Tietoturvallisuuden hallinnan kriittiset onnistumistekijät:

ylimmän johdon sitoutuminen ja organisaation tietoturvatietoisuusohjelma

Jorma Kajava

ABSTRACT

Critical Success Factors in Information Security Management in Organizations:
The Commitment of Senior Management and the Information Security Awareness Programme

Information security has three major points of view: the so-called technical, managerial and end-user related views. This paper focuses on the managerial viewpoint. One central aspect in this approach involves the challenge for global co-operation and harmonization of national legislations. This can best be achieved by following the original British standard" A Code of Practice for Information Security Management". This paper starts from the critical success factors of information security management and extends the research area in a more practical and critical direction. A pertinent question is identifying the real success factors. Any answer to that question must hinge on commitment. In practical terms, senior management must understand the importance of commitment. But that is not enough, they must find means of generating a real information security awareness programme for all employees.

Organizational information security work is high-level team work based on trust and common goals. If its basic solutions are based on the British standard, the most important factors will undoubtedly be economic. Although this paper does not explore the financial aspects of security in depth, they cannot be avoided either, because their effects seep down to every level of security work. Business is like society. There is a frail balance between security and usability, which is currently being endangered by the threat of terrorist actions, for example. The critical factor in maintaining at least some form of balance is commitment. In this respect, senior management has to lead the way. The overarching question is, how do they get end-users to follow them as the world has plunged into a semipermanent threat of war and is pervaded by an atmosphere of continuous information warfare.

Keywords: Information security, Security management, Critical success factors, Management commitment, Information security awareness programme.

JOHDANTO

Tietoturva on luonteeltaan hyvin monisärmäinen. Parker (1981) esitti CIA -mallinsa (Confidentiality, Integrity, Availability), jota valtaosa hallinnollisen tietojenkäsittelyn turvatyöstä sivuaa. Kirjoittaja on esittänyt asiasta näkemyksensä esimerkiksi (Kajava 2000b, 2001c).

Kuitenkin Parkerin varhaisimmat näkemykset tuntuivat kyseisen mallin hakemiselta. Tietoturvan hallinnan kannalta keskeisin alkuaikojen teos on Kanadan Ratsupoliisien kokoama vihkonen (Royal Canadian Mounted Police, 1981), johon esimerkiksi oman valtiovaltamme ohjeet perustuvat (VM 1993, 2000).

Yritysmaailmassa aikaisemmissa keskusteluissa esillä oli voimakkaammin tietoturvan tekniset ratkaisut sekä tietojen ja järjestelmien suojaus. Organisaation tasolla tietoturva tarkoitti aikaisemmin sitä, että johto antoi käyttäjille ohjeita

ja määräyksiä, jotka liittyivät työntekijöiden päivittäisiin työvaiheisiin. Teknisiin suojaratkaisuihin ja erilaisten ohjeiden valvontaan liittyi tarkka kontrolli ohjeiden ja ratkaisujen käytön noudattamisesta.

Tietoturvan hallinta on tullut yhdeksi organisaation johtamisen osamoduuliksi. Lähinnä se liittyy yritysturvallisuuden johtamiseen ja laatutoimintaan. Mitä enemmän levottomuutta maailmalla esiintyy, sitä tärkeämmäksi tietoturvallisuuden hallinta on tullut. Tämä esitys perustuu organisaation tietoturvan hallinnan valvontaan liittyviin avaintekijöihin ja niihin liitettäviin kriittisiin onnistumistekijöihin (A Code of Practice, 1993).

Tietoturvaan liittyvät asiat ovat tulleet tärkeiksi vasta sen jälkeen, kun tietotekniikan kehitys ja yhteistyömahdollisuudet 80 -luvun lopulla lähtivät voimakkaasti yleistymään kaikilla yhteiskunnan tasoilla. Syyskuun 2001 terrori-iskut ovat vaikuttaneet laajasti tietoturvakysymysten keskeiseen asemaan yhteiskunnassa.

Teknologiaan liittyviä turvaratkaisuja on pidetty kaikkein suoraviivaisimpina, jopa helppoina, rahalla ratkaistavina asioina - organisaatio voisi tulkita ne eräänlaisiksi "automaateiksi", aina päällä oleviksi varmistuksiksi. Tämä sillä edellytyksellä, että kaikki työntekijät hyväksyvät ratkaisut, haluavat käyttää niitä. Toiminnalla tähdätään organisaation tietoturvatietoisuuden kasvattamiseen. Toisaalta tällainen teknologiaan liittyvä staattinen tilanne on toiveuni siitä, ettei muutoksia ympäristössä tapahtuisi.

Kokemus on osoittanut, että helppoja ratkaisuja ei ole (Allen, 2002, Kerttula, 1998). Yllättäen on ilmennyt, että teknologiaan liittyvissä perusasioissa on heikkouksia, joista ei ole pystytty sopimaan tai joihin ei ole löydetty kattavaa ratkaisua (Härkönen & Kallio, 2001). Samanaikaisesti teknologia on tullut erittäin monimutkaiseksi. Muutosten hallinta on laajasti ymmärrettynä tullut erääksi ongelma-alueeksi (Anttila et al, 2001)

Ihminen tietotekniikan käyttäjänä on ollut ja tulee olemaan vaikeasti hallittava kokonaisuus. Ihmiset voivat muodostaa organisaation eli toimia tietyn toiminta-ajatuksen mukaisesti yhteisten tavoitteiden saavuttamiseksi. Tietotekniikka on oleellinen osa nykyaikaista yritystoimintaa. Kaikille kaupallisille organisaatioille yhteistä on liikevoiton tavoittelu. Organisaatioiden toiminnan, niin myös tietoturvatoiminnan, yhteydessä voidaan todeta, että toiminnalla tähdätään kustannustehokkuuteen.

Teknologia on edelleen yksi välttämätön peruskomponentti muodostettaessa turvallista ratkaisua. Toinen tietoturvan kannalta oleellinen komponentti on käyttäjä, ihminen, ja kolmas on organisaatio. Tietoturvan kehittäminen tapahtuu näiden kolmen osa-alueen tasapainoisella eteenpäin viemisellä. Tietoturvakysymysten yhteydessä on totuttu tasapainoilemaan käytettävyyden ja turvallisuuden välillä, samoin on toinen tasapainoilualue, yksityisyys vastaan julkisuus. Organisaatioiden päättävässä asemassa olevien henkilöiden on tiedostettava, että tasapainoisen ja turvallisen toiminnan taustalla on kyky ymmärtää, että tietoturva muodostuu harmonisesta vuorovaikutuksesta teknologian, ihmisten ja organisaatioiden toiminnan välillä. Tätä voidaan kutsua tietoturvan hallinnan strategiseksi kolmioksi.

Tässä artikkelissa käsitellään tietoturvan hallintaa Brittien standardin A Code of Practice for Information Security Management (1993) pohjalta. Standardissa on esitetty tietyt avaintoimenpiteet, jotka ovat erityisen tärkeitä kaupan ja elinkeinoelämän organisaatioille. Standardissa esitetään myös tietoturvan hallinnan kriittiset onnistumistekijät. Kirjoittaja on uskaltanut tarttua näihin tekijöihin ja tulkinnut niiden sisältämää sanomaa myös kriittisesti.

Kirjoituksella tähdätään tietoturvan hallinnan kriittisen ajattelun ja tulkinnan herättämiseen. Tärkeämpää kuin kritiikki on ymmärtää asioiden liittyminen maailmanlaajuiseen yhteistyöhön. Esimerkiksi elektroninen kaupankäynti edellyttää eri osapuolilta sitä, että sanomat pystytään lähettämään turvatussa moodissa verkon yli, osapuolet on pystyttävä täysin varmasti tunnistamaan ja he eivät jälkeenpäin pysty kiistämään osallistumistaan.

Tietoturvan hallinnan näkemysten yhdenmukaistamisella eri osapuolien välillä haetaan luotettavia yhteistyömuotoja kaikille verkkoympäristön toiminnoille niin kansallisella kuin maailmanlaajuisella tasollakin. Yhteinen näkemys tietoturvan hallinnasta on välttämätön alihankintatoimitusten yhteydessä, se on myös ulkoistamisen onnistumisen perusedellytys. Ilman sitä esimerkiksi virtuaalisesta yritystoiminnasta voidaan puhua vain virtuaalimaailman tasolla.

TIETOTURVAN HALLINTA JA AVAIN-KONTROLLIT

Tietoturvallisuuden hallintaan liittyvät taustaasiat on syytä ymmärtää, kun A Code of Practice for Information Security Management (1993) ohjeistoa lähtee soveltamaan käytännön tehtäviin. Sen kehitti Britannian kaupan ja teollisuuden keskusjärjestö useiden kymmenien kansallisten johtavassa asemassa olevien yhtiöiden ja organisaatioiden kanssa. Alusta alkaen ohjeiston tarkoituksena oli tuottaa käyttäjilleen taloudellista hyötyä muun liiketoiminnan yhteydessä. Ohjeistoon koottiin johtavien yritysten parhaat tietoturvakäytännöt.

A Code of Practice for Information Security Management (1993) -ohjeiston kokoamisella pyrittiin jo alussa tarjoamaan yhteinen lähestymistapa kehittää, toteuttaa ja myös pyrkiä mittaamaan tietoturvan hallintaan liittyviä käytäntöjä. Jo noin kymmenen vuotta sitten ohjeistolla haettiin luottamusta monikansalliseen verkottuneeseen yritysten väliseen yhteistoimintaan. Alusta alkaen tähdättiin myös siihen, että ohjeistoa tarjottiin yrityksille ja organisaatioille tietoturvatyön yhteiseksi alustaksi.

Yhtenä Code of Practicen kehittäjänä oli British Standads Institution (BSI) ja ohjeistosta tuli standardi (UK) jo vuonna 1994. Suomessa vielä vuoden 1999 versiosta voidaan käyttää termiä viiteasiakirja (BS 7799-1/2: fi, 1999).

Brittien standardia A Code of Practice for Information Security Management (1993) voidaan tulkita tietoturvallisuuden hallinnan ohjeistoksi, jossa esitetään kattava tietoturvajärjestelmä, joka käsittää yleisimmän sekä Britanniassa että muuallakin nykyään sovellettavan tietoturvallisuuskäytännön. Ohjeiston sisältämä opastus on tarkoitettu mahdollisimman laajaan käyttöön. Ohje palvelee yksittäisenä viiteasiakirjana, josta käy ilmi useimmissa tapauksissa teollisuuden ja kaupan tarvitsemat valvontatoimenpiteet ja jota voidaan soveltaa laajasti riippumatta siitä, onko organisaatio suuri, keskikokoinen vai pieni.

Kun tietoturvallisuuden hallintaa varten on käytettävissä yhteinen viiteasiakirja/ standardi, saavutetaan selvää etua verkostoyhteistyön lisääntyessä organisaatioiden välillä. Sen avulla voidaan luoda keskinäistä luottamusta verkottuneiden osapuolten ja kauppakumppanien välille. Sen avulla voidaan luoda hyödykkeiden hallinnan perusta tietotekniikan käyttäjien ja palveluntarjoajien välille. Viiteasiakirja/standardi ei suoraan sovellu esimerkiksi yrityspolitiikan perustaksi, ei myöskään yritysten välisten kauppasopimusten perustaksi. Viiteasiakirja/standardi on muodoltaan opastava ja ohjeellinen. Viiteasiakirjaa/ standardia laadittaessa on oletettu, että siihen sisältyvien säännösten toimeenpano uskotaan riittävän päteville ja kokeneille henkilöille.

Liiketoiminnassa käytettävä tieto sekä sitä tukevat tietojärjestelmät ja -verkot ovat tärkeä yrityksen omaisuuden osa. Sen käytettävyys, eheys ja luottamuksellisuus (Parker, 1981) saattavat olla oleellisia kilpailukyvyn, kassavirran, kannattavuuden, laillisten velvoitteiden noudattamisen ja arvostetun yrityskuvan säilyttämisen kannalta (Kajava, 2001a).

On odotettavissa, että erilaiset turvallisuuteen ja tietoturvallisuuteen liittyvät uhkat leviävät laajemmalle ja niiden vaikutus ylettyy yhä pitemmälle. Samaan aikaan organisaatiot saattavat muuttua turvallisuusuhkien suhteen yhä suojaamattomammiksi, kun riippuvuus tietotekniikkajärjestelmistä ja -palveluista kasvaa.

Verkottumisen kasvu merkitsee uusia mahdollisuuksia tunkeutua luvattomasti järjestelmiin. Suuntaus hajautettuun tietojenkäsittelyyn vähentää mahdollisuuksia tietotekniikkapalvelujen keskitettyyn, asiantuntevaan valvontaan.

Turvatoimenpiteet ovat huomattavasti halvempia ja tehokkaampia, jos ne on sisällytetty tietojärjestelmiin ja -palveluihin niiden vaatimuksia määriteltäessä. Mitä varhaisemmassa vaiheessa tietojärjestelmien suojaus toteutetaan, sitä halvempi ja tehokkaampi se on organisaation kannalta pitkällä aikavälillä (Vahti, 2000).

Kaikkia valvontatoimia ei voi soveltaa jokaiseen tietotekniikkaympäristöön ja niitä tulee käyttää valikoiden paikallisten olosuhteiden mukaisesti. Suuret, kokeneet organisaatiot ovat kuitenkin hyväksyneet laajalti useimmat valvontatoimista suositeltavana hyvänä menettelytapana kaikkiin tilanteisiin riippuen tietenkin rajoittavista tekijöistä kuten ympäristön ja tekniikan rajoituksista. Näitä yleisesti hyväksyttyjä valvontatoimia kutsutaan usein perustason turvatoimiksi, koska niiden muodostaman kokonaisuuden avulla määritellään alan hyvän turvallisuuskäytännön perustaso.

Erityisen tärkeiksi Code of Practice -ohjeistossa on harkittu kymmenen valvontatoimenpidettä. Ne on nimetty valvonnan avaintoimenpiteiksi. Ne muodostavat hyvän lähtökohdan tietoturvan hal-

linnalle. Ne ovat joko olennaisia vaatimuksia, esimerkiksi lainsäädännön asettamia vaatimuksia, tai ne on harkittu tietoturvallisuuden perusasioiksi, esimerkiksi turvallisuuskoulutus. Nämä valvontatoimet (controls), soveltuvat kaikkiin organisaatioihin ja ympäristöihin.

Muutamat valvontatoimenpiteet, esimerkiksi tiedon salaus, saattavat edellyttää asiantuntevia turvallisuusneuvoja ja riskien arviointia niiden tarpeen ja toimeenpanotavan selvittämiseksi. Joissakin tapauksissa Code of Practice -ohjeiston ulkopuoliset, vaativammat lisävalvontatoimet voivat olla tarpeen erityisen arvokkaiden varantojen parempaan suojaamiseen tai poikkeuksellisen suurten turvallisuusuhkien torjumiseen.

Kontrolli voi olla esim. menettelytapa, fyysinen suojauskeino, looginen suojauskeino tai toimintaprosessi, joka auttaa kohdetta ei-toivottujen tapahtumien torjunnassa (Miettinen et al, 1994). Kontrollit eivät ole itseisarvoja. Kontrollien ensisijainen tehtävä on auttaa organisaatiota riskien hallinnassa, mutta niiden tehtävä on vaikuttaa positiivisesti myös kaikkiin niihin tietoturvan osa-alueisiin, joilla organisaation tietoturvan tasoa voidaan parantaa ja/tai saavuttaa kustannussäästöjä. Kontrollit voidaan nähdä nimenomaan tietoturvan osa-alueiden toisena ulottuvuutena, niiden sisään rakennettuina hallintaprosesseina (Pirnes et al, 2000).

Valvonnan avaintoimenpiteet ovat (BS 7799-1, 1999):

- tietoturvallisuuspolitiikan määrittelyasiakirja
- tietoturvallisuutta koskevien vastuiden jako
- tietoturvallisuuden koulutus ja valmennus
- turvallisuuteen liittyvien tapahtumien raportointi
- virustarkistukset
- liiketoiminnan jatkuvuuden suunnitteluprosessi
- tekijänoikeuden suojaamien ohjelmien kopioinnin valvonta
- organisaatiota koskevien tallenteiden suojaaminen
- tietosuoja
- turvallisuuspolitiikan noudattaminen.

Jokaisessa organisaatiossa on kolme erityistä turvallisuusvaatimusten ryhmää (BS 7799-1:fi, 1999):

1. Järjestelmiin kohdistuvat turvallisuusriskit ovat ainutkertainen kokonaisuus, joka käsittää sekä tietoihin kohdistuvat uhkat että vahinkoalttiudet sekä näiden turvallisuusriskien mahdollisen vaikutuksen liiketoimintaan.
2. Lainsäädäntö ja sopimukset asettavat vaatimuksia, jotka organisaation, sen liikekumppanien, tavarantoimittajien ja palveluntoimittajien on täytettävä. Myös organisaatioiden välinen verkottuminen lisää standardisoinnin tarvetta.
3. Organisaatioiden liiketoimiensa tukemista varten kehittämät tietojenkäsittelyn periaatteet, tavoitteet ja vaatimukset ovat ainutkertaisia.

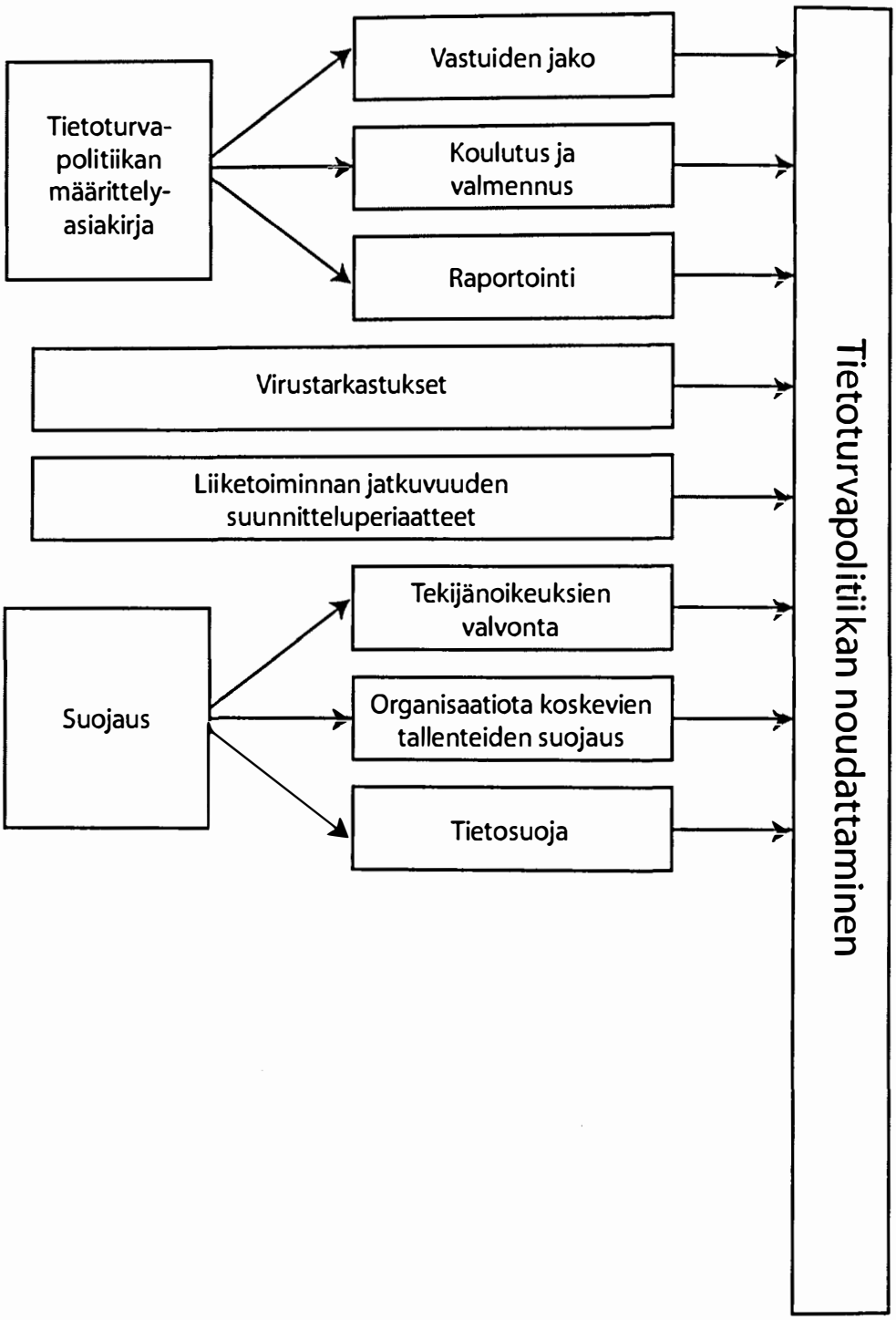
Esimerkiksi kilpailukyvyn kannalta on tärkeää, että turvallisuuspolitiikka tukee näitä vaatimuksia. Tietotekniikan perusrakenteeseen kuuluvien valvontatoimien käyttö tai niiden puuttuminen ei saa haitata liiketoimintojen tehokkuutta. Oikeat valvontatoimet ja tarvittaessa niiden joustavuus tietotekniikan suunnitteluprosessin alusta alkaen on tärkeää työn onnistumisen kannalta.

Tietotekniikan turvallisuuden valvontaan käytettävät varat tulee mitoittaa suhteutettuna informaatioon sisältyvään lisäarvoon ja muuhun riskinalaiseen tietotekniikkavarallisuuteen sekä turvallisuuden häiriytymisestä liiketoiminnalle todennäköisesti aiheutuvaan haittaan. Säännöllinen liiketoiminnan riskien ja tietotekniikan valvontatoimien tarkastelu on sen takia tietoturvallisuuden hallinnan normaali toimenpide. Siinä kiinnitetään huomiota liiketoiminnan muuttuviin vaatimuksiin ja tärkeysjärjestyksiin.

Yleensä riskianalyysimenetelmiä sovelletaan kokonaisiin tietojärjestelmiin ja -palveluihin, mutta sellainen voidaan kohdistaa myös järjestelmän yksittäiseen komponenttiin tai palveluun, jos se on käytännöllistä, realistista ja hyödyllistä.

KRIITTISET ONNISTUMISTEKIJÄT

Kokemus on osoittanut, että seuraavat tekijät ovat usein kriittisiä tietoturvallisuuden onnistuneen toteutuksen kannalta (BS 7799-1, 1999):



Kuva 1. Tulkinta Brittien Standardin (1993) suosituksista tietoturvan hallintaan organisaatioissa.

a) johdon turvallisuustavoitteet ja -toimenpiteet, jotka perustuvat yrityksen tavoitteisiin ja vaatimuksiin

b) johdolta tuleva näkyvä tuki ja sitoutuminen

c) organisaation tietoihin kohdistuvien turvallisuusriskien, sekä uhkien että vahinkoalttiuksien, samoin kuin organisaation sisäisen turvallisuustason hyvä ymmärtäminen. Sen tulee perustua tietojen arvoon ja merkitykseen.

d) turvallisuuden tehokas markkinointi kaikille johtajille ja henkilöstölle.

e) tietoturvallisuuspolitiikkaa ja -standardeja koskevan kattavan opastuksen jakaminen koko henkilökunnalle ja liikekumppaneille.

Kutakin kohtaa tarkastellaan erikseen. Tietoturvasanastoon perehtyneilläkin on joskus tulkintavaikeuksia näiden asioiden yhteydessä. Kuitenkin Code of Practice -ohjeiston tarkoituksena on levittää tietoturvan hallintaan liittyvää tietämystä, rohkaista yhä uusia yritysjohtajia ottamaan tietoturvan hallinnassaan yhtenäinen ohjeisto käyttöönsä. Siksi on perusteltua aukaista tietoturvan hallinnan kriittiset onnistumistekijät astetta tarkemmalle tasolle. Tällä tarkastelulla tavoitellaan kriittisten onnistumistekijöiden paremman ymmärtämisen vaikutusta tietoturvallisuuden johtamiseen, siis koko organisaation toiminnan kehittämiseen.

Johdon turvallisuustavoitteet ja -toimenpiteet

Organisaation on itse pystyttävä luomaan oma turvallisuusmallinsa ja tietoturvapolitiikkansa. Ulkopuolinen pystyy korkeintaan luomaan kehyksiä, joiden mukaan toimintaa kehitetään.

Turvallisuusmallissa (ISO/IEC JTC1/SC27, 1995) on kyse organisaation turvallisuuden kehittämisen organisoinnista erityisesti tietoturvallisuuden kannalta. Siihen kuuluu koko turvallisuusorganisaatio ja sen tehtävät ja tietoturvallisuuden organisointi, kehittäminen, vastuualueet ja resurssit. Kokonaisturvallisuusasioita koordinoimaan ja johtamaan on oltava turvallisuusjohtoryhmä, joka edustaa toiminnan pääalueita ja vastaa siten organisaation kokonaisturvallisuuden kehittämisestä toimintasuunnitelmien ja toimintaa ohjaavien säädösten ja lakien mukaisesti. Turvallisuusjohtoryhmä määrittää vastuutukset nimeten eri turvallisuusalueiden vastuuhenkilöt sekä päättää turvallisuuden edistämiseen käytettävistä resursseista ja toimintavaltuuksista. Turvallisuusjohtoryhmän alaisena toimii pysyviä ja määräaikaisia ryhmiä tai yksittäisiä henkilöitä, joilla on kehittämiskohteena jokin kokonaisturvallisuuden osa-alue (Kajava, 1997).

Erityisesti tietoturvallisuuden kehittämistä ja ylläpitämistä varten tarvitaan suoraan organisaation johdon alainen pysyvä tietoturvaryhmä, joka toimii organisaation tietohallinnon alan tietoturva-asiantuntijana, koordinoi ja valvoo organisaation tietojenkäsittelyjärjestelmien ja tietoliikenneyhteyksien käyttöturvallisuuden parantamista sekä huolehtii järjestelmien ylläpitäjien ja käyttäjien koulutuksesta ja ohjeistamisesta. Turvallisuusjohtoryhmä hyväksyy tietoturvaryhmän valmisteleman organisaation tietoturvapolitiikan, jossa määritellään organisaation tietoturvan toteuttamisen periaatteet ja tavoitteet, toteutuskeinot ja valvonta.

Tietoturvallisuuteen tulee sitoutua kaikilla tasoilla, organisaation johdosta tietojärjestelmien käyttäjiin. Johdon sitoutuminen ja tuki kokonaisturvallisuuden ja tietoturvallisuuden kehittämiseen näkyy myös organisaation kokonaissuunnitelmassa ja talousarviossa toimintaan osoitettuina resursseina. Turvallisuusperiaatteet toteutetaan tietoturvallisuuden osalta organisaation jokaisen tietojenkäsittelyjärjestelmän ylläpidossa ja jokaisen käyttäjän omakohtaisessa päivittäisessä käytössä.

Erityisesti tietoturvallisuuden osalta turvallisuusjohtoryhmä nimeää organisaation tietoturvallisuudesta vastuussa olevan asiantuntijaryhmän eli tietoturvaryhmän ja päättää tietoturvan kehittämisen kokonaisresurssoinnista. Turvallisuusjohtoryhmä hyväksyy organisaation tietoturvapolitiikan, johon organisaation johto siten sitoutuu.

Vastuutus on eräs keskeinen tekijä. Tietoturvaryhmä toimii suoraan organisaation johdon alaisena (Schweitzer, 1990). Tietoturvapäällikkö vastaa turvallisuusjohtoryhmän myöntämien resurssien puitteissa organisaation turvasuunnittelusta, tietoturvan toteutuksesta ja valvonnasta sekä tietoturvatietoisuuden edistämisestä organisaatiossa. Tietoturvasuunnittelijat vastaavat operatiivisesta tietoturvatoiminnasta.

Tietoturvapolitiikassa on määritelty organisaation päämäärät ja tavoitteet tietoturvan kannalta.

Määrittelyn lähtökohtana on organisaation toiminnalliset tavoitteet, organisaation toimintaa koskevat lait, asetukset ja säädökset sekä toimintaa koskevat turvallisuusvaatimukset. Tietoturvapolitiikassa määritetään tietoturvaorganisaatio, vastuut ja raportointimenettely. Politiikassa määritettään myös, kuinka epäkohdat ja väärinkäytökset käsitellään. Tietoturvapolitiikassa määritettään myös tietoturvan toteuttamiskeinot. Näitä ovat organisaation tietoturvauhkien kartoitus ja tietoriskien arviointi, tietoturvastandardien laadinta, järjestelmien ja aineistojen luokitus, tietoturvaratkaisujen toteuttaminen ja tietoturvatietoisuuden edistäminen.

Tietoturvallisuus on kaikkien yrityksen johtoon kuuluvien vastuulla oleva liiketoiminnan alue. Siksi on syytä harkita, tarvitaanko kaikissa organisaatioissa korkean tason työryhmä turvaamaan sitä, että turva-aloitteita ohjataan selkeästi ja että niillä on näkyvä johdon tuki. Jos asioita ei ole riittävästi yksinomaan tietoturvallisuudelle omistettavia säännöllisiä kokouksia varten, niin sopivan, jo olemassa olevan työryhmän tulee ottaa aihe käsittelyynsä.

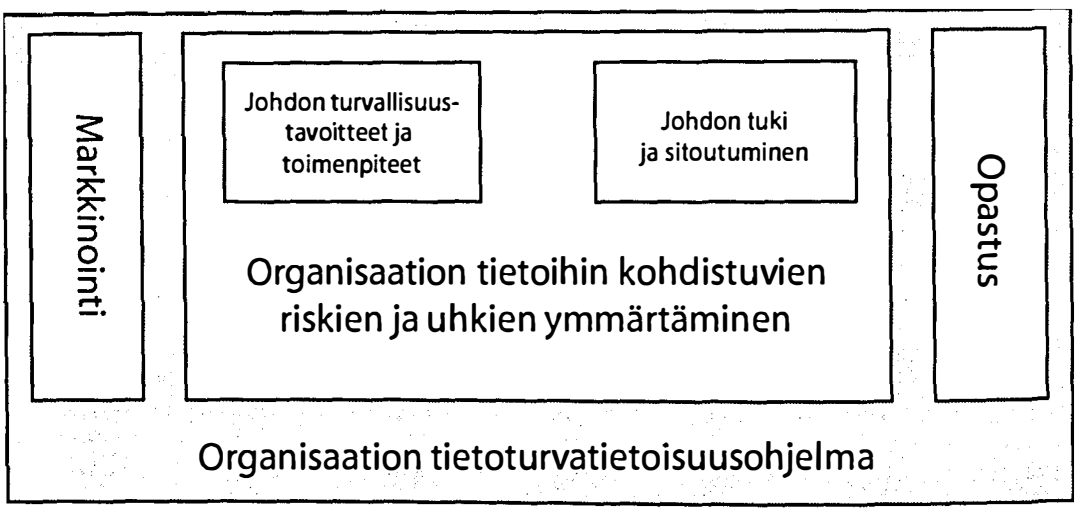
Tietoturvallisuuspolitiikan määrittelyasiakirjan tulee sisältää turvallisuustehtävien jakoa ja velvollisuuksia koskevat yleisohjeet. Niitä tulee tarvittaessa täydentää yksityiskohtaisemmilla paikallisilla, erityisiä kohteita, järjestelmiä tai palveluja koskevilla tulkinnoilla. Niissä tulee selkeästi määritellä yksittäisiä sekä fyysisiä että informaatiota sisältäviä kohteita ja turvaprosesseja, kuten liiketoiminnan jatkuvuussuunnittelua, koskevat paikalliset velvollisuudet.

Turvallisuusmalli on tarkoitettu vain organisaation johdon käyttöön. Tietoturvapolitiikka on tarkoitettu jokaisen organisaation jäsenen käyttöön, samoin se on tarkoitettu organisaation kaikkien sidosryhmien käyttöön. Hyvin laadittu tietoturvapolitiikka julkisesti saatavana voi olla myös organisaation kilpailuetu.

Johdolta tuleva näkyvä tuki ja sitoutuminen

Tietoturvapolitiikka on yrityksen ylimmän johdon kannanotto tietoturva-asioihin. On suositeltavaa, että joku yrityksen johtoon kuuluva ottaa päävastuun tietoturvallisuus-politiikan koordinoinnista. Johtoon tulee tarvittaessa luoda työryhmä tietoturvallisuus-politiikan hyväksymistä, turvatehtävien määrittämistä ja turvallisuuden toteutuksen koordinointia varten.

Tietoturvallisuuden laajaa käsittelyä tulee rohkaista esimerkiksi tarkastajien, käyttäjien ja johdon edustajien yhteistyöllä, jotta ongelmiin kiinnitettäisiin tehokkaasti huomiota. Tarvittaessa tulee hankkia tietoturvallisuuden asiantuntija-apua organisaation käyttöön. Ulkopuolista asiantuntija-apua tulee käyttää, jotta pysyttäisiin perillä alan kehityksestä, standardeista ja arvostuksista ja jotta saataisiin luoduksi hyvä yhteistyö turval-



Kuva 2. Organisaation tietoturvatietoisuusohjelma johdon tarkastelukulmasta.

lisuuteen liittyvien tapausten käsittelyä varten.

Kaikkein tärkeintä tietoturvatyössä on johdolta tuleva näkyvä tuki ja sitoutuminen. Se näkyy organisaatiossa esimerkiksi siten, että tietoturvatyö saa tarvitsemansa resurssit ja tarvittaviin toimenpiteisiin ryhdytään ripeästi. Kuitenkaan ei ole järkevää kasvattaa tietoturvaorganisaation kokoa suureksi. Pieni organisaatio on toimissaan nopea ja joustava, asiantuntemusta on parempi kasvattaa koko organisaation sisällä, siellä missä varsinaiset työprosessitkin ovat.

Johto voi osoittaa sitoutumisensa yksinkertaisesti siten, että se osallistuu erilaisiin tietoturvatilaisuuksiin muun henkilökunnan rinnalla osoittaen tällä sitä, että tietoturva on tärkeää jokaiselle organisaation jäsenelle.

Organisaation tietoihin kohdistuvien turvallisuusriskien ymmärtäminen

Organisaatioiden tiedoista on tullut eräs kaikkein tärkeimmistä pääomista. Niiden asianmukainen suojaus on välttämätöntä. Suojaukseen liittyy erilaisia käsittelyohjeita, luokituksia, säilytysohjeita ja hävittämisohjeita.

Talven 2002 - 03 aikana on ollut useita viruksiin liittyviä uhkia. Erityisesti pk-sektorilla on ollut ongelmia palauttaa toimintojaan virustartunnan jälkeen, koska asianmukaisia varmuuskopioita ei kaikissa tilanteissa ja kaikissa yrityksissä ole ymmärretty ottaa ja säilyttää.

Tiedot luokitellaan perinteisesti julkisiin ja luottamuksellisiin tietoihin. Luottamukselliset tiedot voivat olla vain virkakäyttöön tarkoitettuja tai tietylle suppealle käyttäjäjoukolle tarkoitettuja. Tietoja voidaan luokitella myös salaisiin ja erittäin salaisiin tietoluokkiin. (Kajava, 2000c). Kun useissa tapauksissa organisaatioiden johtamisalusta on muuttunut intranet -pohjaiseksi, niin tietojen käyttö- ja päivitysoikeudet ovat tulleet erittäin tärkeiksi.

Verkottunut työympäristö ja asiakassuhteet tarkoittaa esimerkiksi sitä, että joillekin tärkeille asiakkaille on jouduttu suunnittelu- ja tuotantoyrityksissä antamaan pääsy keskeneräisiin suunnittelutiedostoihin jopa seitsemänä päivänä viikossa. Tuotantoyritykselle jää esimerkiksi 20 % tiedoista omaan käyttöön. Silloin on erittäin tärkeätä pystyä valitsemaan tämä osuus niin, että tiedot eivät karkaa yrityksen hallusta.

Tietoaineistoihin kohdistuvien merkittävien uhkien arviointi on keskeistä tietoturvaan liittyvää työtä. Kuhunkin yksittäiseen järjestelmään liittyvät aineistot ja turvallisuusprosessit tulee yksilöidä ja määritellä selkeästi. Jokainen tietoaineistosta tai turvaprosessista vastuussa oleva johtaja tulee hyväksyä erillisessä prosessissa ja vastuu dokumentoida. Valtuustasot tulee määritellä ja dokumentoida selkeästi.

Aikaisemmin tietoaineistot olivat sotilasvakoilun kohteita. Nyt tilanne on muuttunut siten, että sotilasvakoilun rinnalle on tullut teollisuusvakoilu. Vakoilijoiden ei enää tarvitse olla paikan päällä, vaan esimerkiksi Internetiin ajattelemattomasti pistetyt tiedot on helppo poimia. Ihmisillä ei ole vieläkään ymmärrystä suojella esimerkiksi omaan yksityisyyteensä liittyviä tietoja. Kokonaan toinen asia ovat hakkerit, jotka aukkoja etsimällä tai murtautumalla pääsevät tärkeisiin tietoihin käsiksi. Ihmisten tiedon lisääminen niin tietotekniikassa kuin tietoturvassa on lähivuosien suurimpia haasteita.

Tietoja luokitellaan myös niiden tärkeysluokituksen mukaan. Esimerkiksi Millennium -ongelman yhteydessä tuli selväksi, että varautuminen järjestelmien sortumiseen ja toiminnan palauttamiseen vaatii ajattelutapaa, jossa on varauduttu siihen, että toiminta voidaan palauttaa pahankin katastrofin jälkeen nopeasti, kun on ennalta suunniteltu ja valittu ne ohjelmistot ja tiedostot, jotka kaikkein ensimmäisinä otetaan käyttöön. Tämä edellyttää, että kaikki järjestelmät ja myös tiedostot on etukäteen luokiteltu tärkeysluokkien mukaan ja kaikkein tärkeimmät tiedostoista otetaan ensin käyttöön.

Tulipaloihin ja katastrofeihin, esimerkiksi terrori-iskuihin, on myös tulevaisuudessa varauduttava. Ei riitä, että asianmukaiset varmuuskopiot on palosuojatussa kassakaapissa. Kaapin on sijaittava maantieteellisesti etäällä käyttöympäristöstä. New Yorkin isku osoitti kauheudestaan huolimatta sen, että tietotekniikkafirmat noudattivat varsin tunnollisesti annettuja ohjeita. Mutta tähän tuhoisaan iskuun ei kukaan ollut osannut varautua. Terrori-iskusta toipuminen osoitti, että pelkät varmuuskopiot eivät riitä, vaan yrityksillä on oltava myös maantieteellisesti etäälle sijoitettuja varalaitteita, joissa keskeisimmät ohjelmistot ja tiedostot ovat valmiina.

Myös tietojen elinkaaren loppupää sisältää suuria riskejä. Tietojen hävittäminen ei ole yksinkertainen asia. Paperien tuhoamista varten on syntynyt niin laitetuotantoa kuin palveluyri-

tyksiä. Elektronisen materiaalin hävittäminen on monimutkaisempaa. Vaikka muisteissa olevat tiedot tuhotaan ohjelmointikäskyillä, niin ne pystytään joissakin tilanteissa palauttamaan. Parhaan turvan antaa mekaaninen hävittäminen.

Tietojen hävittäminen nykyaikaisessa verkkoympäristössä voi olla hyvin vaikea tehtävä. Kun viesti liikkuu useiden palvelimien kautta, myös niihin tallentuu sanoma. Tärkeät viestit tulisi lähettää salattuna ja suojatuilla yhteyksillä, mutta myöskin näihin liittyy omat riskinsä.

Turvallisuuden tehokas markkinointi johtajille ja henkilöstölle

Brittien standardissa (BS7799-1:fi, 1999) korostetaan tietoturvallisuuden parantamiseen tähtäävien merkittävien aloitteiden hyväksyntää. On tärkeää määritellä selkeät alueet, joista kukin johtaja on vastuussa. Näin vältetään yksittäiset velvollisuuksia koskevat väärinkäsitykset.

Oma kokemukseni liittyy erilaisiin tietoturvatietoisuuden (Information Security Awareness) lisäämiseen liittyviin mahdollisuuksiin (Kajava et al 1997 a,b).

Tietoturvatietoisuutta ei pidä rajoittaa työntekijöiden valmennukseen eikä myöskään siihen kuvitelmaan, että organisaation kaikki jäsenet kuuliaisesti noudattaisivat annettuja ohjeita ja määräyksiä. Oppiminen on eräs perustekijä kohotettaessa tietoturvatietoisuutta, koska oppiminen vaikuttaa positiivisesti käyttäytymiseen (MacLean, 1992). Tämä on kuitenkin vasta minimitaso. Tietoturvatietoisuus pitäisi pystyä esittämään tiivistetysti ja hyvin organisoidusti. Suoritettua toiminnan tehokkuutta pitäisi pystyä mittaamaan, jotta voitaisiin vakuuttua organisaation tietoturvatietoisuuteen liittyvän ohjelman pätevyydestä. Työskenneltäessä yliopistoympäristössä on havaittavissa, että mitä erilaisimpia menetelmiä ja työkaluja tarvitaan toteutettaessa tietoturvatietoisuutta, koska ihmiset ovat hyvin erityyppisiä persoonina ja tehtävien suorittajina, samoin työympäristöt ovat hyvin vaihtelevia. Tarvitaan siis monentyyppistä tietoturvatietämystäkin. Turvakoulutusta tarvitaan ensisijaisesti siksi, että jokainen käyttäjä sisäistäisi sen, kuinka tärkeätä on seurata annettuja ohjeita. Käyttäjille on tehtävä selväksi myös tietoturvaloukkauksien seuraukset (Straub et al., 1992). Koulutusta tarvitaan myös, jotta haluttu tietoturvatietoisuuden taso ylläpidettäisiin (Kajava, 1996). Lähtökohtana on usein erittäin alhainen tietoturvan taso. Ihmisten mieliin asioiden tärkeyttä voidaan korostaa erilaisilla tietoisuuden kohottamismenetelmillä, kuten kampanjoinnilla ja Hammerin menetelmällä.

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. Näitä kolmea vaihetta on usein käytetty kuvaamaan termin tietoturvatietoisuus saavuttamista (Kajava & Siponen, 1997a).

On esitetty, että tietoturvatietoisuus saataisiin parhaiten ihmisten mieliin erilaisilla kampanjoilla (MacLean, 1992). Tällainen toiminta voidaan osoittaa hyödylliseksi turvakoulutuksen keinoin ja samalla se antaa oikein suoritettuna positiivista vauhtia tietoturva-asioihin, kun ihmiset muistavat turvallisuuden tärkeyden. Toisaalta turvallisuuskampanjat, kuten myös niiden poliittiset ja mainontaan liittyvät vastineensa, saattavat myös nostattaa negatiivisia tunteita, jopa vihaa.

Toinen menetelmä perustuu niin sanottuun Hammerin teoriaan, jossa tietoturvasta tehdään organisaation sisällä suosittu aihe. Oleellista Hammerin teoriassa on, että kaikki haluavat ottaa käyttöönsä organisaatioon tuodun uuden asian (Perry, 1985). Hammerin teoria ja kampanjointi sopivat yhteen suhteellisen hyvin. Lisäksi voidaan ottaa käyttöön toiminnallisia menetelmiä, jotka ovat organisaatiokohtaisia ja todennäköisesti hyödyllisempiä suurissa organisaatioissa (Kajava, J., et al, 1998).

Tietoturvatietoisuuden edistämistä voidaan suorittaa erilaisten tietoturvaan liittyvien kyselytutkimusten ja -kartoitusten yhteydessä. On asian kannalta positiivista kutsua osanottajat

ennen tutkimusta yhteiseen tiedotustilaisuuteen ja tutkimuksen suorittamisen ja analyysin jälkeen uuteen arviointitilaisuuteen. Kun arviointia on yhdessä pohdittu, on luonnollista jatkaa yhdessä organisaation tietoturvan kehittämistä. Organisaation näkökulmasta tietoturvan hallinta on erittäin tärkeä tehtävä - kokonaisuuden kannalta ollaan onnistuttu erittäin hyvin, jos työntekijät haluavat olla mukana kehittämässä organisaationsa tietoturvaa ja siihen liittyvää koulutusta.

Tietoturvallisuuspolitiikan ja -standardien saatavuus

Tietoturvapolitiikka on yritysjohdon kannanotto tietoturva-asioihin. Sen on oltava kaikkien organisaation työntekijöiden saatavilla. Myös yhteistyökumppaneille esitetään tämä asiakirja erääksi konkreettiseksi yhteistyön perustaksi. Tietoturvapolitiikka on myös muiden organisaatioiden ja ns. suuren yleisön luettavissa. Sitä voidaan pitää yrityksen positiivisena käyntikorttina, joissakin tapauksissa myös kilpailuetuna.

Eri yritykset ymmärtävät tietoturvapolitiikan eri tavoilla. Voidaan korostaa nimenomaan organisaation hallinnan suuntaa. Toinen vaihtoehto liittyy tietoturvan teknisiin suojauksiin. On yrityksiä, jotka käyttävät tietoturvapolitiikka -nimitystä suojatessaan tietoliikenneyhteyksiään. Nämä ratkaisut vaativat oman politiikkansa, mutta tämä on yksinkertainen esimerkki siitä, että terminologian yhtenäistäminen on erittäin tärkeä asia.

Tietoturvaan liittyvät standardit ovat yleensä vaikeasti saatavilla, ne ovat kalliita ja tekijänoikeusasiat liittyvät niihin korostetusti. Standardeja ei ole myöskään yleensä mahdollista jakaa henkilökunnalle. Toisaalta standardien kattavuus voi olla kyseenalaista ja tulkinta voi vaatia lisää asiantuntemusta. Näin ei yleensä ole standardien suhteen, mutta tietoturva ja sen hallinta on edelleenkin kehityksensä alkuvaiheissa oleva kokonaisuus.

Standardien jakamisen sijaan organisaation eri ryhmille on syytä kehittää ja jakaa heidän työnsä kannalta keskeisiä suosituksia ja ohjeita, jotka perustuvat olemassa oleviin standardeihin tai niiden tulkintoihin. Organisaatiot tarvitsevat perusohjeet tietoturvasta kaikille työasemien ja verkkojen käyttäjille. Lisäksi eri työtehtäviä varten tarvitaan toimintaympäristökohtaista ohjeistusta. Osa tilanteista käytännön tehtävissä on sellaisia, että on vain yksi tapa toimia, mutta on myös tilanteita, joissa suosittelumoodi ja keskustelu asiantuntijoiden kanssa auttaa viemään asioita eteenpäin.

Yritystoiminta on muuttunut voimakkaasti verkottumisen suuntaan. On erittäin tärkeää, että yhteistyökumppanit ajattelevat yhdensuuntaisesti tietoturva-asioista. Erittäin hyvä lähtökohta on, että kaikkien yhteistyökumppanien tulisi käyttää samoja lähestymistapoja, jopa standardeja tietoturva-asioissa. Mitä tarkemmin asiat pystytään sopimaan etukäteen, sitä selkeämpää työskentely on myöhemmin.

Verkostomaisessa yhteistyössä on tärkeää, että yhteistyökumppanit pystyvät luottamaan toisiinsa. Tyypillistä on myöskin toiminnan hierarkkisuus, toinen tuottaa palveluja, toinen hyödyntää niitä. Mitä tarkemmin tietoturvavaatimukset pystytään määrittelemään ennen toiminnan alkamista sopimuksin, sitä selkeämpää on yhteistyö. Kun säännöt on selvillä, pystytään keskittymään oikeisiin asioihin.

UHKAULOTTUVUUDET

Syyskuun 11. päivän 2001 asiat ovat heijastuneet monin tavoin koko yhteiskunnan toimintaan. Kokemuksia on saatu niin tietoturvan perusasioista kuin järjestelmien elvyttämisestä ja varautumisesta lähitulevaisuuteen. Samoin käytettävyyteen liittyvät asiat tulivat monin tavoin esille.

Perinteinen langallinen tietoliikenne kärsi häiriöistä, jotka aiheutuivat ylikuormituksesta ja katkoksista. Langaton viestintä osoitti käyttökelpoisuutensa katastrofitilanteessa. Oleellista oli ollut, että USA:ssa hyvin monet olivat suhtautuneet matkapuhelimiin lähinnä viihde-elektroniikkana. Vaikea terrori-isku osoitti, että matkapuhelimet ovat erittäin tärkeä apuväline vaikeassa katastrofitilanteessa. Kun yhteiskunnan epävarmuus lisääntyy, kansalaiset myös Yhdysvalloissa tulevat ilmeisesti hankkimaan entistä enemmän langattomia laitteita.

Perinteisissä tietoverkoissa katkokset ja ylikuormitus aiheuttivat suuria ongelmia. Perinteiset joukkoviestimet radio ja televisio maailmanlaajuisina tiedotusvälineinä toimivat moitteettomasti. Internetin toimintamahdollisuuksia suuren katastrofin yhteydessä oli epäilty. Nyt toiminta kesti

kuormituksen eikä rajallisen määrän palvelimia menettäminen haitannut toimintaa merkittävästi.

Tietoturvaan liittyvässä tarkastelussa voidaan todeta, että niin järjestelmät, ohjelmistot kuin tiedostotkin oli asianmukaisesti suojattu maantieteellisesti etäällä olevissa varapaikoissa. Katastrofin suuruus tarkoittaa kuitenkin sitä, että vastaisuudessa on varauduttava terrori-iskuihin siten, että varapaikoissa on myös varapalvelimet.

Mitä voi lähitulevaisuudessa tapahtua? Terroristit ovat ottaneet toistaiseksi aseikseen siviilikulkuneuvoja. Kemiallisista ja biologisista aseista on myös keskusteltu. Milloin on tietokoneiden aika?

Tietoturva-alan asiantuntijat ovat varsin pitkään odottaneet elektronisia sabotaaseja. On ollut joitakin "läheltä piti" -tapauksia. Myös pienempiä vahinkoja on sattunut, virallisia tai poissa julkisuudesta. Esimerkiksi Dorothy Denning (1999) nimesi tietoturvaan liittyvän oppikirjansa enteellisesti "Informaatiosodankäynti ja turvallisuus".

Keskustelu kansalaisten oikeuksista, erityisesti yksityisyyteen liittyvistä kysymyksistä, on näiden terrori-iskujen jälkeen muuttumassa. Tietoyhteiskunta tarvitsee nykyistäkin laajempia kontrolleja kansalaistensa ja yritystensä suojaamiseksi. Jos vielä elokuussa 2001 kontrollit koettiin kansalaisten oikeuksia rajoittaviksi, niin nyt on oikea aika havaita, että kontrollit ovat nimenomaan meitä suojelemassa, ne ovat muuttuneessa tilanteessa kansalaisten ystäviä. Yritysten ystäviä ne ovat olleet jo huomattavasti kauemmin.

Olemassa olevat kontrollit otettiin käyttöön laajassa mitassa esimerkiksi lokakuussa 2002, kun selviteltiin taustatietoja Myyrmannin räjähdykseen. Niin kameratallenteet kuin automaattisen joukkoliikenteen tiedot olivat tärkeä osa edeltävien tapahtumien selvittelyssä. Internet ja sieltä saatavat pomminteko-ohjeet tulivat uudelleen esille. Myös erilaisissa keskusteluryhmissä oli pommiasioita tarkasteltu, mutta Internetiin kohdistuvat kontrollit voidaan kiertää esimerkiksi siirtämällä keskustelu toiselle puolelle maapalloa, jossa on erilainen lainsäädäntö. Eivätkä paikalliset ihmiset ole suomenkielen taitoisia.

Kontrollit rakennettiin aluksi suojelemaan yritysten aineellista omaisuutta. Rikokset ovat muuttuneet viime vuosikymmenen aikana yhä enemmän aineettomaan suuntaan, niistä on tullut tietoomaisuuteen kohdistuvia, kuten teollisuusvakoilu. Kulunhallinnan lisäksi yritykset kontrolloivat tai suunnittelevat kontrolloivansa työntekijöidensä puhelimen, tietokoneen ja sähköpostin käyttöä. Kontrolleihin liittyvä teknologia oli muutama vuosi sitten kallista, nyt sitä saa huomattavasti edullisemmin. Aikaisemmin kontrollien koettiin uhkaavan työntekijöiden yksityisyyttä, niitä pidettiin työntekijöiden näkökulmasta vihamielisinä. Kun tietoyhteiskuntamme on saanut uuden suunnan vihollisuuksien suhteen, on aika muuttaa käsityksiä ja asenteita. Onko siis kontrolleista tulossa kansalaisten ystäviä?

ORGANISAATION TIETOTURVAN PARANTAMINEN

Tietoturvallisuuden parantamiseksi on valmiita ohjeita saatavilla, esimerkiksi BS7799-2:fi (1999) ja Miettinen (1999). Näiden avulla on mahdollista rakentaa oman yrityksen tietoturvan hallinnan perusta. Teoriassa asiat voivat näyttää suhteellisen yksinkertaisilta, mutta käytännössä kaikkia vaihtoehtoja on mahdotonta arvioida.

Vanha ohje on, että laitetaan tietoturvallisuuden yksi osa-alue kuntoon vuodessa ja siirrytään seuraavana vuonna seuraavaan osa-alueeseen. Tällainen ajattelu edellyttää kuitenkin, että koko aluetta tarkkaillaan ja jos jotakin hälyttävää ilmenee, tilanne korjataan välittömästi. Tällainen toiminta tuottaa muutamien vuosien jälkeen tilanteen, jossa voidaan todeta, että organisaation tietoturva on pääosiltaan hallinnassa.

Tietoturvan luonteeseen kuuluu erilaisia tasoja ja ulottuvuuksia. Kriittisissä tilanteissa asioita voidaan tarkastella erillisinä, mutta käytännön ratkaisuihin on aina kietoutunut monia komponentteja. Valmiit ohjeet tai standardit eivät suoraan sovellu noudatettavaksi jossakin määrätyssä organisaatiossa. Ne voivat olla kehikkoja, kun mietitään organisaation toimintojen huomioonottamista käytännön turvaratkaisuja toteutettaessa. Toteutuksen asiantuntijoita ovat organisaation omat henkilöt, joilla on pitkäaikaisen käytännön kokemuksen kautta tietämys asioista.

Aikaisemmin pyrittiin valitsemaan suuresta signaalijoukosta kaikkein oleellisimmat ja vahvimmat. Kun tietokoneet ovat tulleet nopeammiksi ja tehokkaamiksi, on pystytty saamaan uutta tietoa ennen selvittämättömistä tapahtumista. Lähivuosien eräs haaste tulee olemaan, kuinka parempia tietokoneita pystytään hyödyntämään organisaa-

tioiden, yksilöiden ja yhteiskunnan ennakoivan turvallisuuden parantamisessa.

Liiketoimintojen ja organisaatioiden verkottumisen takia prosessimallin käyttö tulee tietoturvan hallinnassa olemaan lähitulevaisuudessa välttämätöntä. Tietoturvan kehittäminen kuuluu suurempaan lohkoon, jossa oleellista on yritysturvallisuuden kehittäminen (Miettinen, 2002). Turvallisuus takaa yrityksille paremmat edellytykset menestyä liiketoiminnoissaan. Tietoyhteiskunnan tavoitteena on kuitenkin paremmin menestyvät yritykset, jotta yksilöille voitaisiin taata parempi yhteiskunta. Myös yksilöön kohdistuvien tiukempien kontrollien avulla.

Tietoyhteiskunnalle on ominaista, että koneet valvovat ihmisten toimintaa. Ihmiset tietävät, että väärinkäytökset saadaan helposti selville palauttamalla tilanne. Tiedot jäävät vain koneille. Jos mitään poikkeavaa ei tapahdu, valvonnasta vastaavien ihmisten ei tarvitse puuttua tilanteeseen. Tieto jatkuvan kontrollin päälläolosta ei tulevaisuudessa tule enää vaivaamaan ihmisiä niin voimakkaasti kuin nyky-yhteiskunnassa. Kun yksilö ei syyllisty luvattomaan saati rikolliseen toimintaan, hänen ei tarvitse pelätä kontrolleja. Vaikka ne on alun perin suunniteltu palvelemaan yrityksiä ja organisaatioita, niin nyt on havaittavissa, että ne tarjoavat tukea myös lainkuuliaisille kansalaisille.

Terrori-iskujen tavoitteena on pyrkiä tuhoamaan olemassa oleva yhteiskunta. Syyskuun 2001 tapahtumat ovat osoittaneet, että kansakunnat ovat voimistaneet yhdessä ponnistuksensa terroritoimintaa vastaan. Samalla on ainakin toistaiseksi lopetettu keskustelu avoimuuden lisäämisestä. Vaikka arvostamme suuresti kansalaisten yksityisyyttä ja vapautta, niin yleinen mielipide on siirtynyt kannattamaan läpinäkyvää kontrollia. Kontrollista on tulossa tietoyhteiskunnan kansalaisen ystävä. Ei kansalaisia vastaan, vaan yhteiskunnan suojelemiseksi terroriteoilta.

KRIITTINEN ARVIOINTI

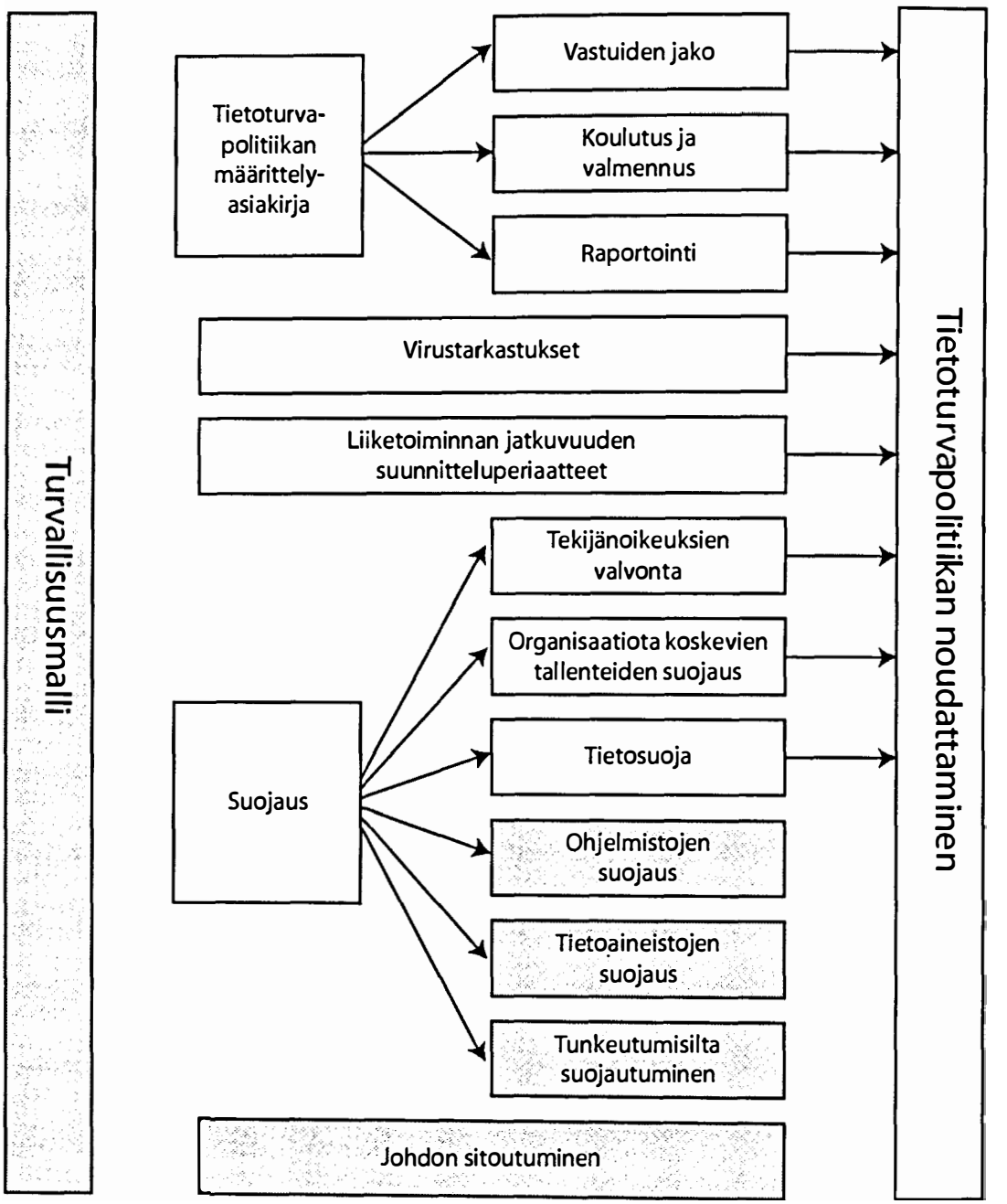
Turvallisuuden opastamiseen ei ole yhtä menetelmää. Jokaisella käyttäjäryhmällä tai tietotekniikan asiantuntijalla on erilaiset vaatimukset, ongelmat ja tärkeysjärjestys tehtävästä ja organisaatiosta riippuen. Monessa organisaatiossa tähän on kiinnitetty huomiota kehittämällä eri henkilöstöryhmille yksilölliset tulkintaohjeet. On suositeltavaa, että organisaatiot, jotka päättävät ottaa käyttöön erilaisen rakenteen tai ehkä kehittävät paikallisen tulkintaohjeen, säilyttäisivät viittaukset Code of Practice -standardiin. Näin tulevat liikekumppanit tai tarkastajat voivat verrata tätä standardia ja organisaation omia turvallisuusohjeita (BS 7799-1:fi, 1999).

Valvonnan avaintoimenpiteitä tarkkailemalla voidaan todeta, että kaikki esitetyt komponentit tähtäävät tietoturvallisuuden noudattamiseen organisaatiossa (BS 7799-1:fi, 1999). Tietoturvapolitiikan määrittelyasiakirjassa korostetaan erityisesti vastuiden jakoa, koulutusta ja valmennusta sekä tapahtumiin liittyvää raportointia. Erillisiä kokonaisuuksia ovat virustarkastukset ja liiketoiminnan jatkuvuuden suunnittelu. Suojaukseen liittyvään kokonaisuuteen kuuluvat tekijänoikeuden suojaamien ohjelmien kopioinnin valvonta, organisaatiota koskevien tallenteiden suojaaminen sekä tietosuoja, joka tarkoittaa organisaation henkilökunnan yksityisyyteen liittyvien tietojen suojaamista.

Olen itse pitänyt kaikkein vaikeimpana tietoturvakysymyksenä hakkerointia (Kajava, 1999, 2000a). Jo pelkästään tunkeutumisella tai sen yrityksellä saadaan paljon pahaa aikaiseksi, mutta siihen voidaan lisätä esimerkiksi virusten levittämistä tai taloudellisia rikoksia, jotka voivat liittyä esimerkiksi luottokorttitietojen anastuksiin. Kun tiedossa on, mitä haittaohjelmia Internetin kautta voidaan hakea, niin jo hyvin vaatimattomalla tietotekniikan osaamisella esimerkiksi terrorijärjestön jäsen voi saada suurempia tuhoja aikaiseksi kuin syyskuun 2001 mustana tiistaina tapahtui. Kyseiseen terroritoimintaan ei tarvitse kaapata lentokonetta, ei tarvitse osata ohjata sitä!

Valvonnan avaintoimenpiteitä tarkasteltaessa huomio kiinnittyy asiantilaan, johon toimenpiteet johdattavat, tietoturvallisuuden noudattamiseen. Kun tilannetta hahmottelee, niin turvallisuusmalli olisi jo tasapuolisuuden nimissä mainittava koko tilanteen lähtökohdaksi.

Brittien standardia BS7799:a on kehuttu erinomaiseksi apuvälineeksi kehitettäessä organisaatioiden tietoturvaa. Itse olen suhtautunut siihen eräin osin kiitellen, mutta samalla olen esittänyt varauksia toisista osioista. USA on omaksunut kyseisen standardin mukailtuna ISO 17799 -standardina. Jälkimmäisen soveltamisesta oli tilaisuus kuunnella esitelmä (Baskerville, R., 2001). Tietoturvallisuuden eri tasot organisaatioissa esitettiin, kuitenkin jäin kaipaamaan kahta



Kuva 3. Parannettu ehdotus organisaatioiden tietoturvan hallintaan.

asiaa. Toinen oli tietoaineistoturvallisuus (Data Security), toinen ohjelmistoturvallisuus (Software Security). Kyseiset asiat voi löytää mainituista standardeista vain viittauksenomaisina. Oleellisin piirre ISO 17799 -standardissa (2001) on, että aikaisemmin asiat esitettiin mieluummin suositusten muodossa, nyt niihin puututaan voimakkaammin käyttämällä termiä control.

Suomessa kaivataan erityisesti käytännönläheisiä ohjeita pk -teollisuuden tarpeita varten. Kun käyttää Brittien standardia, niin huomaa, että se on suunnattu suurille, kansainvälistä toimintaa yli valtiollisten rajojen harjoittaville yrityksille. Pk-sektorille sen ohjeet soveltuvat vain rajallisesti. Kuitenkin verkottuneessa maailmassa teollisuuden ja kaupan laaja yhteistyö perustuu siihen, että suuret yritykset ovat verkottuneet pienempien kanssa. Pk-yritykset tuottavat erilaisia ulkoistettuja palveluja ja alihankitaan liittyviä osatoimituksia isommille yrityksille. Toiminta yhden suuren yrityksen tasolla on hierarkkista useassa kerroksessa. Jos yhden pienen yrityksen tietoturvassa on vakavia puutteita, niin se heijastuu nopeasti myös suureen yritykseen, joka puolestaan on verkottunut muihin isoihin organisaatioihin.

Code of Practicella haettiin nimenomaan suurten yritysten maailmanlaajuista yhteistyötä, joka lähtee tietoturva-asioiden yhdensuuntaistamisella suurten yritysten tasolla. Mutta samanaikaisesti olisi erittäin tärkeää saada pienet yritykset mukaan tietoturvatyöhön, jotta niiden sektorilta ei olisi odotettavissa uusia tietoturvauhkia maailmanlaajuiseen yhteistyön. Olisi saatava erittäin pian pk -yrityksille suunnattu vastaava käytännönläheinen ohjeisto, joka olisi käytössä kaikissa maailmakaupan keskeisissä valtioissa.

Nykyisessä tilanteessa joudumme olemaan varautuneita mitä uskomattomimpiin terrori-iskuihin ja silloin juuri kyseisten alojen ymmärtäminen on erittäin tärkeää. Asian toinen puoli liittyy kansainväliseen tietojenkeruujärjestelmään, jota käytetään vakoilussa. Echelon oli aluksi kehitetty sotilasvakoilua varten, mutta se on soveltunut myös teollisuusvakoiluun. USA on järjestelmän kehittäjä ja Englanti on sen tärkeä liittolainen. Taistelu terrorismia vastaan ei oikeuta jättämään kahta turvallisuuden aluetta vähemmälle huomiolle - tietoaineisto- ja ohjelmistoturvallisuus ovat muuttuneet koko yhteiskunnan kannalta kaikkein keskeisimmiksi kysymyksiksi.

Syyskuun 2001 terrori-iskut vaikuttivat yhteiskunnan toimintaan siten, että tietoturvakysymykset ovat tulossa kaikkein tärkeimmiksi. On arvioitu, että tietoturva on lähivuosien tietoyhteiskunnan toimintojen "moottori", liikkeellepaneva voima.

Odotukset tietoturvatuotteiden voimakkaasta kasvusta ovat toteutuneet, mutta kasvu on pääasiassa toteutunut Yhdysvaltojen sisäisenä toimintana. Investointeja ei epävarmassa tilanteessa ole uskallettu suunnata laajasti Eurooppaan, "epävarmalle alueelle". Suomalaisten vientiin tarkoitettujen ohjelmistotuotteiden joukossa tietoturvatuotteet ovat olleet hyvin tärkeässä asemassa, mutta kysynnän suunnasta johtuen omat kansalliset yrityksemme toimivat tällä hetkellä "hyvin matalalla tasolla", pienellä volyymilla.

Matkalla tietoyhteiskuntaan aikakausi on vaihtunut. Avoimuuden rinnalla hyväksytään vähitellen erilaisten kontrollien olemassaolo. Tietoturvan hallinnan näkökulmasta erittäin tärkeänä reaktiona pidetään myös sitä, että nyt ymmärretään tietoturvallisuuden johtamisen merkitys. Aikaisemmin esitettyjen kymmenen avaintoimenpiteen yläpuolelle nousee uusi toimenpide. Muuttuneen yhteiskunnan tärkein avaintoimenpide on organisaation ylimmän johdon sitoutuminen tietoturvaratkaisuihin ja tietoturvan johtamisen tukemiseen. Toinen keskeinen alue on työntekijöiden mukaansaaminen tietoturvatoimintaan, joka voisi tapahtua tietoturvatietoisuusohjelman avulla.

YHTEENVETO

Tietoturvan käytännön ratkaisut liittyvät hyvin usein liiketoimintaan. On kuviteltu, että kun tietoturvan eri alueet on systemaattisesti käyty läpi ja tehty asianmukaiset muutokset ja hankittu tarvittavat tietoturvatuotteet, asiat olisivat hyvässä kunnossa. Mutta on muistettava, että tietoturva ei ole mikään projekti, se on koko yrityksen eliniän jatkuva prosessi.

Jos tietoturvan tasoja ei tunneta syvällisesti, niin voidaan turvautua valmiisiin ratkaisuihin, apuvälineisiin tai jopa "temppuihin". Kuitenkin jokaisen organisaation toiminnassa on paljon asioita, joiden turvallisuutta voidaan parantaa vain ymmärtämällä oma toiminta ja rakentamalla sen päälle laaja ratkaisu, jossa myös ihmisten asema on huomioitu. Pelkästään yhtä tasoa tutkimalla ja sille parhaan ratkaisun tekemisellä ei saada käytännön kannalta turvallista ratkaisua, koska tosi-

tilanteissa kokonaisuuteen vaikuttaa hyvin moni asia. On korostettava, että tietoturvallisuus ei ole ON / EI -asia.

Tietoturvan hallinnan kannalta oli tärkeää tehdä päätös siitä, että keskeisillä teollisuusvaltioilla niin Euroopassa, Yhdysvalloissa kuin Australiassa on yhteinen lähestymistapa tietoturvan hallintaan. Ei ole haettu parasta vaihtoehtoa, vaan oleellista on ollut saada aikaan yhteinen päätös valittavasta lähestymistavasta. Siitä on kehittynyt eri alueille standardi toiminnan perustaksi.

Yhteinen näkemys on tärkeä osa toimintaa, mutta olisi palattava jälleen perusasioihin - ei ole olemassa valmista tietoturvaa, vaan se vaatii alinomaista prosessointia. Kun on päästy sopuun yhteisestä toiminta-alustasta, niin seuraavana vaiheena on lähteä kehittämään alustaa niin suurten monikansallisten yritysten tarpeita varten kuin lähteä ajamaan politiikkaa, joka tuottaisi myös pk-yritysten käyttöön yhteisen standardoidun ohjeistuksen. Vaikka yritysten kokoluokka poikkeaa erittäin suuresti toisistaan, niin tietoturvavahingot voivat olla yhteisiä. On totuttu ajattelemaan, että suuret yritykset voivat joutua isojen vahinkojen kohteeksi, mutta pienissä vahingot on suhteutettava niiden toiminnan volyymiin.

Tietoyhteiskunnassa vahingot eivät koske pelkästään yksittäistä yritystä, vaan seurauksena saattaa olla koko verkottuneen toiminnan tappio. Siksi pk -yritysten turvallisuus on kaikkien velvollisuus.

Toinen yhteenvetoajatus liittyy terrorismiin. Syyskuun 2001 jälkeen lähti liikkeelle voimakas tietoturvainvestointeja suosivaa kehitys. Se odotettiin yltävän myös Eurooppan. Kävi kuitenkin toisin. Tietoturvainvestoinnit suunnattiin yrityksiin USAssa. Vastaavasti eurooppalaiset tietoturvafirmat ovat kokeneet ankeita aikoja, niiden tuotteita ei ole huolittu kriittisessä tilanteessa ratkaisemaan USAn yritysten tietoturvaongelmia.

Syyskuu 2001 sai aikaan voimakkaan tietoturvatuotteiden hankinta-aallon. On tärkeää, että yrityksiä pyritään suojaamaan mahdollisilta ja myös mahdottomilta uhkilta asianmukaisin järjestelyin. Painopiste on ollut teknologiassa. Code of Practice on ollut eräs ensimmäisistä herätteistä saada tietotekniikan käyttäjille standardoitua yhteneväiset ohjeet tietoturvasta ja sen hallinnasta.

Toinen vaihe voisi olla enemmän ihmisiin painottunut. Yritysten ylimmän johdon olisi ymmärrettävä yhä laajemmin tietoturvaan sitoutumisen merkitys. Ei riitä, että ylin johto ymmärtää tietoturvauhkien vaarallisuuden, heidän olisi oltava hyvin perillä myös tietoturvallisuustyön johtamisesta ja siihen liittyvistä vastuista. Eräs tärkeä vastuualue liittyy siihen, että kaikki työntekijät pyrittäisiin saamaan erilaisten tietoturvatietoisuus -ohjelmien pariin.

Jos tietoturvan hallinta tuntuu tämän päivän ihmisistä mahdottomalta tehtävältä, niin tulevaisuudessa tämä on erittäin tärkeä kysymys: Tuleeko tietoturvasta sellainen komponentti, joka on aina läsnä, hiljainen tietojenkäsittelykomponentti? Siis voisiko tulevaisuuden ihminen sopeutua yhteiskuntaan, jossa kontrollit olisivat ubicomp -komponentteina, ärsyttäisikö passiivisena oleva ubicomp -tietoturva ihmistä vähemmän?

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

LÄHTEET

Allen, J.H. (2002), CERT Verkkotietoturvan hallinta. Addison Wesley. IT Press, Edita Publishing Oy. Helsinki.

Anttila, J., Kajava, J., Miettinen, J. E. (2001): Changes in ITC Security Education due to Changing Technology. In Jan Knop and Peter Schirmbacher (eds.): "The Changing Universities - The Role of Technology". Proceedings of the 7th International Conference of European University Information Systems (EUNIS 2001). Humboldt-University at Berlin. March 26 - 30. Berlin, Germany.

Baskerville, R. (2001), Managing Security for Internet Speed Software Development: Emergent Systems Development Security. Visiting lecture. University of Oulu. 8th November. Oulu.

BS7799-1:fi. (1999), Standardi. - Tietoturvallisuuden hallinta. Osa 1: Tietoturvallisuuden hallintajärjestelmiä koskeva menettelyohje. Suomen standardisoimisliitto SFS, 15.2.

BS7799-2:fi. (1999), Standardi. - Tietoturvallisuuden hallinta. Osa 2: Tietoturvallisuuden hallintajärjestelmiä koskevat vaatimukset. Suomen standardisoimisliitto SFS, 15.2.

A Code of Practice for Information Security Management, (1993), Department of Trade and Industry. DISC PD003. British Standard Institution, London, UK.

Information Technology - Code of Practice for Information Security Management. (2001), BSI ISO/IEC 17799: 2000. BS 7799-1: 2000. BSI. London, UK.

Denning, D. (1999), Information Warfare and Security. Addison Wesley Longman, Inc. ACM. Reading, MA.

Härkönen, J. & Kallio, J. (2001), Kansallisen tietoturvallisuusstrategian tarve Suomessa. Liikenne- ja viestintäministeriön mietintöjä ja muistioita B 36/2001. Helsinki.

ISO/IEC JTC1/SC27, (1995), Guidelines for the Management of IT Security (GMITS).

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

Kajava, Jorma, (1997), Turvallisuusmalli organisaation tietoturvatoiminnan perustana. Oulun yliopisto, tietojenkäsittelyopin laitos, Sovellukset ja hallinto, Sarja D 8, OULU UNIVERSITY PRESS, tammikuu, Oulu.

Kajava, Jorma & Siponen, Mikko T. (1997a), Effectively Implemented Information Security Awareness - An Example from University Environment. In Jan HP Eloff and Rossouw von Solms, editors: Information Security - from Small Systems to Management of Secure Infrastructures. Proceedings of WG 11.2 and WG 11.1 of TC11 (IFIP TC-11 Sec'97, 13th International Information Security Conference). IFIP, 13 - 16th May, Copenhagen, Denmark.

Kajava, Jorma & Siponen, Mikko T. (1997b), IT Security Awareness - Issues for Industry. In Arto Karila & Timo Aalto (eds.): Encouraging co-operation. Proceedings of the Second Nordic Workshop on Secure Computer Systems (NORDSEC'97). Helsinki University of Technology, Department of Computer Science and Engineering, Telecommunications Software and Multimedia Laboratory, TLM - C 2, 6 - 7th November, Espoo, Finland.

Kajava, Jorma & Siponen, Mikko, (1998), Tietoturvatietoisuus yliopiston tietoturvan hallinnassa. IV yliopistojen atk-keskusten tietoturvaseminaari (toim. Kaisu Ranta). Oulun yliopisto, ATK -keskus, 11 - 12.2. Oulu.

Kajava, Jorma, (1999), Hakkerit ja yliopistoympäristö. Invited speech. FRAUD FORUM'99. Sonera Ldt. Helsinki/ Finland & Stockholm/Sweden 3-5.6.

Kajava, Jorma (2000a), Hackers - the Most Insidious Threat to the Information Society. In Nätets juridik. Nordisk årsbok i rättsinformatik 1999. Red. Ari Koivumaa. Stockholm: Jure AB. s. 35-43.

Kajava, Jorma (2000b), Tietoturvan yksilöön ja organisaatioon kohdistuvat haasteet 2000 -luvun alussa - Information Security Challenges for Users, End-Users and Organizations in the Beginning of the new Millennium (Abstract in English). Hallinnon tutkimus - Administrative Studies. Volume 19, Number 2. Tampere.

Kajava, Jorma (2000c), Luokitus kertoo tiedon tärkeyden yritykselle. Kaleva nro 83/2000, Oulu, 25.3. P. 2.

Kajava, Jorma (2001a), Tietoturvan merkitys IT -sidonnaisissa liiketoimintaprosesseissa. Tehokas ja kehittyvä IT. Nykyaikaisten liiketoimintaprosessien kehittämisen haaste. IIR Finland Oy (Institute for International Research). Innopoli, Espoo. 25 - 26. huhtikuuta.

Kajava, Jorma (2001b), Sisäpiiririkokset tietoverkoissa - kulisseista parrasvaloihin. Viestimies, Vol. 56 nro 3. Syyskuu. Helsinki. Pp. 22 - 25.

Kajava, J. (2001c), Johdatus tietoturvaan: perusluonne ja tasot. Johdatus tietojenkäsittely-tieteisiin -kurssin luento. Oulun yliopisto. Tietojenkäsittelytieteiden laitos. 31. lokakuuta. Oulu.

Kerttula, Esa, (1998), Tietoverkkojen tietoturva, Liikenneministeriö, EDITA, Helsinki.

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. & Kajava, Jorma, (1994), Tietoriskien arviointi - Risk Analysis and Risk Assessment - an Overview of Basic Ideas and Commonly Used Techniques (abstract in English). University of Oulu, Department of Information Processing Science, Research Papers Series A 20, Oulu, May.

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

Miettinen, Juha E., (2002), Yritysturvallisuuden käsikirja. Kauppakaari. Helsinki.

The NIST handbook, An Introduction to Computer Security. (1995), NIST special publications in October.

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

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

Pimes, Jari, Sahlman, Anssi, Kajava, Jorma, (2000), Tietoturva ja sisäinen valvonta - Information Security and Internal Control (Abstract in English). University of Oulu, Department of Information Processing Science, Working Papers Series B 62. OULU UNIVERSITY PRESS, November. Oulu.

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

Schweitzer, J. A. (1990), Managing Information Security: Administrative, Electronic, and Leagal Measures to Protect Business Information. Second Edition. Butterworths. Boston.

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.

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

Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus. (2000), Vahti, Valtionhallinnon tietoturvallisuuden johtoryhmä 3/2000. Valtiovarainministeriö. Helsinki.