hyväksymispäivä arvosana

arvostelija

Tietoturvapolitiikat

Riitta Mäkinen

Helsinki 20.4.2003

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Tietoturva nykyaikaisessa liiketoimintaympäristössä -seminaari

Sisältö

1 Johdanto…… 1

2 Tietoturvallisuus…… 1

3 Tietoturvapolitiikat……2
3.1 Yrityksen tietoturvapolitiikka…….. 3
3.2 Alemman tason politiikat…… 4
3.3 Toimintaohjeet……..4
3.4 Esimerkki politiikkarakenteesta…… 5

4 Tietoturvapolitiikkojen laatiminen…….. 5
4.1 Vaatimukset tietoturvapolitiikoille……5
4.2 Tietoturvapolitiikkojen ristiriitaisuudet ja niiden ratkaiseminen 6
4.3 Tietoturvapolitiikkojen kerroksellisuus…… 8

5 Tietoturvapolitiikkojen käyttöönotto……9
5.1 Turvakulttuuri……9
5.2 Markkinointi…….. 10
5.3 Koulutus…… 10
5.4 Tarkkailu ja valvonta……11

6 Elinkaarimalli…….. 11

7 Yrityksen peruspolitiikat…….. 13
7.1 Tietotekniikan käyttöpolitiikka…… 13
7.2 Ylläpitäjien käyttöpolitiikat ja järjestelmien ylläpitopolitiikat….. 14
7.3 Tiedon turvaamisen politiikka…… 14
7.4 Palomuuripolitiikka…… 14

8 Yhteenveto…… 15

Lähteet…… 16

1 Johdanto

Yritysturvallisuuden tavoitteena on taata yrityksen toiminnan häiriötön jatkuminen sekä normaalioloissa että poikkeustilanteissa. Yritykset ovat entistä riippuvaisempia tietotekniikasta ja samalla yritysten tietojärjestelmät ja tietoliikenneverkot joutuvat yhä lisääntyvässä määrin alttiiksi tietoturvallisuutta vaarantaville tekijöille. Tämän seurauksena yritysten tietotekninen haavoittuvuus on lisääntynyt ja tietoturvallisuudesta on tullut olennainen osa yritysturvallisuutta.

Tieto on yrityksen omaisuutta ja tietoa on suojattava samoin menetelmin kuin yrityksen muutakin omaisuutta. BS7799 –tietoturvastandardin [SFS98] mukaan tiedon suojattavat ominaisuudet ovat

- luottamuksellisuus: tietoa pääsevät käsittelemään vain ne, joilla on siihen käyttöoikeus
- eheys: tieto ja sen käsittelytavat ovat täydellisiä ja virheettömiä
- käytettävyys (saatavuus): tieto ja sen käsittelytavat ovat aina tarvittaessa valtuutettujen käyttäjien saatavilla

Tietoturvallisuuden ytimen muodostavat tietoturvapolitiikat, joiden avulla määritellään yritystoiminnan vaatiman tietoturvallisuuden kohteet ja periaatteet sekä jaetaan vastuut ja velvollisuudet. Tietoturvapolitiikkojen avulla on pystyttävä toteuttamaan, johtamaan ja ylläpitämään yrityksen koko tietoturvallisuus. Koska tietoturvapolitiikat koskettavat tavalla tai toisella yrityksen koko henkilöstöä, ne ovat sidoksissa yrityskulttuuriin ja yrityksen henkilöstön tietoturvatietämyksen tasoon.

2 Tietoturvallisuus

Valtioneuvoston periaatepäätöksessä [Val99] tietoturvallisuus on määritelty seuraavasti:

> Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen *luottamuksellisuutta, eheyttä ja käytettävyyttä* turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta tai vahingoilta.

Samassa periaatepäätöksessä [Val99] tietoturvallisuus on suunnittelun, toteutuksen ja valvonnan helpottamiseksi jaoteltu osa-alueisiin seuraavasti: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus,

tietoliikenneturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus sekä käyttöturvallisuus.

Tietoturvaan liittyy oleellisena osana yrityksen liiketoiminnan riskianalyysi. Määrittelemällä ydinprosessit saadaan selville, mitä halutaan suojata. Lisäksi on määriteltävä uhat eli miltä halutaan suojautua sekä uhkien todennäköisyys. Jokaista suojattavaa kohdetta arvioidaan sen perusteella, mitä uhkia aiheutuu tiedon luotettavuudelle, eheydelle ja saatavuudelle. Tämän jälkeen riskianalyysin avulla voidaan tehdä päätökset riskien pienentämiseksi, siirtämiseksi tai hyväksymiseksi.

Tiedon suojaamiseen liittyvien toimenpiteiden on kohdistuttava paitsi itse tietoon myös tekniikkaan, jonka avulla tietoa luodaan ja käytetään [Har03]. Suojattavia kohteita ovat laitteistot, ohjelmistot, data, henkilöt, dokumentaatio ja tarvikkeet [Rfc97]. Klassisia uhkia ovat valtuutukseton tiedon ja/tai tietojenkäsittelyresurssin käyttö, vahingossa tai ilman valtuutusta tapahtunut tiedon paljastaminen tai palvelunesto. Tämän lisäksi voi olla erilaisia yrityskohtaisia uhkia, jotka on tunnistettava [Rfc97].

Tiedon suojaaminen edellyttää myös optimointia ja ristiriitojen ratkomista. Turvamenetelmien ylläpito vaatii työtä ja aiheuttaa kustannuksia, joten turvallisuuskin on tasapainoilua tarpeiden ja kustannusten välillä. Optimoinnissa on oleellista pyrkiä etukäteen määrittelemään tietoturvarikkomuksesta mahdollisesti aiheutuvien menetysten hinta. Turvattavan kohteen turvamenetelmien ylläpitäminen ei saa olla kalliimpaa kuin turvarikkomuksesta syntyvät kustannukset [Vir02].

Helppokäyttöisyyskin on usein ristiriidassa turvallisuuden kanssa. Tietojärjestelmän käyttö on helpointa silloin, kun käyttäjiltä ei vaadita salasanaa. Samalla se on myös turvattominta. Tietojärjestelmän toimittaja pyrkii toimittamaan järjestelmän mahdollisimman avoimena, koska silloin se varmasti toimii erilaisissa ympäristöissä. Asiakkaan tehtäväksi jää tietoturvaaukkojen paikkaaminen.

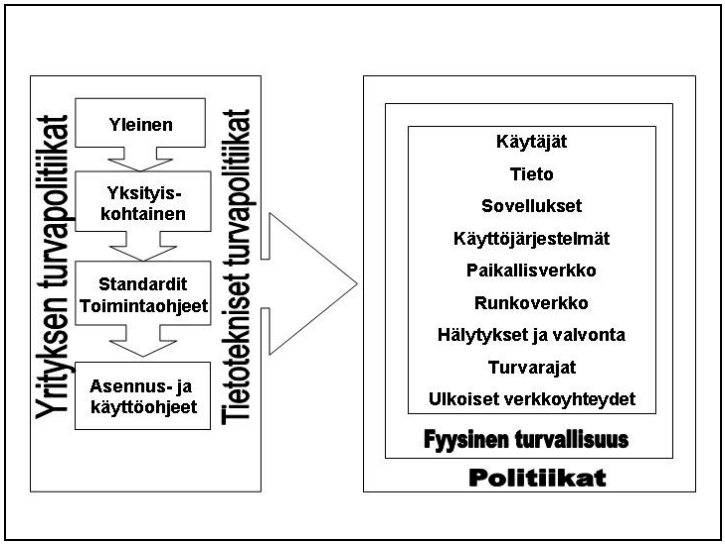
Turvallisuuteen liittyvät myös ristiriidat työntekijöiden ja yrityksen välillä. Yrityksen eri osastoilla saattaa olla keskenään erilaiset tarpeet tiedon turvaamiseksi tai työntekijällä on erilaiset tiedon turvaamistarpeet kuin työnantajalla [Vir02].

3 Tietoturvapolitiikat

Tietoturvallisuus toteutetaan tietoturvapolitiikoilla, jotka kohdistetaan tietoturvan eri osa-alueisiin. Tietoturvapolitiikan avulla yrityksen johto ohjaa ja tukee tietoturvan toteutumista. Tietoturvapolitiikkojen avulla henkilöstölle

kerrotaan tiedon suojaamisvaatimukset ja määritellään käytännöt, joiden avulla nämä vaatimukset täytetään [Rfc97].

Politiikat muodostavat hierarkkisen rakenteen (kuva 1), jossa ylimpänä on yrityksen johdon hyväksymä yrityksen tietoturvapolitiikka. Siitä johdetaan alemman tason politiikat, joiden perusteella muodostetaan käytännön toimintaohjeet ja järjestelmien turvamääritykset [Far01]. Näin turvatoimet ulotetaan kattamaan koko organisaatio.



Kuva 1. Turvapolitiikkahierarkia [Far01, Har03]

Politiikkarakenteen ylimmät tasot ovat hallinnollisia politiikkoja, jotka alaspäin mentäessä konkretisoituvat teknisiksi politiikoiksi, toimintaohjeiksi ja yksityiskohtaisiksi asennusmäärityksiksi. Jokainen käyttäjän tietoturvaohje ja jokainen tekninen määritys tulee olla johdettavissa tietoturvapolitiikoista.

Tietoturvastandardi BS7799 [SFS98] on laadittu organisaatioiden tietoturvallisuuden varmistamistoimenpiteiden suunnittelua, toteutusta ja ylläpitoa varten. Standardien perusteella voidaan määritellä useita satoja yksittäisiä tietoturvapolitiikkoja, joiden avulla organisaatiot voivat taata turvallisen tietojenkäsittelyn kaikilla tietoturvallisuuden osa-alueilla.

3.1 Yrityksen tietoturvapolitiikka

Yrityksen johdon hyväksymä tietoturvapolitiikka on johdon kannanotto yrityksen tietoturvallisuudesta. Siinä yritysjohto ilmaisee näkemyksensä siitä, mitä tavoitteita yrityksen tietoturvalle tulee asettaa. Tietoturvapolitiikassa todetaan tietoturvan kohteet ja periaatteet sekä määritellään vastuut. Yrityksen tietoturvapolitiikassa on myös otettava huomioon lakien ja sopimus-

ten toiminnalle asettamat vaatimukset. Tietoturvapolitiikkaa on myös säännöllisesti tarkastettava ja arvioitava [SFS98].

Tietoturvastandardissa BS7799 [SFS98] todetaan:

> Tietoturvapolitiikan määrittelyasiakirjan tulee olla johdon hyväksymä, se tulee julkaista ja siitä tulee tiedottaa tarkoituksenmukaisesti kaikille työntekijöille. Siitä tulee ilmetä johdon sitoutuminen turvallisuuteen ja organisaation näkemys tietoturvallisuuden hallinnasta. Standardin mukaan asiakirjan tulee sisältää ainakin seuraavia asioita
>
> - tietoturvallisuuden, sen yleistavoitteiden, soveltamisalan ja merkityksen määrittely keinona tietojen yhteiseen käyttöön
>
> - tietoturvallisuuden tavoitteita ja periaatteita tukeva yritysjohdon kannanotto
>
> - organisaation kannalta erityisen tärkeiden tietoturvallisuuden menettelytapojen, periaatteiden, standardien ja vaatimusten noudattamista koskeva tiivis selvitys.

Yrityksen tietoturvapolitiikka määrittelee tietoturvallisuuden perusvaatimukset ja antaa siten lähtökohdat tietoturvan suunnittelemiseksi ja toteuttamiseksi.

3.2 Alemman tason politiikat

Alemman tason tietoturvapolitiikat ovat eri osa-alueille kohdistettuja yksityiskohtaisia politiikkoja, joilla ohjataan tietoturvan toteutusta. Nämä politiikat ovat yrityksen tietoturvan ydin. Politiikat voidaan jakaa kahteen luokkaan: teknisiin ja hallinnollisiin [Sip00]. Teknisissä turvapolitiikoissa keskitytään tietokoneturvallisuuteen ja tiedon suojaamiseen teknisin keinoin. Hallinnollisilla politiikoilla puolestaan ohjataan ja säädellään käyttäjien toimia siten, että tietojen käsittely on turvallista.

3.3 Toimintaohjeet

Toimintaohjeet ovat politiikoista johdettuja yksityiskohtaisia soveltamisohjeita. Niissä kerrotaan, miten politiikoissa suojattaviksi määritellyt kohteet turvataan. Toimintaohjeissa kuvataan vaihe vaiheelta, miten tietyssä toiminnossa säilytetään haluttu tietoturvan taso. Toimintaohjeiden lisäksi tarvitaan vielä asennusohjeita, käyttäjäohjeita ja muita yksityiskohtaisia ohjeita.

3.4 Esimerkki politiikkarakenteesta

Tietoturvapolitiikassa määritellään, että tietoon ja liiketoimintaprosesseihin pääsyä tulee valvoa turvallisuus- ja liiketoimintavaatimusten mukaisesti. Tästä seuraa, että käyttäjät tulee tunnistaa. Tavallisimmin tunnistus tapahtuu käyttäjätunnuksen ja salasanan perusteella.

Seuraavalla tasolla on salasanapolitiikka, jossa määritellään, että käyttäjän tulee noudattaa hyvää turvallisuutta salasanan valinnassa ja käytössä. Tästä seuraa toimintaohje, jossa käyttäjiä neuvotaan, miten salasanoja tulee käyttää ja minkälaiset salasanat ovat hyviä. sekä kehotetaan käyttäjiä toimimaan ohjeen mukaisesti. Tämän lisäksi useissa järjestelmissä on mahdollista teknisesti pakottaa käyttäjät noudattamaan sovittua käytäntöä esimerkiksi salasanojen mutkikkuudesta, pituudesta ja vaihtoväleistä.

4 Tietoturvapolitiikkojen laatiminen

Guel [Gue01] toteaa, että kaikkia politiikkoja ei kenties kirjoiteta, koska luotetaan siihen, että käyttäjät toimivat oikein. Käyttäjät eivät kuitenkaan aina toimi oikein, joten politiikkoja tarvitaan. Vaikka kaikki lähtökohtaisesti toimivat oikein ja rehellisesti, aina sattuu erehdyksiä ja virheitä. Guelin [Gue01] mukaan on epärealistista uskoa, että kaikkiin resursseihin voisi aina luottaa. Esimerkkinä hän mainitsee varsin tavalliset laite- ja ohjelmistovirheet. Turvapolitiikkojen tehtävänä on estää sekä virheistä johtuvat haittavaikutukset että tahalliset väärinkäytökset.

4.1 Vaatimukset tietoturvapolitiikoille

Tietoturvapolitiikkojen on katettava yrityksen koko tietoturvallisuuden alue, eli niiden on oltava riittäviä. Politiikkojen avulla on huolehdittava siitä, että tietojen luottamuksellisuus, eheys ja saatavuus on turvattu kaikilla tietoturvallisuuden osa-alueilla sekä normaali- että poikkeusoloissa.

Turvapolitiikoissa on määriteltävä selkeästi vastuunjako käyttäjien, ylläpitäjien ja johdon kesken [Rfc97].

Tietoturvapolitiikkojen laatimisessa tärkeää on löytää tasapaino turvallisuuden ja liiketoiminnan tarpeiden välillä. Tarpeettomia rajoituksia ei tule esittää, tietoturvapolitiikkojen on oltava tarpeellisia ja ymmärrettäviä. Silloin käyttäjät hyväksyvät ne ja noudattavat niitä. Perusteettoman tiukoilla politiikoilla saatetaan joutua tilanteeseen, jossa turvallisuus tuntuu haittaavan yrityksen toimintaa. Silloin säännöistä joko ei välitetä tai keksitään keinot niiden kiertämiseksi.

Tietoturvapolitiikkojen on oltava ajantasaisia, sillä muuten ne menettävät uskottavuutensa. Niitä on myös jatkuvasti arvioitava. On varmistettava, että tietoturvapolitiikat ja niistä johdetut turva-asetukset eivät ole niin heikot, että ne avaavat verkon valtuutuksettomalle käytölle, mutta eivät myöskään niin vahvat, että ne estävät tietojärjestelmien asianmukaisen käytön.

Tietoturvapolitiikkojen pitää olla ristiriidattomia eivätkä ne saa olla päällekkäisiä. Päällekkäisyys vaikeuttaa ylläpitoa ja heikentää politiikkojen käytettävyyttä. Ristiriidattomuus vaikuttaa itsestään selvältä vaatimukselta, mutta sen toteuttaminen on vaikeaa. Tietoturvaan sisältyy ristiriitoja riippuen siitä, kenen näkökulmasta asiaa tarkastellaan. Koska politiikat ohjaavat tietoturvan toteuttamista, ristiriidat heijastuvat myös politiikkoihin.

4.2 Tietoturvapolitiikkojen ristiriitaisuudet ja niiden ratkaiseminen

Nopea muutos yritysten hallinnollisissa rakenteissa on aiheuttanut suuria muutoksia myös siinä, miten turvallisuusasiat yrityksissä hoidetaan [Vir02]. Virtanen [Vir01] kuvaa, miten vanhassa hierarkkisessa yritysmallissa käskytyssuhteet olivat selkeät: ylempi taso kontrolloi alempaa ja alempi oli vastuussa myös omista alatasoistaan. Nykyaikaisessa yrityksessä eri yksiköt voivat olla hyvinkin itsenäisiä, jopa kilpailla keskenään. Tällaisissa malleissa ei ole selkeää käskytysrakennetta ja vastuu tietoturvasta on hajautettu yksikkötasolle. Yksiköillä saattaa olla erilaiset tietoturvantarpeet, jolloin yksiköillä on keskenään ristiriitaisia tietoturvapolitiikkoja. Tiukat tulosvastuut ja henkilökohtaiset tulostavoitteet kiristävät liiketoiminnan vaatimuksia ja tietoturvavaatimukset saattavat tuntua liiketoiminnan esteiltä. Toimintaolosuhteet saattavat muuttua nopeasti, eikä tietoturvapolitiikkoja ehditä päivittämään samassa tahdissa liiketoiminnan muutosten kanssa. Silloin saatetaan joutua tilanteisiin, joissa yhden säännön noudattaminen rikkoo toista sääntöä.

Siponen [Sip00] kuvaa neljä eri tilannetta, jossa tietoturvapolitiikat voivat olla keskenään ristiriitaisia ja esittää viisi lähtökohtaa turvaohjeiden laatimiseksi siten, että ristiriidat voidaan välttää. Ristiriitatilanteita saattaa aiheutua silloin, jos

- kaksi sääntöä on ristiriidassa keskenään
- jossakin tilanteessa ohjeen noudattaminen heikentää tietoturvaa
- muodollisen säännön noudattaminen estää liiketoimintamahdollisuuden
- turvallisuussäännön kirjaimellinen noudattaminen on ristiriidassa ylemmän tietoturvapolitiikan kanssa.

Siponen [Sip00] esittää seuraavat lähestymistavat ristiriitojen ratkaisemiseksi:

1. Kiellettyä on kaikki, mikä ei ole erikseen sallittua
2. Sallittua on kaikki, mikä ei ole erikseen kiellettyä
3. Yhtä tietoturvaohjetta voidaan muodollisesti rikkoa, jos se tuo enemmän hyötyä tietoturvallisuudelle tai liiketoiminnalle kuin ohjeen noudattaminen
4. Ohjeet ovat suosituksia, joita ei ole pakko noudattaa
5. Yleistettävyyden malli, jossa toiminnan hyväksyttävyyden mittarina on käyttäjän kuvitelma siitä, sallittaisiinko toiminto kaikille muillekin tai siitä, mitä ylläpitäjä vastaavassa tilanteessa sallisi tehtävän.

Ensimmäinen malli on perinteinen tietoturvamalli. Se on käyttäjille selkeä ja sopii muuttumattomaan, vakaaseen ympäristöön. Tällaiseen ympäristöön on myös helppo kirjoittaa tietoturvapolitiikat. Malli ei kuitenkaan sovi muuttuviin olosuhteisiin, joissa se vahvasti rajoittaa toimintaa. Malli on käyttökelpoinen ylläpitäjien kannalta ja se on yhä tavallinen erityisesti yritysten tietoliikenneverkoissa.

Toisen mallin mukaan sallituksi voi olettaa kaiken, mitä ei erikseen ole kielletty. Käyttäjät suhtautuvat tietoturvaan usein tämän mallin mukaisesti, joten se on helppo omaksua, kunhan kieltojen määrä pysyy kohtuullisena. Malli johtaa kuitenkin helposti joko tietoturvan menetykseen tai hallitsemattomaan määrään kieltäviä politiikkoja.

Kolmas malli hyväksyy sen, että tietyissä tilanteissa liiketoiminnan vaatimukset voidaan tulkita tietoturvaa tärkeämmiksi. Tällöin tulee olla kysymys joko poikkeustilanteesta, jolloin tilapäisesti toimitaan vastoin tietoturvapolitiikan vaatimuksia tai jostakin yksittäisestä tapauksesta, joka hoidetaan poikkeuksellisella tavalla. Malli tuo joustavuutta toimintaan ja sen avulla käyttäjien on kenties helpompi hyväksyä tietoturvapolitiikat. Tapaukset, joissa tietoturvapolitiikat tietoisesti ohitetaan, tulee olla sovittuja ja dokumentoituja poikkeuksia. Päätöstä tietoturvapolitiikan ohittamisesta ei pidä jättää käyttäjille.

Neljäs malli asettaa käyttäjät politiikkojen ja ohjeiden yläpuolelle. Tietoturvan toimintaohjeita voi noudattaa, mutta voi myös toimia toisin. Malli mahdollistaa tietoturvan toteutumisen, mikäli politiikat ovat ymmärrettäviä ja tarvittava tietoturva voidaan toteuttaa käyttäjille näkymättömästi. Tietoturvan toteutuminen jää kuitenkin epämääräiseksi, koska toimintaohjeita ei voi vaatia noudatettaviksi.

Viidennessä mallissa käyttäjät joutuvat miettimään, mitä toimenpiteitä ylläpitäjät vastaavassa tilanteessa sallisivat. Käyttäjät joutuvat miettimään ja

ratkaisemaan asioita, jotka eivät kuulu heidän varsinaisiin työtehtäviinsä. Tietoturvan kannalta tulos on todennäköisesti varsin tasapainoton, joihinkin tietoturvakysymyksiin suhtaudutaan tarpeettoman tiukasti ja toisista taas ei välitetä lainkaan.

4.3 Tietoturvapolitiikkojen kerroksellisuus

Yrityksen tietoturvapolitiikassa on yleisellä tasolla määritelty, mitä halutaan suojata. Yksityiskohtaisemmat alemman tason politiikat kohdistetaan tietyille osa-alueille: tietoliikenneverkko, langattomat verkot, tietojärjestelmät, palvelinalustat, työasemat, kannettavat tietokoneet, etäkäyttö. Näissä politiikoissa otetaan kantaa myös suojaustapoihin: salaus, tunnistus, pääsynhallinta.

Edellisessä kappaleessa esitetyistä malleista ei yksikään sovellu yrityksessä ainoaksi tietoturvapolitiikkojen lähestymistavaksi. Politiikat toteutetaan teknisin keinoin aina kun se on mahdollista ja muissa tapauksissa toimintaohjeilla, joiden noudattamista myös valvotaan. Tähän rakenteeseen kaksi ensimmäistä mallia soveltuu hyvin. Kolmas mallikin soveltuu osin politiikkalähtöiseen tietoturvan hallintaan. Silloin on vain tarkemmin määriteltävä politiikkojen kohdealueet ja mahdolliset poikkeukset.

Neljännessä ja viidennessä mallissa korostetaan käyttäjien päätösvaltaa ja politiikkoja joko noudatetaan tai jätetään noudattamatta käyttäjien oman harkinnan perusteella. Tällöin ei enää voi puhua tietoturvapolitiikoista vaan yrityksen tietoturva on erilaisten ohjeiden varassa.

”Älä laita kaikkia munia samaan koriin”, varoittaa Landwehr [Lan01]. Yksittäiset turvaamismenetelmät voivat olla puutteellisia tai ne voivat pettää. Menetelmiä pitää olla useita, erilaisia ja toisiaan täydentäviä [Lan01]. Kun tietoturvan rakentaa kerroksittaiseksi, yhdellä tasolla oleva turva-aukko voidaan sulkea toisella tasolla. Palomuurista on päästettävä liikennettä sisään, joten tarvitaan virustorjuntaohjelmia, liikenteen salausta ja lokitietojen seurantaa. Jos johtaja ei koskaan kirjaudu ulos verkosta, johtajan huoneen ovi pidetään lukossa.

Eri kerroksilla voidaan kuitenkin toteuttaa erilaisia malleja. Tietoliikenneverkossa ja palomuurinhallinnassa politiikat voidaan teknisesti toteuttaa ”kiellettyä on kaikki, mikä ei ole erikseen sallittua” -mallin mukaisesti. Erikseen voidaan osa liikenteestä sallia ja estää kaikki muu. Toinen malli, jossa sallittua on kaikki, mitä ei ole erikseen kielletty, voidaan teknisesti toteuttaa Internet-käytössä. Joillekin sivustoille pääsy voidaan estää, mutta kaikki muu jää vapaaksi. Sähköpostin käyttöpolitiikan noudattaminen puolestaan jää suurelta osin käyttäjien oman harkinnan varaan.

”Kova kuori ja pehmeä sisus” on usein käytetty tietoturvan toteutuspolitiikka [Rfc97]. Yrityksen ulkoista liikennettä tarkkaillaan ja suodatetaan tehokkaasti, mutta sisäverkkoa pidetään luotettavana eikä siinä toteuteta vastaavia turvatoimia. Tietoturva säilyy hyvänä, jos ulkokuorta ei murreta ja jos sisäiset käyttäjät ovat luotettavia. Tässä mallissa luotetaan vahvasti palomuurin tuomaan suojaan. Jos tunkeutuja pääsee palomuurin läpi, sisäverkon valtaaminen käy helposti [Rfc97].

Tietoturvapolitiikat tulee rakentaa siten, että mahdollisimman hyvä tietoturvan taso saavutetaan sellaisten pakollisten politiikkojen avulla, jotka voidaan teknisesti toteuttaa ja joiden toteutumista voidaan myös valvoa. Pelkästään teknisin keinoin ei tietoturvaa pystytä toteuttamaan kuin osittain. Tietoturvaa tulee lisäksi varmistaa ja tehostaa hallinnollisilla toimintaohjeilla. Hyvien tietoturvapolitiikkojen ansiosta henkilöstön on mahdollista toimia oikein ja tietoturvallisella tavalla.

5 Tietoturvapolitiikkojen käyttöönotto

Tietoturvapolitiikkojen käyttöönottoon liittyy oleellisena osana tiedottaminen. Tietoturvapolitiikoista ei ole hyötyä, jos käyttäjät eivät niistä tiedä eivätkä osaa niitä noudattaa.

Tietoturvallisuudessa on pohjimmiltaan kysymys luottamuksesta ja siitä kehen luotetaan ja milloin. Luotetaanko kaikkiin, ei kehenkään vai joihinkin joissakin tilanteissa. Vaikka kaikki periaatteessa toimisivatkin oikein, vahinkoja sattuu. Ihmiset saattavat vahingossa toimia väärin tai ohjelmaan on saattanut vahingossa jäädä turva-aukko. Tietoturvapolitiikkojen tarkoituksena on estää sekä vahingoista että tahallisesta toiminnasta aiheutuvat tietoturvan vaarantumiset.

5.1 Turvakulttuuri

Tietoturvapolitiikkojen hyväksyntä riippuu yrityksen turvakulttuurista. Virtanen [Vir02] toteaa, että aikaisemmin keskuskoneympäristöissä oli luonnollista noudattaa erilaisia käyttörajoituksia ja -vaatimuksia. Ylläpitohenkilöstö oli koulutettua ja pätevöitynyttä laitteiden ja tietoliikenneverkon ylläpitoon. Lisäksi usein myös käyttäjiltä vaadittiin koulutusta. Henkilökohtaiset tietokoneet muuttivat kulttuurin. Ne tulivat vapauttamaan käyttäjät atk-osastojen määräysvallasta ja sallivat käyttäjien muokata työasemia omien tarpeidensa mukaisesti. Mitään yhtenäisiä toimintaperiaatteita ei ollut, työasemat olivat yksilöllisesti varusteltuja ja käyttäjät ylläpitivät niitä itse rajoituksetta ja parhaan taitonsa mukaisesti. Työasemien vakiointi ja ylläpitotehtävien keskittäminen pois käyttäjiltä on tulkittu työnteon estämiseksi.

5.2 Markkinointi

Tietoturvapolitiikkojen hyöty on markkinoitava tehokkaasti [Woo99]. Yrityksen henkilöstölle on selvitettävä, että tietoturvapolitiikkojen tarkoituksena ei ole pystyttää tarpeettomia ja työtä haittaavia raja-aitoja, vaan niiden avulla mahdollistetaan liiketoiminnan vaatimusten mukainen avoimuus. Tiedotuksessa on painotettava sitä, että tietoturvapolitiikkojen avulla yrityksen johto on sitoutunut turvaamaan yrityksen liiketoiminnan.

Yrityksen todellinen tietoturvan taso riippuu huomattavasti johtajien ja työntekijöiden asenteesta ja siitä, kuinka he hyväksyvät toimintasäännöt ja käyttöohjeet [Vir02]. Turvallisuuden tulee olla osa yrityskulttuuria ja työntekijöiden jokapäiväistä työskentelyä [Vir02].

5.3 Koulutus

Henkilöstön koulutus on tärkeä osa tietoturvapolitiikkojen käyttöönottoa. Kone toimii annettujen sääntöjen mukaisesti, vaikka ei sääntöjä ymmärrä-kään. Ihmiset sen sijaan eivät välttämättä noudata määräyksiä, joita he pitävät tarpeettomina [Hen03]. Tietoisuuden lisääminen tietoturvaan liittyvistä asioista auttaa käyttäjiä ymmärtämään tietoturvapolitiikkojen merkityksen jokapäiväisessä työskentelyssä. Teknologiasta, palomuureista ja tunnistusjärjestelmistä ei ole hyötyä, jos työntekijät kertovat tietoturvaan liittyviä asioita puhelimessa satunnaisille kyselijöille. Koulutuksen tulee auttaa henkilöstöä ymmärtämään syyt, minkä vuoksi tietoturvapolitiikat ja toimintaohjeet on otettu käyttöön. Silloin niitä myös noudatetaan paremmin kuin jos käyttäjille vain opetettaisiin säännöt, joita tulee totella [Hen03].

Virtanen [Vir02] painottaa, että koulutus on tärkeää kaiken tasoisille käyttäjille. Peruskäyttäjät pyrkivät toimimaan ohjeiden mukaisesti, jolloin on tärkeää, että turvaohjeet ovat asianmukaiset. Edistyneemmät käyttäjät pyrkivät usein optimoimaan työskentelyään. Jos turvakoulutus on ollut riittämätöntä, työn tehostaminen saatetaan tehdä tavalla, joka ei ole tietoturvan mukaista. Erityisen tärkeää kouluttaminen on tehokäyttäjille, jotka pyrkivät aktiivisesti ratkomaan tietojenkäsittely-ympäristössään olevia ongelmia ymmärtämättä ongelmaan liittyvää kokonaisuutta ja yrityksen tietojenkäsittely-ympäristön vaatimuksia [Vir02]. Koulutuksessa tulee painottaa erityisesti sitä, kuinka ongelmat voidaan välttää tai kuinka ne ratkaistaan yrityksen tietoturvavaatimusten mukaisesti [Vir02].

Koulutuksen avulla käyttäjät tietävät, mitä toimenpiteitä tulee tehdä missäkin tilanteessa. Kaikille yrityksen tietotekniikan kanssa tekemisiin joutuville käyttäjille muodostuu myös selkeä käsitys siitä, mikä on hyväksyttävää toi-

mintaa. Koulutuksen ja tiedottamisen avulla poistuu myös mahdollisuus käyttää tietämättömyyttä virheiden selityksenä.

Käyttäjien kouluttamisen lisäksi tulee myös tietotekniikkatoimittajille ja liikekumppaneille kertoa yrityksen tietoturvapolitiikkaan ja -standardeihin liittyvistä asioista.

5.4 Tarkkailu ja valvonta

Tietoturvapolitiikkojen toteutumista on tarkkailtava ja valvottava. Tarkkailu on osa tietoturvaa ja sitä tehdään jatkuvasti. Se sisältää mm. palomuuriasetukset, verkon hallintaohjelmistot ja virustorjunnan. Tarkkailun avulla kerätään tietoa, jonka avulla voidaan toipua sattuneista vahingoista [Max01]. Valvonta perustuu satunnaisiin, mutta säännöllisiin tarkastuksiin, joiden avulla varmistetaan, että tietoturvapolitiikat ovat asianmukaisia ja että niitä noudatetaan. Turvapolitiikkojen noudattamista voidaan tehostaa sanktiomäärittelyillä silloin, kun politiikan toteutumista ei voida teknisesti pakottaa.

Työntekijöiden toimenpiteiden valvonnassa ja valvonnan hyväksyttävyydessä on suuria maakohtaisia eroja. Yhdysvalloissa työnantajat valvovat ja rajoittavat työntekijöiden Internet-käyttöä ja sähköpostia huomattavasti enemmän kuin Suomessa. Virtasen [Vir02] mukaan erot johtuvat erilaisesta kulttuurista: yhdysvaltalaisessa yksilöllisyyttä korostavassa kulttuurissa työntekijät ovat itsenäisiä suhteessa työnantajaansa, kun taas suomalaisessa yhteisöllisessä kulttuurissa työntekijät ovat vahvasti sidoksissa työnantajaansa.

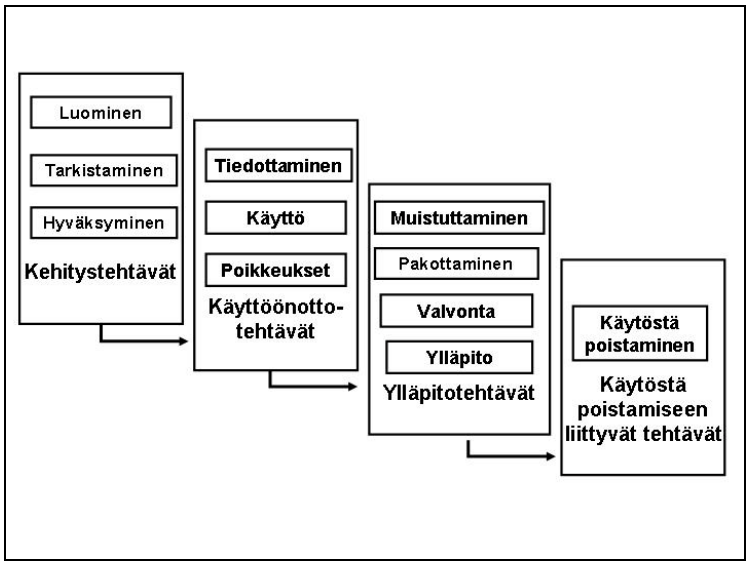
Suomalaisille työpaikka on tärkeä osa elämää ja sen vuoksi suomalaisista on oikeutettua hoitaa työpaikalla myös henkilökohtaisia asioita. Niinpä suomalaisilla työpaikoilla ei juurikaan valvota eikä rajoiteta työntekijöiden sähköpostin tai Internetin käyttöä. Myös lainsäädäntö, jossa henkilön yksityisyyden suoja on määritelty varsin suureksi, tukee työntekijän oikeuksia. Työnantajalla on oikeus rajoittaa sähköpostin käyttö ainoastaan työasioita koskevaksi, mutta työnantajalla ei ole oikeutta lukea työntekijän viestejä.

6 Elinkaarimalli

Tietoturvapolitiikkojen kehittäminen ei ole pelkästään sitä, että kirjoitetaan tietystä aiheesta politiikka ja ryhdytään noudattamaan sitä. Ei riitä myöskään, että työntekijöille tiedotetaan uudesta politiikasta ja valvotaan, että sen määräyksiä ryhdytään noudattamaan [How03]. Tietoturvapolitiikkojen tehokas hyödyntäminen edellyttää tietoturvapolitiikkojen elinkaaren määrittelyä. Elinkaarimallin avulla voidaan hallita turvapolitiikkojen laatimista ja

ylläpitoa. Tietoturvapolitiikan elinkaareen sisältyy useita vaiheita. Politiikka on kirjoitettava, sille on saatava johdon hyväksyntä, se on levitettävä käyttöön, käyttäjien on se hyväksyttävä, se on pidettävä ajantasaisena ja lopulta se on poistettava käytöstä [How03]. Tietoturvapolitiikkojen vaiheet on dokumentoitava huolellisesti. Elinkaarimallin vaihejako selkeyttää dokumentointia ja mallin avulla tietoturvapolitiikat voidaan luontevasti tuottaa osana yrityksen laatujärjestelmää.

Howard [How03] esittää yksitoista vaihetta, jotka tietoturvapolitiikka käy läpi elinkaarensa aikana. Turvapolitiikkojen elinkaari muodostuu politiikan kehittämisestä, käyttöönotosta, ylläpidosta ja käytöstä poistamisesta. Kukin vaihe jakaantuu edelleen osatehtäviin (kuva 2).



Kuva 2 Tietoturvapolitiikkojen elinkaari [How03]

Kehittämisvaiheessa määritellään politiikan tarve ja kohde sekä määritellään politiikkaan liittyvät vastuut. Politiikka kirjoitetaan yrityksen standardien mukaisesti ja annetaan asiantuntijaryhmän tarkistettavaksi. Tarkistuksessa varmistetaan, että politiikan avulla turvataan se, mitä on tarkoitus turvata. Viimeisenä tehtävänä on hankkia politiikalle johdon hyväksyntä. Kun hyväksyntä on saatu, siirrytään seuraavaan vaiheeseen.

Käyttöönottovaiheessa politiikka on levitettävä yritykseen. Politiikasta on tiedotettava kaikille, joita se koskee. On sovittavat tavat, joilla politiikkaa voidaan parhaiten noudattaa eri tilanteissa ja on määriteltävä poikkeustilanteet, joissa politiikkaa ei sellaisenaan voida noudattaa.

Ylläpitovaiheessa huolehditaan siitä, että käyttäjät ovat tietoisia politiikasta ja että politiikka pysyy ajantasaisena. Politiikan käyttöä ja toteutumista seurataan ja tarvittaessa sitä päivitetään.

Politiikka poistetaan käytöstä silloin, kun yrityksessä ei enää käytetä tekniikkaa, johon politiikka on liittynyt tai kun on otettu käyttöön korvaava politiikka.

7 Yrityksen peruspolitiikat

Vastuu tietoturvasta ja sen toteutumisesta on yrityksen koko henkilöstöllä. Tietoturvapolitiikkojen perustarkoituksena on kertoa käyttäjille, ylläpitäjille ja yritysjohdolle jokaisen velvollisuudet ja vastuut yrityksen teknologian ja tiedon suojaamisessa sekä määritellä tavat, joilla vaatimukset täytetään [Rfc97]. Politiikat voidaan kohteensa mukaan jakaa käyttäjä-, ylläpitäjä- ja infrastruktuuripolitiikkoihin [Max01]. Guelin [Gue01] mukaan yrityksen tärkeimmät tietoturvapolitiikat ovat tietotekniikan käyttöpolitiikka ja sen osana etäkäyttöpolitiikka, tiedon turvaamispolitiikka ja palomuuripolitiikka. Luetteloon voi vielä lisätä ylläpitäjien käyttöpolitiikan ja tietojärjestelmien ylläpitopolitiikat.

7.1 Tietotekniikan käyttöpolitiikka

Yrityksen kenties tärkein tietoturvapolitiikka on koko henkilöstöä koskeva tietotekniikan käyttöpolitiikka. Sen avulla määritellään, miten yrityksen tietotekniikkaa saa käyttää ja miten sitä ei saa käyttää. Käyttöpolitiikka koskee laitteita, ohjelmistoja, tietojärjestelmiä ja tietoliikennettä. Käyttöpolitiikassa kuvataan käyttäjän suhde yrityksen tietotekniikkaan. Siinä on kerrottava, miten yrityksen tietoja ja tietoresursseja käsitellään, miten eri järjestelmien käyttäjätunnuksia ja salasanoja käytetään sekä saako sähköpostia ja Internet-yhteyksiä käyttää henkilökohtaisiin tarpeisiin. Käyttöpolitiikassa voidaan myös määritellä, kuinka suhtaudutaan yrityksen tietojärjestelmiä koskeviin ulkopuolisiin kyselyihin. Käyttöpolitiikka on kirjoitettava selkeästi ja siinä on käytettävä termejä, jotka käyttäjät ymmärtävät.

Käyttöpolitiikassa on myös kerrottava, miten työntekijöiden tietotekniikan käyttöä valvotaan. Valvotaanko sähköpostia ja kerätäänkö Internet-käytöstä loki-tietoja. Lisäksi on kerrottava, miten ja ketkä kerättyä tietoa käsittelevät.

Tietotekniikan käyttöpolitiikkaan liittyy myös tietojärjestelmien etäkäyttöpolitiikka. Siinä määritellään periaatteet sille, ketkä saavat ottaa etäyhteyden tietojärjestelmiin ja millä menetelmillä etäyhteyden ottaminen on sallittu. Etäkäyttöön liittyy puolestaan muita politiikkoja, mm. salauspolitiikka, henkilökohtaisten erillisverkkojen politiikka ja langattomien verkkojen politiikka.

7.2 Ylläpitäjien käyttöpolitiikat ja järjestelmien ylläpitopolitiikat

Ylläpitäjien tulee työskennellä turvallisten menetelmien mukaisesti ja noudattaa yrityksen tietoturvapolitiikkoja [Max01]. Ylläpitäjillä tulee myös olla hyväksytty tietotekniikan käytön ja tietoturvallisen ylläpidon politiikka, jossa määritellään ylläpitäjien oikeudet ja velvollisuudet. Ylläpitäjien työturvallisuuden vuoksi käyttöoikeudet eri tietojärjestelmiin on määriteltävä tarkasti pienimmän valtuutuksen periaatteen mukaisesti. Koska ylläpitäjillä on tehtäviensä vuoksi mahdollisuudet päästä laajasti käsiksi yrityksessä käsiteltävään tietoon, ylläpitäjien tietoturvaosaamisen tason on oltava korkea.

Tietojärjestelmien haavoittuvuuksien hyödyntämistä ja järjestelmiä kohtaan suunnattuja hyökkäyksiä voidaan torjua ottamalla käyttöön tietojärjestelmien ylläpitopolitiikat. Politiikkoihin ja toimintamalleihin kuuluu tarpeettomien palvelujen poistaminen palvelimista ja työasemista, ylläpitotunnusten käyttäminen ainoastaan ylläpitotehtävissä, vakiotunnusten poistaminen järjestelmistä, ajantasaisen virustorjunnan ylläpito sekä tietoturva-aukkojen ja turvapäivitysten säännöllinen seuraaminen.

7.3 Tiedon turvaamisen politiikka

Tiedon turvaamisen politiikka kuuluu infrastruktuuripolitiikkoihin. Siinä määritellään, miten luottamuksellista tietoa käsitellään, säilytetään ja siirretään. Politiikan päämääränä on varmistaa, että tieto on asianmukaisesti suojattu muuttumiselta ja paljastumiselta. Tiedon turvaamisen politiikkoja ovat tunnistamiseen ja järjestelmien käytön valvontaan liittyvät politiikat. Käyttöoikeus- ja tunnistuspolitiikkojen avulla varmistetaan, että oikeat henkilöt pääsevät käsiksi oikeaan tietoon oikealla tavalla. Pienimmän valtuutuksen – politiikan mukaisesti jokaisella tule olla oikeuksia täsmälleen sen verran kuin työtehtävien hoitaminen edellyttää.

Käytettävyysvaatimuksissa määritellään, millaisina aikoina tietojärjestelmien tulee olla käytettävissä. Tiedon turvaamisen politiikkaan kuuluvat myös lokitietojen keräämiseen ja seurantaan liittyvät politiikat.

7.4 Palomuuripolitiikka

Palomuuri- ja turvarajapolitiikka on myös infrastruktuuripolitiikka. Siinä määritellään palomuurien ja muiden turvarajalaitteistojen ja –ohjelmistojen ylläpitoprosessit, vastuut ja muutoksenhallintaan liittyvät toimenpiteet. Politiikassa linjataan myös se, kenellä on oikeus saada tietoja asetuksista ja miten tietoja säilytetään. Palomuuri on tärkeä osa yritysturvallisuutta, joten sääntöjen on oltava tarkkoja ja rajoitusten tiukkoja.

8 Yhteenveto

Tietoturvapolitiikkojen avulla johdetaan ja ylläpidetään yrityksen tietoturvaa. Turvapolitiikat laaditaan yrityksen riskianalyysin, siitä johdettujen uhkien ja uhkien arvioinnin perusteella. Politiikoilla turvataan tiedon suojattavia ominaisuuksia: luottamuksellisuutta, eheyttä ja saatavuutta. Politiikat kohdistetaan tietoturvan kaikkiin osa-alueisiin.

Turvapolitiikat muodostavat hierarkkisen rakenteen, jossa ylimpänä on yrityksen johdon hyväksymä yrityksen tietoturvapolitiikka. Siinä johto ilmaisee tahtonsa tietoturvan toteuttamiseksi. Alemman tason politiikat kohdistuvat yksittäisiin osa-alueisiin ja niistä johdetaan konkreettiset toimintaohjeet.

Politiikkojen on oltava kattavia, tarpeellisia ja uskottavia sekä ajantasaisia ja ristiriidattomia. Elinkaarimallin avulla on mahdollista hallita tietoturvapolitiikkojen laatimista ja ylläpitoa. Elinkaarimallin avulla tietoturvapolitiikat voidaan liittää osaksi yrityksen laatujärjestelmää. Ilman laatujärjestelmän tukea, on vaarana, että politiikat ovat puutteellisia, ristiriitaisia tai vanhentuneita, niillä ei ole johdon tukea eivätkä käyttäjät tiedä niistä mitään.

Tietoturvan kerroksellisuutta tuetaan tietoturvapolitiikkojen avulla. Eri kerroksissa voidaan toteuttaa erilaisia politiikkoja. Näin saadaan tietoturvarakenteeseen joustavuutta ja pystytään helpommin tasapainoilemaan liiketoiminnan vaatimusten ja tietoturvallisuuden välillä. Yhdessä kerroksessa tapahtuva tietoturvan heikennys voidaan paikata toisessa kerroksessa.

Turvapolitiikat otetaan käyttöön tietoturvakoulutuksen ja tehokkaan tiedottamisen avulla. Tietoa on jaettava selkeässä ja ymmärrettävässä muodossa. Käyttäjien tulee ymmärtää, että yrityksen tietoturvan tasoon vaikuttaa se, mitä he tekevät ja miten he toimivat. Henkilöstöä kuvataan usein tietoturvan heikoimmaksi lenkiksi, jonka mukana koko tietoturva menetetään. Kunnollisen koulutuksen ja hyvän tiedottamisen avulla käyttäjistä voidaan kehittää yrityksen tietoturvan tukipilareita.

Tietoturvan toteutumisen kannalta on välttämätöntä, että yrityksen johto sitoutuu harjoitettuun tietoturvapolitiikkaan. Sitoutumisen tulee näkyä esimiesten omassa toiminnassa ja heidän tekemissä päätöksissä. Tietoturvapolitiikkojen hyväksymiseen ja käyttöönottoon vaikuttavat yrityksen hallintomallit ja yrityksessä vallitsevat toimintakulttuurit. Tietoa kunnioittavassa ja tietoturvallisuutta korostavassa yrityskulttuurissa kaikkien on helppo toimia tietoturvan mukaisesti.

Tietoturvan toteutumisen ensimmäisenä edellytyksenä ovat hyvät ja liiketoiminnan tavoitteita vastaavat tietoturvapolitiikat, seuraavaksi tärkeimpiä tekijöitä ovat sitoutuneet johtajat, tietoturvatietoiset työntekijät ja asiantuntevat ylläpitäjät, hyvät valvontaprosessit ja asianmukainen tekniikka. Nämä ovat kriittiset tekijät, joiden turvin yrityksessä voidaan noudattaa tietoturvallista kulttuuria ja toteuttaa hyvä tietoturvan taso.

Lähteet

Far01 Farrar, W., *Security awarness starts in IT*. The SANS Institute, USA, 2001.
[Myös http://www.sans.org/rr/aware/IT.php]

Gue01 Guel, M., *A short primer for developing security policies*. The SANS Security Policy Project, The SANS Institute, USA, 2001.
[Myös http://www.sans.org/resources/policies/]

Har03 Hare, C., Firewalls, ten percent of the solution: a security architecture primer. Teoksessa *Information Security Management Handbook*, vol 4, 4th edition, toim. Tipton, H., Krause, M., Auerbach Publications, USA, 2003, sivut 699-781.

Hen03 Henry, K., The human side of information security. Teoksessa *Information Security Management Handbook*, vol 4, 4th edition, toim. Tipton, H., Krause, M., Auerbach Publications, USA, 2003, sivut 239-261.

How03 Howard, P., The security policy life cycle: functions and responsibilities. Teoksessa *Information Security Management Handbook*, vol 4, 4th edition, toim. Tipton, H., Krause, M., Auerbach Publications, USA, 2003, sivut 297-311.

Lan01 Landwehr, C., Computer Security. *International Journal of Information Security*, vol 1, issue 1, Springer-Verlag, 2001.
[Myös http://link.springer.de/link/service/journals/10207/tocs/t1001001.htm]

Max01 Policies, procedures and enforcement. Teoksessa *Maximum security*, toim. Anonymous

Rfc97 Network working group, *Request for comments 2196.* toim. Fraser, B., 1997
[Myös ftp://ftp.funet.fi/pub/standards/RFC/rfc2196.txt]

Sip00 Siponen, M., Policies for Construction of Information Systems´ Security Guidelines, Five approaches*, Proc. IFIP TC11 16th Annual Working Conference on Information Security: Information Security for Global Information Infrastructures*, Beijing, China, elokuu 2000, sivut 111-120.

SFS98 *BS 7799-1:fi, Tietoturvallisuuden hallinta*. Osa 1. Tietoturvallisuuden hallintaa koskeva menettelyohje, Suomen standardisoimisliitto SFS, 1998

Val99 *Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta*, VM 0024:00/02/99/1998, Helsinki, 1999. [Myös http://www.vm.fi/tiedostot/pdf/fi/6294.pdf]

Vir02 Virtanen, T., *Four views on security*. Väitöskirja, Teknillisen korkeakoulun tietoliikenneohjelmistojen ja multimedian julkaisuja, Otamedia Oy, Espoo 2002. [Myös http://www.tml.hut.fi/~tpv/ opiskelijat/tpv.pdf]

Woo99 Woodward, D., *Security policy management in the Internet age*, Townsend&Taphouse, 1999
[Myös htp://www.itsecurity.com/papers/wickpol.htm]