

Fujitsu on myös Suomen johtava SAP-ratkaisujen tarjoaja. Fujitsu on ollut SAPin Service Partner vuodesta 1995 alkaen ja solminut Channel Partner -sopimuksen vuonna 1998. Gold SAP Channel Partner -aseman Fujitsu sai vuonna 2009. Lisäksi Fujitsu on Hosting Partner vuodesta 2005.

Suomen Fujitsu on Cisco Silver Partner, mikä edellyttää kymmeniä Cisco-sertifikaatteja sekä myynnissä että tuotannossa. Cisco antoi tammikuussa 2008 Suomen Fujitsulle kumppanuuden korkeimman tunnustuksen, Customer Satisfaction Excellencen.

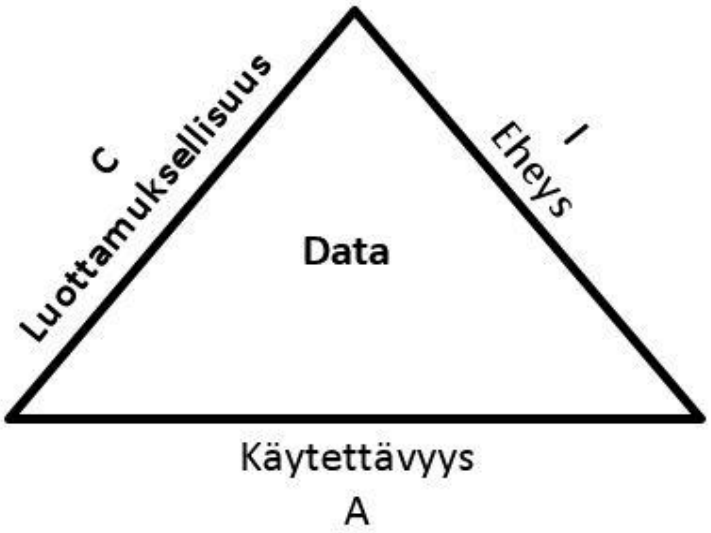
Kesäkuussa 2003 Fujitsu ja Nokia julkistivat globaalin allianssin, joka keskittyy langattomien yritysratkaisujen kehittämiseen. Allianssi hyödyntää Nokian yritysmarkkinoille suunnattua päätelaitevalikoimaa ja mobiilialustoja sekä Fujitsun laajaa konsultoinnin, järjestelmäintegraation ja hallintapalvelujen osaamista.

Fujitsulla on Suomessa kaksi tytäryhtiötä: Nice-business Solutions Finland Oy (Nice) ja Isoworks Oy. Fujitsun ja Nokian omistaman Nicen ydinosaamista ovat sovellukset niiden suunnittelusta aina elinkaarensa päätökseen. Isoworks on erikoistunut ict-järjestelmien ylläpitoon ja huoltoon.

Ohjelmisto- ja tuotekehityskumppaneita ovat muun muassa BEA, Cisco, Cognos, Efecte, GoodMood, HP, F-Secure, Microsoft, SAP, Nokia, Oracle, Seven, Siebel ja SUN. Palvelutuotantokumppaneita ovat muun muassa BMC, Elisa, EMC ja TDC Song. Tietoturvakumppaneita ovat muun muassa Avain Technologies, Birdstep Technology, Cybertrust, Blancco, Check Point, Cisco, Commtouch, F-Secure, Louhi Networks, Microsoft, McAfee, Nexus, SSH, Stonesoft, Sun Microsystems ja Symantec. (Fujitsu Finland Oy 2010.)

3 Tietoturvan osatekijät

Tietoturva koostuu kolmesta pääosa-alueesta: luottamuksellisuudesta, eheydestä ja saatavuudesta (Confidentiality, Integrity, Availability = CIA), joita yhdessä pidetään tietoturvan pääperiaatteina (kuvio 1). Muita osa-alueita ovat todentaminen, pääsynvalvonta ja kiistämättömyys. Kaikki osa-alueet pitävät sisällään tiedon eri muodoissa. Tieto voi olla tiedostoja, tiedonsiirtoa tai keskusmuistissa olevia bittien joukkoja. Seuraavissa kappaleissa on kaikki osa-alueet tarkemmin selitettyinä. Nämä osa-alueet ovat tietoturvan perusta ja niihin viitataan tutkimuksen myöhemmissä vaiheissa. (Järvinen 2002, 22.)



Kuvio 1. CIA – Tietoturvan pääperiaatteet.

Luottamuksellisuus – Confidentiality

Luottamuksellisuudella tarkoitetaan pääsyn estämistä niiltä, joilla ei ole oikeutta tietoihin. Tietojen luku- tai muokkausoikeus annetaan etukäteen käyttäjille, joille pääsy on tarkoitus antaa. Luottamuksellisuus saavutetaan käyttäjän todentamisella. Todentaminen käsitellään myöhemmässä kappaleessa. Tiedon luottamuksellisuuden määrittelevät yritykset itse Suomen lakien ja asetusten pohjalta. Luottamuksellisuus voidaan menettää antamalla tahattomasti yrityksen tietoja ulkopuoliselle tai käyttöoikeuksien väärinkäytöllä. (Järvinen 2002, 22; Krutz & Vines 2003, 3.)

Eheys – Integrity

Tiedon eheydellä tarkoitetaan sitä, ettei ulkopuolinen taho pysty luvatta muokkaamaan tai tuhoamaan tietoa. Eheys termi pitää sisällään datan ja järjestelmän eheyden. Eheys voi joutua uhatuksi virusten, hakkereiden tai levyvian johdosta. Eheyden turvaamiseen on monia keinoja, joita käytetään ilman, että käyttäjä edes huomaa niitä. Esimerkkejä eheyden turvaamisen keinoista ovat tarkistussummat, lokitiedostot, tiedonsiirron protokollat, erilaiset sisäiset tarkistukset ja tarkistusohjelmat (virusohjelmat). Tietojen salaaminen turvaa myös eheyttä mutta voi lisätä siirto- ja käsittelyvirheitä. Eheys on erittäin tärkeää tietojen arkistoinnissa. Esimerkiksi yritysten arkistotietojen pitää pysyä muuttumattomina tai ainakin tallentaa lokitiedostot, joista voidaan todeta muuttumisen tapahtumahetki ja tekijä. (Järvinen 2002, 22; Stallings 2008, 8.)

Saatavuus – Availability

Saatavuudella tarkoitetaan tietojärjestelmien toiminnallisuuden turvaamista ja tietojen olemista käytettävissä niille, jotka niitä tarvitsevat. Tietojärjestelmät pitävät sisällään tiedot ja palvelut, joita käyttäjä tarvitsee. Tietojärjestelmien pitää olla käynnissä aina silloin, kun tietoa halutaan käyttää, mikä usein tarkoittaa 24 tuntia 7 päivänä viikossa. Saatavuuden takaamiseen yleensä riittävät varmuuskopiointi ja laitteiden toiminnan turvaaminen. (Järvinen 2002, 24.)

Todentaminen – Authentication

Todentamisella saavutetaan luottamuksellisuus, joka tarkoittaa yhteyttä haluavan tahon varmentamista eli onko taho se mikä väittää olevansa. Yhteyttä haluava taholla voidaan tarkoittaa käyttäjää, laitetta, tiedon alkuperää tai ohjelmakoodia. Käyttäjien todentaminen tapahtuu käyttäjätunnuksella ja salasanalla sekä mahdollisesti myös jollain muulla tekniikalla, esimerkiksi sormenjälkitunnistuksella tai sähköisellä avaimella. Laitteen todentaminen tapahtuu IP- ja MAC-osoitteen avulla. Internetistä saadun tiedon todentaminen on hankalaa, koska julkaisijan perusteella pitää päätellä onko tieto luotettavaa. (Järvinen 2002, 24-25.)

Pääsynvalvonta – Access Control

Pääsynvalvonnalla tarkoitetaan menetelmiä, joilla valvotaan ja rajataan kohteiden käyttöä. Pääsynvalvonnasta huolehtivat käyttöjärjestelmä ja käytettävä sovellus, jotka päästävät vain todennetut käyttäjät järjestelmän tietoihin. Pääsynvalvontaan kuuluu myös käytön valvonta, joka sisältää tiedostojen avaukset ja muokkaukset, mitä ohjelmia on käytetty ja ketkä ovat järjestelmään kirjautuneet. Käytönvalvonnan lokitiedostoista pystytään selvittämään mahdollisia tahallisia tai tahattomia tietoturvarikkomuksia. Pääsynvalvontaprosessi sisältää tunnistuksen, todennuksen, valtuutuksen ja toimenpiteiden tallennuksen. Pääsynvalvonnassa voidaan käyttää yksilöpohjaista, sääntöpohjaista ja roolipohjaista pääsynvalvontaa. (Järvinen 2002, 27; Karvi 2010.)

Kiistämättämyys – Non-Repudiation

Kiistämättömyydellä tarkoitetaan järjestelmän kykyä tunnistaa ja tallettaa järjestelmää käyttävän tahon tiedot. Kiistämättömyyden tarkoituksena on varmistaa tiedon alkuperä ja todentaa valtuudettomasti käyttävä taho. Esimerkiksi sähköiset kaupat hyödyntävät tätä todistamaan tilauksen vastaanottoa ja lähettämistä. Kiistämättömyys edellyttää tapahtumiin aikaleiman. Kiistämättömyys voidaan saavuttaa käyttäen aiempia periaatteita eheydestä ja todennuksesta. (Järvinen 2002, 27-28.)

4 Hallinnollinen turvallisuus

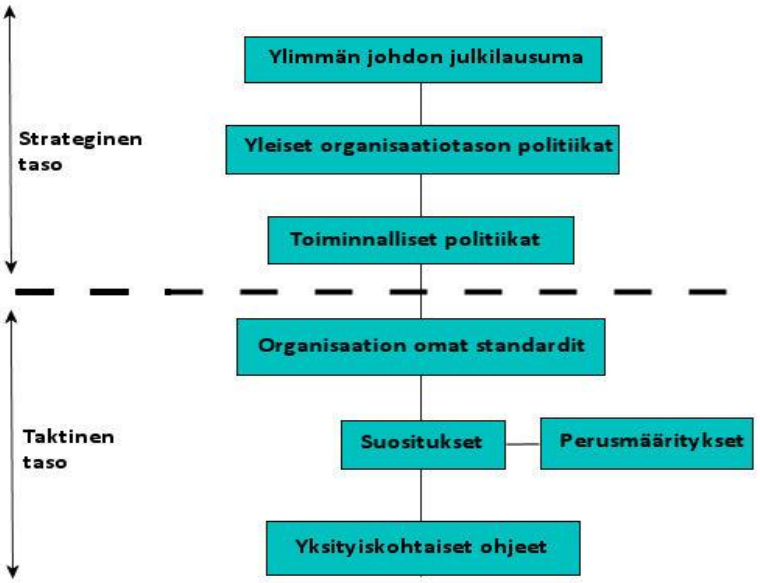
Hallinnollinen turvallisuus koostuu pakollisista ja valinnaisista tietoturva-asioista ja toimenpiteistä, jotka standardit määrittelevät. Hallinnolliseen turvallisuuteen kuuluu turvallisuuspolitiikka, politiikkahierarkia, tietoturvariskien hallinta, turvallisuustietoisuus ja sitä koskevat lait, asetukset ja viranomaismääräykset.

Turvallisuuspolitiikka

Turvallisuuspolitiikka sisältää organisaation tietoturvatavoitteet, jotka ovat osana suurempaa kokonaisuutta. Turvallisuuspolitiikan toimivuuden edellytyksenä on, että ylin johto sitoutuu siihen. Johdon on ymmärrettävä lakien, asetusten ja viranomaismääräysten asettamat tietoturvavaatimukset. Johdon pitää tiedottaa henkilöstöä turvallisuusasioista. Henkilöstöllä pitää olla mahdollisuus osallistua turvallisuusasioiden valmisteluun.

Politiikkahierarkia

Politiikkahierarkia koostuu tietoturvaan liittyvistä politiikoista, standardeista, suosituksista ja yksityiskohtaisista ohjeista. Kuviossa 2 olevassa politiikkahierarkia mallissa (kuvio 2) alempana olevat tasot eivät ole vähemmän tärkeitä kuin ylemmät. (Vainikka 2008.)



Kuvio 2. Politiikkahierarkia. (Vainikka 2008.)

Ylimmän johdon julkilausuman tarkoituksena on korostaa organisaation toiminnassa tarvittavia tietoteknisiä osia, tukea organisaation tietoturvallisuutta ja antaa valtuudet alempien tasojen määrittämiseen ja johtamaan tietoturvallisuuteen liittyviä prosesseja. Toiminnalliset politiikat jaetaan kolmeen osaan: säätelevät politiikat, neuvoa antavat politiikat ja tiedottavat politiikat. Organisaation omat standardit määrittelevät valittujen tekniikoiden yhtenevän käyttötavan. Perusmääritykset sisältävät yleisen minimisuojatason. Suositukset antavat neuvoja mitä pitäisi missäkin tilanteessa tehdä, mutta eivät kuitenkaan ole pakollisia. Yksityiskohtaiset ohjeet kertovat, miten standardit ja politiikat toteutetaan. (Vainikka 2008.)

Tietoturvapolitiikka

Organisaatioiden on luotava tietoturvapolitiikka, joka luo perustan tietoturvaa koskeville ohjeistuksille ja koulutuksille. Tietoturvapolitiikkaan ei ole valmista mallia, jonka mukaan sen voi tehdä. Tietoturvapolitiikan tulee olla selkeästi kirjoitettu ja pitää käsitellä asioita yleisellä tasolla. Tietoturvapolitiikan pitäisi olla saatavilla oman organisaation henkilöstölle, yhteistyökumppaneille ja asiakkaille. Tietoturvapolitiikka sisältää yleensä seuraavia asioita:

- tietoturvan tavoitteet ja niihin liittyvät toimenpiteet
- tietoturvaan liittyvät roolit ja vastuut
- organisaation henkilöstön tietoturvakoulutus
- tietojenkäsittelyn suojaaminen
- organisaation tominnan jatkuvuus- ja toipumissuunnittelun yleiset linjat
- tietoturvapolitiikan laiminlyönnin seuraamukset.

Tietoturvapolitiikan ehdottomat vaatimukset ISO/IEC 27001:2005 –tietoturvastandardin mukaan ovat

- tietoturvapolitiikan luominen
- tietoturvapolitiikan hyväksyminen organisaation johdossa
- tietoturvapolitiikasta tiedottaminen koko henkilöstölle

- tietoturvapolitiikka on päivitettävä määräajoin, varsinkin merkittävien muutosten jälkeen. (ISO/IEC 27001:2005.)

Tietoturvariskien hallinta

Tietoturvariskien hallinta on tärkein osa tietoturvallisuutta. Tietoturvariskien hallinnan tarkoituksena on pienentää riskien mahdollisuutta. Tietoturvariskien hallinta tarvitsee ylimmän johdon täyden tuen. Jos ylin johto ei sitoudu, ei riskienhallinnalla ole käytännössä mahdollisuutta onnistua. Tietoturvariskien hallintapolitiikan tulisi olla osana organisaation riskinhallintapolitiikkaa. Tietoturvariskien hallinta vaatii organisaatiolta usein omaa osastoa, joka on perehtynyt asiaan. Riskinhallintaryhmillä ei yleensä ole tietotaitoa tietoturvan osalta. Tietoturvariskien hallinnan tärkein tehtävä on toiminnan ja suojattavien tietojen kohteisiin kohdistuvien tietoturvariskien alentaminen sille tasolle, että yritys pystyy turvallisesti kestämään ja jatkamaan toimintaansa normaalisti. Tietoturvariskien poistaminen täysin ei ole mahdollista vaan ainoastaan niiden pienentäminen hyväksyttävälle tasolle. Tietoturvariskien hallinta koostuu riskien arvioinnista ja niiden hallinnasta, joista muodostuu kokonaisuus, jolla käsitellä mahdollisia riskejä. Standardi ISO/IEC 27001:2005 sisältää käsittelymekanismiosan, joka on standardin pakollinen osa. Tietoturvariskien arviointi on yksi tärkeimmistä standardin osista. (Krutz & Vines 2003, 15.)

Tietoturvariskien hallinta jaetaan kahteen lähestymistapaan: proaktiivinen lähestymistapa ja reaktiivinen lähestymistapa. Proaktiivisessa lähestymistavassa tietoturvariskien hallinta tapahtuu ennakoivasti eli ennen kuin jotain tapahtuu. Proaktiivinen lähestymistapa on suositeltavampi ja kustannustehokkaampi. Reaktiivinen lähestymistapa perustuu siihen, että toimitaan kun jotain on jo tapahtunut. Reaktiivinen lähestymistapa ei ole suositeltava ja kustannukset voivat nousta huomattavasti korkeammalle kuin ennakoivassa lähestymistavassa.

Tietoturvariskien käsittelyssä voidaan käyttää kahta strategiaa: tietoturvariskien hyväksymistä tai tietoturvariskien pienentämistä hyväksyttävälle tasolle. Jos riski hyväksytään, niin sille ei muuta tehdä. Näin voidaan menetellä, jos tietoturvariskin haittavaikutus organisaation toimintaan on riittävän pieni.

Tietoturvariskien pienentäminen

Tietoturvariskien hallinta voidaan siirtää jonkin toisen organisaation vastuulle. Tietoturvariskejä voidaan pienentää ottamalla tarvittavat vakuutukset tai siirtämällä tieto- ja viestintätekniikat toisen organisaation vastuulle.

Tietoturvariskin pienentämisessä pitää tehdä ja ottaa käyttöön tarpeelliset suojatoimet. Suojatoimet eivät poista tietoturvariskiä vaan alentavat sitä. Suojatoimet voivat myös lisätä uuden tietoturvariskin.

Tietoturvariskin poistaminen tarkoittaa käytännössä tietoa sisältävien kohteiden poistamista käytöstä.

Tietoturvariskien arviointiprosessi

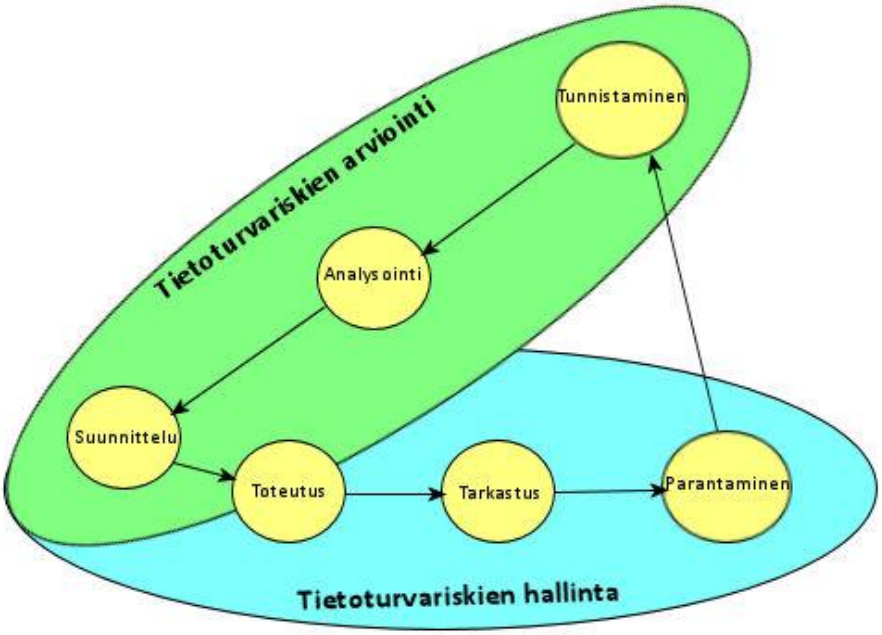
Arviointiprosessin tarkoituksena on tunnistaa tietoturvariskit ja niiden vaikutus organisaation toimintaan. Vaikutusta analysoidaan ja tietoturvariskin pienentämistä hyväksyttävälle tasolle voidaan suunnitella. Tietoturvariskien arviointiprosessi jaetaan kolmeen osaan:

- Tunnistamisvaiheessa tunnistetaan suojattavien kohteiden uhat.
- Analysointivaiheessa analysoidaan tunnistamisvaiheen tulokset ja selvitetään mahdolliset tietoturvariskit sekä luokitellaan ne vakavuuden mukaan.
- Suunnitteluvaiheessa suunnitellaan tarvittavat toimenpiteet tietoturvariskien pienentämiseksi. Tietoturvavaatimusten pitää olla tiedossa.

Tietoturvariskien analysointiin on kaksi lähestymistapaa: määrällinen eli kvantitatiivinen analyysi ja laadullinen eli kvalitatiivinen analyysi. Kvantitatiivisella analyysilla pyritään määrittämän kaikkien riskianalyysin elementtien rahallinen arvo. Riskianalyysin elementtejä ovat muun muassa suojatoimet, uhkien esiintymistiheys ja hyväksikäytön todennäköisyys. Arviointiprosessissa ei kuitenkaan käytetä pelkästään määrällistä analyysia vaan tarvitaan myös laadullinen analyysi, jossa luokitellaan uhkien vakavuus ja suojatoimien toimivuus niitä vastaan.

Tietoturvariskien hallintaprosessi

Tietoturvariskien hallintaprosessi on jatkuvan parantamisen prosessi. Yleisesti käytetty nimitys on PDCA-prosessi, joka saa nimensä vaiheista Plan, Do, Check ja Act (ISO/IEC 27001:2005). Hallintaprosessin päätarkoituksena on määritellä organisaation tietoturvariskien hyväksyttävä taso ja vaiheet, joilla tietoturvariskit voidaan pienentää hyväksytylle tasolle, sekä huolehtia siitä, että tietoturvariskit pysyvät hyväksytyllä tasolla. Hallintaprosessi suoritetaan aina arviointiprosessin jälkeen.



Kuva 1. Tietoturvariskien arviointi- ja hallintaprosessi.

Tietoturvallisuustietoisuus

Tietoturvallisuustietoisuus tarkoittaa yleistä tietoturvatietoisuutta ja suojatoimien ymmärtämisen tärkeyttä. Tietoturvallisuustietoisuus on tärkeä osa tietoturvaa. Tietoturvasta 80 % on ihmisen toimintaa, joten tietoturvallisuustietoisuutta ei pidä väheksyä. Riittävällä koulutuksella organisaation työntekijät saadaan ymmärtämään toimiensa vaikutukset ja organisaation tietojen suojaamisen tarve. Koulutukset vähentävät henkilökunnan suorittamaa luvatonta tietojen käyttöä, edistävät suojatoimien tehokkuutta ja auttavat välttämään tietojenkäsittelyresurssien tuhlausta tai väärinkäyttöä. Tietoturvallisuutta edistävän materiaalin pitää olla helposti saatavilla ja ajan tasalla.

Lait, asetukset ja viranomaismääräykset

Suomen lainsäädännössä ei ole tietoturvalakia vaan siihen liittyvät asiat ovat useiden lakien ja määräysten yhteydessä. Lait, asetukset ja viranomaismääräykset on pyritty kirjoittamaan siten, ettei tulevaisuudessa niitä tarvitsisi muuttaa vaikka teknologia kehittyy. Lakiasioiden sijoittaminen eri lakeihin vaikeuttaa ja aiheuttaa ylimääräistä työtä käytännön toteuttamisessa. Tietoturvaa sääntteleviä Suomen lakeja ja asetuksia ovat muun muassa:

- Rikoslaki (19.12.1889/39)
- Sopimaton menettely elinkeinotoiminnassa (22.12.1978/1061)
- Työsopimuslaki (26.1.2001/55)
- Yhteistoimintalaki (30.3.2007/334)
- Suomen perustuslaki (11.6.1999/731)
- Viranomaisten toiminnan julkisuus (21.5.1999/621)
- Henkilötietolaki (22.4.1999/523)
- Arkistolaki (23.9.1994/831)
- Sähköisen viestinnän tietosuojalaki (16.6.2004/516)
- Yksityisyyden suoja työelämässä (13.8.2004/759)

- Tekijänoikeuslaki (8.7.1961/404)
- Viestintämarkkinalaki (23.5.2003/393)
- Kuluttajasuojalaki (20.1.1978/38)
- Verkkotunnuslaki (13.3.2003/228)
- Sähköinen allekirjoitus (7.8.2009/617)

5 Fyysinen turvallisuus

Fyysinen turvallisuus koostuu ihmisten, prosessien, toimintatapojen ja teknisten laitteiden kokonaisuudesta. Fyysisen turvallisuuden suunnittelussa suositellaan käyttämään vyöhykemallia, jossa suojattavat kohteet sijaitsevat sisimmällä alueella. Suojatoimet voidaan valita vasta, kun organisaatio on selvittänyt mahdolliset haavoittuvuudet, uhat, uhka-agentit ja uhkien kohteet.

Osa-alueet ja uhkien luokittelu

Fyysinen turvallisuus sisältää seuraavat osa-alueet:

- rakennusten tilojen ja niihin sijoitettujen IT-laitteiden suojaaminen fyysisiltä uhilta
- suojautuminen ympäristöuhilta
- suojautuminen sähkö- ilmastointi- ja lämmitysjärjestelmien toimintahäiriöuhilta.

Uhat voidaan luokitella seuraavalla tavalla:

- Ympäristöperäiset uhat, joita ovat tulvat, vesivahingot, myrskyt, tulipalot, rakennuksen romahdus ja maanjäristykset.
- Tuki- ja jakelujärjestelmiin liittyvät uhat, esimerkiksi energiajakelun menetys ja viestintäliikenteen häiriöt.
- Ihmisen aiheuttamat uhat, kuten valtuudeton pääsy, sabotaasi, ilkivalta, organisaation oman henkilöstön tekemät virheet tai onnettomuudet, varkaudet ja lakot. (Vainikka 2008.)

Kulunvalvonta

Kulunvalvonnan tarkoituksena on estää luvaton kulku, mutta tarkoituksena on myös toteuttaa luvallinen henkilökulku mahdollisimman joustavasti. Kulkuavain, henkilökortti ja yksityiskohtaiset kirjalliset ohjeet annetaan vain allekirjoitusta vastaan. Kulkulupa ja avain saadaan kulusta tai tilasta vastaavalta organisaatiolla ja ne pitää tarkastaa määrävälein. (VAHTI 2002.)

Kulunvalvontajärjestelmien osatekijät voidaan jakaa seuraavasti: rekisteröinti, tunnistaminen, liikkeen ilmaisu, estäminen, saattaminen ja päästäminen. Videojärjestelmien avulla voidaan valvoa kulkua laitetiloihin ja niiden tapahtumia. Työnantajan on perusteltava työntekijöille, miksi videojärjestelmän käyttöönotto on tarpeen ja millaisia valvontamenetelmiä tullaan käyttämään. Vieraiden tulee ilmoittautua vastaanottopisteeseen, jossa heille annetaan esillä pidettävä vieraskortti. Vieras noudetaan ja saatetaan vastaanottopisteeseen vierailtavan organisaation toimesta. Vastaanottopisteellä pitää olla lista henkilöistä, jotka saavat mennä yksin laitetiloihin. IT-laitetilojen osalta pidetään kirjaa vierailijoista, ajankohdista sekä vierailun syystä. (VAHTI 2002.)

Laite- ja kytkentätilat

Osastoivien seinien ja välipohjien sisällä kulkevien kaapeleiden ja putkien läpivientien pitää olla samaa paloluokkaa kuin seinien ja välipohjien. Osastot erottavien ovien ja laitetilojen ovien palonkestoajan pitää olla sama. Kaikkien tilojen seinien, kattojen ja lattioiden pintakerrosten syttymisherkkyys ja palonleviämisluokka on oltava luokkaa 1. Miehittämättömän IT-laitetila pitää sijoittaa rakennuksen keskelle ikkunattomaan tilaan ja osastoida muista tiloista. Tiloissa pitää olla savuilmaisimet ja sammutusjärjestelmä. (VAHTI 2002.)

Sähkönsyöttö

Keskeytymättömän sähkönsaannin takaa UPS, joka suojaa laitteet sähköverkon aiheuttamilta häiriöiltä. UPS-laitteita suositellaan käyttämään kaikkien IT-laitetilojen katkeamattoman sähkönsyötön varmistamiseksi. UPS-laitteisto on mitoitettava siten, että se takaa virransyötön kunnes varavoima saadaan käyntiin ja kytkettyä.

Laitteistoa pitää koekäyttää ja huoltaa säännöllisesti. Varavoiman on riitettävä kaikille IT-laitetilassa oleville laitteille, kuten IT-laitteille, ilmastoinnille, jäähdytykseen ja valaistukseen.

IT-laitteiden sähkönsyötön on täytettävä jännitetason ja taajuuden vaatimukset. Jännitepiikkien ja taajuuden vaihteluiden on pysyttävä tietyissä rajoissa, etteivät laitteet vaurioidu. (VAHTI 2002.)

Laitteistoturvallisuus

Laitteistoturvallisuuden tavoitteena on ehkäistä omaisuuden häviäminen, vahingoittuminen, varastaminen tai luvaton muuttaminen sekä näiden vaikutukset. Laitteistoturvallisuus koostuu tietojenkäsittely- ja tietoliikennelaitteiden kokoonpanosta, ylläpidosta ja laadunvarmistukseen liittyvistä toimenpiteistä. Laitteistoturvallisuuden osa-alueet on selitetty taulukossa 1. (Teeriaho 2008.)

Taulukko 1. Laitteistoturvallisuuden osa-alueet (ISO/IEC 17799:2005).

Laitteiden sijoitus ja suojaus	Ympäristövaarojen ja luvattoman tunkeutumisen riskien pienentäminen
Peruspalvelut	Laitteistojen suojaaminen sähkökatkoilta ja muilta peruspalvelujen häiriöiltä
Kaapeloinnin turvallisuus	Sähkökaapelointi ja tietoliikennelinjojen suojaus vaurioilta ja salakuuntelulta
Laitteiden huolto	Asianmukainen huoltaminen käytettävyyden ja eheyden ylläpitämiseksi
Laitteiden turvallisuus toimitilojen ulkopuolella	Ulkopuolella olevien riskien huomiointi ja suojatoimien käyttöönotto
Laitteistojen turvallinen poistaminen ja kierrätys	Luottamukselliset tiedot ja lisensoidut ohjelmistot on poistettava ennen hävittämistä tai kierrätystä
Tietojen poisvienti toimitiloista	Laitteiden, ohjelmistojen ja tietojen poisvienti on erikseen luvitettava

6 Henkilöstöturvallisuus

Henkilöstöturvallisuus tarkoittaa toimenpiteitä, joilla suojataan yritystä oman henkilöstön aiheuttamilta uhkilta ja riskeiltä. Turvallisuustoimenpiteet voivat olla ennalta ehkäiseviä, valvovia tai jälkikäteen tapahtuvia. (Kouri 2005.)

Henkilöstöturvallisuuteen kuuluu:

- henkilöstön aiheuttamien tietoturvauhkien hallinta
- henkilöstöön kohdistuvien tietoturvauhkien hallinta
- tietojärjestelmien käyttömahdollisuuden varmistaminen
- organisaation tietojen ja laitteiden käyttöoikeuksien rajaaminen
- henkilöstön roolit ja vastuut
- varahenkilöiden nimeäminen
- tietojärjestelmä- ja tietoturvakoulutuksen järjestäminen
- henkilöstön taustaselvityksen teettäminen.

Henkilöstöturvallisuutta käsitellään henkilöstöhallinnan prosessin mukaan eli työntekijän palkkauksessa, työsuhteen aikana ja työsuhteen päättymisessä tehtävien toimenpiteiden mukaan.

Ennen työsuhteen alkua

Tavoitteena on varmistaa, että työntekijät, yhteistyökumppanit ja 3. osapuolien henkilöt ymmärtävät vastuunsa ja ovat sopivia heille harkittuihin tehtäviin, sekä vähentää varkauksia, petoksia ja toimintojen väärinkäytöstä aiheutuvia riskejä.

Työntekijöiden, yhteistyökumppanien ja 3. osapuolien roolit ja vastuut ovat määriteltävä ja dokumentoitava organisaation tietoturvapolitiikan mukaan.

Kaikkien osapuolten tausta on tarkistettava asiaan kuuluvia lakeja ja määräyksiä noudattaen. Tarkistusten on oltava suhteessa liiketoimintavaatimuksiin, tiedon luokitukseen ja mahdollisiin riskeihin.

Sopimusvelvoitteiden osana osapuolten henkilöiden on hyväksyttävä ja allekirjoitettava työsopimuksiensa ehdot, joista on käytävä ilmi osapuolten tietoturvavastuut. (ISO/IEC 17799:2005.)

Työsuhteen aikana

Tarkoituksen on varmistaa, että osapuolet ovat tietoisia tietoturva uhkista ja niiden merkityksestä, omista velvollisuuksista ja vastuistaan. Varmistaa, että heillä on keinot tukea organisaation tietoturvapolitiikkaa tehdessään tavanomaisia työtehtäviään sekä vähentää erehdyksestä johtuvia riskejä. (ISO/IEC 17799:2005.)

Johdon vastuulla on pitää huolta, että osapuolien henkilöstö noudattaa organisaation politiikkoja ja menettelytapoja. Osapuolille on annettava toimenkuvan mukainen koulutus organisaation politiikoista, menettelytavoista ja niiden muutoksista. Organisaation turvallisuusmääräysten rikkomisesta aiheutuvat rangaistukset on määriteltävä. (ISO/IEC 17799:2005.)

Työsuhteen päättyminen tai muuttaminen

Tarkoituksena on varmistaa, että osapuolien henkilöt poistuvat organisaation palveluksesta tai heidän työsuhdettaan muutetaan säännönmukaisesti.

Jos työsuhde päättyy tai muuttuu on se määriteltävä ja osoitettava selkeästi.

Osapuolien on palautettava kaikki organisaation suojattavia tietoja sisältävät kohteet työsuhteen, yhteistyö- tai muun sopimuksen päättyessä.

Osapuolien käyttöoikeudet on lakkautettava tai muokattava riippuen päättykö työsuhde vai muuttuuko sen luonne. (ISO/IEC 17799:2005.)

7 Tietoaineiston turvallisuus

Tietoaineiston turvallisuus tarkoittaa eri tallennusmuodoissa olevien organisaation tietojen suojaamista ja turvallista tuhoamista. Tietoaineiston turvallisuus käsittää:

- tietojen luokittelun
- tietojen turvallisen käsittelyn
- tietojen turvallisen säilyttämisen
- tietojen varmistamisen ja tarvittaessa palautuksen
- varmistusmedioiden turvallisuuden
- turvallisen tietojen tuhoamisen.

Tietojen luokittelu

Tietojen luokittelu mahdollistaa käsittelyohjeiden tekemisen. Luokittelun tarkoituksena on erotella kriittiset tiedot muista tiedoista. Luokittelun avulla käyttäjät pystyvät tunnistamaan organisaation kannalta kriittisen tiedon. Tiedot jaetaan organisaatiosta riippuen yleisesti neljään luokkaan tiedon arkaluontoisuuden mukaan. Taulukossa 1 on selitettynä mitä mikäkin luokitus tarkoittaa. Taulukossa 2 on esimerkki luokitusten käytössä yrityksessä. (Kemppainen 2009.)

Taulukko 2. Luokitusten selitykset (Kemppainen 2009).

Erittäin salainen	Tieto on erittäin kriittistä yrityksen liiketoiminnan ja sen jatkuvuuden kannalta ja väärinkäytettynä aiheuttaa merkittäviä taloudellisia vahinkoja. Tietoja ei saa näyttää ulkopuolisille ja omalle henkilöstöllekin erittäin rajoitetusti.
Salainen	Salainen tieto on henkilölle henkilökohtaisesti annettu, hänen työtään koskeva tieto, jonka joutuminen vääriin käsiin aiheuttaisi vakavia ongelmia yrityksen liiketoiminnalle. Tietoa ei saa näyttää ulkopuolisille, omalle henkilöstöllekin sitä voi näyttää vain tarpeen vaatiessa.
Yhtiönsisäinen	Yhtiönsisäinen tieto on yrityksen henkilökunnan käyttöön annettu yrityksen liiketoimintaa koskeva tieto. Tietoja saa näyttää omalle henkilöstölle vapaasti ja ulkopuolisillekin organisaation eduksi.
Julkinen	Julkinen tieto on yrityksen valmistamaa tai saamaa tietoaineistoa, joka on julkista ja tarkoitettu olemaan ulkopuolisten saatavissa. Tietojen oikeellisuus on tärkeää ja sitä on pyrittävä käyttämään ainoastaan organisaation eduksi.

Taulukko 3. Esimerkki tietojen luokittelusta (Tietoturvaopas 2010).

	1. Julkinen	2. Sisäinen	3. Luottamuksellinen	4. Salainen
Käsittelypaikka	Ei rajoituksia	Käsittelyssä on huomioitava, että tieto ei ole sivullisten nähtävillä tai kuultavilla	Sivullisilta eristetty tila, johon ei näe eikä kuule tilan ulkopuolelta	Sivullisilta eristetty tila, johon ei näe eikä kuule tilan ulkopuolelta
Tallennus / arkistointi	Ei rajoituksia	Ei julkisesti saatavilla. Yrityksen tiloissa	Lukittu säilytyspaikka, pääsynvalvonta. Yrityksen tiloissa	Kassakaappi, sähköinen tallenne salattuna, Yrityksen tiloissa
Tulostus	Ei rajoituksia	Sallittu jaetulle tulostimelle valvottuna	Sallittu jaetulle tulostimelle valvottuna	Sallittu paikalliselle tulostimelle
Kopiointi	Ei rajoituksia	Tiedon käyttäjän määriteltävissä	Tiedon omistajan määriteltävissä	Tiedon omistajan määriteltävissä, kopiot kirjattava
Jakelu	Ei rajoituksia	Tiedon käyttäjän määriteltävissä	Tiedon omistajan määriteltävissä	Tiedon omistajan määriteltävissä
Matkustus	Ei rajoituksia	Ei rajoituksia	Valvottuna käsimatkatavarana	Suljettu kirje, valvottuna, sähköinen tallenne salattuna
Puhelin	Ei rajoituksia	Ei rajoituksia	Ei sallittu julkisilla paikoilla.	Ei sallittu
Sähköposti	Ei rajoituksia	Ei rajoituksia	Salattuna julkisessa verkossa	Salattuna yrityksen hyväksymällä menetelmällä
Paperimateriaalin tuhoaminen	Ei rajoituksia	Lukittu tarkoitukseen varattu keräysastia	Lukittu tarkoitukseen varattu keräysastia tai silppuri	Tuhoaminen silppurilla tiedon omistajan toimesta
Elektronisen-materiaalin tuhoaminen	Ei rajoituksia	Poistaminen / Lukittu tarkoitukseen varattu keräysastia tai silppuri	Poistaminen / Lukittu tarkoitukseen varattu keräysastia tai silppuri	Ylikirjoitus yrityksen hyväksymällä menetelmällä, mikäli teknisesti mahdollista / Tuhoaminen silppurilla tiedon omistajan toimesta

Etätyö

Tietojen turvallisuudesta on huolehdittava myös organisaation ulkopuolella esimerkiksi matkustaessa ja etätöissä. Kannettavien ja matkapuhelimien käytössä pitää noudattaa erityistä varovaisuutta, ettei liiketoiminnallisia tietoja vaaranneta. Matkustaessa pitää ottaa huomioon, mitä kanssamatkustajien on mahdollista nähdä tai kuulla. Tietojen luokittelussa on huomioitava matkustus ja etäkäyttö, millaisia rajoituksia asetetaan tiedonkäsittelyyn. Etäkäytöstä pitää olla organisaation turvallisuusohjeet ja niitä pitää noudattaa. (ISO/IEC 17799:2005.)

Tietoaineiston varmistus

Tietoaineiston varmistaminen takaa tiedon saatavuuden, joten varmistukset on tehtävä säännöllisesti. Varmistukset on suunniteltava huolellisesti. Varmistusten suunnittelussa on otettava seuraavat asiat huomioon:

- varmistusten rytmi
- ohjeet varmistusten tekemiseen
- varmistusten valvonta
- varmistusten arkistointi
- varmistettujen aineistojen pääsyoikeudet
- varmistusmedioiden turvallinen siirtäminen
- varmistusten palauttamisen testaus.

8 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus on tietoturvan osa-alue johon kuuluu käyttöjärjestelmien ja muihin ohjelmistoihin kohdistuvat toimet, kuten

- tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt
- tarkkailu-, ja paljastustoimet
- lokimenettelyt ja laadunvarmistus
- ylläpito ja päivitys
- dokumentaation ylläpito
- virustorjunnasta huolehtiminen. (VAHTI 2003.)

Ohjelmistojen laadun varmistus

Laadun varmistus tapahtuu asianmukaisia menetelmiä käyttäen, niiden suunnittelussa, toteutuksessa, testauksessa, versionhallinnassa ja katselmuksissa. Ohjelmistot pitää hankkia luotettavalta ohjelmistotoimittajalta. Ohjelmistojen yhteensopivuus pitää ottaa huomioon ennen hankintaa.

Haittaohjelmat

Haittaohjelmat ovat itsenäisiä ilkeämielisiä ohjelmia tai sen osia, joiden tarkoitus on aiheuttaa vahinkoa, vakoilla, mainostaa tai varastaa tietoa. Tunnetuimpia haittaohjelmia ovat virukset, madot ja vakoiluohjelmat. Yleensä haittaohjelmat koostuvat kahdesta osasta: leviämiskoodista ja toimintakoodista. Leviämiskoodin tarkoitus on varmistaa, että ohjelma siirtyy tietokoneesta toiseen. Toimintakoodin tarkoitus on tehdä toimenpiteet, johon se on suunniteltu. Haittaohjelmien nimeämiseen ei ole mitään yhtenäistä tapaa, vaan kaikki torjuntaohjelmistovalmistajat nimeävät haittaohjelmat omalla tavallaan. Tietojärjestelmien käyttäjäoikeuksien rajoittaminen usein estää tai rajoittaa haittaohjelmien toiminnan. (Jäppinen 2002.)

Virukset

Virus on ohjelmakoodi, joka tarttuu toiseen ohjelmaan ja muokkaa niiden toimintaa. Virus lisää omaa koodiaan luotettuun ohjelmaan. Virus tarvitsee isäntäohjelman levitäkseen. Virus pitää aktivoida ajamalla sen koodi, muuten se ei tee mitään. Virukset voidaan jakaa hetkellisiin viruksiin ja asuviin viruksiin. Hetkellinen virus toimii vain ohjelman ajon ajan ja asuva virus siirtää itsensä tietokoneen muistiin ja toimii sieltä käsin. (Jäppinen 2002.)

Ohjelmistovirukset voidaan jakaa seuraavasti

- Liitetyt virukset. Liittävät itsensä isäntäohjelmaan. Ne kopioivat oman koodinsa isäntäohjelman koodin alkuun. Ohjelman käynnistyksessä käynnistyy virus ennen isäntäohjelma.
- Ympäröivät virukset. Toimivat ennen ohjelman alkua ja uudestaan ohjelman lopussa. Voivat piilottaa jälkensä.
- Sopeutuneet virukset. Mukautuvat osaksi isäntäohjelmaa. Isäntäohjelman rakenteen pitää olla tuttu.
- Vaihdokkivirukset. Siirtävät itsensä jonkin toisen ohjelman tilalle.

Muut virukset:

- Boot-sektorivirukset. Asettuvat tietokoneen boot-sektorille ja aktivoituvat tietokoneen käynnistyessä.
- Muistissa oleilevat virukset. Jäävät muistiin ohjelman suorituksen jälkeen. Leviävät suoritettaviin ohjelmiin.
- Kirjastovirukset. Sijaitsevat jaetuissa ohjelmakirjastoissa, joita monet ohjelmat käyttävät.
- Makrovirukset. Asettuvat ajettaviin makroihin. (Jäppinen 2002.)

Madot

Madot ovat itsenäisiä ohjelmia, jotka kopioivat itseään verkon yli tietokoneesta toiseen ja pyrkivät leviämään mahdollisimman tehokkaasti. Madot eivät tarvitse

isäntäohjelmaa. Madot hyödyntävät ohjelmistojen tunnettuja heikkouksia. Madot kuljettavat usein mukanaan viruksia tai toimivat kuin virukset. Nykyisin sähköpostimadot ovat yleisimpiä matoja. Madon aktivoituessa se yleensä etsii tietokoneelta sähköpostiosoitteita, joihin lähettävät itsensä ja mahdollisesti joitain tiedostoja tietokoneelta. Madot hyödyntävät ihmisten heikkouksia ja leviävät sähköpostin liitetiedostoina. Madot sisältävät usein oman SMTP-koodin. (Jäppinen 2002.)

Troijalaiset

Troijalaiset tekevät normaalin toimintansa lisäksi piilossa jotain muuta. Troijalainen voidaan naamioida esimerkiksi peliksi tai muuksi hyötyohjelmaksi. Troijalainen voi sisältää mitä tahansa toimintoja. Troijalainen voi esimerkiksi kalastaa käyttäjätunnuksia ja salasanoja tai tuhota tietoja kovalevyltä. (Jäppinen 2002.)

9 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan siirrettävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamista siirron aikana. Tietoturvallisuuden päämääränä on varmistaa tietoliikennelaitteiden fyysinen turvallisuus sekä tiedon alkuperä, koskemattomuus ja luottamuksellisuus. (Paavilainen 2003; Rosendahl 2003.)

Taulukko 4. Tietoliikenneturvallisuuden osa-alueet (Paavilainen 2003).

Järjestelmän hallinta	Tietojärjestelmät, hyväksikäyttö	
	Sovellustason protokollat	OSI 7
		OSI 6
Verkonhallinta	Yhteystason protokollat, yhteyksien hallinta	OSI 5
		OSI 4
	Verkkotason protokollat, reititys	OSI 3
		OSI 2
Siirtoteiden hallinta	Fyysiset yhteydet, kaapelit, laitteet	OSI 1

Uhat

Yleisiä tietoliikenneverkkojen uhkia ovat salakuuntelu, esiintyminen toisena henkilönä, viestien toisto, tiedon muuntaminen, väärinreititys, ilkeämieliset ohjelmat ja verkon palvelujen estäminen. Uhkien kohteita ovat organisaation sisäinen verkko, organisaation Internetiin liitetyt palvelimet ja tietoliikenneverkossa tapahtuva liikenne.

Tunkeutujat

Tunkeutujat jaetaan yleensä seuraaviin ryhmiin

- Script-kiddies – hyödyntävät muiden tekemiä ohjelmia
- White-hat hackers – asiantuntijoita, jotka etsivät tietoturva-aukkoja
- Black-hat hackers – pahantekijöitä
- Insiders – organisaation omia työntekijöitä
- Cyber criminals – järjestäytyneen rikollisuuden edustajia.

Tunkeutumismenetelmät

- Sosiaaliset menetelmät – maanittelu, houkuttelu, uhkailu, jne
- Olan yli vilkuilu – esimerkiksi salasanan tai muun arkaluontoisen tiedon vilkuilu
- Tekniset menetelmät, joita ovat muun muassa haittaohjelmien käyttäminen, tietoliikenteen hakkerointi (verkon salakuuntelu tai reititystaulujen väärentäminen) ja tietokoneeseen tunkeutuminen (luvaton käyttö verkon yli tai paikallisesti).

PING-pyyhkäisy

PING-pyyhkäisyssä käydään läpi suuri määrä IP-osoitteita lähettämällä niihin ICMP ECHO –paketteja. Jos IP-osoite vastaa, niin kohdekoneen portit skannataan avoimien porttien löytämiseksi.

Porttiskannaus

TCP-yhteydessä yksinkertaisinta on yrittää avata jokaiseen porttiin erillinen yhteys. Jos avaaminen onnistuu, niin portti on avoin. Kohde havaitsee skannauksen helposti ja merkitsee jokaisen yhteyden lokeihin.

SYN-skannauksessa lähetetään SYN-paketti jokaiseen kohteen porttiin. Jos portti on avoin, niin kohde vastaa SYN/ACK –paketilla, jonka jälkeen tunkeutuja peruuttaa yhteyden muodostuksen RST/ACK –paketilla. Jos kohteen portti on suljettu, se vastaa

RST/ACK- tai ICMP Destination Unreachable –paketilla. RFC793 eli TCP-protokollan määritelmä mahdollistaa porttiskannauksen, koska määritelmän mukaan järjestelmän pitää vastata SYN-pakettiin RST-paketilla.

Internet

Internetissä tapahtuva kommunikointi perustuu TCP/IP –pinon protokolliin. Pakettikytkentäisessä verkossa data hajotetaan ensin paketeiksi, jonka jälkeen paketit lähetetään tietoverkkoon reitittimeltä toiselle ja lopulta päätyvät kohteeseen, joka kasaa paketit yhteen. Datapakettien sisältö on luettavissa reitin varrella, jos salausta ei ole käytetty. Mahdollisia Internetin uhkia ovat salasanojen haistelu, pakettien väärentäminen ja reitityshyökkäys. Datapaketin lähetyksessä kohteen nimeä vastaava TCP/IP –osoite kysytään DNS-palvelimelta, johon murtautumalla pystytään ohjaamaan paketit väärään osoitteeseen.

Palvelunestohyökkäys

Palvelunestohyökkäys perustuu suureen määrään viestejä, jotka lähetetään kuormittamaan palvelinta tai tietoliikenneverkkoa, jolloin sen toiminta estyy. Esimerkiksi sähköpostihyökkäyksessä lähetetään niin paljon sähköpostia, että palvelin täyttyy tai kaatuu. Hajautetussa palvelunestohyökkäyksessä käytetään monia kaapattuja botti-verkon koneita, jotka lähettävät samaan osoitteeseen viestejä.

Smurf –hyökkäys

Smurf –hyökkäyksessä lähetetään PING-paketti (ICMP ECHO –paketti) johonkin internetiin liitettyyn tietoliikenneverkkoon levitysviestinä. Jokainen viestin vastaanottanut tietokone vastaa PINGiin (ECHO REPLY –paketti), jolloin tietoliikenneyhteys kuormittuu voimakkaasti. Kaikkiin paketteihin on väärennetty lähettäjän osoitteeksi kohteen IP-osoite. Smurf-hyökkäys pystytään estämään siten, että estetään ulkopuolelta tulevat verkon levitysosoitteeseen menevät paketit.

SYN-tulva

SYN-tulva hyökkäyksessä käytetään TCP-protokollan yhteyden avaamispyyntö paketteja (SYN-paketti), joita lähetetään kohteelle väärennetyllä lähdeosoitteella. Kohde varaa omia resurssejaan yhteydelle ja lähettää SYN/ACK-paketin yhteyden avaamispyynnön lähettäjälle ja jää odottamaan vastausta. SYN-tulvaa pystytään

torjumaan pienentämällä vastauksen odotusaikaa ja IDS-järjestelmällä (Intrusion Detection System).

Land-hyökkäys

Lähetetään SYN-paketti kohteen avoimeen porttiin, jonka lähdeosoitteeksi on väärennetty kohteen IP-osoite ja lähdeportti on väärennetty samaksi kuin kohdeportti. Käyttöjärjestelmästä riippuen tämä hyökkäys voi estää kaikki kohdeporttiin tulevat yhteydenottoyritykset kunnes kone lopettaa väärennetyn yhteydenottoyrityksen käsittelyn. Land-hyökkäys hidastaa kohde konetta ja voi saada aikaan sen kaatumisen. Land-hyökkäykset ovat estettävissä palomuurilla.

Suojatut tietoliikenneyhteydet

TLS (Transport Layer Security)

TLS perustuu SSL (Secure Socket Layer) tekniikkaan. TLS on yleinen internetissä käytettävä suojausprotokolla (https://...). TLS toimii TCP/IP:n päällä ja sovellusten alla. TLS käyttää omaa TCP porttia 443. TLS mahdollistaa joustavan symmetrisen salaus, tiiviste- ja autentikointimenetelmän valinnan.

IPSec (Internet Protocol Security)

IPSec sisältää joukon yleiskäyttöisiä protokollia, joilla suojataan TCP/IP –liikennettä. Suojaus tapahtuu koneiden välillä, eikä käyttäjien välillä. IPSec tukee VPN:ää ja kahta turvallisuusprotokollaa (AH ja ESP).

SSH (Secure Shell)

SSH on suomalaisen SSH Communications Security’n kehittämä ohjelmisto, jolla voidaan tunneloida tietoliikenneyhteyksiä. Toimii itsenäisenä ohjelmana työasemissa ja palvelimissa TCP-protokollan päällä käyttäen porttia 22. Yhteyden muodostus koostuu kolmesta erityyppisestä protokollasta: siirtoprotokollasta, käyttäjätunnistusprotokollasta ja yhteysprotokollasta. Siirrettävä data on salattu, eikä sitä voi analysoida matkan varrella.

VPN (Virtual Private Network)

VPN muodostaa suojatun yhteyden yleisen verkon sisällä. VPN luo oman virtuaalisisäverkon. VPN yhteydet voidaan jakaa kahteen osaan: Access VPN ja Intranet ja extranet VPN. Access VPN on suojattu yhteys organisaation ulkopuolelta organisaation tietoliikenne verkkoon. Intranet ja extranet VPN yhdistää tietoliikenneverkot yleisen verkon yli yhdeksi loogiseksi sisäverkoksi. VPN yhteyden muodostukseen käytetään monia eri salausprotokollia. VPN muodostetaan usein palomuurin läpi, joten vahva autentikointi on tärkeää.

10 Yhteenveto

Työn tavoitteena oli tehdä tietoturvaohjeistus käyttötuen henkilöille. Tämä toteutui ja sitä käytetään uusien ja vanhojen työntekijöiden kouluttamisessa. Tietoturvaohjeistus käyttötuelle ei ole täydellinen tietoturvaohjeistus, vaan tukee yrityksen yleistä tietoturvakoulutusta. Tietoturvaohjeistusta ylläpidetään koulutusta pitävien henkilöiden toimesta.

Teoriaosaa kirjoittaessa tietoturva ja varsinkin sen tärkeys yrityksen toiminnassa tuli tutuksi. Tietoturva perustuu lähinnä ihmisen toimintaan, eikä niinkään tekniikkaan. Täydellistä tietoturvaa ei ole olemassakaan, vaan uhat pienennetään halutulle tasolle tai hyväksytään sellaisenaan. Tietoturvasta vastaa viime kädessä yrityksen johto, joten heidänkin on tutustuttava aiheeseen, vaikkei heillä olisi IT-alan koulutusta.

Tietoturvaohjeistusta tehdessä hyödynsin oppimaani teoriatietoa, Fujitsun materiaaleja ja työkokemustani käyttötuessa. Tietoturvaohjeistus itsessään on ironisesti salattu tietoturvasyistä.

LÄHTEET

Fujitsu Finland Oy. Viitattu 22.1.2010.
http://www.fujitsu.com/fi/.

ISO/IEC 17799:2005. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje.

ISO/IEC 27001:2005. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje.

Jäppinen, P. 2002. Ohjelmistoturvallisuus. Viitattu 30.9.2010.
http://www2.it.lut.fi/kurssit/02-03/010627000/ohjelmisto.pdf.

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo Finland Oy.

Karvi, T. 2010. Tietoturvan perusteet. Helsingin yliopisto tietojenkäsittelytieteenlaitos. Viitattu 16.9.2010.
http://www.cs.helsinki.fi/u/karvi/turva-perusteet-luvut-1-3.pdf.

Kemppainen, S. 2009. Tietoturvallisuuden sertifiointi ISO/IEC 27001 –tietoturvallisuus-standardilla. Lahden Ammattikorkeakoulu Yrityshallinto. Viitattu 17.9.2010.
https://publications.theseus.fi/bitstream/handle/10024/2932/Kemppainen_Simo.pdf?sequence=1.

Kerttula, E. 2000. Tietoverkkojen Tietoturva. Helsinki: Edita.

Kouri, I. 2005. Henkilöstöturvallisuus ja fyysinen turvallisuus. Teknillinen korkeakoulu. Viitattu 16.9.2010.
http://www.tml.tkk.fi/Opinnot/T-110.460/2005/htt_2005_0210_IK_kasitteet_ja_hallintakeinot.pdf.

Krutz, R & Vines, R. 2003. Tietoturvasertifikaatti, The CISSP Prep Guide – Mastering the Ten Domains of Computer Security. Suom. Erkki Suominen. IT Press.

Paavilainen, J. 2003. Tietoliikenneturvallisuus. Viitattu 8.10.2010.
http://www.cs.uta.fi/titu/luennot/6_luento_tietoliikenneturvallisuus.pdf

Rosendahl, M. 2003. Tietoturva palvelee kaikkia. Viitattu 8.10.2010. http://www.helsinki.fi/atk/lehdet/103/Tietoturva%20palvelee%20kaikkia.html.

Stallings, W. 2008. Computer Security. Pearson education.

Teeriaho, J. 2008. Tietoturva. Viitattu 7.10.2010. http://ta.ramk.fi/~jouko.teeriaho/Tietoturva4a.pdf.

Tietoturvaopas, 2010. Viitattu 17.9.2010. http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/index.html.

VAHTI 2002. VAHTI 1/2002. Tietoteknisten laitetilojen turvallisuussuositus. Viitattu 30.9.2010. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20020101Tietot/name.jsp

VAHTI 2003. VAHTI 4/2003. Valtionhallinnon tietoturvakäsitteistö. Viitattu 30.9.2010. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp