# Tietoturvan yksilöön ja organisaatioon kohdistamat haasteet 2000-luvun alussa

*Jorma Kajava*

*ABSTRACT*

*Information Security Challenges for Users, End-Users and Organizations in the Beginning of the new Millennium*

The information society is built for the benefit of the people. Its various activities could be made more effective by providing a versatile range of services. The current tendency is to integrate services as a basic component of the infrastructure of the information society. However, as users are the most important part of the society, the only sustainable way to develop the information society is to promote information security in parallel with the development of new technical solutions. Increased security opens up new perspectives for users and end-users alike. Both groups face certain security threats and should be involved in discussions around security. As a matter of fact, the management of organizational information security work is a major challenge for security people. The first useful tool in this area is discussion of information security awareness.

Keywords: information security, information society, security management, security awareness, end-user perspectives in security.

## 1. JOHDANTO

Tietotekniikan käyttäjien tietoturvasta huolehtiminen on eräs keskeinen kysymys tulevassa yhteiskunnassamme. Siihen on kiinnitetty huomiota eniten organisaatioissa, sen sijaan tavalliset kotikäyttäjät ovat jääneet hyvin vähälle. Kuitenkin lähitulevaisuuden tietoyhteiskunta on nimenomaan sellainen, jossa myös organisaatioiden ulkopuolella tapahtuva toiminta tulee yhä voimakkaammin perustumaan Internetin palvelujen käyttöön - esimerkiksi sähköposti, tietojen haku Internetin kautta, sähköinen kaupankäynti, asioiminen viranomaisten kanssa.

Organisaatiot ovat kouluttaneet henkilöstöään niin tietotekniikan osaamisessa kuin tietoturvan perusteissakin ja laatineet eri käyttäjäryhmille ohjeistoja. Joskus tuntuu, että tietoturvaratkaisut hidastavat koko työntekoa, joissakin tapauksissa ne tekevät työskentelystä ikävää. Jos ratkaisujen syvällisempää merkitystä ei ole ymmärretty, joku työntekijä voi keksiä tietoturvaratkaisun kiertävän vastineen - ja kaikkein suurimmat tietoturvaan liittyvät uhkat ovat odottamassa.

Tietojenkäsittelyssä on koettu viidenkymmenen vuoden aikana selviä muutostilanteita. Aikoinaan tietokonesukupolviksi kutsuttiin vaiheita, joiden rajapinnassa koko tietojenkäsittelyyn liittyvä teknologia täysin muuttui. Mikrotietokoneiden alentuneet hinnat toivat ne vähitellen lähes kaikkien saataville. Koneiden, ohjelmistojen ja tiedostojen yhteensopivuus loi pohjan laajemmalle verkkojen käytölle. Mutta kun käyttöolosuhteet paranivat, myös erilaisten väärinkäytösten määrä alkoi kasvaa. Nyt tapahtuva kehitys on vastaavanlainen suuri läpi koko yhteiskunnan menevä aalto, ilman tietoturvaratkaisuja ja alan tietoisuutta toiminta ei voi jatkua kuin hetken.

Tässä artikkelissa käsitellään tietoturvaan liittyviä uusia haasteita, jotka kohdistuvat niin yksilöön kuin organisaatioon. Yksilö tarkoitaa tässä kansalaista, tarkennettuna sellaista kansalaista, joka käyttää tietokonetta kotonaan tai työpaikallaan, mahdollisesti molemmissa. Haaste kohdis-

Kirjoitusta koskevat kommentit pyydetään osoittamaan kirjoittajalle: Jorma Kajava, Oulun yliopisto, Tietojenkäsittelytieteiden laitos, PL 3000, 90014 OULUN YLIOPISTO. E-mail: jorma.kajava@ oulu.fi
Haluan osoittaa kiitokseni Hallinnon Tutkimus –lehden anonyymeille arvioijille. Samoin haluan kiittää kirjoitukseni aiempaan versioon saamistani hyödyllisistä kommenteista.

tuu niin yksilöitä kuin organisaatioita vaaniviin tietoturvaan liittyviin uhkiin ja loukkauksiin ja niiden ennalta torjumiseen tai niiden aiheuttamista vahingoista toipumiseen.

Suomesta on puhuttu uusien tietoliikenneratkaisujen huippulaboratoriona. Asiaan liittyi ensimmäisessä vaiheessa kielteinen leima. Kansalaisia alettiin jakaa tietotekniikan osaajiin, menestyjiin, ja häviäjiin. Nyt tämä keskustelu on laajentunut, aivan niinkuin Internet muuttaa asiat globaaleiksi. Aikaisemmin jo puhuminen kolmannesta maailmasta oli raskasta, mutta sellaiset tulevaisuudentutkijat kuten Alvin Toffler (1980) ja Ervin Laszlo (1990) pystyivät kuitenkin esittämään positiivisia vaihtoehtoja. Nyt puhutaan uuden viestintä- ja informaatioteknologian ulkopuolelle jäävien muodostamasta"neljännestä" maailmasta (ks. esim. Castells 2000). Tämä maailma on huomattavasti vaikeampi kysymys.

## 2. TIETOTURVA

Tietoturvallisuuden kehittämisen päätavoite on hyvän tietojenkäsittelytavan ja asianmukaisen perusturvallisuustason luominen (Royal Canadian Mounted Police, 1981). Hyvään tietojenkäsittelytapaan kuuluu erottamattomasti tietoturvallisuus. Asianmukaista perusturvallisuustasoa tarvitaan, koska organisaatioiden tiedot, järjestelmät ja palvelut muodostavat taloudellisesti arvokkaan ja valtakunnan turvallisuuden kannalta tärkeän omaisuuden.

Valtioneuvoston periaatepäätöksessä (1993) tietoturvallisuudella tarkoitetaan asiaintilaa, jossa tiedot, järjestelmät ja palvelut on asianmukaisesti suojattu sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta.

Tietoturvallisuus perustuu tiedon kolmeen eri perusominaisuuteen eli luottamuksellisuuteen, eheyteen ja käytettävyyteen (Parker 1981).

- Luottamuksellisuus (confidentiality) tarkoittaa sitä, että tiedot ovat vain niiden käyttöön oikeutettujen käytettävissä eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön.
- Eheys (integrity) tarkoittaa sitä, että tiedot ja järjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ne ole laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.
- Käytettävyys (availability) tarkoittaa sitä, että järjestelmien tiedot ja järjestelmien muodostamat palvelut ovat niihin oikeutettujen käytössä etukäteen määritellyssä vasteajassa.

Tietoturvallisuus määritellään näiden kolmen peruskäsitteen avulla, joten niitä kutsutaankin tietoturvallisuuden dimensioiksi. Jos ajatellaan tietoturvallisuutta tietoliikenneympäristössä ja nimenomaan verkkopalvelujen tarjoajan ja käyttäjän kannalta, niin silloin käytettävyyden tilalle voidaan nostaa palveluvarmuus. Verkkoympäristössä palvelut ovat esimerkiksi tiedonsiirtopalveluja, syöttö- ja tulostuspalveluja ja tietokantapalveluja.

- Palveluvarmuus (serveability) tarkoittaa sitä, että tarjolla olevia resursseja on tarvittaessa saatavissa ja ne on pidettävissä käytössä halutun ajan. Palveluvarmuus on riippuvainen resurssien määrällisestä mitoituksesta ja niiden käyttövarmuudesta. Resursseilla tarkoitetaan kaikkia järjestelmään kuuluvia resursseja, kuten laite-, ohjelmisto- ja henkilöresursseja.

Parker (1981) liittää dimensionsa tietoturvakontrollien kuvaukseen, jossa tavoitellaan järjestelmien täydellisyyttä ja paikkansapitävyyttä, johon liitetään myös käyttäjän tunnistus ja järjestelmän pääsynrajoitukset. Esitetyt dimensiot liittyvät järjestelmän käytön seurantaan. Parker (1995) laajensi järjestelmänsä dimensioita. Hän käyttää termejä utility, authensity ja posession.

Miettinen (1999) esittää vastaavasti:

- Aitous (authensity) tarkoittaa sitä, että tiedot ovat alkuperäisiä eikä niitä ole väärennetty.
- Hallussapidossa (posession) on kyse siitä, kuinka yksittäinen henkilö voi käsitellä yrityksen tietoja. Tähän liittyy esimerkiksi tietovarkaudet.
- Hyödyllisyys (usability) tarkoittaa sitä, että tiedot ovat sellaisessa muodossa, että niitä voidaan käyttää vaivattomasti päivittäisessä toiminnassa.

Valtiovarainministeriö (1999) määrittelee termin todentaminen:

- Todentaminen (authensity) tarkoittaa osapuolten (henkilö tai järjestelmä) luotettavaa tunnistamista.

Kerttula (1998) määrittelee myös termin kiistämättömyys:

- Kiistämättömyys (non-repudiation) takaa, että lähettäjä ja vastaanottaja kumpikaan eivät pysty kieltämään siirtämäänsä tietoa. Kiistämättömyys tarkoittaa tapahtuneen todistamista jälkeenpäin, jolloin tavoitteena on juriidinen sitovuus.

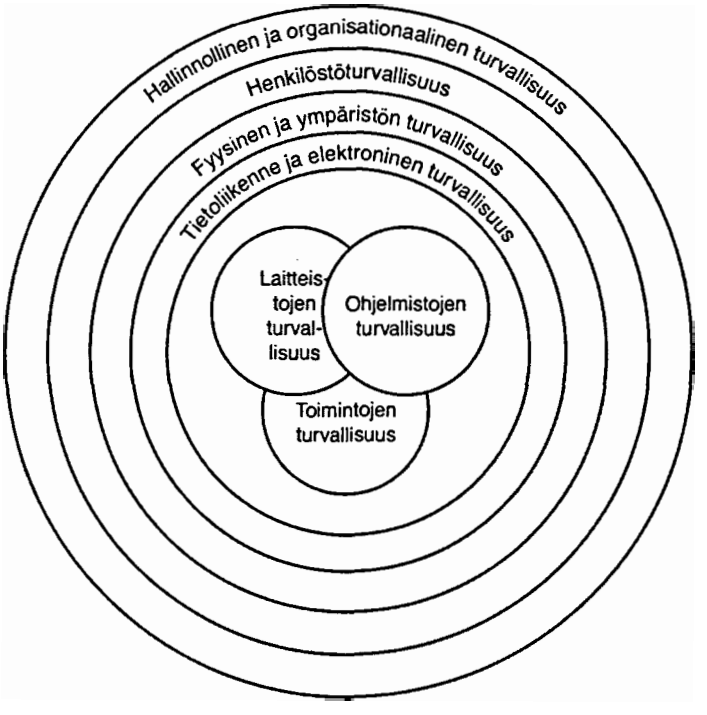
Mainitaan vielä kaksi yleisesti käytössä olevaa dimensiota (ISO-IEC, 1994): seurattavuus (accountability) ja luotettavuus (reliability). Näiden tietoturvallisuuden perusominaisuuksien laajuus on tavallaan kansalaisia hämmentävä tekijä. Erilaisissa käytännön ratkaisuissa aina muutama näistä nousee tärkeäksi, mutta kaikki muutkin vaikuttavat kokonaistilanteeseen. Toisaalta tässä luetellut ovat tämänhetkisiä eniten esillä olevia perusominaisuuksia, ensi vuonna voimme painottaa jo seuraavia tietotekniikan kehityksen mukanaan tuomia perusominaisuuksia.

Valtioneuvoston periaatepäätöksen valtionhallinnon tietoturvallisuudesta (1999) tarkoituksena on parantaa organisaatioiden toimintojen ja tietojenkäsittelyn tietoturvallisuuden ja henkilötietojen tietosuojan tasoa kehittämällä valtionhallinnon tietoturvallisuusperiaatteita ja antamalla tietoturvallisuuden hallintaa ja kehittämisohjeita koskevia suosituksia. Lisäksi päätös täsmentää tietoturvallisuuden työnjakoa ja vastuita sekä yksilöi keskeisiä viranomaisten tehtäviä.

Tietoturvallisuus muodostuu useista eri osa-alueista, jotka muodostavat yhtenäisen kokonaisuuden. Osa-alueet kytkeytyvät aina toisiinsa, vaikka niitä voidaan tarkastella erillisinä. Jaottelu pienempiin osiin on järkevää tehdä käytännön syistä, sillä se helpottaa aiheen käsittelyä. Jaottelu voidaan tehdä periaatteessa useilla eri tavoilla ja lähtökohdista riippuen voi syntyä erilaisia jaotteluja.

Valtioneuvoston periaatepäätöksessä (1993) tietoturvallisuuden osa-alueita käsitellään kuvion 1 mukaan. Ainoa poikkeus on, että toimintojen turvallisuutta ei esitetä, vaan tilalle on otettu osa-alueet, jotka liittyvät tietoaineistoturvallisuuteen ja käyttöturvallisuuteen.

Kuvassa 1 on esitetty oleellisimmat tietojen-




***Kuva 1.*** *Tietoturvallisuuden osa-alueet (Computer Security Handbook, 1984)*

käsittelyn turvaamisen osa-alueet. Jaottelu helpottaa aiheen käsittelyä ja kuvastaa sitä, kuinka turvaamisen eri alueet ovat organisaatioriippuvaisia, eli kaikissa organisaatioissa ei ole tarpeen käsitellä turvaamisen kaikkia osa-alueita. Perinteisesti tietojenkäsittelyn turvaamisen kehittämisessä on huomio kiinnitetty alueille, joilla voidaan saada aikaan näkyviä tuloksia, kuten fyysinen turvallisuus painottuen pääsykontrolleihin ja palosuojaukseen sekä tietojen ja tiedostojen turvaamiseen. Laajemmassa tarkastelussa voidaan painottaa hyvän turvallisuuspolitiikan tärkeyttä, kunnollisten turvaohjelmien suunnittelua ja implementointia sekä tehokkaiden elpymissuunnitelmien suunnittelua ja testausta. Nopean tietoteknisen kehityksen aiheuttamat muutospaineet vaikuttavat voimakkaina myös tietojenkäsittelyn turvaamiseen. Pysyvinä ja olennaisina osina tietojenkäsittelyssä säilyvät kuitenkin ihmiset, menetyksen uhka ja tiedot, joihin uhka kohdistuu. Tietoturvallisuustarkastelu on syytä aloittaa kokoamalla haavoittuvuus-kohteet, kartoittamalla niihin liittyvät uhkat ja selvittämällä uhkien todenäköisyydet eli riskit. Joissakin tapauksissa on selvintä ottaa uhkan varalta vakuutus, toisessa tapauksessa uhkaa vastaan täytyy suojautua asianmukaisesti ja kolmas suunta liittyy riskin ottamiseen, siis siihen, että uhkan todennäköisyys on erittäin pieni.

Tietoliikenteeseen ja elektroniseen turvallisuuteen liittyvät asiat eivät olleet ongelmia suljettujen järjestelmien ja verkkojen aikakaudella. Tietoverkot kehittyvät erittäin nopeasti ja laitteet, ohjelmat ja ohjelmointiympäristöt ovat tulleet yhä avoimemmiksi. Lähivuosina tämä alue on kaikkein kriittisin tietoturvan ja samalla myös organisaation mielekkään toiminnan kannalta. On syytä muistaa, että kokonaisuuden turvallisuus on sillä tasolla, millä heikoimman osa-alueen turvallisuus on.

## 3. KÄYTTÄJÄT

Tietotekniikan yhteydessä termin käyttäjä tulkinta suomenkielellä on verrattain selvä. Englanninkielinen vastaava termi "user" tarkoittaa nimenomaan kotikäyttäjää tai organisaatioista riippumatonta ammattilaista. Toinen termi "end-user" suomennetaan myös käyttäjäksi, loppukäyttäjäksi, joka tuntuu kömpelöltä, mutta kuvaa juuri työntekijän asemaa suuren organisaation laajojen prosessien tai ohjelmistojen käyttäjänä ketjun viimeisenä, sekä hyötykäyttäjäksi, joka kuvaa ehkä neutraaleimmalla tavalla tilannetta.

User-tyyppisellä käyttäjällä tietoturvaan liittyvät vastuut ja sitoumukset ovat hänen omassa hallinnassaan, kuten erilaisten verkkopalvelujen käyttöön liittyvät vastuut. Sen sijaan end-user toimii osana organisaatiota, jolla on niin tietotekniikkaan kuin tietoturvaan liittyvät politiikat, joita hänen on noudatettava. Samoin organisaation hyötykäyttäjän on noudatettava organisaation hänelle antamia tietoturvaohjeita ja –periaatteita.

Tietoturvaratkaisujen yhteydessä usein todetaan itsestäänselvyytenä, että käyttäjät ovat koko ratkaisun heikoin osa. Tästä huolimatta tietoturvatyö on suurelta osin tarkentunut niin tutkimuksen, kaupallisten tuotteiden kuin laajenevien järjestelmien osalta voimakkaammin teknologiaan kuin ihmisen huomioimiseen turvallisen ratkaisun osana.

Tietokoneen käyttäjien muuttuva työskentelyympäristö tekee tämän kysymyksen vielä ajankohtaisemmaksi. Internetiä käytetään yhä laajemmin uusiin sovelluksiin, kuten sähköinen kaupankäynti, pankkiasioiden hoito kotoa tai asiointi viranomaisten kanssa, joiden yhteydessä vaaditaan erittäin korkeaa tietoturvaa. Tämä tarkoittaa sitä, että alueelle tulee uusia käyttäjäryhmiä, joista vain osa on perillä tietoturvaan liittyvistä kysymyksistä. Osalla ihmisistä ei ole tietoa kaikista niistä asioista, jotka olisi ymmärrettävä ja hallittava uusien mahdollisuuksien yhteydessä. Olemme tottuneet siihen ajatukseen, että tietoturvaa kehitetään nimenomaan organisaation toiminnan turvaamiseksi, jokainen organisaation palkansaaja pyritään ottamaan tietoturvatietoisuutta kehittävään työhön mukaan. Mutta nyt tilanne on uusi, nämä uudet käyttäjät eivät olekaan organisaation työntekijöitä vaan yksittäisiä asiakkaita, kansalaisia.

Yksittäiset käyttäjät eivät noudata minkään organisaation tietoturvapolitiikkaa, varsin harvoilla heistä on edes tietoa siitä, että valmiita tietoturvaohjeita tietokoneiden käyttäjille on saatavana. Tämä suuri käyttäjien joukko asettaa tietokoneiden modernille käytölle sen perusvaatimuksen, että käytön pitää olla turvallista. Vieläpä siten painotettuna, että turvajärjestelyjen pitää olla helppokäyttöisiä ja tehokkaita. Jos näin ei ole, he mieluummin siirtyvät käyttämään seuraavan palveluntarjoajan järjestelmiä.

Minkälaisia uhkia tavalliseen tietokoneen kotikäyttäjään voi kohdistua? Vaikka kansalainen ei käyttäisi aktiivisesti omaa tietokonettaan, häneen voi kohdistua esimerkiksi suoramainonnan tungettelua. Siis osoitetiedot ovat joutuneet vääräIle omistajille tai käyttäjä on vain jakanut tai luvannut varomattomasti tietonsa erilaisten rekisterinpitäjien käyttöön. Toisaalta myös henkilörekisterilakiin kohdistuvia rikkomuksia on tapahtunut.

Asioitaessa suurissa ketjuuntuneissa tavarataloissa ja keskusliikkeiden myymälöissä on totuttu siihen, että vuoden mittaan ostoksista saa tietyn prosentin palautusta, kun käyttää asiakaskorttia. Kansalaisista kerätään ostosten maksamisen yhteydessä erittäin paljon tietoa, muutakin kuin palautukseen liittyvää. Tämä tieto paljastaa harjaantuneelle tutkijalle henkilön kulutustottumukset ja myös käyttäytymistapoja. On tultu alueelle, jossa voidaan kysyä, haluaako asiakas todella luopua kyseisistä yksityisyyteensä liittyvistä, sinänsä vaarattoman tuntuisista tiedoista. Edelleen voidaan kysyä, voiko niitä saada käyttöönsä myös joku ulkopuolinen?

Ihmisten terveyteen liittyvät tiedot ovat myös luottamuksellisia. Jos henkökunnassa on esimerkiksi sellaisia henkilöitä, jotka eivät vajavaisen koulutuksensa takia ymmärrä suojella asiakkaiden tietoja, tulossa on suuria ongelmia.

Kun kansalainen siirtyy tietokoneen käyttäjäksi, hän voi joutua sähköpostia käyttäessään monien ongelmien vaivaamaksi. Vaikka sähköpostiviestillä on kirjesalaisuuteen verrattava suoja, monia väärinkäytöksiä on sattunut. Aikaisemmin jouduttiin toimimaan sen periaatteen mukaisesti, että salaista viestiä ei lähetetty sähköpostin välityksellä. Nyt on osoittautunut, että varsin vähän informaatiota sisältävissä salaamattomissa viesteissäkin voi olla ulkopuolisille sieppaamisen arvoista tietoa, esimerkiksi muita sähköpostiosoitteita. Selväkielisenä lähetetyt viestit tulevat ilmeisesti poistumaan käytöstä lähivuoden aikana.

Käyttäjän liikkuessa verkoissa hänestä jää jäljet ketjun kumpaankin päähän ja lisäksi kaikkiin niihin palvelimiin, joiden kautta hän on tietoisesti tai tietämättään kulkenut. Vaatimattomallakin ammattitaidolla on mahdollista saada verkoissa liikkuvan henkilön jäljet, jopa viestit selville. Verkoissa liikuttaessa salaus tulee välttämättömäksi toimenpiteeksi.

Henkilön yksityisyyden (privacy) suojaamiseksi on tärkeää, että hän ei kerro tarpeettomia asioita itsestään esimerkiksi sähköpostin osoiteosassa tai kotisivullaan. Jo sallimalla sähköpostiosoitteensa julkisen levittämisen henkilö voi joutua roskapostin (spam) uhriksi. Kotiosoitteen ja henkilötunnuksen sekä valokuvan julkaiseminen verkossa on arvelluttava riski, erityisesti suomalaiset henkilötiedot ovat kansainvälisten rikollisten suosiossa. Jos henkilö liittää vielä asuntonsa pohjapiirroksen mukaan kotisivulleen ja kertoo olevansa tietyn jakson matkoilla, voiko parempia vihjeitä ammattirikollisille enää antaa?

Sähköinen kaupankäynti, asioiminen viranomaisten kanssa ja maksaminen sekä tuotteiden toimitus tietoverkkojen kautta ovat lähivuosina myös suuremman kansalaisjoukon arkisia rutiineja. Ensimmäinen kysymys on henkilöllisyyden todistaminen. Tässäkin yhteydessä puhutaan aitoudesta eli käyttäjän todentamisesta (authensity) ja kiistämättömyydestä (non-repudiation). Henkilön sähköinen tunnistaminen (HST) kyseisen toimikortin avulla perustuu digitaaliseen allekirjoitukseen. Tekniseen ratkaisuun liittyy myös todentamisessa käytettävät autentikointimenetelmät ja –protokollat.

Kansalaisiin ja tietokoneen käyttäjiin kohdistuvat tietoturvauhkat ovat varsin monentyyppisiä. Suojautuminen on aloitettava tietotekniikan ymmärtämisestä ja käytön oppimisesta. Seuraava vaihe liittyy tietoturvan perusratkaisujen käyttöönottoon. Aluksi voidaan käyttää tietokoneen käyttäjän perusohjeita tietoturvasta, samoin julkisesti saatavilla olevia salaustuotteita. Kun perusasiat on kunnossa, tarvitaan tietoturvatietämyksen lisäämistä. Vuosien päästä nämä välivaiheet ehkä käyvät tarpeettomiksi, siirrytään suoraan käyttämään tietoturvallisia ratkaisuja. Jos tällainen läpinäkyvä turvallinen tietoyhteiskunta joskus toteutuu, voidaan jo nyt kysyä, mihin ovat joutumassa nämä nykyiset tietoturvauhkat ja niiden parissa työskentelevät rikolliset? Mitä uusia väärinkäytöksien mahdollisuuksia ihmiset voivatkaan luoda?

## 4. ORGANISAATION TIETOTURVAN HALLINTA

Koko organisaation tietoturvaohjeistuksen peruskysymys on, että korkein johto ymmärtää tieturvan tärkeyden, hyväksyy tietoturvaratkaisut ja kannattaa tietoturvakoulutusta ja työntekijöiden

ammattitaidon tason nostoa. Tämä tarkoittaa myös, että ylin johto sitoutuu tietoturvaratkaisuihin. Nämä ovat kovia vaatimuksia, kun organisaatioissa jatkuvasti mietitään uusia säästöjä ja toimintojen ja kulujen karsimisia. Monessa yrityksessä on vielä vallalla vanha ajattelutapa, että tietoturva maksaa paljon, mutta ei tuota mitään.

Organisaation johdon kannalta tärkeää olisi luoda tietoturvaorganisaatio, joka on suoraan ylimmän johdon alainen. Sen on siis valvottava koko organisaation tietoturvaa, sekä hyväksikäyttäjien että myös eri johtoportaiden. Jos puhumme hyväksikäyttäjien tietoturvaohjeista, niin vastaavasti organisaation ylimmän johdon vastuulla on, että organisaatiolla on kattava ja ajantasalla oleva tietoturvapolitiikka.

Pienille ja keskisuurille organisaatioille oleellista on, että niillä on tietoturvaohjeet työntekijöilleen ja tulevaisuudessa myös oma tietoturvapolitiikka. Vaikka varsinaisia tieturvahenkilöitä ei olisikaan, jokaisen työtekijän ja organisaation johdon on ymmärrettävä tietoturvan merkitys ja se, että tietoturva koskee organisaation jokaista jäsentä.

Jos siirrytään tarkastelemaan suurta organisaatiota, huomataan, että siellä tarvitaan yhä laajempia tietoturva- ja turvallisuusohjeita. Myös varsinaisia tietoturva-alan ammattilaisia tarvitaan. Mutta on muistettava, että tietoturvasta huolehtimisen täytyy olla organisaation jokaisen henkilön velvollisuus.

1980 -luvun lopulla suuren organisaation tietoturvaohjeistus nähtiin laajana kokonaisuutena. Puhuttiin ns turvajärjestelmästä. Ylimpänä komponenttina oli kohdejärjestelmän tietoturvapolitiikka. Sen alapuolella oli atk -tietoturvapolitiikka ja atk -tietoturvamalli, joka sisälsi tietoturvallisuusstrategian, noudatettavat linjat, menetelmät ja tarkistuslistat, toimenpiteet ja seurannan (Saari 1988).

Brittien käyttämä standardi (BS 7799, 1999a) on tietoturvallisuuden hallintajärjestelmiä koskeva menettelyohje. Siinä lähdetään tietoturvallisuuspolitiikasta ja käydään läpi osa-alueet: tietoturvallisuuden organisointi, tietoaineistojen luokitus ja valvonta, tietoturvallisuus henkilöstön kannalta, fyysinen turva ja turva ympäristöä vastaan, tietokoneiden ja tietoverkkojen hallinta ja järjestelmään pääsyn valvonta. Standardin toisessa osassa (BS 7799, 1999b) esitetään tietoturvallisuuden hallintajärjestelmiä koskevia vaatimuksia, kuten hallintakehyksen luominen, toteuttaminen, dokumentointi, dokumenttien valvonta ja tallenteet. Samoin esitetään valvontatoimet eriteltyinä.

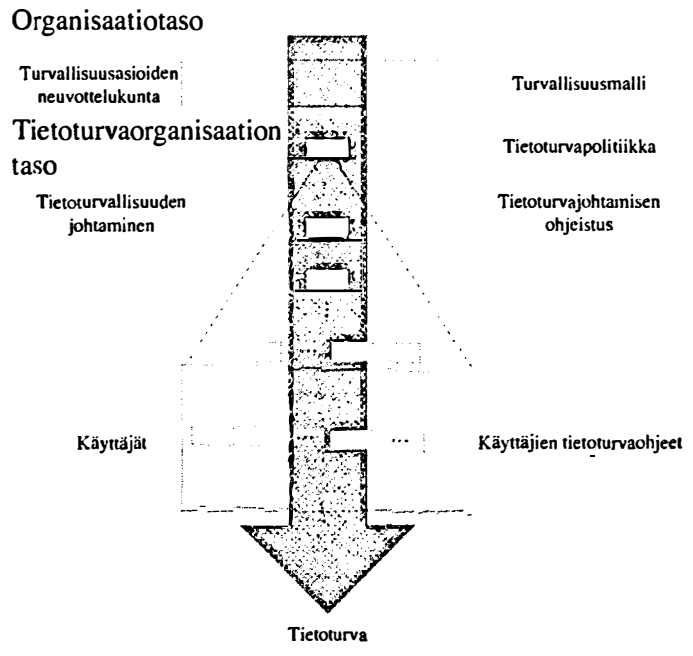
Miettinen (1999) esittää tietoturvallisuuden johtamisen välineinä päivittäisestä toiminnan johtamisesta siirtymisen toiminnan suunnitteluun aikajänteellä 0-1 vuotta, lyhyen aikavälin suunnittelun (1–3 vuotta) strategioineen ja politiikkoineen ja pitkän aikavälin suunnitteluun (3–5 vuotta), johon kuuluu yrityksen visiot ja arvot. Yrityksen olemassaolon tarkoitus on kiteytetty toiminta-ajatuksessa. Tietoturvallisuuden johtamisen päävaiheet ovat riskien tunnistus, suojaustason määrittely, suojausten suunnittelu, suojausten toteutus, suojausten valvonta, suojaustason kehittäminen ja suojaustason mittaaminen.

Valtiovarainministeriö (1999) esittää, että tietoturvallisuuden hallintaa ja ohjausta varten viranomaisilla tulee olla ajantasainen tiedonkäsittelyn turvaamissuunnitelma ja poikkeusolojen varalta tiedonkäsittelyn valmiussuunnitelma. Suunnitelmiin sisältyy organisaation tiedonkäsittelyriippuvuuden, tietotekniikan käyttöön liittyvien uhkatekijöiden ja riskien arviointi sekä niiden hallinnan edellyttämien turvaamis-, toipumis- ja varautumistoimenpiteiden määrittely ja toteuttamissuunnitelmat.

2000 –luvun alussa ovat kaikki edellisten vuosikymmenten turvallisuuden ja tietoturvan kehittämiseen liittyvät ohjeet voimassa. Jos aikaisemmin tietoturvauhkat kohdistuivat sisäpiiriasioihin, viruksiin, tunkeutumisiin ja puhelinliikenteeseen, niin nyt meillä on uusi tilanne. Internet –maailma on auennut nopeasti erittäin suurille joukoille. Internetin kattavasta tietoturvasta ei voida edelleenkään puhua, toisaalta Internet tuo kaikkien uhkakuvien lisäksi uusia mahdollisuuksia.

Modernissa organisaatiossa voidaan tietoturvan hallintaa tarkastella useilla eri tekniikoilla. Tietoturvan hallinta sisältää tietoturvatarpeiden jäsentelyn ja suunnittelun. Tähän kuuluu myös tietoturvastrategian ja -tavoitteiden seuranta sekä tietoturvapolitiikan määrittäminen. Painopiste on riskien arvioinnissa sekä riskianalyysien ja hallintaprosessien suoritustavassa. Tietoturvan hallintaan kuuluu myös tietoturvan suojakeinojen (Controls) toteuttaminen tietoturvasuunnitelman mukaisesti ja niiden jatkuva seuraaminen ja soveltuvuuden testaaminen sekä yleisesti kokonaisvaltaisen tietoturvastrategian vaikutusten seuraaminen.

Kuvassa 2 on esitetty suuren organisaation




***Kuva 2.*** *Tietoturva organisaatiossa*

tietoturva. Oleellista siinä on, että tietoturva menee läpi koko organisaation, "top–down". Ylin johto, kuvassa turvallisuusasioiden ohjausryhmä/ neuvottelukunta, määrittää turvallisuusmallin, jossa on esitetty tietojen ja informaation käsittelyn turvallisuus, lakisääteiset turvakysymykset, organisaatioon mahdollisesti kohdistuvat rikolliset toimenpiteet ja organisaation eri ryhmittymien välinen yhteistyö. Turvallisuusasioiden ohjausryhmän on nämä asiat organisoitava ja työhön liittyvät vastuut on yksiselitteisesti määriteltävä. Samoin turvallisuusasioiden johtoryhmä osoittaa varat tai resurssit tietoturvatyöhön, kuitenkin korostaen kustannustehokkuutta. Johtoryhmän on myös määritettävä, miten käytännön turvatoiminnot organisoidaan ja vastuutetaan. Samoin tietoturvaorganisaation rakenne on määriteltävä.

Kuvassa 2 on esitetty myös käytännön turvallisuustyön johtaminen ja loppukäyttäjien ohjeistus.

Tietoturvan hallintaprosessi koostuu pienemmistä osaprosesseista ja on luonteeltaan jatkuva prosessi. Olennainen osa siinä on katselmoinnit, joita voidaan tehdä jatkuvasti tietyin aikavälein järjestelmän elinkaaren aikana. Katselmointeja seuraa toimenpiteitä, joilla korjataan suojakeinoissa mahdollisesti havaittuja puuteita, tai toteutetaan uusia tietoturvaa parantavia menetelmiä. Jos järjestelmään tehdään suuria muutoksia, tulee riskit arvioida uudelleen, jotta tietoturva olisi ajantasalla järjestelmän kehityksen kanssa. Suojaukset havaituille heikkouksille tulee suunnitella ja toteuttaa mahdollisimman pian. Uusiin suojauksiin liittyy omat haavoittuvuutensa ja ne saattavat synnyttää uusia riskejä. Tämän vuoksi suojausmenetelmien valinnassa on käytettävä huolellisuutta, jotta todettuja riskejä todella vähennetään eikä uusia synnytetä.

Tietoturvan hallintaprosessiin kuuluu oleellisena osana tietoturvaosaamisen ja -tietämyksen varmistaminen. Tietoturvatietämystä lisäävän koulutusohjelman tiedot tulee antaa niin organisaation johdolle kuin organisaation alemmilla tasoilla työskenteleville henkilöille. Koulutusohjelman sisältö voi vaihdella kohdehenkilön työnkuvan mukaan. Organisaation kokonaisvaltainen tietoturvan koulutusohjelma kehitetään ja toteutetaan vaiheittain siten, että jokainen vaihe rakentuu edellisen vaiheen päälle.

Tietotekniikan hyväksikäyttäjän kannalta oleellista on, että tietoturvaohjeita on monenlaisia.

Työaseman ja mikrotietokoneen käyttäjällä on tietyt perusohjeet ja virusten torjuntaan omat ohjeet. Lisäksi organisaatiossa voi olla käytössä langattoman puhelimen käytön (NMT, GSM, sisäinen) tietoturvaohjeet, faxin käyttäjän tietoturvaohjeet, UNIX -käyttäjän tietoturvaohjeet, UNIX -ylläpitäjän tietoturvaohjeet, verkon käyttäjän tieto-turvaohjeet, Internetin käyttäjän tietoturvasuositukset jne.

Moniin muihinkin asioihin on tarpeellista laatia omat tietoturvaohjeet. Keväällä 1995 osallistuimme "Information Security in Outsourcing" – yhteistyöprojektiin (Kajava ym 1995). Siinäkin laadittiin oma tietoturvaohjeensa, tarkastelukulma oli sidoksissa asiakkaaseemme, joka suorittaa ohjelmistojen ja järjestelmien ulkoistamista. Tuloksena oli ohjeisto, joka soveltui useisiin ulkoistamisprosesseihin, mutta esiintyi myös useita tapauksia, joihin se oli liian tarkka tai kokonaan sopimaton. Seuraavana vaiheena oli laatia yleisemmällä tasolla oleva ulkoistamisen tietoturvapolitiikka palvelua tarvitsevan asiakkaan vaatimusten mukaan. Jos tarkastellaan yhä laajempia kokonaisuuksia, niin esimerkiksi ohjelmistojen ulkoistamiseen tarvittaisiin useita rinnakkaisia tietoturvapolitiikkoja (Kajava & Jurvelin 1996).

On syytä olla varovainen, ettei työntekijöiden koko työskentelyprosessia sidota liiaksi kaikenlaisiin ohjeisiin ja rajoituksiin. Esimerkiksi organisaation tietoturvapolitiikan tärkeyttä, jopa välttämättömyyttä korostetaan. Kuitenkaan pelkkä tietoturvapolitiikka, ei myöskään erilaiset hyväksikäyttäjien tietoturvaohjeet, ole tärkeitä. Mutta erittäin tärkeää on, miten vaatimukset toteutetaan ja miten tätä prosessia valvotaan.

Edellä esitetyssä kuvassa 2 on kyseessä suuri organisaatio. Jotta tietoturva toteutuisi mahdollisimman hyvin, on työvaiheita, joissa asioiden on tapahduttava juuri annettujen ohjeiden mukaan, ylhäältä alas. Nykyaikana tällainen asioiden hoitaminen käskyttämällä, imperatiiveilla, aiheuttaa myös vastustusta. Aina tulee turva-alueella olemaan kuitenkin sellaisia osioita, joihin vain tiukat määräykset pätevät. Mutta on myös sellaisia alueita, joissa käyttäjien mielipiteet voidaan toteuttaa tai asioista voidaan yhdessä keskustella, jopa parantaa organisaation toimintaa.

Tietoturvan hallinnalla pyritään systemaattisesti ennalta torjumaan organisaatioon kohdistuvia todennäköisiä uhkia. 20 vuotta sitten tietojenkäsittely-ympäristö oli vielä keskuskoneeseen sidottu ja todennäköisimmät uhkat tulivat organisaation sisältä. Nyt olemme palanneet lähtötilanteeseen sikäli, että ulkoa tulevista uhkista valtaosa pystytään torjumaan, mutta sensijaan sisäpiiriin liittyvät tapaukset käyvät yhä hankalammiksi selvittää.

Helmikuussa 2000 julkisuuteen on jälleen tullut tapauksia, joissa liikeyrityksen toiminnat on pystytty tyrehdyttämään suorittamalla ns. palvelujen estäminen hajautetulla sähköpostihyökkäyksellä. Kun samaa kohdetta pommitetaan useista työasemista yhtä aikaa, on selvää, että järjestelmän toiminta saadaan estettyä. Tämäkin tilanne on sikäli poikkeuksellisen hankala, että tällaista hajautettua palvelujen estoa varten on verkon kautta saatavissa valmiita työkaluja.

Yritysten kannalta jatkuva ongelma on erilaiset hakkerien suorittamat hyökkäykset. Järjestelmiä ei koskaan saada täysin aukottomiksi, alinomainen valvonta ja myös hyökkäysten torjunta sitoo resursseja. Suomessa ei ollut tuomioistuinten päätöksiä hakkeritapauksista vielä viime vuodelta saatavana, nyt uudella vuosituhannella on eräs tapaus saatu päätökseen ja seuraava varsin laaja juttu tulee oikeuskäsittelyyn. Aikaisemmin jopa jotkut tuomarit eivät käsittäneet, kuinka vakavia ongelmia hakkerien toiminnasta aiheutuu.

Vuonna 2000 on ilmennyt useita sähköpostiviestien sieppaamisia. Jotta näiltä voitaisiin ainakin osittain välttyä, tulee koko sähköpostiliikenne yritysmaailmassa siirtymään salattuun muotoon. Maaliskuussa 2000 hakkerit tunkeutuivat Englannissa sähköisen kaupankäynnin järjestelmään ja saivat haltuunsa yli 20 000 henkilön luottokorttien tiedot. Vastaavia viestejä on tullut myös USAsta.

Teollisuusvakoilu tulee yhä keskeisemmäksi ongelmaksi. Ilmitullut Yhdysvaltain turvallisuudesta vastaavan järjestön National Security Agencyn (NSA) organisoima vakoilu Euroopan Unionin sisäistä liiketoimintaa kohtaan aiheuttaa sen, että tietoturvallisuutteen liittyvät asiat tulevat vielä nykyistäkin tärkeämmäksi. Jo muutamia vuosia tiedossa ollut, mutta vasta nyt laajempaa julkisuutta saanut ns ECHELON -tiedustelujärjestelmän käyttö on herättänyt kansalliset hallitukset. EU:n julkituoman tutkimusraportin ydin on, että rakennetun maailmalaajuisen järjestelmän avulla Yhdysvaltain kansallisen turvallisuuden virasto pystyy sieppaamaan käytännössä kaikki

puhelin- ja sähköpostiviestit ja seulomaan niistä kiinnostavan aineiston avainsanoihin perustuvan hakujärjestelmän avulla. Esimerkkinä EU:n keskuudessa käytävästä keskustelusta voisi olla arviointi teknologioihin liittyvistä poliittisista kontrolleista ( EUROPEAN PARLIAMENT, 1998).

ECHELON –järjestelmän paljastuminen on osoittanut todeksi väitteet, ettei mikään viestiliikenne ole salassa vakoilulta. Mutta tilanne on nyt johtamassa Euroopan Unionin sisällä keskusteluihin, joissa väitetään, että NSA on vaikuttanut kaikiin niihin ohjelmistoihin, joita Microsoft, Netscape ja Lotus myyvät Yhdysvaltain ulkopuolelle. Lisäksi väitetään, että lähes kaikissa tietokoneissa olisi sisälläjärjestelmä, jonka avulla NSA pystyisi murtamaan salauksen ja saamaan viestien sisällöt selville. Myös keskustellaan siitä, että Yhdysvaltain ulkopuolelle myytävien järjestelmien turvatasoa olisi tietoisesti alennettu.

Usean vuoden ajan Euroopassa on keskusteltu siitä, miten Yhdysvallat on rajoittanut myymiinsä tietoturvatuotteisiin liittyvää salausta. Kysymys on ollut nimenomaan salauksessa käytettävien merkkijonojen pituudesta. On tullut ilmi, että määrätyt heikkoon salaukseen perustuvat turvatuotteet on pystytty liian helposti avaamaan. Sen sijaan sellaisia tuotteita, jotka käyttävät vahvaa salausta, on ollut vaikeaa saada käyttöönsä. Toisaalta tietoturvakysymysten kanssa työskentelevät ovat vuosien ajan olleet tietoisia siitä, että Internetin kautta on ollut saatavana monenlaisia hakkerien työkaluja, joilla myös salauksia pystytään murtamaan. Uutta ei ole myöskään se, että tärkeää viestiä ei ole järkevää lähettää sähköpostin kautta edes suojattuna, ei Internetin kautta, ei myöskään puhelimen välityksellä. Kun nyt Suomessakin pyritään siihen, että sähköpostiliikenne salataan, niin voimme ehkä salata todellisuudessa viestit toisiltamme, mutta mitä ilmeisimmin niin ammattivakoojat kuin ammattirikollisetkin saavat ne auki, jopa helposti. Tärkeät viestit on syytä saattaa perille varmemmilla viestiyhteyksillä.

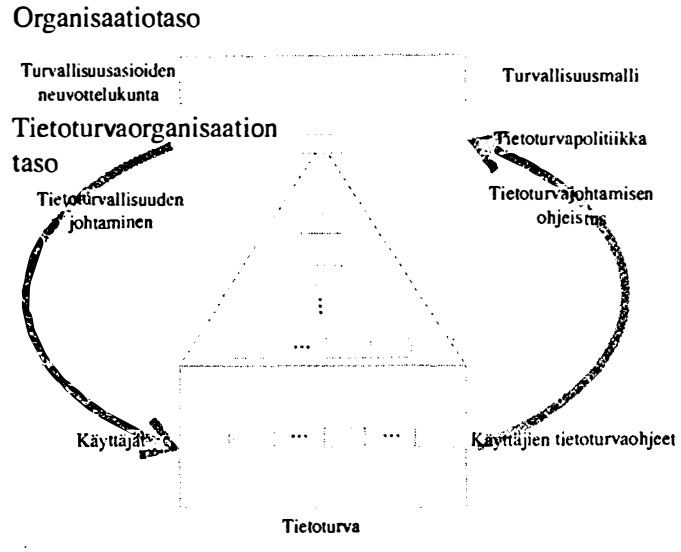
Organisaation tietoturvan hallinnalle tullaan asettamaan jo lähiaikoina huomattavan paljon suurempia vastuita. Vaikka vakavimmat tietoturvan loukkaukset eivät pääsekään julkisuuteen, jo esille tulleet tapauksetkin osoittavat, kuinka tärkeää on luoda koko organisaation kattava hyvä tietojenkäsittelytapa.

## 5. KÄYTTÄJIEN HUOMIOIMINEN TIETOTURVATYÖSSÄ

Osa organisaatioiden toiminnasta on sellaista, että on vain yksi määrätty tapa hoitaa tehtävät. Mutta on myös tehtäviä, joiden mielekäs suoritustapa voidaan yhdessä päättää. Silloin parempi vaihtoehto on antaa ensin suosituksia ja pyytää niistä palautetta sellaisilta henkilöiltä, joiden tehtäväkentään kyseiset tietoturva-asiat keskeisesti liittyvät. Tuloksena voi olla vuorovaikutteinen, osallistuva työskentely, jossa jokainen alueen työntekijä voi osallistua työskentelyympäristön parantamiseen.

Kuvassa 3 on esitetty jatkuva vuorovaikutteinen tietoturvallisuuden parantamiseen liittyvä prosessi. Jokainen työntekijä tuntee olevansa tärkeä. Tätä korostaa vielä se, että myös tietoturvasta vastaava johto osallistuu keskusteluun ja yhdessä kehitetään parempaa ja turvallisempaa työskentely-ympäristöä. Tämä prosessi on jatkuvaa työtä. Tietotekniikan yhteydessä jokainen uusi kehitysaskel tuo lukuisia uusia uhkia. Onnistunut työntekijöiden ja organisaation turvallisuusjohdon vuoropuhelu tarkoittaa myös sitä, että yhdessä parannetaan paitsi työympäristöä myös sen tietoturvatietoisuutta.

Uudet haasteet osoittavat, että tietoturvan loukkauksiin joudutaan varautumaan yhä laajemmin. Kun yhteydet ulkomaailmaan on saatu turvalliselle tasolle, yhä suurempi uhka järjestelmän toiminalle on jälleen kahden vuosikymmenen jälkeen oma henkilökunta. Esimerkiksi asianmukaisesti hoidettu intranet –ratkaisu rajoittaa ulkopuolisten pääsyn järjestemään suhteellisen hyvin. Ongelmaksi tulevat omat käyttäjät liikkuessaan toimitilojensa ulkopuolella. Helmikuussa 2000 on paljastunut eräs sisäpiiriläisen tekemä vakava rikos, joissa tekotapa on samantyyppinen kuin 20 vuotta aikaisemmin tehdyissä vastaavissa rikoksissa, mutta tekniikka nykyaikainen. Jos aikoinaan pankkivirkailija ohjasi ihmisten tilienhoidon yhteydessä laskutoimituksissa syntyneet pennien murto-osat omalle tililleen ja jäi kiinni, niin vuonna 2000 on ilmennyt esimerkiksi tapaus, jossa pitkään organisaation sisällä luottamuksellisissa tehtävissä toiminut asiantuntija oli ohjannut osan asiakkaille osoitetuista korvauksista omalle tililleen. Kun prosessissa ulkopuolisena oleva pankkivirkailija oli alkanut ihmetellä rahavirtojen kulkua, asia selvitettiin ja rikokseen syyl-




***Kuva 3.** Vuorovaikutteinen tietoturva organisaatiossa*

listynyt saatiin kiinni. Tämäkin tapaus osoittaa, kuinka tärkeitä organisaatioiden sisäiset kontrollit ovat. Mutta osoittakoon tämä tapaus myös sen, että vaikka tietoturvaan kohdistuu yhä uudenlaisia uhkia, niin myös kaikki entiset uhkat ovat olemassa.

Henkilöiden taustojen tarkistus oli tärkeä kriteeri valittaessa työntekijöitä 1990 –luvun alussa yrityksiin. Nyt yksityisyyteen liittyvät seikat tarkoittavat, että taustan selvitys ei ole tavalliselle yrittäjälle helppoa. Jo sopimattomasta työntekijästä eroon pääsy on vaikeaa, mutta jos työntekijällä on myös rikollisia taipumuksia ja tietotekniikan osaaminen hallussaan, hänen aiheuttamansa vahingot voivat olla arvaamattoman suuret.

Samalla kun organisaation sisäpiiriuhkien merkitystä tarkastellaan uudelleen, myös fyysiset turvatarkastukset tehostuvat. Meillä tilanne on konkreettisesti näkynyt siten, että lennolle lähtevien matkustajien on alistuttava varsin tarkkoihin turvatarkastuksiin. Oleellista on, että matkustaja ei pääse kuljettamaan koneeseen esimerkiksi räjähtävää pommia. Jos tarkastelua laajennetaan Suomesta koko maailman käsittäväksi, niin on maita ja "kulttureja", joissa esimerkiksi rikollisten kanssa yhteistyöstä kieltäytyviä virkamiehiä on muistettu kirjekuoreen pakatulla muovipommilla. Myös varautuminen tämänkaltaisiin sabotaaseihin tulee aikanaan mietittäväksi myös Pohjoismaissa. Tosin pommi ei ole ensi sijassa tietoturvauhka, mutta kirjeeseen sijoitettuna jo lähempänä.

Sisäiset kontrollit ovat tulleet myös yhä tärkeämmiksi. Oleellista on, että kaikkia organisaatiossa toimivia henkilöitä voidaan seurata ja tarkkailla, ehkä ylintä johtajaa lukuunottamatta. Hän on myös sisäisen tarkastuksen ylin vastuuhenkilö. Organisaatioissa esiintyy usein keskustelua siitä, miten sisäinen tarkastus ja tietoturvatyö organisoidaan yrityksen hierarkian sisällä. Jo vastuu sisäisestä tarkastuksesta tulisi olla suoraan kytkettynä ylimmän johtajan toimenkuvaan, tietoturvaan liittyviä vastuita näyttää organisaatioissa haluavan niin tietohallinnosta vastaavan yksikön johto kuin atk –keskuksen johtokin. Mutta tietoturvayksikön on pystyttävä kontrolloimaan myös kyseisiä yksikköjä suoraan yrityksen hallituksen tai toimitusjohtajan alaisena.

Koska sisäpiiriuhkat ovat voimistuneet viime aikoina huomattavasti, niin yritysten on valvottava työntekijöitään entistä voimakkaammin. Kuitenkin yleinen suunta on kohti vapaampaa yhteiskuntaa, ihmisiin luottaen. Mutta luottamuksen voi rikkoa tuhansien työntekijöiden joukossa yksi häirikkö. Todennäköisyys sille, että isossa jou-

kossa on yksi häiriintynyt, on varsin suuri. Jos lisätään paineet työpaikalla ja myös yksityiselämässä, näitä häiriintyneitä voi ilmaantua enemmänkin kuin vain edellä mainittu yksilö.

Huumeiden käyttö maailmalla on lisääntynyt huomattavasti. On mahdollista, että myös Suomessa suuressa työntekijäjoukossa on käyttäjä tai jopa muutamia. Jos heitä ei saada valvontaan ajoissa, on odotettavissa erittäin suuria menetyksiä. Vanha ennakkoluulo on luokitella kyseisten aineiden käyttäjät "laitapuolen ihmisiksi", mutta on muistettava, että monet tietotekniikan asiantuntijat työskentelevät pitkiä aikoja paineiden alaisina. Silloin sortuminen on jonkun kohdalla mahdollista. Jos tällainen henkilö käsittelee kaikkien arkaluonteisimpia tietoja, menetyksiä ei voida myöhemmin korvata. Siksi on odotettavissa, etta huumetestit tulevat lähivuosina paitsi kouluihin, myös tietotekniikan huippuyrityksiin.

Jos vuorovaikutteista työskentelyilmapiiriä halutaan myös jatkossa korostaa ja arvostaa, tietoturvasta pitäisi pitemmällä ajalla rakentaa huomaamaton, läpinäkyvä komponentti. Tietoturvatietoisuuden lisääminen tulisi olla perussuunta organisaation toimintaa kehitettäessä, mutta organisaatiolla tulisi olla välineet ja mahdollisuudet poimia ja poistaa haitallinen komponentti keskuudestaan. Jopa sellainen ihminen, joka ei toimi yrityksen toimintaperiaatteiden ja toiminta-ajatuksen mukaisesti, vaan vahingoittaa yritystä.

2000 –luvun alussa Suomessakin on alettu keskustella siitä, kenellä on oikeus avata sähköpostisanomia. Periaatteena on ollut, että sähköpostilla on sama lainsuoja kuin kirjeillä, kirjesalaisuus. Asiaan on tullut lisäväriä, kun työntekijä on poistunut yrityksestä. Jos työnantaja on kustantanut henkilökunnalleen tietojärjestelmän ja verkkoyhteydet työntekoa varten, voiko hän myös aukaista viestit, jotka oleellisesti liittyvät työnantajan liiketoimintaan?

Voidaan sanoa, että eräissä yrityksissä työntekijät menettivät yksityisyytensä jo siinä vaiheessa, kun maisemakonttorit tulivat muotiin. Sähköpostin henkilökohtaisuudesta tultaneen jatkamaan kekusteluja lakituvassa. Koska työntekijöiden mahdollisuudet syyllistyä sisäpiirin rikoksiin ovat kuluneen talven aikana nousseet erittäin oleellisiksi uhkiksi, kun ulkoa päin tulevat uhkat on pystytty paremmin torjumaan, työntekijöiden huomaamaton tarkkailu tulee yhä tärkeämmäksi. Kun aikoinaan pankkitoiminnassa virkailijoiden työtä yritettiin muuttaa voimakkaammin tulospalkkauksen suuntaan, päätelaitteisiin sijoitettiin laskurit, jotka ilmaisivat, kuinka monta näppäilyä henkilö teki ja kuinka monta kertaa hän käytti korjausnäppäintä työpäivän aikana. Kun henkilöt tiesivät tämän sisäisen kontrollin olemassaolon ja vaikutuksen, se aiheutti lisää paineita ja myös uusia virheitä. Nyt vuosikymmenien jälkeen kansainvälisissä yrityksissä mietitään, kuinka työntekijää voitaisiin kontrolloida entistä paremmin. Kameravalvonta on yksi suunta, tietokoneen näytön seuranta toinen, puhelimen seuranta kolmas vaihtoehto. Jos verrataan toimintaa esimerkiksi pankkiautomaatteihin liitettyjen valvontakameroiden toimintaan, niin kyseessä on pohjimmiltaan samantyyppisestä toiminnasta, jossa taltioidut tapahtumat voidaan palauttaa uudelleen käsittelyyn rikoksen selvittelyssä. Mutta nyt on se ero, että pankkiautomaatin valvontakamera taltioi laitteen toimintaan liittyviä tapahtumia laitteen ulkopuolelta, keskusteluissa esillä olevat ratkaisut taltioisivat yhden henkilön toimintaa oman työasemansa ääressä tai vieläpä laitteen sisällä.

Jos keskustelu on siirtymässä läpinäkyvään turvalliseen, pelotteilla maustettuun työskentely-ympäristöön, niin onko mahdollista, että työskentely tärkeillä paikoilla kestäisi vielä nykyistä tarkemman kontrollin. Jo nyt yhteiskunnan avainhenkilöiden on julkistettava omaisuutensa ja velkansa ennen uuden toimen vastaanottamista. Mutta työntekjän yksityisyys työpaikalla, voidaanko siitä edes keskustella. Millaista yksityisyyttä esimerkiksi läpinäkyvä yksityisyys olisi?

## 6. TIETOTURVATIETOISUUDEN LEVITTÄMINEN

1990 –luvun alussa tietoturva-asiat näyttivät ratkeavan hyväksikäyttäjien ohjeiden tekemisellä ja niiden noudattamisen seurannalla sekä asiaan kuuluvilla tietoturvaratkaisuilla. Seuraava vaihe oli, että hyväksikäyttäjien muuta tietotekniikan osaamista oli laajennettava.

Tietoturvatietoisuutta (Information Security Awareness) ei pidä rajoittaa työntekijöiden valmennukseen eikä myöskään siihen kuvitelmaan, että organisaation kaikki jäsenet kuuliaisesti noudattaisivat annettuja ohjeita ja määräyksiä. Oppiminen on eräs perustekijä nostettaessa

tietoturvatietoisuutta, koska oppiminen vaikuttaa positiivisesti käyttäytymiseemme (MacLean 1992). Tämä on kuitenkin vasta minimitaso, jota ei aina kirjallisuudessa tietoturvatietoisuuden yhteydessä edes huomioida oppimisprosessiin, vaikka näin tulisi olla. Tietoturvatietoisuus pitäisi pystyä esittämään tiivistetysti ja hyvin organisoidusti alusta alkaen. Suoritettua toiminnan tehokkuutta pitäisi pystyä mittaamaan, jotta voitaisiin vakuuttua organisaation tietoturvatietoisuuteen liittyvän ohjelman pätevyydestä. Mitä erilaisimpia menetelmiä ja työkaluja tarvitaan toteutettaessa tietoturvatietoisuutta, koska on hyvin erityyppisiä henkilöitä ja tehtäviä, samoin työympäristöt ovat hyvin vaihtelevia. Tarvitaan siis monentyyppistä tietoturvatietämystäkin. Turvakoulutusta tarvitaan ensinnäkin siksi, että jokainen käyttäjä sisäistäisi sen, kuinka tärkeätä on seurata annettuja ohjeita. Käyttäjille on tehtävä selväksi myös tietoturvaloukkauksien seuraukset (Straub ym. 1992). Koulutusta tarvitaan myös, jotta haluttu tietoturvatietoisuuden taso ylläpidettäisiin (Kajava 1996). Ihmisten mieliin asioiden tärkeyttä voidaan korostaa erilaisilla tietoisuuden kohottamismenetelmillä, kuten kampanjoinnilla (ks. alla luku 6.1) ja Hammerin menetelmällä (ks. alla luku 6.2).

### *6.1. Tietoturvatietoisuuden kohottamisen menetelmät*

Tietoturvatietoisuuden vaiheet ovat seuraavat:

- ihmisten huomio kiinnitetään turva-asioihin
- hankitaan käyttäjähyväksyntä
- käyttäjät saadaan oppimaan ja sisäistämään tietoturvatoimenpiteiden välttämättömyys.

Ensimmäisessä vaiheessa ihmisten huomio suunnataan tietoturvaan liittyviin asioihin ja yritetään saada heidät kiinnostumaan. Toinen vaihe liittyy käyttäjähyväksyntään. Jos tässä on onnistuttu, on tärkeää saada käyttäjät myös hyväksymään oman organisaationsa tietoturvapolitiikka. Kolmannessa vaiheessa käyttäjät ovat sisäistäneet turvakoulutuksessa saamansa tiedot ja taidot ja osallistuvat organisaation tietoturvapolitiikan mukaiseen toimintaan. Tutkimuksissa käytetään näitä kolmea vaihetta kuvaamaan tietoisuus -termin saavuttamista.

Voidaan sanoa, että tietoisuus on kaikkien järjestelmien suurimpien heikkouksien paras varotoimenpide, ja silloin tarkoitetaan nimenomaan inhimillistä tekijää (Ceraolo 1996). Tietoturvatietoisuus ohjelmana olisi toteutettava organisaation kaikilla tasoilla lähtien yrityksen korkeimmasta johdosta, jonka pitäisi olla tietoinen siitä, että organisaatiolle pitäisi saada aikaan tietoturvapolitiikka ja sitä pitäisi ylläpitää (ISO-IEC-27, 1995). Tätä seuraa turvallisuusmallin luonti ja sen jälkeen tietoturvapolitiikka vastuiden määrityksineen (Kajava & Siponen 1996). Tietoturvatietoisuus ohjelmana tarkoittaa myös sitä, että käyttäjät pystytään pitämään yrityksen "turvajoukkoina" ja samalla varmistetaan yrityksen turvastrategian menestys (Curran 1996). Onnistuneesta toiminnasta seuraa, että organisaation kaikki osat tukevat turvaohjelmaa (Wood 1982). Organisaation ylimmän johdon on hyväksyttävä turvallisuusasiat, luotava resurssit ja taloudellinen tuki tietoturvalle. Tietoturvatietoisuutta ohjelmana pitäisi pystyä myös arvioimaan, jopa mittaamaan objektiivisesti sen tehokkuuden perusteella. Kuitenkin ongelma tulee myös siitä, etteivät useimmat organisaatiot käytä takaisinkytkentää tai mittaa oman tietoturvatietoisuusohjelmansa onnistumista (MacLean 1992). Turvallisuusjohtamisen tulisi huomioida takaisinkytkentä ja suorittaa tarvittavat toimenpiteet. Takaisinkytkennän tulisi perustua toimintaan, jossa turva-asioita tarkastellaan sekä organisaation että hyväksikäyttäjien näkökulmasta ja erityisesti käyttäen tuloksia, jotka on saatu eri turva-alueiden mahdollisten mittausten yhteydessä.

Tietoturvatietoisuuden ohjelmana tulisi sisältää ainakin seuraavat kohteet (ISO-IEC-27, 1995):

1. Yhtymän tietoturvapolitiikkaan liittyvät vaikuttimet samoinkuin politiikkaan, ohjeisiin, direktiiveihin ja riskien hallinnan strategiaan liittyvät laajennukset, joiden avulla riskeihin ja turvatoimenpiteisiin liittyvät asiat voidaan ymmärtää syvällisemmin.
2. Tietoturvaohjelman/suunnitelman toteuttaminen ja turvatoimenpiteiden tarkistukset.
3. Tietojen suojaamiseen liittyvät perustarpeet.
4. Luokitusjärjestelmän perustamisen, joka sisältää informaation suojaamisen.
5. Tarve raportoida tietoturvaloukkauksista ja niiden yrityksistä ja tutkia niitä.
6. Turvallisuuteen liittyvien parannusten merkitys hyväksikäyttäjille ja organisaatiolle.
7. Menettelytavat, vastuut ja työn kuvaukset.

8. Turvatarkastukset (auditointi) ja joustavat tarkastukset (chek).
9. Muutoksen ja rakenteenhallinta.
10. Seuraukset toiminnasta, joka on tapahtunut ilman valtuutusta.

Informaatiota tietoturvakoulutuksesta lähettää hyvin moni tiedonsiirtokanava, mutta juuri tämän informaation tulisi olla harkittua. Suurissa yrityksissä vastuutus yhtymän tietoturvatietoisuuden edistämisestä tulisi kuulua yhtymän tietoturvapäällikölle (ISO-IEC-27, 1995). Samoin tietoturvatietoisuusohjelma tulisi hyväksytyttää johdon tietoturva-asioiden neuvottelukunnassa (Code of Practice, 1993).

On esitetty, että tietoturvatietoisuus saataisiin parhaiten ihmisten mieliin erilaisilla kampanjoilla (MacLean, 1992). Tässä toiminnassa voitaisiin hyödyntää turvakoulutuksen keinoja ja samalla saada positiivista vauhtia tietoturva-asioihin, kun ihmiset muistaisivat turvallisuuden tärkeyden. Toisaalta turvallisuuskampanjat, kuten myös niiden poliittiset ja mainontaan liittyvät vastineet, saattavat nostattaa negatiivisia tunteita, jopa vihaa.

### *6.2. Hammerin menetelmä*

Toinen vastaava menetelmä perustuu niinsanottuun Hammerin teoriaan, jossa tietoturvasta tehdään organisaation sisällä suosittu aihe. Oleellista Hammerin teoriassa on, että kaikki haluavat ottaa käyttöön organisaatioon tuodun uuden asian, jota jatkuvasti tuodaan esille, taotaan (Perry 1985).

Hammerin teoria ja kampanjointi sopivat yhteen suhteellisen hyvin. Lisäksi voidaan ottaa käyttöön seuraavia voimakkaasti toiminnallisia menetelmiä. Nämä menetelmät ovat organisaatiokohtaisia ja ne ovat hyödyllisimpiä suurissa organisaatioissa, joissa kuitenkaan tietoturvaan liittyvä aineisto ei aina ole kaikkein tasokkainta (Perry 1985):

*- Tietoturvasta vastaavien päällikkötason henkilöiden pitäisi osallistua tietoturvaseminaareihin. Useimmat yrityksen henkilöt tahtovat tietää, mitä heidän päällikkönsä tekevät ja mitä he haluavat. Jos yritys järjestää turvaseminaareja ja yrityksen vaikutusvaltainen johto osallistuu niihin, se herättää kaikenlaisia kysymyksiä ja koskee erityisesti keski- ja alinta johtotasoa. Tämä tilanne saa heidät oppimaan enemmän turvallisuusasioista ja tämä mielenkiinto heijastuu läpi organisaation alimmille tasoille asti.*

Vuonna 2000 on korostettava sitä, että tietoturva on tärkeä koko organisaation kannalta: ylimmän johdon on oltava sitoutunut tietoturvaratkaisuihin, organisaation kaikki tasot jakavat vastuun tietoturvan ylläpidosta ja tietoturvatoiminnoille osoitetaan niiden tarvitsemat resurssit. Tämän osallistumisen pitäisi heijastua myös organisaation johtamistoimintoihin.

*- Vuokraa konsultti tarkastamaan organisaation turvallisuusohjelma. Tilannetta tehostaisi se, että asiantuntija tulisi ja kertoisi ihmisille, että yhä enemmän huomiota tulisi kiinnittää tietoturvaratkaisuihin. Mitä suurempi on konsultin arvonanto, sitä mieluisammin tietoturvatoiminta otetaan vastaan.*

Toisaalta ei saa unohtaa sitä, että konsultti on aina ulkopuolinen ja nostattaa epäilevän kysymyksen: kuinka konsulttiin voidaan luottaa? Konsultti voi auttaa löytämään uudenlaisen ratkaisun tietoturvaongelmaan, mutta kuitenkin organisaation vastuulliset jäsenet tekevät lopulliset päätökset. Tästä on luonnollisena seurauksena se, että konsultti saattaa työskennellä lukuisissa yrityksissä, mutta miten hän toimii ristiriitaisissa tilanteissa?

*- Korosta tietoturvaloukkauksia. Vastuullisen johdon pitäisi olla tietoinen tietokonerikoksista. Jos vastuullinen johtaja esittää kysymyksiä tietokonerikoksista tai varautumissuunnitelman tekemisestä tulevaisuutta varten, siitä saattaa tulla erityinen sysäys koko tietoturvatietoisuuden tason kehittämiseksi.*

Vastuullisen johdon on pidettävä mielessä, että tietoturva on ainoastaan niin vahva kuin järjestelmän heikoin lenkki. Ei voida rakentaa täysin varmaa järjestelmää - tai sen yhteydessä ei pystytä työskentelemään. Tämä jättää "oven auki" mahdollisille väärinkäytöksille, joiden yhteydessä käytetään uusinta teknologiaa tai joitakin yksinkertaisia vanhoja menetelmiä. Johdon pitäisi osoittaa mielenkiintonsa tätä toimintaa kohtaan ja tehdä suunnitelmia tulevaisuuden varalle.

*- Lisää sisäisten ja ulkoisten tarkastusten turva-arviointia. Pyydä organisaation tarkastajia, joko sisäisiä tai ulkoisia tai molempia, suorittamaan sellaisia tietoturva-arviointeja, jotka kohdistuvat tietoturvatietoisuuden, siihen liittyvien kontrollien ja väärinkäytösten säännölliseen tarkistukseen. Tämä johtaa kasvavaan määrään*

*kommentteja, jotka ovat tekemisissä organisaation tietoturvan kanssa ja siksi niillä on tietty tärkeä asema organisaation toiminnan yhteydessä.*

Mutta muista, täytyy olla menetelmiä, joilla tarkastetaan tarkastajia.

*- Luo tietoturvapolitiikka. Jos organisaatiolla ei ole tietoturvapolitiikkaa, luo sellainen politiikka, jolla saadaan aikaan välitön tietoisuus sen tärkeydestä. Tämä korostuu erityisesti siinä tapauksessa, että yrityksen vastuullinen johto vaatii tällaisen politiikan tuottamista.*

Vuonna 2000 on välttämätöntä, että kaikilla organisaatioilla on turvallisuusmalli. Organisaatioilla täytyy olla toimiva tietoturvapolitiikka ja muita turvaohjeita johdolle ja hyväksikäyttäjille. Tietoturvapolitiikkaan on sisällytettävä ne menetelmät, päämäärät ja kontrollit, joilla tietoturvaperiaatteita toteutetaan. Sen on myös sisällettävä toimenpiteet, jotka koskevat turvaorganisaatiota, resursseja, vastuita ja väärinkäytöksistä raportointia. Erityisesti johdon pitäisi tukea tätä toimintaa voimakkaasti.

Tietoturvatietoisuuden mittaamisella yritetään tutkia ja vahvistaa työn tehokkuutta ja turvallisuuteen liittyviä tuloksia. Mutta jo pelkästään kysymys tietoturvan mittaamisesta ei ole suoraviivainen tehtävä. Käytössä on erilaisia menetelmiä, joilla saadaan absoluuttisia numeerisia tuloksia. Voidaan kuitenkin todeta, että usein tällaiset menetelmät ovat mahdottomia laajennettavaksi oman suppean käyttöalueensa ulkopuolelle, koska tietoturvaan laajemmin ymmärrettynä liitetään myös henkilökohtaisia tuntemuksia. On tiettyjä yhtymäkohtia mitattaessa tietojärjestelmien tietoturvaa ja toisaalta laatua.

Tutkimukseen soveltuu yksinkertainen tapa arvioida neljän tason avulla tietoturvatietoisuuden kehittämisen vaikuttavuutta (Walsh 1996):

Pitivätkö työntekijät siitä?
Oppivatko työntekijät sen?
Sovelsivatko työntekijät sitä työskentelyssään?
Oliko valmennuksella vaikutusta myös organisaation alimmille tasoille?

Jos puhutaan vaativampien mittausten vaikeudesta, on muistettava kyseisessä ympäristössä vallitseva työtilanne. Kaikki voimavarat joudutaan monessa organisaatiossa kiinnittämään pelkästään siihen, että järjestelmät ja verkot saadaan pysymään toimintakunnossa.

Tietoturvatietoisuuden merkitystä organisaation tietoturvan hallinnalle ei saa ymmärtää väärin tai aliarvioida. Turvakoulutuksen tulisi levitä organisaation kaikille tasoille lähtien ylimmästä johdosta, jonka ehdoton sitoutuminen on erittäin tärkeää. Turvallisuuden parantamiseen liittyvät hankkeet heijastuvat myös positiivisesti ulkopuolisten yhteistyökumppanien toiminnassa.

Tietoturvatietoisuus -ohjelman menestyminen riippuu erityisesti organisaation tasolla tehdyistä ratkaisuista, se sisältää asiantuntijoille ja hyväksikäyttäjille suunnattua valmennusta ja koulutusta tietoturvatietoisuus -ohjelman mukaisesti. Tietoisuus -ohjelmassa pitäisi määrittää erikseen myös kyseisen organisaation perinteisiin liityyvät sosiaaliset vaatimukset, koska vain ymmärtämällä ja kunnioittamalla inhimillisiä tekijöitä pystytään vahvistamaan se, että työntekijät kaikilla tasoilla hyväksyvät ohjelman. Tämä on tärkeä tekijä kokonaisuudessa ja vasta sen sisäistettyään on mahdollista tehokkaasti parantaa tietoturvaa organisaation sisällä.

## 7. LÄPINÄKYVÄ YHTEISKUNTA JA MIKROTASON YHTEISTYÖ

Tietoturvaan liittyvä tiedottaminen on joissakin kanavissa pohjautunut sensaatioiden ja ilmi tulleiden rikkomusten ja väärinkäytösten aukaisemiseen julkisuudessa, paljon vähemmän on tietoturvaan liittyvää tiedotusmateriaalia ollut jaossa. Vahinkojen ennalta torjuminen on ollut suhteellisen vaimeaa. Myöskään loukkausten ja väärinkäytösten kohteeksi joutuneet yritykset eivät aina tuo vahinkojaan muiden arvioitavaksi. Julkisuus laskee vain yrityksen mainetta ja arvoa.

Yleensä järjestelmiä suunniteltaessa joudutaan tasapainottelemaan sillä, onko tärkeämpää korostaa enemmän käytettävyyden vai turvallisuuden merkitystä. Jos palvelujen tarjoaja yrittää vaikuttaa yksityisiin asiakkaisiinsa ilman organisaatioissa käytettäviä ohjeita ja sääntöjä niin, että nämä kehittäisivät toimintaansa ja käyttäytymistään verkkoympäristössä, asiakkaat valitsevat yleensä aina käytettävyyden tärkeimmäksi. Voidaan kysyä, onko tämä tilanne sellainen, johon ei voida vaikuttaa. Kuinka voitaisiin kehittää käyttäjien näkemystä siitä, että kumpikin ominaisuus olisi tärkeä ja välttämätön toiminnan laajetessa. Jos kehitystyössä onnistutaan, voidaan päästä sellaiseen tilanteeseen, että kumpikin ominaisuus pystytään samanaikaisesti täyttämään.

Jotta tähän päästäisiin, tietoturva-asiat on teh-

tävä suurelle yleisölle tutuikisi. On joitakin asioita, jotka kiinnostavat kaikkia. Esimerkisi pankkikorttien käyttöön liittyvät väärinkäytökset on koettu kaikkia kansalaisia kiinnostaviksi. Valitettavasti tietoturvaan liittyvä valistus tässäkin tapauksessa ylittää uutiskynnyksen vasta vahingon jo tapahduttua.

Edellinen osoittaa, että yksilöiden, tietotekniikan koti- tai yksityiskäyttäjien, olisi syytä tarkastella tilannetta samoin kuin suurissa organisaatioissa on jo vuosien ajan tehty. Käyttäjien olisi oltava perillä siitä, että heidän järjestelmänsä ja laitteistonsa eivät ole haavoittumattomia. Mitä tällaiset haavoittuvuuskohdat voisivat olla? Minkälaisia vahinkoja mahdollisesti voi sattua? Jos vahinko sattuu, miten sen vaikutuksia voidaan minimoida? Minkä suuruinen on mahdollisen riskin todennäköisyys? Mitä voidaan vakuuttaa, kuinka suuria riskejä on mahdollista ottaa? Minkälaisia turvaratkaisuja on valmiina saatavana kansalaisten tarpeisiin? Omalla osaamisella niin tietotekniikan kuin tietoturvatietoisuuden alalla on erittäin suuri merkitys torjuttaessa tai vältettäessä tietoturvauhkia.

Olemme siirtymässä mobiiliin yhteiskuntaan. Tämä tarkoittaa sitä, että tietojen saatavuus ja henkilön tavoitettavuus paranee. Tietoyhteiskunnan yhteydessä on tarjottu mahdollisuutta informaation vapaasta saatavuudesta maailmanlaajuisesti. Asioilla myös pyritään rahastamaan, tekijänoikeusasiat ovat osittain ratkaisematta, mutta kuitenkaan kenelläkään ei ole vastuuta verkkojen kaikkien tietolähteiden oikeellisuudesta. Mobiilin vaiheen toinen merkitys on siinä, että henkilöllä on mukanaan siirrettävä laite, puhelin ja Internet -liittymä, jonka avulla hän on lähes aina tavoitettavissa ja toisaalta hän voi seurata olinpaikastaan riippumatta tapahtumia laajasti. Seuraava askel on, että jo osittain toimivat tietoturvaratkaisut on sulautettu luonnolliseksi osaksi kokonaisuutta. Voidaan vähitellen alkaa puhua läpinäkyvästä, turvallisesta yhteiskunnasta.

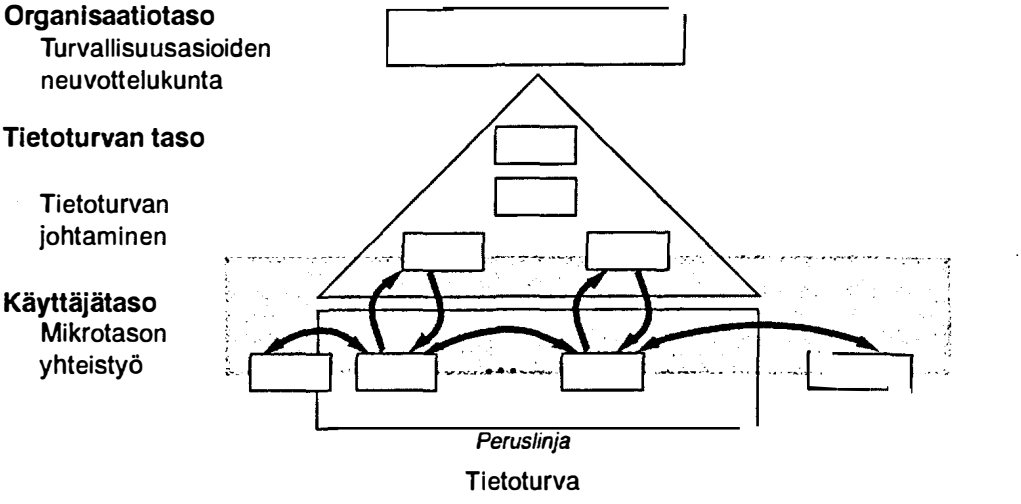
Eräs läpinäkyvän yhteiskunnan piirre on se, että tietoturvaratkaisut ovat osana kokonaisuutta, mutta niin hyvin ja tehokkaasti toteutettuina, että tietokoneen käyttäjä ei huomaa niitä oman toimintansa kannalta ylimääräisinä operaatioina eikä koneen toiminnan hidastumisena.

Salaus on nykyisen ja myös tulevan yhteiskunnan tietoturvan tärkein komponentti. Se on perusta, työskentelyalusta, josta kaikki tietoturvatyö lähtee. Seuraava työskentelyalusta liittyy verkkojen turvaamiseen. Tietoliikenteessä käytettävät tasomallit sisältävät turvamoduulinsa, samoin käytetään tietoturvaprotokollia.

Läpinäkyvä turvallinen yhteiskunta tarkoittaa siis sitä, että salaus ja muut tietoturvaan liittyvät ratkaisut ovat käytössä. Niiden lisäksi tarvitaan valvontaa, voimme puhua jopa kontrolleista. Silloin vain tietokoneet valvovat toimintaa, ihmisten ei tarvitse puuttua siihen normaalitilanteissa. Mutta jos jotakin sattuu, voidaan asiat nopeasti selvittää tietokoneen keräämistä lokitiedostoista. Tämä tieto tarkoittaa sitä, että yksittäinen tietokoneen käyttäjä voi työskennellä ilman paineita valvonnan alaisena, mutta hän on samalla tietoinen siitä, että jos hän syyllistyy luvattomiin tekoihin, asiat voidaan selvittää lokitiedostojen avulla ja ne kelpaavat myös juridiseksi näytöksi rikkomuksesta.

Läpinäkyvässä yhteiskunnassa pelote – funktiolla on tärkeä merkitys. Pelotteena voi olla tieto rikollisen toiminnan odottamatomasta havainnoinnista tai se, että käyttäjät tietävät kontrollien olemassaolon. Pelotteet on tarkoitettu suojaamaan nimenomaan satunnaisilta väärinkäytöksiltä, sillä ne eivät estä tahallisia harkittuja tekoja. Kontrolli -termin merkitystä voidaan tässä yhteydessä laajentaa siten, että se voi olla politiikka, menetelmä, käytäntö, laite tai ohjelmoitu mekanismi kontrollitavoitteen saavuttamiseksi. On hyvä, että käyttäjät tietävät, että valvontamekanismi on olemassa, mutta jos siitä tiedotetaan liikaa, se saattaa herättää joissakin kokeiluhaluisissa tietyn testausmielialan.

Kuvassa 4 on esitetty mikrotason yhteistyö tietoturvan kehittämisestä organisaatioissa. Oleellista tässä kuvassa on se, että yrityksen tietoturvasta alimmalla tasolla vastaavat ovat yhteistyössä muihin oman organisaationsa hyötykäyttäjiin, joilla on omiin tehtäviinsä liittyvät tietoturvaohjeet. Aina kun tulee epäselviä tapauksia, on syytä keskutella. Kun ohjeissa huomataan puuteita, ne olisi pystyttävä välittömästi tarkentamaan ja ottamaan korjatut versiot heti käyttöön. Kun yhden käyttäjäryhmän ohjeissa ilmenee puuteita, silloin olisi tarkastettava ja tarvittaessa korjattava myös kaikkien rinnakkaisten käyttäjäryhmien ohjeet. Tietoturva-asiantuntijoiden olisi kerrottava omalle organisaatiolleen muutoksista ja tutkittava niiden vaikutusta muille käyttäjäryhmille. Myös käyttäjien välinen yhteistyö ja keskustelu voi parantaa laadittuja ohjeita. Mikrotason yhteistyö tarkoittaa siis organisaation valmistus-




***Kuva 4.*** *Mikrotason yhteistyö tietoturvan kehittämisessä organisaatioissa.*

puolen, konkreettisten työtehtävien suorittajien välistä horisontaalista yhteistyötä. Se tarkoittaa myös työntekijöiden ja työnjohdon välistä vertikaalista yhteistyötä, tällöin työnjohdossa on mukana myös tietoturva-alan asiantuntija.

Tulevaisuuden tietoyhteiskunnassakin tulee olemaan tietoturva-asioita, joissa on toimittava heti ja voimakkaasti. Suurin osa asioista on kuitenkin sellaisia, että ne hioutuvat yhteistyön kautta. Kun yritysten yleinen työskentelyilmapiiri saadaan mahdollisimman korkeaksi, silloin myös lähes jokainen yrityksen työntekijä saadaan sitoutettua tietoturvatyöhön mukaan.

## 7. YHTEENVETO

Tietoyhteiskunnan rakennuskomponentit ovat laitteet, koneet, ohjelmistot, tiedonsiirto ja ihmiset. Tietoyhteiskunnan kehitystä nopeuttaa liikeelämä, joka luo ihmisille ja organisaatiolle odotuksia uudentyyppisistä ratkaisuista. Onnistuneesti markkinoidut odotukset niin tietojenkäsittelyssä kuin tietoliikenteessä purkautuvat ostoina. Ainakin osa uusista ratkaisuista on erittäin tärkeitä, mutta on myös paljon tuotteita, joiden kehittyneistä ominaisuuksista on hyötyä vain muutamille asiantuntijoille, vaikka niitä tarjotaan kaikille.

Tavoitteena on luoda parempi tietoyhteiskunta. Turvallisuus ja tietoturva ovat sen peruskomponentteja. Yhteiskunta muodostuu ihmisistä ja organisaatioista. Tietoyhteiskuntakehityksestä osattomaksi jäävien muodostama "neljäs maailma" (Castells 2000) on "tunnistettu" Kaliforniassa, Berkeleyn yliopistossa, ei meillä. Mutta Castellsin mukaan neljäs maailma on läsnä kaikkialla, ei yksin kehitysmaissa. Osaammeko me suomalaiset omassa "tietoliikenteen kansallisessa laboratoriossamme" torjua tämän maailman? Keskusteluun liitty kysymys vallasta. Kenellä se on? Verkolla – kummallinen vastaus, mutta niin on tilannekin. Kukaan ei hallitse eikä vastaa Internetistä. Mitä sen jälkeen?

Vuonna 2000 yhteiskunta on erittäin voimakkaasti riippuvainen tietotekniikasta. Tämän tilanteen voi kokea herkkyytenä, mutta myös erittäin vakavana haavoittuvuutena. Teknologia tuottaa yhä parempia ratkaisuja myös tietoturvan alueella, mutta ihmisten valmiudet ottaa näitä asioita käyttöön ovat jo rajalliset. Jos palaamme vielä 1970 ja 1980 – lukujen ennustuksiin ja simulointeihin, oleellista on se, että todellisuudessa globaalit ilmiöt ovat niin laajoja, ettei niitä pystytä tietokoneiden avulla täysin hallitsemaan. Ratkaisu voisi olla hermoverkon kaltainen, jollaisia suppeassa mielessä meillä on käytössä joissakin uusimmissa tietokoneissa. Laaja ratkaisu sensi-

jaan perustuu jokaisen ihmisen henkilökohtaiseen hermoverkoon – ja jokaisen maapallon ihmisen yhteiseen hermoverkkojen verkkoon. Siis, valta on verkossa!

## LÄHTEET


Castells, Manuel (2000) Neljäs maailma TV-2, 7.1.2000. klo 21.00 - 21.30.

A Code of Practice for Information Security Management (1993) Department of Trade and Industry. DISC PD0003. British Standard Institution, London, UK.

BS7799-1:fi. Standardi. – Tietoturvallisuuden hallinta. Osa 1: Tietoturvallisuuden hallintajärjestelmiä koskeva menettelyohje. Suomen standardisoimisliitto SFS, 15.2.1999.

BS7799-2:fi. Standardi. – Tietoturvallisuuden hallinta. Osa 2: Tietoturvallisuuden hallintajärjestelmiä koskevat vaatimukset. Suomen standardisoimisliitto SFS, 15.2.1999.

Ceraolo, J.P. (1996) Penetration testing Through Social Engineering. Information Systems Security. Vol. 4, No 4. Auerbach.

Computer Security Handbook The Practitioners Bible (1984) Computer Security Institute. Mac/Donnel Printers, USA.

Curran, Terri (1996) Implementing Successfull Security Awareness Programs. 23rd Annual Computer Security Conference and Exhibition, CSI, November 11 - 13, Chigaco, Il.

EUROPEAN PARLIAMENT (1998) An Appraisal of Technologies of Political Control. Working document, (PE 166 499), Luxembourg, 6 January .

ISO-IEC-27 (1994) Guidelines for the Management of IT Security (GMITS): Part 1 –Concepts and models for IT Security.

ISO-IEC-27 (1995) Guidelines for the Management of IT Security (GMITS)

Kajava, Jorma & Heikkinen, Sami J.P. & Jurvelin, Paavo & Viiru, Tero & Parviainen, Päivi (1996), Tietojenkäsittelyn ulkoistaminen ja tietoturva - Information Security Research from Outsourcing Process, (abstract in English). University of Oulu, Department of Information Processing Science, Working Papers Series B 42, Oulu.

Kajava, Jorma & Jurvelin, Paavo (1996) Outsourcing as a Business Option in Secure IT Environment. University of Oulu, Department of Information Processing Science, Working Papers Series B 45, Oulu.

Kajava, J. & Leiwo, J. (1996) Information Security for Workstations - Implications for End-Users. In: von Solms, R. (ed.): Notes on Information Security Management 1995. International Federation for Information Processing. Port Elizabeth, South Africa.

Kajava, J. (1996) Organisaatioiden tietoturvaohjeistus. Turvapäivät Otaniemessä, Teknillinen korkeakoulu, Espoo.

Kajava, J. & Siponen, M.T. (1996) Security Management and Organizations - Bottom up or Top down Approach? In: Jonsson, Erland (ed.): Proceedings of Nordic Workshop on Secure Computer Systems (NORDSEC '96) SIG Security and Chalmers University of Technology, Gothenburg, Sweden.

Kajava, J. & Siponen, M.T. (1997 a) Effectively Implemented Information Security Awareness - An Example from University Environment. In: Eloff, Jan HP & von Solms, Rossouw (eds.): Information Security - from Small Systems to Management of Secure Infrastructures. Proceedings of IFIP/Sec' 97 WG 11.2 and WG 11.1 of TC11, Copenhagen, Denmark.

Kajava, J. & Siponen, M.T. (1997 b) IT Security Awareness - Issues for Industry. In: Karila, A. & Aalto, T. (eds.): Encouraging co-operation. Proceedings of the Second Nordic Workshop on Secure Computer Systems (NORDSEC'97). Helsinki University of Technology, Espoo, Finland.

Lazlo, E. (1990), Evolution.

MacLean, Kevin (1992) Information Security Awareness - Selling the Cause. In: Gable, G. & Caelli, W. & Ng, F. & Ranai, K. & Soh, C. (eds.): Security and Control: From Small Systems to Large. Proceedigs of the IFIP TC 11/Sec'92. Singapore, 27-29 May.

Miettinen, Juha E. (1999) Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan, Kauppakaari, Helsinki.

The NIST Handbook, (1995): An Introduction to Computer Security, NIST special publications in October 1995. Saatavilla osoitteesta:
http://csrc.nist.gov/nistpubs/800-12/

Perry, William E. (1985) Management Strategies for Computer Security. Butterworth Publisher, Boston.

Parker, Donn B. (1981) Computer Security Management, Prentice Hall, Reston, USA.

Parker, Donn B. (1995) A New Framework for Information Security to Avoid Information Anarchy. In: Eloff, J.H.P. & von Solms, S.H. (eds.): Information Security – the Next Decade, Proceedings of the IFIP TC11 eleventh conference on information security. Chapman & Hall, London, UK.

Royal Canadian Mounted Police (1981) Security in the EDP Environment. Security Information Publication, Second Edition. Gendarmere Royale du Canada. Canada, October.

Saari, J. (1988) Tietoturvallisuuden käsikirja. Otava. Keuruu.

Siponen, M.T. & Kajava, J. (1998) The Various Dimensions of IT Security Awareness. In: Barzdins, J. (ed.): Databases and information Systems. Third International Baltic Workshop on Databases and Information Systems, 15 - 17 April, Riga, Latvia.

Straub, D. & Carson, P. & Jones, E. (1992) Deterring Highly Motivated Computer Abuses: A Field Experiment in Computer Security. In: Gable, G. & Caelli, W. & Ng, F. & Ranai, K. & Soh, C. (eds.): Security and Control:

From Small Systems to Large. Proceedigs of the IFIP TC 11/Sec'92. Singapore, 27-29 May.

Thomson, M.E. & von Solms, R. (1997) An Effective Information Security Awareness Program For Industry. In Eloff, Jan HP & von Solms, Rossouw (eds): Information Security - from Small Systems to Management of Secure Infrastructures. Proceedings of WG 11.2 and WG 11.1 of TC11. IFIP, 13 - 16th May, Copenhagen, Denmark.

Toffler, A. (1981) The Third Wave. Pan Books. London, UK.

Walsh, Tom (1996) Implementing Successfull Security Awareness Programs. 23rd Annual Computer Security Conference and Exhibition, CSI, November 11 - 13, Chigaco, Il.

Wong, K. & Watt, S. (1990) Managing Information Security - A Non-technical Management Guide, Elsevier & Computer Weekly, Southampton, UK.

Wood, Michael B., (1982), Computer Security, UK.

Tietojenkäsittelyn turvaaminen tietoyhteiskunnassa (1996) Puolustustaloudellinen suunnittelukunta, Tietojärjestelmäjaosaston ohje n:o 1, Helsinki.

Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa Valtiovarainministeriö, Helsinki 4.2.1993 (VM 1/73/93).

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, Valtiovarainministeriö, Helsinki 11.11.1999, (VM 0024: 02/99/1998). Saatavilla osoitteesta: http://www.vn.fi/vm/kehittaminen/tietoturvallisuus/vahti/vahti.htm