

KANSALLISEEN TIETOTURVALLISUUSSTRATEGIAAN
LIITTYVÄ
TIETOTURVAKATSAUS

13.6.2002

Kansallinen tietoturvakatsaus

1	TIIVISTELMÄ	3
2	TAUSTA JA RAJAUKSET	5
	2.1 Katsauksen sisältö	5
	2.2 Muut rajaukset	7
3	YHTEISKUNTA JA TIE TOTURVALLISUUS	9
	3.1 Yhteiskunnan lisääntyvä riippuvuus tiedosta	9
	3.2 Tietoturvallisuus yhteiskunnassa	10
	3.3 Luottamuksen merkitys	12
	3.4 Kansainvälisyys	14
4	TIE TOTURVALLISUUDEN UHKATEKIJÄT	16
	4.1 Uhkien merkitys	16
	4.2 Muutosvoimat ja ajurit	17
	4.3 Uhat yhteiskunnan sektoreilla	20
	4.3.1 Uhat yhteiskunnan tasolla	20
	4.3.2 Julkisen sektorin uhat	21
	4.3.3 Yritysten uhat	23
	4.3.4 Yksityishenkilöihin käyttäjinä kohdistuvat uhat	27
5	TOTEUTUNEET TOIMENPITEET TIE TOTURVALLISUUDEN EDISTÄMISEKSI	29
	5.1 Tietoturvaluuteen liittyvä sääntely	29
	5.2 Tietoturvatietoisuus	30
	5.3 Vastuullisuusnäkökulma	31
	5.4 Eettiset periaatteet	32
	5.5 Demokratiaperiaatteet	32
	5.6 Vastatoimet	33
	5.7 Riskien arviointi	35
	5.8 Teknisten tietoturvaluustoimenpiteiden implementointi	35
	5.9 Tietoturvaluisuuden hallinnointi	36
	5.10 Keskeiset toteutuneet tietoturvaluustoimenpiteet sektoreittain	37
	5.10.1 Tietoturvaluustoiminta yhteiskunnassa	37
	5.10.2 Julkinen hallinto	38
	5.10.3 Yritykset	39
	5.10.4 Yksityishenkilöt	40
6	YHTEENVETO	41

1 TIIVISTELMÄ

Tämä tietoturvakatsaus on tehty kansallisen tietoturvastrategiatyön osana, ja se tarkastelee laajasti aiheen problematiikkaa: tietoturvauhkia, tietoturvallisuuden tason arviointia, eri osapuolilta edellytettäviä ja jo toteutuneita vastatoimia. Katsauksessa on erityisesti tuotu esiin vasta viime vuosina akuuteiksi nousseita ilmiöitä. Teknisiä yksityiskohtia on pyritty välttämään, ja tietoturvallisuuden yhteiskunnallinen merkitys on tuotu selkeästi esiin. Tämän vuoksi katsauksessa korostuu luottamuksen saavuttamisen ja säilyttämisen tärkeys.

Tässä tilannekatsauksessa lähtökohtana on ns. kaupallinen tietoturvataso: riskejä pyritään pienentämään, kunnes niiden pienentämisestä aiheutuvat kustannukset ylittävät saavutettavan hyödyn. Tämän lisäksi on organisaatioita, joiden tavoitteena on ns. absoluuttinen turvallisuus ja tietoturva: pyritään mahdollisimman hyvään tietoturvallisuuden tasoon lakien, toiminnan luonteen tai muiden seikkojen velvoittamina.

Tietoturvallisuus on käsitettävä toimintaympäristön ominaisuutena, joten sen kehittäminen ja ylläpito on jatkuva prosessi. Usein tietoturvallisuus mielletään vain tietojen suojaamiseksi ulkopuolisten käytöltä, mutta tietoturvallisuus on käsitettävä laajemmaksi kokonaisuudeksi, joka kattaa tietojen käytettävyyden ja tietoturvallisuuden hallinnoinnin.

Katsauksen näkökulma tietoturvallisuuteen on tietoyhteiskunnan turvaaminen. Suo messä tietoyhteiskunnan kehitys on ollut nopeaa, jolloin eri toimijoiden on saattanut ollut vaikeaa arvioida kehitykseen liittyviä tietoturvallisuushkia. Tietoyhteiskunnassa toiminta on verkostoitunut, jolloin kokonaisturvallisuuden hallinnasta on tullut yhä haasteellisempaa. Turvallisuus lähtee koko liiketoiminnan hallinnasta ja päättyy teknologisiin ratkaisuihin.

Vaikka katsauksessa on tarkasteltu uhkia yhteiskunnan sektoreittain, on jokaisen sektorin sisällä merkittävää vaihtelua niin lähtötilanteissa kuin tavoitteiden asetannassa. Sektorikohtainen tarkastelu on valittu helpottamaan tietoturvallisuuden vaikutusten sitomista yhteiskunnallisiin asioihin ja ilmiöihin. Erityisesti on otettava huomioon, että suurin osa tietoturvallisuuden uhista kohdistuu kaikkiin yhteiskunnan sektoreihin joko suoraan tai verkostoitumisen johdosta välillisesti.

Tietoturvaan käytettävissä olevat resurssit ovat rajalliset, joten kaikkien toimijoiden tulee tehdä yhteistyötä ja suunnata resurssit koordinoitusti. Toistaiseksi yhteistyö ei kaikilta osin ole ollut riittävää. Tietoturvaumat ovat merkittävässä määrin kansainvälinen ongelma, joten kansainvälinen yhteistyö on monien uhkien torjunnassa avainasemassa.

Tietoturvallisuuden perusongelma on riskitietoisuuden puutteet. Yksittäiset kansalaiset ja samat henkilöt työelämässä eivät tiedosta tietoverkkoihin ja -järjestelmiin liittyviä turvallisuushkia, jolloin toiminnassa ei aina noudateta riittävän tietoturvallisia menettelyjä. Jos laiminlyö oman tietoturvallisuutensa, aiheuttaa merkittäviä riskejä muillekin.

Useat eri organisaatiot ovat tehneet merkittävää tietoturvallisuustyötä. Yksityisellä sektorilla tietoturvallisuusohjelmia valmistavat yritykset ovat tuoneet markkinoille tietoturvallisuutta edistäviä ratkaisuja. Teleoperaattorit ja rahoitussektori ovat tehneet pitkäjänteistä työtä, kuten myös elinkeinoelämän etujärjestöt.

Myös julkisen sektorin tietoturvallisuustyöllä on pitkät perinteet. Aktiivisia tietoturvallisuuden edistäjiä ovat valtiovarainministeriön johdolla toiminut Valtion tietoturvallisuuden johtoryhmä (Vahti) ja Viestintävirasto. Kuntasektorin tietoturvallisuustyössä pääpaino on ollut kuntien itsenäisellä työllä, missä sitä ovat merkittävästi auttaneet Julkisen hallinnon tietohallinnon neuvottelukunta (Juhta), Kuntaliitto ja sisäasiainministeriö. Tietoturvallisuuden tilan arvioidaan olevan yleisesti hyvä teleoperaattoreilla, rahoitussektorilla, kaupan alan suurilla toimijoilla, suurissa teollisuusyrityksissä sekä valtionhallinnossa. Heikoin tilanne on yksityishenkilöiden osalla. Pienten ja keskisuuren yritysten tilanteen arvioidaan olevan jonkin verran yksityishenkilöitä parempi. Kuntasektorilla tilanne vaihtelee suuresti.

Arvioidaan, että kansallisen tietoturvallisuuden parantaminen edellyttää sekä kotimaista että kansainvälistä yhteistyötä ja koordinoitua.

Tässä katsauksessa on noussut esiin seuraavia osa-alueita kansallisen tietoturvallisuuden kehittämiseksi:

- ihmisten perusvalmiuksien kehittäminen
- tiedottamisen, koulutuksen ja ohjeiden tarve
- sektorien välisen vuoropuhelun ja tiedonvaihdon lisääminen
- kuntasektorin valmiuksien kehittäminen
- nykyistä kattavampi seuranta tietoturvallisuuden tasosta ja tietoturvallisuusloukkauksista
- kriittisen infrastruktuurin turvallisuus
- tietoturvallisuuteen liittyvän yritystoiminnan ja markkinoiden edistäminen
- riskien kartoituksen ja hallinnan edistäminen
- tietoturvallisuusnäkökohtien laajempi huomioon ottaminen lainsäädäntötyössä
- verkostojen tietoturvallisuuden kehittämisen edistäminen

Yllä mainitut kehittämisaalueet eivät ole tärkeysjärjestyksessä, ja niiden priorisointi jää jatkotyöhön.

Suomalaisessa yhteiskunnassa tietoturvallisuus toiminta on sektorikohtaista, ja panostukset vaihtelevat. Sektorien erilaisuuden vuoksi koko yhteiskuntaa kattavaa tietoturvallisuuden ohjausta ei ole syytäkään toteuttaa.

2 TAUSTA JA RAJAUKSET

Valtioneuvosto on asettanut tietoturvallisuusasioiden neuvottelukunnan valmistelemaan kansallista tietoturvallisuusstrategiaa. Strategian on tarkoitus valmistua syksyllä 2002. Strategiatyön tueksi on keväällä 2002 laadittu kansallinen tietoturvakatsaus.

Tietoturvakatsauksella on useita osin rinnakkaisia tavoitteita:

- arvioida merkittävimpiä Suomeen kohdistuvia tietoturvallisuusuhkia
- arvioida Suomen tietoturvallisuuden tasoa
- käsitellä tietoturvallisuuden merkityksen kasvuun vaikuttaneita seikkoja
- tukea kansallisen tietoturvallisuusstrategian laadintaa.

Motto: Verkostoituminen ja uusi teknologia lisäävät liiketoiminta- ja palvelumahdollisuuksia. Kansallista tietoturvastrategiaa tarvitaan, jotta yhteiskunnan eri toimijoiden rajalliset tietoturvatyön voimavarat voidaan kohdentaa yhdessä, tunnistaa yhteistyön keskeiset alueet, ja näin taata tietoon pohjautuva toiminnan laadukkuus ja palveluiden käytettävyys. Tämä edellyttää eri osapuolten toiminnan häiriöttömyyttä ja luottamuksellisuutta sekä tietojen oikeellisuutta omassa ja erityisesti verkoston toisiin osapuoliin suuntautuvassa toiminnassa.

Tietoturvallisuuden sisältö on yleisesti käytetyn määritelmän mukaan laaja: sillä tarkoitetaan eri muodoissa olevien tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista niihin kohdistuvien riskien hallitsemiseksi soveltuvilla toimenpiteillä. Tietoturvallisuuden katsotaan yleensä toteutuvan, kun voidaan varmistaa tietojen luottamuksellisuus, eheys ja käytettävyys. Käytännössä tämä tarkoittaa mm. autentikointia eli todentamista, auktorisointia (valtuuttamista) eli oikeuksien hallintaa, tietojen ja tietoliikenteen salausta sekä kiistämättömyyttä. Kaiken edellytyksenä on strateginen näkemys tietoturvallisuudesta osana laadukasta toimintaa.

Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista henkilötietojen käsittelyssä. Tätä tarkoitusta varten henkilötiedot on suojattava oikeudettomalta tai henkilöä vahingoittavalta käytöltä.

2.1 Katsauksen sisältö

Katsaus tarkastelee ensin tietoyhteiskuntakehitystä ja sen myötä syntyvää uudenlaista vuorovaikutusverkkoa, joka yhdistää ihmisiä ja tietojärjestelmiä. Viime kädessä tämän verkon kasvaminen edellyttää kansalaisten ehdoilla tapahtuvaa kehitystä. Eräs kehityksen merkittävä hidaste on ollut luottamuksen puute, johon on ratkaisevasti vaikuttanut puutteellinen tieto tietoturvallisuudesta sekä käsitys, että tietoturvallisuuden yleinen taso on heikko. Luottamuksen ja tietoturvallisuuden välistä yhteyttä käsitellään käyttäjän, palvelun tarjoajan, palvelun välittäjän ja yhteiskunnan näkökulmista.

Tämän katsauksen painopiste on *tietoturvallisuuden strategisessa merkityksessä osana liike- ja muuta toimintaa sekä tietoyhteiskunnan luottamuksen ylläpitämisessä*. Strategianäkökulmasta tarkastellaan organisaatioiden toiminnan tietoturvallisuuteen liittyviä uhkia ja niiden vastatoimia. Tekninen näkökulma sisältää avoimien verkkojen ja niihin

kytkeytyvien tietojärjestelmien hyödyntämisen osana yhteiskunnan, hallinnon, yritysten ja kansalaisten toimintoja. Tarkastelun ulkopuolelle on rajattu puhutun tiedon tietoturvaluus sekä ja kirjoitetun tiedon tietoturvaluus, silloin kun tieto on paperilla tai muulla kuin sähköisellä tietovälineellä.

Nopea tietoverkottuminen on siirtänyt monia perinteisen turvallisuusjohtamisen ja riskienhallinnan tehtäviä tietoturvaluudelle ja siten myös tämän tarkastelun piiriin: fyysiset turvallisuusuhat kuten tulipalot ja varkaudet vaarantavat niin tieto- kuin muunkin turvallisuuden. Muita tietoturvaluuteen liittyviä näkökulmia, kuten sähköinen kaupan käynti ja sähköiset palvelut, käsitellään tarvittavassa laajuudessa. Suljettujen erillisverkkojen tietoturvaluuden erityiskysymyksiä ei tässä yhteydessä käsitellä.

Tässä katsauksessa käsitellään luottamuksen merkitystä yhteiskunnallisissa asioissa, ja tietoturvaluuden toteutumista edellytyksenä luottamuksen synnylle ja säilymiselle. Myös EU:n komission eEurope-tiedonannossa korostetaan, että tietoyhteiskunnan kehitysprosessiin sisältyy voimakas yhteiskunnallinen ulottuvuus. Tietoyhteiskunnassa täytyy vallita kuluttajien luottamus viranomaisiin, kaupallisiin toimijoihin ja toisiinsa, eikä muitakaan sosiaalisia näkökohtia saa laiminlyödä.

Katsauksessa tietoturvaluutta on lähestytty ensisijaisesti eri sektorien ja toimialojen uhkien sekä näitä vastaan suunnattujen toimien kautta. Tietoturvaluus ei ole erillinen tehtäväalue, vaan se liittyy tiiviisti jokapäiväiseen toimintaan, laadun ylläpitoon ja kehittämiseen. Toimiva tietoturvaluuskokonaisuus edellyttää koko organisaatiota koskevia toimintaperiaatteita, suunnitelmia ja niiden toimeenpanoa.

Tietosuoja ja yksityisyyden suoja käsitellään tässä katsauksessa vain sinä laajuudessa, kuin kokonaisuuden kannalta edellytetään.

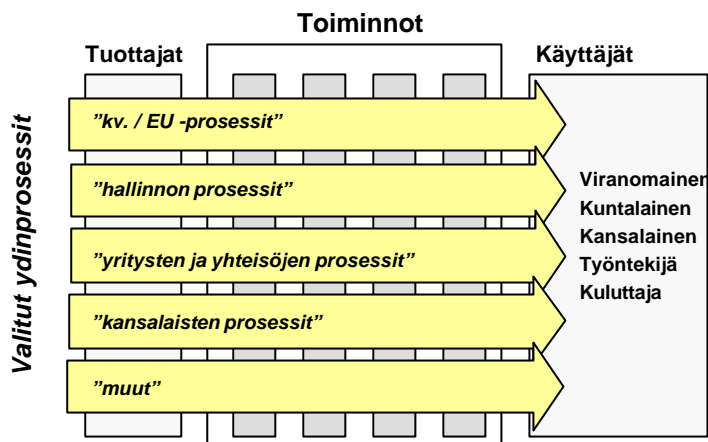
Tietoturvan yksityiskohtien tarkastelu liittyy voimakkaasti katsantokantaan: uhka, joka toiselle on merkittävä, on toiselle vähäpätöinen. Yhteiskunnan eri toimintojen ja tilanteiden tietoturvakysymykset tulee käsitellä erikseen ja sovittaa yleiseen tietoturvakäsitteistöön.

Tietoturvaluuden edistämiseksi tehtyjen toimenpiteiden ja niiden painopistealueiden tarkastelussa käytetään kokoavana lähestymistapana prosessinäkökulmaa ja yhteiskunnan tietoturvaluuden kehittämisperiaatteita. Viimeksi mainittuun luetaan normit (lait, asetukset, määräykset), tietoturvaluustietoisuus, vastuullisuus ja eettiset periaatteet, demokratiaperiaatteet, vastatoimet, riskien arviointi, teknisten tietoturvaluustoimenpiteiden implementointi ja tietoturvaluuden hallinnointi. Erityisesti OECD:ssä on nähty tärkeäksi, että toimenpiteiden tarkastelussa käytetään yhteismitallista lähestymistapaa, jolla eri maiden toimenpiteitä voidaan verrata toisiinsa sekä sovittaa yhteen eri näkökohtia¹. Parhaillaan OECD jatkokehittää vuoden 1992 mallia.

Katsauksen prosessilähtöisessä tarkastelussa tunnistetaan toimintaprosessit, joissa kansallisen tietoturvaluuden kehittämisen merkitys on suuri. Samalla tunnistetaan eri toimintojen yhtymäkohtia, joita ovat mm. koulutus, yhteistyö, valvonta, tiedotus, standardointi ja infrastruktuuri.

¹ OECD:n Neuvoston tietoturvaluussuositus, tietoturvaluusperiaatteet ja perustelumustio, 26.11.1992. Valtiovarainministeriö 5/93.

Painopisteenä ovat tietoturvallisuuteen kohdistuvat uhat ja uhkien torjunta. Tietoturvallisuuden toteutumisen luomien mahdollisuuksien laajempi tarkastelu on tarkoituksellisesti jätetty pois.



Kuva. Prosessilähestymistavan periaatteet² sovellettuna katsauksen aihepiiriin.

Tässä katsauksessa ydinprosesseja tarkastellaan erityisesti julkisen hallinnon, yritysten ja kansalaisten näkökulmasta sekä tärkeiden prosesseja mahdollistavien toimintojen kautta. Tuottajanäkökulman sisäisiä ominaisuuksia (esim. yrityksen sisäiset tietoturva-toimenpiteet) ei tarkastelussa painoteta.

2.2 Muut rajaukset

EU-komission tiedonannossa³ verkkoturvallisuutta pidetään omana tietoturvallisuuden osa-alueena. Tietoturvallisuutta käsitellään tässä kuitenkin laajempaan kuin pelkästään tietoverkkojen turvallisuutena, vaikka Internet on jo käsitettävä elimelliseksi osaksi tietoyhteiskunnan julkisia IP-verkkoja ja niiden kautta tapahtuvaa toimintaa. Tieto- ja viestintätekniikka (ICT⁴) ei ole vain verkkojen, teknologioiden ja palveluiden tuottamista ja hyödyntämistä, vaan tärkeitä ovat myös kuluttajien luottamus, tietosuoja ja sosiaaliset näkökohdat.

Tietoturvallisuus liittyy tiiviisti organisaatioiden hallinnan yleisiin keinoihin. Organisaatioiden toimintaprosessien kokonaistoimivuuden kehitystyötä on tehty laatujärjestelmien ja laadunhallinnan kehitys hankkeissa. Tämä kehitystyö on levinnyt viime vuosina myös julkiselle sektorille. Hyvin hallitussa toimintaprosessissa on myös tietoturvan hallinta otettu huomioon. Tietoturvakysymykset laadunhallinnan näkökulmasta eivät kuitenkaan sisälly tämän tarkastelun piiriin.

Organisaatioiden toimintatapojen, tavoitteiden ja rakenteiden muutokset ovat jatkuvia ja saattavat johtaa merkittäviin tietoturvariskeihin, erityisesti muutosvaiheen aikana. Myös

² Prosessijohtaminen. Ydinprosessien uudistaminen ja yrityksen suorituskyky. Jouko Hannus, HM&V Research Oy, 1994.

³ Komission tiedonanto Neuvostolle, Euroopan Parlamentille, Talous- ja Sosiaalikomitealle ja Alueiden komitealle; Verkko- ja tietoturva: Ehdotus Eurooppalaiseksi lähestymistavaksi (KOM 2001) s 298.

⁴ ICT = Information and Communication Technologies

tämä muutoshallinnan tarkastelukulma on esityksen ulkopuolella. Muissa yhteyksissä tietoturvallisuutta tulisi tarkastella myös muutosjohtamisen näkökulmasta.

Teknologiaan läheisesti liittyvien tietoturvaohjeiden osalta syvällisemmän tarkastelun tulee perustua yleisten tietoturvasuositusten lisäksi kyseisen teknologian erityispiirteisiin. Esimerkkinä mainittakoon tietojärjestelmien etäkäytön, vuorovaikutteisen digiTV:n ja yleisten verkkojen välityksellä toteutettujen automaatiojärjestelmien (ns. IP-automatio) tietoturvasuositukset.

3 YHTEISKUNTA JA TIETOTURVALLISUUS

Strategian tarve

- "Tietoturvallisuus on tietoyhteiskunnan palo- ja liikenneturvallisuutta."
- "Tietoturvallisuus parantaa laadukkaan toiminnan mahdollisuuksia."
- "Yhteiskunta tarvitsee tietoturvallisuutta, koska tietoturvallisuuden uhat kohdistuvat yhteiskunnan keskeisimpään hyvinvoinnin ja kehityksen lähteeseen, tietoon."
- "Tietoturvallisuudelle on ominaista, että verkottuneessa yhteiskunnassa yksittäiset toimijat eivät täysin ymmärrä oman tietoturvallisuutensa vaikutuksia muille. Tämän vuoksi tarvitaan kokonaisuuden hallintaa ja strategiaa."
- "Tietoverkoista on muodostumassa kiinteä osa yhteiskuntaa ja sen ilmiöitä. Tietoturvallisuusstrategialla pyritään takaamaan näiden turvallisuus uudessa ympäristössä".
- "Tietoturvallisuusstrategiaa tarvitaan, jotta yhteiskunnan niukkoja voimavaroja voidaan kohdentaa oikein tietoturvatyöhön."

3.1 Yhteiskunnan lisääntyvä riippuvuus tiedosta

Suomen yhteiskuntakehitys on ollut poikkeuksellisen teknistä vahvan ICT-toimialan ja siihen kohdistettujen panostuksen vuoksi. Hyödyntämisen teknologiaharppaukset ovat olleet nopeita. Juuri kun Suomessa päästiin PC-aikakauteen, otettiin Internet käyttöön ja heti sen yleistyttyä alkoi mobiilisovellusten aika. Toisaalta uusiin teknologioihin mahdollisuuksiin perustuvia palveluja on kehitetty ilman, että ne ovat saavuttaneet juurikaan hyväksyntää käyttäjien keskuudessa. Tietoyhteiskunnan palvelut eivät ole vielä kokeneet läpimurtoa.

Kehityksessä on selkeästi nähtävissä perustietotekniikan laaja ja vaikiintunut hyödyntäminen suomalaisissa yrityksissä ja julkisen hallinnon yksiköissä. Tietoyhteiskunta on Suomen tietoyhteiskuntastrategian uudistamishankkeen loppuraportissa⁵ määritelty seuraavasti:

Tietoyhteiskunta on yhteiskunta, jossa tieto ja osaaminen ovat sivistyksen perusta ja keskeinen tuotannontekijä ja jossa tieto- ja viestintätekniikka tukee laajasti yksilöiden, yritysten ja muiden yhteisöjen vuorovaikutusta, tiedon välittämistä ja hyödyntämistä sekä palveluiden tarjoamista ja niiden saavuttamista.

Useilla alueilla Suomi on maailman kärkiluokkaa. Vuonna 2000 Suomessa oli 57 tietokonetta 100 asukasta kohden. Internet-ostosten tekemisessä sijoittuvat suomalaiset eurooppalaisessa vertailussa varsin hyvin. Lähes 40% Internetin käyttäjistä on ainakin "joskus" ostanut verkkokaupasta⁶. Suomalaisen yritysten kytkeytyminen Internetiin on

⁵ Elämänlaatu, osaaminen ja kilpailukyky: Tietoyhteiskunnan kehittämisen perustelut, Rainio, A, Kautto-Koivula, K. (toim.), Helsinki, Sitra, 1998

⁶ eEurope 2002, eEurope Benchmarking Report.

maailman huippuluokkaa, mutta verkkokauppaa harjoittavien yritysten osuus on EU:n keskitasoa. Internetiä ostotoiminnassa hyödyntävien yritysten osuus puolestaan on kärkitasoa: vuonna 2000 yli 90% yli 10 hengen yrityksistä hyödynsi Internetiä ostotoiminnassa⁷.

EU:n eEurope-ohjelma pyrkii ohjaamaan koko Euroopan tietoverkkojen hyödyntäjiksi niin nopeasti kuin mahdollista. EU:n ohjelmassa tietoyhteiskunnan tasoa arvioidaan lukuisilla mittareilla, kuten verkkojen hyödyntäminen kotitalouksissa, hallinnon tarjoamat verkkopalvelut, verkottumisen kustannukset, tietoturvaongelmat, koulujen verkottuminen. Näilläkin mitattuna Suomi on tietoyhteiskuntakehityksessä eurooppalaista kärkitasoa.

Palveluita tuottaessaan tietoyhteiskunta kuluttaa rajallisia luonnonvaroja vähemmän kuin teollinen yhteiskunta: palveluita valmistetaan, jaellaan ja kulutetaan sähköisessä muodossa. Globalisaatio on alkanut todella vasta tietoyhteiskunnassa, jossa kansainvälistyminen koskettaa kaikkia kansankerroksia ja kulttuureja.

Tietoyhteiskuntakehitys ei ole ongelmaton, kuten eivät yhteiskunnalliset muutokset yleensäkään. Kipeimpiä ongelmia ovat teknologian nopean kehityksen aiheuttama sosiaalinen jako, osaamisen erot, hyvinvoinnin epätasaisen jakautumisen tuomat ongelmat ja turvallisuushaasteet.

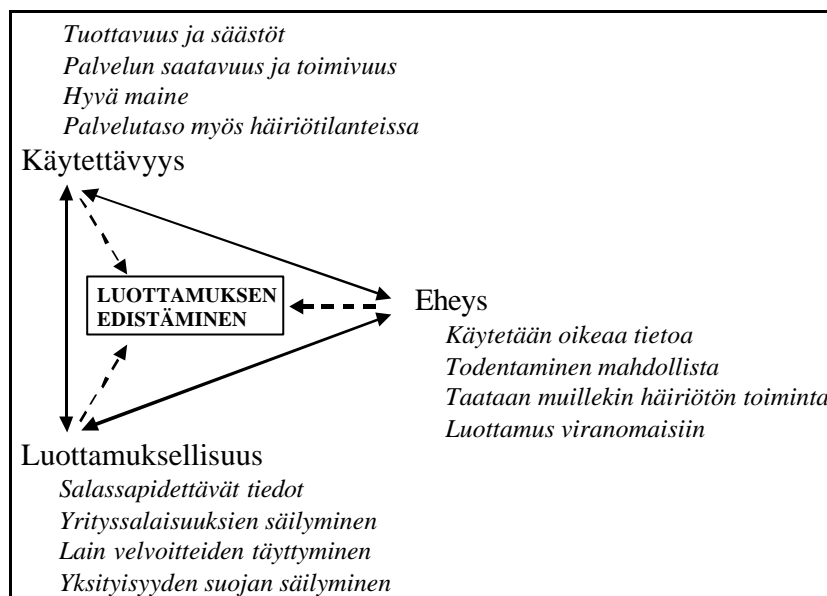
Tietoturvallisuuden parantamisen kannalta tietoyhteiskuntakehitys muodostaa kasvavan haasteen: tottumattomat käyttäjät on saatava innostumaan palveluista, ja heidän luottamuksensa on saavutettava niin yksityishenkilöinä kuin yrityksen edustajana tai työntekijäinä.

3.2 Tietoturvallisuus yhteiskunnassa

Tietoturvallisuutta parantamalla pyritään estämään häiriöiden synty, suojaamaan tietoon ja palveluihin kohdistuvia hyökkäyksiä vastaan, säilyttämään luottamus ja varmistamaan toiminnan jatkuvuus myös erilaisissa häiriötilanteissa. Tämä tapahtuu kaikilla yhteiskunnan tasoilla yksilöstä ja kansainväliselle tasolle saakka. Tietoturvallisuustyö ei ole irrallinen ilmiö, vaan sen tulee tukea muuta toimintaa.

Muutosten nopeus tuottaa jatkuvasti uusia haasteita, kun aikaisemmat ongelmat katoavat ja nykyisistä ratkaisuista tulee merkityksettömiä. Tietojärjestelmien välisten yhteyksien kasvu, erilaisten järjestelmien ja laitteiden lisääntyminen sekä konvergenssi verkkojen ja tietojärjestelmien sisällä ja niiden välillä ovat luoneet tilanteen, jossa tietoturvaa joudutaan tarkastelemaan yhä suurempina kokonaisuuksina. Kokonaisuuden laajentuessa haasteena on eri osien turvallisuuden integrointi, jotta tietoturvallisuus olisi toimiva kokonaisuus, eikä kokoelma erillisiä ratkaisuja.

⁷ Tilastokeskus: Tiedolla tietoyhteiskuntaan 3, 2001



Kuva. Neuvottelukunnassa syntynyt näkemys tietoturvallisuuden kehittämisellä tavoiteltavista hyödyistä. Oman tietoturvallisuuden kehittäminen kunkin näkökulman kautta (käytettävyys, eheys, luottamuksellisuus) näkyy hyötyinä myös palvelun muille osapuolille.⁸

Verkoissa ja tietojärjestelmissä siirretään, käsitellään ja säilytetään yhä enemmän arkaluonteista ja taloudellisesti arvokasta tietoa, mikä houkuttelee tekemään hyökkäyksiä. Tietoturvan merkitys on lisääntynyt myös välillisesti. Verkossa on tarjolla lukuisia palveluita, kuten pankkipalvelut, joiden käytettävyyden puutteet vaikuttavat nopeasti palvelun asiakkaiden toimintaan. Tätä kautta saattavat vaikutukset heijastua myös laajemmalle, mikäli pankkipalvelun käytettävyyden lasku vaikeuttaa palvelun asiakkaiden kyyneä hoitaa velvoitteitaan kolmansiin osapuoliin nähden.

Tietoyhteiskunnassa monet toimet tähtäävät tiedonsaannin varmistamiseen ja helpottamiseen. Kommunikaation ytimenä oleva Internet turvaa rakenteensa vuoksi varsin hyvin tiedon saatavuuden, mutta ei sellaisenaan muita tietoturvallisuuden elementtejä: luottamuksellisuutta ja eheyttä. Internetin hajautetun rakenteen vuoksi ei ole ole massa samanlaista käyttäjän tunnistusta ja tietoliikenteen suojausta kuin esimerkiksi puhelinverkossa, joten kattavien tietoturvallisuusratkaisujen luominen avoimessa verkossa edellyttää monen osapuolen yhteistoimintaa.

Tietokoneista ja tietoverkoista on muodostunut osittain oma ns. virtuaalimaailmansa, jossa perinteinen kasvatuksen mukanaan tuoma vastuullisuus saattaa heikentyä helpommin kuin fyysisessä maailmassa. Teko, joka reaali maailmassa yleisesti mielletään rikokseksi tai ainakin moraalisesti tuomittavaksi (esim. luvaton tunkeutuminen), ei virtuaalimaailmassa ole saanut samaa kohtelua. Tietojärjestelmiin tunkeutumisesta on eräissä

⁸ *Luottamuksellisuus* tarkoittaa, että tieto tai viesti on ainoastaan niiden henkilöiden käytettävissä, joille se on tarkoitettu. Viestinnän luottamuksellisuus on Suomessa perustuslaillinen oikeus (Perustuslain 10§). Yksityisyyden suojan toteutumisen kannalta juuri tietojen luottamuksellisuus on keskeisessä asemassa, ja viranomaisen toiminnan kulmakiviä on tietojen luottamuksellisuuden säilyminen. *Eheydellä* tarkoitetaan, ettei tietoa ole asiattomasti muutettu ja että tieto on johdonmukaista ja oikeaa. *Hyvä käytettävyys* lisää tehokkuutta ja asiointikokemuksen miellyttävyyttä sekä kohottaa palvelutasoa.

alakulttuureissa muodostunut urheiluun ja peleihin verrattavaa toimintaa. Rikkeiden tekemiseen liittyy usein harkittua toimintaa, pitkälistä suunnittelua ja valmistelua.

Valtionhallinnon tietoturvallisuuden kehittämiseksi leimallista ovat korkeat vaatimukset, joita on asetettu laeissa ja muissa säädöksissä. Lisäksi valtiovarainministeriö on antanut asiaa koskevia ohjeita. Koko tietoturvallisuuden perustan tulee olla riittävä ja kunnossa, koska riskiä ei ole varaa ottaa: kansalaisten luottamuksen säilyttäminen on välttämätöntä.

Yrityksissä palveluiden käytettävyys on keskeinen tuottavuustekijä, minkä vuoksi käytettävyyden merkitys korostuu tietoturvallisuustyössä. Yritys toiminnan kannalta tietoturvallisuuden tehtävä on yrityksen liiketoiminnan ja yritys salaisuuksien suojaaminen kilpailijoilta sekä henkilöstön yksityisyyden suojaaminen, mahdollisesti asiakasrekisteritietojen suojaaminen sekä sähköisen liiketoiminnan alalla asiakkaiden luottamuksen synnyttäminen verkossa toimimiseen. Samalla tulee huolehtia toiminnan jatkuvuudesta sekä käytettävien tietojen oikeellisuudesta: tiedon on oltava käytettävissä tarvittaessa ja sen on oltava oikeaa ja johdonmukaista. Tietoyhteiskuntakehitys ja verkottuminen vaativat lisää herkkyyttä nopeaan toimintaan ja päätöksiin.

Verkostopohjaisen yhteistyön kehittyessä joudutaan asettamaan aivan uudenlaisia vaatimuksia koko yhteistyön etiikalle ja myös tietoturvallisuuden toteuttamiselle. On havaittu merkkejä, että verkkopalvelujen käytön leviäminen on hidastunut, kun palveluiden tietoturvaan on kohdistunut epäilyjä.

Kansalaisten ja yksilöiden tasolla tietoturvallisuus, yksityisyyden suoja ja luottamus tietoyhteiskunnan palveluihin ovat perusedellytyksiä palveluiden käytön yleistymiselle. Tietoturvaongelmat ovat tulleet yleisen keskustelun kohteeksi vasta viime vuosina, joten tiedot Internetin tietoturvaongelmista ovat usein varsin pinnallisia.

Nopeasti muuttuvassa ympäristössä esiintyy taipumusta ali-investoida turvallisuuteen. Tilanteen arvioidaan jatkossa jopa pahenevan erityisesti tavallisten kansalaisten palveluiden osalta. Sähköisen asioinnin toimintaohjelmaehdotus⁹ korostaakin, että henkilön oikeutta, etuutta tai velvoitteita koskevissa tai muuta henkilötietojen käsittelyä vaativissa kansalaisten sähköisissä asiointipalveluissa on oltava varmenteisiin perustuva henkilön luotettava tunnistaminen.

3.3 Luottamuksen merkitys

Kaikki sosiaalinen toiminta perustuu viime kädessä luottamukseen¹⁰. Luottamus sisältää pelisäännöt siitä, kuinka tuotettua, itse pääteltyä tai toisesta osapuolesta saatavilla olevaa tietoa ja mielikuvia käytetään liike- ja muussa toiminnassa.

Toimittaja-asiakas -suhteet perustuvat yhä useammin keskinäiseen luottamukseen. Luottamus on tässä mielessä tuotemerkki eli brandi, ja sen perusteella toteutuva yhteis-

⁹ Hallinnon sähköisen asioinnin jaoston ehdotus julkisen hallinnon sähköisen asioinnin toimintaohjelmaksi 2002-2003 "Kohti hallittua murrosta - julkiset palvelut uudella vuosituohannella"

¹⁰ Suomen kielessä sanat luottamus ja luottamuksellinen ovat hyvin lähellä toisiaan. Englanninkielisessä kirjallisuudessa taas luottamus (trust) ja luottamuksellinen tieto (personal information) ovat hyvin selkeästi erotettavissa toisistaan. Tässä esityksessä luottamuksella tarkoitetaan edellistä.

toiminta on luottamuksen ilmenemismuoto. Luottamus osapuolten välillä voi olla yksi-
puolista tai molemminpuolista.

Luottamusta tietoverkkoon ja siellä oleviin palveluihin voidaan edistää yleisillä keinoil-
la: tietoturvan perusteiden opettaminen peruskoulutuksessa, viranomaisten toimien joh-
donmukaisuus, EU:n ja Suomen toimien yhdenmukaisuus, lehdistön toiminta, toimittajien
koulutus, riippumaton konsultointi ja selkeä kansallinen tietoturvastrategia. Puolu-
eettomien kolmansien osapuolten auditoinnit sekä sertifikaatit lisäävät luottamusta
verkkopalveluihin.

Luottamus julkiseen sektoriin ja yritystoimintaan on tärkeä säilyttää. Mahdolliset viran-
omaisten tietoturvallisuusvahingot vähentävät nopeasti kansalaisten kokemaa
luottamusta julkisen sektorin toimintaan, vaikka todelliset vahingot olisivat vähäisiä.
Yrity maailmassa luottamuksen menettäminen saattaa vahingoittaa merkittävästi
liiketoimintaa.

Tietoturvallisuuden ja etenkin tietosuojan murtuminen aiheuttaa luottamuksen menetyk-
sen, joko paikallisesti ja tilapäisesti tai pahimmillaan koko yhteiskunnan tasolla ja pit-
käaikaisesti. Esimerkiksi verkkopankkipalveluita käytetään jo laajasti, ja niitä pidetään
turvallisina ja käytettävyydeltään hyvinä. Näillä palveluilla on myös välillinen merkitys
muihin tietoyhteiskunnan palveluihin: niiden tietoturvan romahtaminen voisi olla mer-
kittävä askel taaksepäin kaikkien sähköisten palvelujen luottamuksen osalta.

Myös tosiasioihin perustumaton, aiheeton luottamus voi aiheuttaa suuria riskejä suo-
jautumisen laiminlyöntien ja huolimattoman toiminnan seurauksena.

Sähköisen kaupankäynnin kehittämistä pidetään yleisesti toivottavana sen kustannuste-
hokkuutta lisäävien ominaisuuksien ja ekologisten hyötyjen ansiosta. Sähköisen kau-
pankäynnin kehittymisen yhtenä merkittävänä edellytyksenä on luottamus Internet-
verkossa toimimisen tietoturvallisuuteen. Merkittävän globaalien varmennepalveluyritys
Verisignin mukaan¹¹ 85% Internet-verkon käyttäjistä ja palvelutarjoajista koki verkon
epäluotettavaksi, eivätkä he mielellään lähettäneet luottokorttitietojaan Internetissä. Toi-
saalta yleisen peruskoulutuksen ja tiedon puutteen vuoksi verkon käyttöön liittyy varsin
usein virheellisiä käsityksiä. Nämä saattavat johtaa turhaan luottamuksen puutteeseen
tai toisaalta mahdollisuuteen, ettei todellisia riskejä tunnisteta.

3.3.1 Luottamuksen rakentuminen

Luottamus voi perustua toisen osapuolen tuntemiseen, mielikuviin tai kolmannen osa-
puolen lausuntoon. Luottamuksen perusteena voi myös olla osapuolen asema tai toimi.
Yhteiskunnassa on erilaisia luottamuksen välittäjiä eli palveluitaan tarjoavia luotettavia
kolmansia osapuolia (TTP, Trusted Third Party). Perinteisesti näitä ovat olleet notaarit
ja pankit. Tietoverkossa tapahtuvassa kommunikaatiossa on kolmannen osapuolen käyt-
töyleistymässä luottamuksen rakentamisen keinona: yksityisyyden suojaa edistävän or-
ganisaation logo yrityksen verkkosivuilla kertoo tämän noudattavan kyseisen organisa-
ation hyväksymiä käytäntöjä.

Tärkeä ehto luotettavan kolmannen osapuolen luotettavuuden kannalta on, ettei sillä ole
intressejä keskenään kanssakäymisessä olevien osapuolten viestinnän tai muun toimin-

¹¹ Building an E-Commerce Trust Infrastructure, Verisign, 3/2002

nan sisältöön. Käyttäjien luottamuksen vahvistamiseksi ja kolmansien osapuolten käytettävyyden parantamiseksi olisi edullista, että kolmansilla osapuolilla olisi niiden tietoturvallisuuden tasosta kertova sertifikaatti aivan kuten laatutoiminnassa, jossa laatusertifikaattia käytetään yhtenä edellytyksenä alihankkijoiden valinnassa.

Erityisesti tietoverkkopalveluissa luottamus saattaa ketjuuntua. Kohteen A luottaessa kohteeseen B, joka puolestaan luottaa kohteeseen C, voi A:n luottamus ulottua C:hen saakka. On voitava esimerkiksi luottaa siihen, että työntekijä, joka on saanut verkkotunnuksen ja käyttöoikeudet verkostoituneen kumppaniyhtiön verkkoon, käyttää niitä sovitusti.

3.3.2 Luottamuksen toteuttaminen ja verifiointi verkossa

Kun tietoverkoissa tapahtuva toiminta perustuu luottamukseen, se on voitava tarvittaessa viestittää. Henkilöiden ja palvelujen tunnistaminen voidaan toteuttaa varmennejärjestelmällä (julkisen avaimen infrastruktuuri, PKI), joka on keskeinen keino luottamuksen lisäämiseksi ja välittämiseksi verkossa. Varmennejärjestelmä tulisi saada osaksi yleistä tietoverkkoinfrastruktuuria.

Varmenteiden käytettävyyden parantamiseksi on käynnissä sekä maailmanlaajuisia että eurooppalaisia kehitys- ja standardisointihankkeita (mm. EESSI, CEN, ETSI). Euroopassa luotettavia, vahvoja varmenteita toimittavat ns. laatuvarmentajat¹² (qualified certifier), jotka on auditoitu ja joiden toimintaa kansalliset viranomaiset valvovat. Auditoiden akkreditointi on vielä avoin kysymys, joka tulisi ratkaista pikaisesti ainakin Euroopan tasolla.

Tarve tunnistaa yksittäinen palvelun käyttäjä riippuu palvelusta. Tunnistukseen on kehitettävä erilaisia menettelyjä. Yleisiä ovat salasanan ja tunnuksen käyttö, muuttuvan etukäteen toimitetun salasanan käyttö (ns. kertakäyttösalasana) sekä uusimpana varmenteen käyttö.

Vastapuolen antama tunniste (käyttäjätunnus, salasana, sertifikaatti) tulee voida todentaa (verifioida) luottamuksen synnyttämiseksi. Varmenteella luotu digitaalinen identiteetti todennetaan julkisesta hakemistosta, mikä vastaa nykyistä puhelinverkon avulla toteutettua luottokortin tarkistusmenettelyä.

Sähköpostipalveluissa voidaan myös käyttää varmennetta tunnistuksen välineenä: sähköpostin allekirjoittaminen varmentaa lähettäjän identiteetin.

Luottamuksen todentamiseen on kehitetty muitakin menetelmiä. Esimerkiksi TrustE on USA:ssa kehitetty järjestelmä, jossa yritykset sitoutuvat noudattamaan sovittuja pelisääntöjä käyttäjän yksityisyyden turvaamiseksi. Tämän sitoumuksen todistaa TrustE-sinetti, joka sijoitetaan web-sivulle. Sivulta on linkki tietohakemistoon, josta voidaan tarkistaa yrityksen todella noudattavan sovittuja pelisääntöjä.

3.4 Kansainvälisyys

Merkittävä osa sähköisestä kaupasta on kansainvälistä kauppaa; tavarakaupan lisäksi myös verkosta hankittavat palvelut ovat kansainvälistymässä. Tämä kaikki on sopusoin-

¹² EU direktiivi sähköisestä allekirjoituksesta

nussa EU:n peruseriaatteiden kanssa ja johdonmukainen jatke verkon luomille uusille mahdollisuuksille.

Kansainvälistymistä tapahtuu tietoverkoissa myös huomaamattomasti. Yksityinen verkkokansalainen ei useinkaan ole tietoinen, missä maassa ja minkä maan lainsäädännön alainen on palvelin, jolta hän hakee tietoa. Teko, joka yhdessä on kriminalisoitu ja toisessa moraalisesti tuomittavaa, voi kolmannessa olla hyväksyttyä. Kansainvälisesti leviävät haittaohjelmat tuovat kansainvälisen elementin jokaisen käyttäjän postilaatikkoon.

Suomalainen yhteiskunta on kansainvälisissä vertailuissa turvallinen ja luottamus toisiin ihmisiin on varsin korkea¹³. Tietoturvallisuuteen tämä vaikuttaa kaksitahoisesti: luottamus vähentää valvonnan ja turvatoimien määrää, mutta toisaalta se altistaa uhille, jotka syntyvät väärästä luottamuksesta. Suomessa yleensä luotetaan työntekijöihin, eikä organisaatioiden sisältä tulevaa tietoturvallisuusuhkaa koeta tai tunnusteta merkittäväksi, vaan tietoturvallisuustoimenpiteet painottuvat ulkoisten uhkien torjuntaan.

¹³ Esimerkiksi vuonna 1996 Suomessa tehtiin 83 vakavaa rikosta 100 000 asukasta kohden. Ruotsissa luku oli 124, Iso-Britanniassa 125, Saksassa 211, Ranskassa 269 ja Yhdysvalloissa lähes 600. Lähde: Tilastokeskuksen verkkopalvelu

4 TIETOTURVALLISUUDEN UHKATEKIJÄT

4.1 Uhkien merkitys

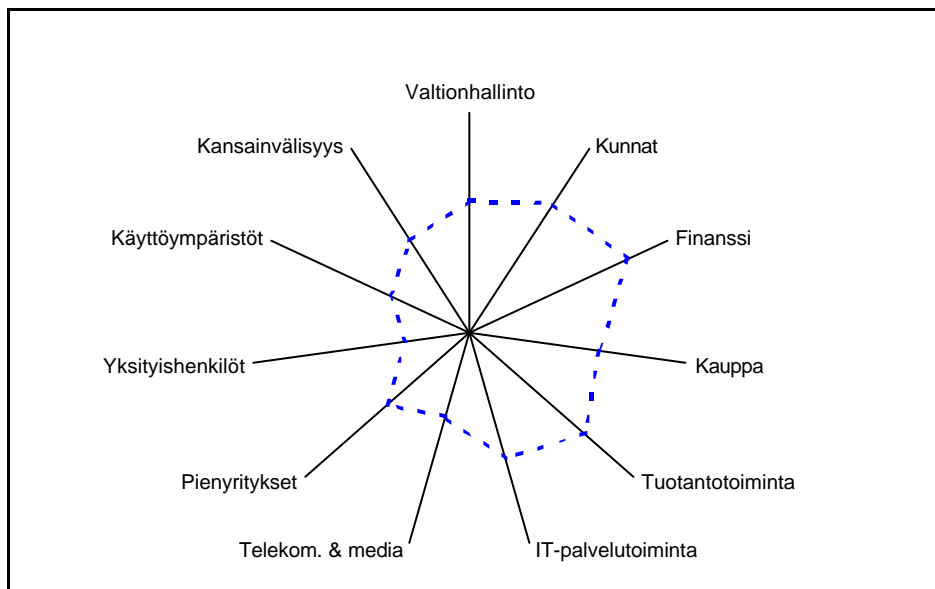
Tietoyhteiskunnan toimintatavat ja uhat ovat enenevästi globaaleja. Tältä osin tarvitaan kansainvälistä yhteistyötä ja tiedonvälitystä. Myös perusteknologioiden osalta useat asiat ovat kansainvälisesti yhteisiä.

Kansainvälisissä uhissa ilmenemismuoto, lähde ja kohde ovat käytännössä riippumattomia sijaintimaasta. Tietokonevirukset, muut haittaohjelmat sekä ohjelmistojen tietoturva-aukot ovat tällaisia uhkia. Uhka kuitenkin toteutuu paikallisena ilmentymänä, joten kansainvälisiä uhkia vastaan tarvitaan kansallisia toimenpiteitä.

Internet kattaa jo nykyään lähes kaikki yhteiskunnan toiminta-alueet henkilökohtaisesta kommunikaatiosta viranomaisasiointiin. Verkosto yhdistää erilaisia kulttuureja ja rikko kansallisia rajoja sekä on luonut uuden markkina-alueen, jota on nimitetty myös kybertaloudeksi.

Internetin tietoturvakysymysten ratkaiseminen on tärkeää yrityksille ja muille organisaatioille, valtioiden turvallisuudelle sekä koko järjestäytyneen yhteiskunnan toiminnalle.

Tietoturvauhista osa on merkitykseltään luultua vähäisempiä. Esimerkiksi Internetissä tarjottavaan palveluun kohdistunut tietoturvarikos saa julkisuutta, josta saatetaan virheellisesti päätellä, että kaikkien verkkopalveluiden tietoturvallisuuden taso on matala.



Kuva. Työryhmätyöskentelyssä käytetty työkalu uhkien tarkasteluun ja arvio tietoturvauhkien kohdentumisesta suomalaisen yhteiskunnan eräisiin keskeisiin osa-alueisiin (osin päällekkäisiä, selitetään tekstissä tarkemmin). Riskien arvioidaan olevan sitä paremmin hallinnassa, mitä kauempana keskipisteestä katsottuna käyrä leikkaa kunkin akselin.

Uhkien kohdentumista ja vaikutuksia käsitellään yhteiskuntasektoreittain: julkinen hallinto, yritystoiminta, yksityiset kansalaiset sekä kaikki edellä mainitut käsittävä yhteiskunnallinen taso. Toiminta yksityishenkilöinä (kansalaisena, kuntalaisena ja kuluttajana) ja toiminta käyttäjänä (työntekijänä tai viranhaltijana) tarkastellaan erikseen.

Kullakin toimialalla on erilaisia toimijoita, joten arviot ovat vain suuntaa-antavia. Useimpia toimijoita sivuaa yhteisenä haasteena tietoyhteiskunnan tottumattomien peruskäyttäjien määrän kasvu.

Kaikki ennakoiva työ ja tietoisuuden lisääminen on oleellinen uhkien vähentämisessä. Näitä ja muita toteutuneita toimia käsitellään tarkemmin luvussa 5.

4.2 Muutosvoimat ja ajurit

4.2.1 Yritystoiminnan muutoksia

Yritystoiminnassa on käynnissä jatkuva muutos, jossa yritykset pyrkivät keskittymään ydinliiketoimintaansa ja ulkoistavat muita toimintojaan. Tätä on tapahtunut joko yhtiöittämällä tai siirtämällä toimintaa ulkopuoliselle yritykselle, joka tarjoaa samaa palvelua muillekin yrityksille. Tästä käytetään nimitystä ulkoistaminen (*outsourcing*).

Verkostoituminen lisää verkoissa liikkuvan ja saatavilla olevan tiedon määrää sekä nopeuttaa päätöksentekoa. Ongelmia syntyy usein siksi, että kaikilla ei ole verkostoitumisen edellyttämiä tietoja ja taitoja. Myöskään verkostossa liikkuvan tiedon arvoa tai oikeellisuutta ei aina voi mitata. Verkostoituminen tekee vanhanaikaiseksi ajatuksen yrityksen rajoista sen turvallisuusvyöhykkeen rajoina ja edellyttää tietoturvaluottamustoiminnan sopeutumista nopeisiin muutoksiin.

Yksi verkostojen kehittymisen perusajatus on uuden talouden työvälineiden käyttö yritysverkoston hallinnassa: Internet tarjoaa mahdollisuuden yritysten tietojärjestelmien väliselle yhteydelle ja yhteiskäytössä oleville, kolmannen osapuolen hallinnoimille tietojärjestelmille. Vastuunjako ja tietoturvaluottamisuuden takaaminen tällaisessa yhteistyössä on uutta ja osin selkiytymätöntä.

Verkostot ovat tulevaisuudessa enenevästi palveluverkostoja. Uhkia tietoturvaluottamisuudelle muodostavat tietojen siirto yritysten välillä ja yrityksiä käyttäjäoikeudet toistensa järjestelmiin. Oikeuksien hallinta tulee nopeampitempoiseksi ja tilannekohtaiseksi. Eri osapuolten tietoturvaluottamisuuden taso voi poiketa merkittävästi, eikä erojen selvittäminen ole helppoa.

Verkostoituminen luo myös edellytyksiä tietoturvaluottamisuuden parantamiselle. Tieto hyväksi havaituista toimintatavoista leviää aiempaa nopeammin, ja alihankkija voi hyödyntää päämiehen tietoturvaluottamisuusratkaisuja. Tämä tulee kyseeseen etenkin pienten yritysten osalta.

4.2.2 Käyttäjät eri rooleissa

Usein toistetun lausuman mukaan käyttäjät ovat tietoturvaluottamisuuden heikoin lenkki. Käyttäjille kohdistuu erilaisia vaatimuksia: heidän tulee toimia tehokkaasti, luovasti ja

tietoturvallisesti. Vaatimusten ollessa keskenään ristiriidassa saatetaan tietoturvallisuus sivuuttaa.

Toimiessaan työntekijänä yksityishenkilö toimii yleensä edustamansa yrityksen tai muun organisaation lukuun. Yritys saattaa tarjota tietoturvallisuuteen liittyviä teknisiä ratkaisuja (palomuurit, tunnistusmenetelmät) sekä hallinnolliset järjestelyt (tietoturvaorganisaatio, tietoturvallisuuspolitiikka). Käyttäjät voivat toimia kuitenkin varsin itsenäisesti ja sivuuttaa nämä. Tällaisen toiminnan tietoturvallisuusvaikutukset saattavat olla erittäin merkittäviä. Vaikka toimia ohjaavat organisaation hallinnolliset määräykset ja organisaatiokulttuuri, merkittävä vaikutus on käyttäjän omalla tietoturvallisuustietoisuudella ja -osaamisella.

Useimmissa organisaatioissa on käyttäjiä, jotka eivät tiedosta tietoturvallisuuden toiminnan merkitystä. Organisaatiokulttuurissa tietoturvallisuudesta saatetaan olla valmiita hiljaisesti tinkimään tehokkuuden kustannuksella. Syitä tähän on lukuisia, mutta usein tietoturvallisuusohjelmat ovat vaikeita käyttää, hidastavat tuottavaa toimintaa ja ovat ohitettavissa.

Koko organisaatiota uhkaavia asioita ovat esimerkiksi käyttäjän pois päältä kytkemä virustorjunta ja vanhentuneet salasanat, jotka voivat avata yrityksen järjestelmät haittaohjelmille ja luvattomalle tunkeutumiselle. Ideaalitapauksessa ratkaisut ovat käyttäjille ns. läpinäkyviä: käyttö on helppoa, eikä käyttäjä välttämättä edes tiedä hyödyntävänsä jotain tietoturvaohjelmaa.

4.2.3 Mobiliteetti - organisaatioiden kontrolliympäristön muutos

Yhä merkittävämpi osa tietojenkäsittely- ja viestintälaitteista on käytössä organisaation fyysisten tilojen ulkopuolella. Tyypillisimpiä ovat salkkutietokoneet (laptop), puhelimet, kommunikaattorit ja kämmentietokoneet (PDA-laitteet). Laitteiden käyttöön liittyy erilliskäyttöä (käyttö itsenäisenä laitteena), etäkäyttöä (tietojärjestelmien käyttöä organisaation toimipisteen ulkopuolelta), käyttöä kotona ja muita uusia käyttömuotoja. Käyttöä voi tapahtua ympärivuorokautisesti ja siihen voi yhdistyä erilaisia käyttötilanteita. Hyöty- ja vapaa-ajan käyttöä voi tapahtua rinnakkain ja käyttäjinä olla mahdollisesti muitakin kuin laitteen omistaja tai nimetty käyttäjä.

Organisaatioiden kannalta mobiiliudessa on kyse kontrolliympäristön muutoksesta. Toiminta, joka yrityksen tiloissa on täysin turvallista ja hallittua, voi mobiilikäytössä muuttua uhkia sisältäväksi, joten käyttöä on voitava rajata ja siitä on annettava ohjeita.

Tärkeä mobiliteetin mukanaan tuoma uhka on luvaton pääsy laitteisiin tallennettuun tietoon ja niissä oleviin ohjelmiin. Varkaus, katoaminen, muistikortin tai -laitteen joutuminen väärin käsiin voi aiheuttaa tiedon joutumista asiattomille tahoille. Laitteen katoaminen sinänsä on jo merkittävä tiedon menetyksen ja käytettävyyden alenemisen uhka. Laitteissa on tyypillisesti vähintään yksinkertaisia suojausmekanismeja, mutta nykyisiä organisaatioiden tietoturvaratkaisuja (kuten virustorjunta, palomuurit, salaus tai varmenteet) ei aina voida täysmittaisesti soveltaa ja hallinnoida. Toimivia kokonaisratkaisuja on saatavilla lähitulevaisuudessa.

Erityisesti kämmentietokoneiden ja kommunikaattorien tietoturvasuoja ei tänä päivänä ole riittävällä tasolla. Teknisiä ratkaisuja tietoturvallisuuden parantamiseen on saatavilla

yhä enemmän, mutta toistaiseksi näiden käyttö on vähäistä. Itse laitteen lisäksi uhkakonaisuuden muodostavat liikkuvien laitteiden tietoliikenneyhteydet.

Myös mobiililaitteet edellyttävät tyypillisesti vähintään samaa turvatasoa kuin muut organisaation tietoturvaratkaisut.

4.2.4 Kansainväliset uhat

Tietoturvaauhkien kannalta Internetissä ja siihen kytketyissä tietojärjestelmissä ei ole valtioiden välisiä rajoja. Internet ja muut uudet tekniikat tuovat mukanaan aivan uusia tietoturvallisuusuhkia, mutta korostavat myös eräitä vanhoja uhkia.

Tietokonevirukset ja muut haittaohjelmat leviävät maapallon yli jopa muutamassa tunnissa, eikä pääosa viruksista erottele tartunnan kohteita niiden kansallisuuden perusteella. Vaikka vakava tietokonevirusepidemia ei olisikaan vielä saavuttanut Suomea, voivat vaikutukset tuntua: tietoliikenneyhteydet saattavat katkeilla tai ulkomaisten palveluiden käytettävyys kärsiä.

Kansainväliselle rikollisuudelle uudet tekniikat ovat tarjonneet mahdollisuuden tehostaa rikollista toimintaa. Talousrikollisuus ja huumekauppa ovat hyötäneet tehostuneesta tiedonvälityksestä ja mahdollisuudesta salata niin toiminta, viestiliikenne kuin tekijöiden henkilöllisyys.

Kansainvälisen järjestäytyneen rikollisuuden ulottuminen Suomeen on kuitenkin pitkälti johtunut muista seikoista kuin tietoverkkojen teknologisesta kehityksestä.

4.2.5 Uudet teknologiat

Teknologiassa itsessään olevat riskit ovat usein sitä vaivampia, mitä uudemmassa ja mutkikkaammassa tekniikasta on kyse. Uuden teknologian mukana saattaa tulla esiin tietoturvallisuusriskejä, jotka eivät suoraan liity itse tekniikkaan vaan sen käyttäjien toimintaan: teknologian käyttöä ei hallita tai käyttötavat eivät ole tietoturvallisia. Mobiliteetti on hyvä esimerkki tästä.

Uusiin teknologioihin yleisesti liittyvä piirre on, että ne lisäävät yhteyksiä järjestelmien (tai ihmisten) välillä ja kohdistuvat laajempiin käyttäjäkuntiin. Tämä tuo mukanaan tilanteen, jossa yhden järjestelmän (tai ihmisen) toiminnan tietoturvallisuuspuutteet vaikuttavat entistä laajemmin ja nopeammin.

Uusia teknisiä ratkaisuja kehittävien ihmisten tietoturvaluustietoisuus ei aina ole riittävä, eivätkä he itsekään täysin hallitse kehittämäänsä tekniikkaa. Kehitystyössä käytetyt työmenetelmät voivat olla vääriä, tai laadun valvonta ei ole asianmukaisesti hoidettu. Kireässä kilpailutilanteessa saatetaan ottaa tietoisia riskejä tuotteiden tietoturvallisuudesta, jotta niiden markkinoille tulo ei viivästyisi. Tämä on saattanut olla yrityksen kannalta perusteltua, sillä kuluttajat eivät osaa tai halua arvostaa tietoturvallisuusominaisuuksia. Avoimen lähdekoodin ohjelmien yleistymisen, ohjelmistotalojen vastuuntunnon lisääntymisen (osin vastauksena avoimeen lähdekoodiin) sekä tietoturvallisuus- ja laatusertifikaattien yleistymisen ovat kaikki uhkia vähentäviä positiivisia signaaleja.

Teknisten uhkien arviointia voidaan tehdä esimerkiksi seuraavien tekijöiden perusteella:

- Onko päätelaite yhteydessä avoimeen IP-verkkoon vai ei?
- Käytetäänkö langattomia siirtoteitä, jotka ovat alttiita salakuuntelulle?
- Käytetäänkö jatkuvaa tietoliikenneyhteyttä?
- Onko liittymä yhteiskäyttöinen? Jaetut tai yhteiskäyttöiset liittymät, kuten DSL-kaapeliverkkoliittymät, julkiset WLAN:t ja pienyritysten yhteiset verkot ovat avoimia kaikille verkkoon liittyville. Sovellusten ja käyttöjärjestelmien suljetuus vaikeuttaa turvallisuuden arviointia.
- Onko tietojärjestelmä suunniteltu käytettäväksi avoimissa tietoverkoissa vai onko se siirretty sinne suljetusta ympäristöstä?

Yleisesti arvioidaan, että lähivuosina laajamittaisessa käytössä olevien teknologioiden määrä kasvaa ja niiden hallinnan vaatimukset (ml. tietoturvan hallinta) ylittävät yhä useammin organisaation sisäisen osaamistason, mikä johtaa ulkoistamisen ja palveluiden hankintaan. Uhkana on, että ulkoistaminen ei ole tietoturvan kannalta hallittua. Toisaalta monilla ulkoistuspalveluita tarjoavilla yrityksillä on laatu- ja tietoturvasertifikaatti.

Tietoturvariski onkin samalla laaturiski: tietoturvallisuuden heikko taso saattaa merkitä, että toiminta täytyy niitä kriteerejä, jota sille on asetettu.

Tietoturvallisuuden kannalta keskeisten toimintojen ulkoistaminen on usein perusteltua varsinkin nopeasti muuttuvan ja vaikeasti hallittavan tietotekniikan osalta.

4.3 Uhat yhteiskunnan sektoreilla

Yhteiskunnan eri sektorien kohtaamat uhat ovat pääosiltaan samoja, mutta uhkien merkitys vaihtelee. Käsiteltävän tiedon luonne, tietoa käsittelevät järjestelmä, resurssit ja toiminnan erityispiirteet vaikuttavat osaltaan siihen, miten vakavana uhka ilmenee.

4.3.1 Uhat yhteiskunnan tasolla

Tietoyhteiskunta voi toimia sujuvasti vain, kun sen kriittinen infrastruktuuri on täysimääräisesti käytettävissä. Kriittistä infrastruktuuria ylläpitävät organisaatiot ovat tässä suhteessa yhteiskunnan kannalta keskeisessä asemassa. Kriittisen infrastruktuurin mahdolliset toimintahäiriöt voivat johtaa pitkäaikaisiin tarjonnan häiriöihin ja mahdollisesti muihin dramaattisiin seurauksiin.

Kriittistä infrastruktuuria ovat:

- energiahuolto
- telekommunikaatio ja media
- liikenne
- julkiset peruspalvelut, kuten sosiaali- ja terveyspalvelut, vesi- ja elintarvikehuolto, palo- ja pelastustoimi sekä poliisi

- valtiohallinto, kuten valtioneuvosto ja ministeriöt, keskeiset keskusvirastot, valtion maksuliikenne, tulli, puolustusvoimat, verohallinto, ajoneuvohallintakeskus ja maanmittauslaitos
- rahoitussektori

Näille kaikille on yhteistä voimakas riippuvuus modernista tietotekniikasta, tietojärjestelmistä sekä viestintä- ja tietoverkoista, joten perusinfrastruktuurin toiminnan vaarantumisen voidaan arvioida olevan merkittävin tietoyhteiskunnan kohtaamista tietoturvallisuusuhista.

Verkostoitumisen, alihankintapalvelujen ja tietoverkkojen käytön yleistymisen kriittisessä infrastruktuurissa lisäävät samalla kaikkien toimintojen riippuvuutta verkkoinfrastruktuurista. Verkostoituneiden yritysten tietojärjestelmiä ketjutetaan entistä yleisemmin, joten eri osapuolten tuotanto-, palvelu-, markkinointi- ja resurssienhallintaohjelmistot ovat yhä useammin yhteydessä toisiinsa.

Peruspalveluita tuottavien järjestelmien ja perusrekistereiden (kuten väestökirjanpito ja kaupparekisteri) toimivuus on tärkeä osa infrastruktuuria. Merkittävä osa näistä on keskitettyjä, mutta useisiin toimipisteisiin ja osapuoliin verkotettuja järjestelmiä. Tavoite on lisätä hajautusta ja toisiaan varmentavia järjestelmiä.

Kuljetustoiminnan riippuvuus tietotekniikasta on jatkuvasti lisääntynyt, ja logistiikan toiminen edellyttää useita tietojärjestelmiä. Tavaravirtojen ohjailun lisäksi eri liikenne- ja logistiikkamuodot vaativat erilaisia ohjausjärjestelmiä etenkin keskitetyissä liikenne- ja logistiikkamuodoissa, kuten ilmailu ja raideliikenne.

Liiketoiminnan perusedellytys on rahoitussektorin toimivuus. Maksuliikenteen pysähtyminen saattaisi laimauttaa talouselämän melko nopeasti. Kokonaisuutena arvioiden uhat ovat tietoyhteiskunnassa pitkälti sidoksissa elinkeinoelämän toimintaan ja toimivuuteen.

Verkostoitumisen myötä yhä useammat yritykset eivät ole itsenäisiä toimijoita, vaan osa kokonaisuutta: yrityksen oma tietoturvaluus vaikuttaa sen sidosryhmien tietoturvaluuteen.

Organisoitu toiminta yhteiskuntaa vastaan on merkittävä uhka jo normaalioloissa, sillä mahdollinen informaatio- ja tietoturvakäynti tultaneen aloittamaan rauhanaikana. Sabotaasit ja muut poliittisväritteiset toimet voivat levitä Suomeen ilman, että Suomi itse olisi mitenkään osallisena siinä kriisissä, johon toimet alunperin liittyvät.

Käyttäjien tahattomat teot ovat edelleen potentiaalinen uhka jopa yhteiskunnan tasolla, erityisesti kriittisen infrastruktuurin järjestelmien hallinnassa tapahtuvien inhimillisten virheiden kautta.

4.3.2 Julkisen sektorin uhat

Julkisen sektorin on laaja ja heterogeeninen kokonaisuus, jonka tärkeimmät osat ovat valtiohallinto ja kunnat. Julkiseen sektoriin kohdistuvat uhat vaihtelevat tarkasteltavasta julkishallinnon yksiköstä riippuen suuresti, mikä hankaloittaa julkisen sektorin käsittelyä kokonaisuutena. Toisaalta tietoturvaluusustyötä helpottaa julkisen hallinnon normipohja, joka on laajempi kuin muiden sektoreiden.

Julkisen sektorin järjestelmien välillä on paljon riippuvuussuhteita. Kokonaisuuden toimivuuden kannalta kriittisessä asemassa ovat perusrekisterit sekä – aivan kuten yksityisellä sektorilla – kriittisen infrastruktuurin toiminta.

Viranomaisten sähköiset palvelut ovat vasta kehityksensä alkuvaiheessa. Sähköisten palvelujen tietoturvasuhteet riippuvat merkittävästi palvelujen luonteesta eikä verkkopalveluita tarjoavia järjestelmiä ole integroitu varsinaisen palvelun tuottaviin tietojärjestelmiin (taustajärjestelmät) kuin vähäisessä määrin.

Viranomaisten tarjoamien sähköisten asiointipalvelujen käytön vähyys ei niinkään johdu asiakkaiden epäluottamuksesta palveluja tai tietoverkkoja kohtaan, vaan pääosin muista seikoista. Hidasteista mainittakoon palvelun tarjoajien resurssien puute, palveluiden puutteellinen yhteys viranomaisten tietojärjestelmiin ja nykyisten ohjausmallien tehostustarpeet, jotta nämä kykenisivät vastaamaan uusiin haasteisiin.¹⁴

Merkittävä osa julkisten palveluiden käyttäjistä on sähköisten palveluiden ulottumattomissa, sillä tietoverkkoyhteydet eivät ole kaikkien saatavilla tai Internetiä ei osata käyttää. Useat julkiset palvelut ole luonteeltaan asiakkaan toistuvasti tarvitsemia standardipalveluja, joita voidaan välittää tietoverkoissa. Myös kansalaisten käyttötottumukset muuttuvat tekniikoita hitaammin.

Yhteiskunnan toiminnan kannalta keskeisessä asemassa on joukko perusrekistereitä, joita hyödyntäviä järjestelmiä on erittäin paljon. Tietojärjestelmien toiminta on yhteiskunnan toiminnan kannalta ensiarvoisen tärkeää. Näiden toimintojen tietoturvasuhteiden vaarantuminen aiheuttaa nopeasti mitattavia suoria vahinkoja, ja murtaa myös luottamusta muihin keskeisiin järjestelmiin. Mikäli julkisuuteen tulisi tieto vakavasta tietoturvasuhteiden ongelmasta, vaikuttaisi tämä varsin todennäköisesti useiden julkisen sektorien palveluiden julkisuuskuvaan.

Kuntien tietoturvasuhteet liittyvät läheisesti palveluihin, joita kuntalaisille tarjotaan. Suuret kunnat ja kuntainliitot, jotka tarjoavat monipuolisia palveluita ja hyödyntävät tietotekniikkaa laajassa mittakaavassa, kohtaavat tietoturvasuhteiden ikään kuin suurena monialakonsernina.

Kunnallisten ja muiden julkisten palvelujen alueella alihankinta on yleistymässä. Tämä johtaa laajempaan yleisten verkkojen käyttöön ja siten myös tietoverkkojen tietoturvan entistä keskeisempään rooliin. Määräykset ja ohjeet tulee sovittaa tietoverkkoympäristöön nykyisen paperipohjaisen ympäristön sijaan. Jo organisaatioiden toimintatapojen täsmentäminen parantaa tietoturvasuhteita.

Erityisesti terveydenhuollon tietosuojavaatimukset ovat korkeat. Sähköisten prosessien mahdollistamiseksi painopistettä tulisi siirtää tietoturvasuhteiden tason nostamiseen. Tällä on taloudellisesti suuri yhteiskunnallinen merkitys. Siirtyminen digitaaliseen tiedon tallennukseen ja siirtoon on tietoturvan hallinnan kannalta edistysaskel jo sinällään, vaikka merkittävä osa tietoturvasuhteiden riskeistä ei ole tekniikan keinoin ratkaistavissa.

¹⁴ Hallinnon sähköisen asioinnin jaoston ehdotus julkisen hallinnon sähköisen asioinnin toimintaohjelmaksi 2002-2003: "Kohti hallittua murrosta - julkiset palvelut uudella vuosituohannella"

4.3.3 Yritysten uhat

Elinkeinoelämän etuja ajavat järjestöt ovat edistäneet tietoturvallisuutta erityisesti koulutus- ja julkaisutoiminnalla.

Yritysten riskianalyyseissä on yleisesti havaittu, että pienehköt riskit ovat yleisiä, isot harvinaisia. Tämä havainto pitää paikkaansa perinteisiä riskejä tarkasteltaessa, mutta tietoturvallisuusriskien kannalta tilanne on monitahoisempi.

Tietojärjestelmäintegraation johdosta tilanne on osin muuttumassa, ja ketjuuntumisesta johtuen riskien vaikutus laajenee. Sinänsä pienillä tietoturvariskeillä on merkittäviä taloudellisia vaikutuksia jo niiden aiheuttaman tarkistustyön vuoksi. Pieni riski voi helposti johtaa suuremman riskin toteutumiseen, mikäli kyseessä on kriittisen tietojärjestelmän kriittinen komponentti.

Yritysten kohdalla riskienhallinnan kehittämisen ongelmaksi on todettu myös tapahtuneiden vahinkojen salaaminen: yritykset saattavat jättää ilmoittamatta tapahtuneita riskejä pitääkseen asian pois julkisuudesta¹⁵. Toisaalta rutiininomaisia tilanteita on organisaatioissa paljon, minkä vuoksi ilmoituskynnys on epäselvä. Keinoja tämän kynnyksen alentamiseksi tulisi kehittää.

Yritysmuodolla ja organisaation koolla ei sinänsä ole suoraa yhteyttä tietoturvallisuusuhkien hallintaan, vaan ratkaisevaa ovat tietoturvallisuuteen käytettävissä olevat voimavarat, jotka vaihtelevat elinkeinoelämän eri toimijoilla. Suurten yritysten tietoturvallisuusyksiköiden panostus ja ammattitaito on korkeatasoista.

Yleisenä yrityssektorin uhkana on, että yritysten johto ei miellä omaa vastuutaan eikä riittävästi edistä liiketoiminnan tarpeiden tasolla tapahtuvaa tietoturvallisuustyötä. Tämä sekä tietoturvallisuuden hallinnoinnin puutteellisuus (tietoturvapoliittikka, resurssit, koulutus) muodostanevat vakavimmat uhat yritysten tietoturvallisuutta kohtaan.

Tietoturvariskejä kasvattavat ainakin seuraavat tekijät:

- Yrityksen toimialana on korkea teknologia, rahoitus, sähkö, energia tai media. Suomessa on kansainvälisesti arvioiden useita huomattavia yrityksiä juuri näillä toimialoilla.
- Yrityksessä on paljon houkuttelevia hyökkäyskohteita. Suurissa yrityksissä on enemmän hyökkäyskohteita kuin pienissä, ja suuret yritykset ovat julkisuudessa pieniä useammin. Pörssiyritysten riski joutua hyökkäyksen kohteeksi on suurempi kuin muiden yritysten.
- Yritys tarjoaa verkkopalveluita tai harjoittaa verkkokauppaa.
- Yrityksen julkisuuskuva on huono tai sen tietoturvallisuuden tasosta on esitetty epäilyjä.

¹⁵ Computer Crime and Security Survey 2002 mukaan 34% vakavien tietoturvaluhyökkäysten kohteeksi joutuneista yrityksistä ilmoitti tapahtuneesta poliisiviranomaisille. Tärkeimmät syyt ilmoittamatta jättämiseen ovat negatiivinen julkisuus (75%) ja kilpailijoiden mahdollinen hyötyminen asiasta (72%). Iso-Britannian kauppa- ja teollisuusministeriön (DTI) julkaiseman Information Security Branches Survey 2002 arvioi poliisiviranomaisille tehtävän ilmoituksen ”...kiinnostavan kaikkein vähiten”. Syiksi arvioidaan vaikutukset julkisuuskuvalle sekä viranomaisten huomion herättäminen.

- Yrityksellä on puutteellinen tietoturvastrategia tai sen toiminnan tietoturvasuustaso on heikko.

Luvaton tunkeutuminen yritysten tietojärjestelmiin on vakava uhka erityisesti korkean teknologian, telekommunikaatioalan ja rahoitussektorin yrityksissä, jotka toisaalta ovat yleensä suhtautuneet tietoturvasuuteen vakavasti ja panostaneet turvaratkaisuihin.

Yritysvakoilussa tietoverkkoja hyödynnetään aiempaa useammin. Tietoverkkojen kautta tapahtuvan yritysvakoilun laajuutta on erittäin vaikea arvioida, mutta potentiaalisena uhkana se on merkittävä.

Tietokonevirukset muodostavat tietoturvasuuhuhan, johon yritykset ovat varautuneet kohtuullisen hyvin. Tämä pätee erityisesti suuriin yrityksiin, joissa virushyökkäys on tietoturvasuustapahtuma, jonka vastatoimenpiteet voidaan tavallisesti tehdä automatisoidusti. Nopeasti leviävät uudet haittaohjelmat silti saattavat aiheuttaa yhteiskunnallisesti merkittäviä vahinkoja, mutta yksittäisen tietokoneviruksen aiheuttamat vahingot jäävät yleensä pieniksi.¹⁶

Organisaatioiden riippuvuus yksittäisestä henkilöstä saattaa muodostua tietoturvasuutta vaarantavaksi. Keskeisestä toiminnosta saattaa vastata vain yksi henkilö, jonka toimintaa valvotaan puutteellisesti.

4.3.3.1 Operaattorit, telekommunikaatioala ja media

Palveluoperaattoritoiminnan ja mediapalveluiden kannalta palveluiden luotettavuus (tiedon eheys) ja niiden käytettävyys ovat erityisen tärkeitä. Näiden palveluiden tietoturvasuuden pettämisellä saattaa olla jopa yhteiskunnallisia vaikutuksia. Julkisuus nostaa verkkopalvelun houkuttelevuutta tietoturvasuushyökkäysten kohteena: onnistunut tietomurto tuottaa runsaasti julkisuutta sitä haluavalle. Tiedon sisällön muuttamiseen tähdännyt hyökkäys saattaa johtaa virheellisen informaation leviämiseen ja pahimmassa tapauksessa tiedotusvälineiden nauttiman yleisen luottamuksen murene- miseen.

Joukkotiedotus on varsin hajautunutta, joten tämän kaltainen uhka ei ole merkittävä tiedon yleisen saatavuuden kannalta. Oikeaa tietoa on saavilla muista lähteistä. Uhka on siinä, että luotettavana pidetystä lähteestä tullut väärä tieto tai palvelun toimimattomuus voi aiheuttaa vääriä toimia ja yleistä epätietoisuutta.

4.3.3.2 IT-palvelutoiminta

Avoimien tietoverkkojen hyödyntäminen IT-palveluyritysten toiminnassa on lisääntynyt merkittävästi. Osaltaan tähän on vaikuttanut edellä kuvatut talouselämään vaikuttaneet muutosvoimat, mutta toisaalta myös parantuneet tietoturvasuusvälineistöt.

Huomattava osa tietoturvasuuspalveluista on osana muuta palvelutarjontaa: verkonvalvonnassa, sovellusvuokrauksessa ja ns. hosting-palvelussa. Lisäksi tietotekniikan

¹⁶ Virusten aiheuttamista vahingoista on esitetty useita arvioita. Computer Economicsin arvion mukaan vuosina 1999-2001 kuusi laajimmin levinnyttä virusta aiheutti maailmalaajuisesti noin 15 miljardin euron vahingot. Suomessa olevaan tietokoneiden määrään suhteutettuna tämä merkit si vuositasolla noin 50-100 miljoonan euron vahinkoja pääasiassa yrityksille.

palveluyritykset tarjoavat myös suoraan tietoturvallisuuteen liittyviä palveluita. Palveluyrityksissä on suunnitelmalliseen tietoturvatyöhön ryhdytty panostamaan voimallisesti.

Käytettävyyden alenemisen taloudellinen vaikutus voi olla suuri.

Käyttöpalvelusopimuksissa palvelutason mittaaminen ja sen alittamisesta aiheutuvat sanktiot ovat yleistyneet. Asiakkaat ovat muutenkin tulleet tietoisiksi tietoturvallisuudesta ja alkaneet vaatia näyttöjä palveluiden tietoturvan implementoinnista.

Käyttöpalveluyritysten hyvä tietoturvallisuus on edellytys monen muun yrityksen tietoturvallisuudelle. Myös fyysistä turvallisuutta koskevat uhat kuten tulipalo, vesivahinko tai muu ”perinteinen” onnettomuus ovat merkitykseltään tietoliikenteeseen kohdistuvien uhkien veroisia.

Osa IT-palveluyritysten kohtaamista tietoturvallisuusongelmista tulee niiden asiakkaana olevien yritysten kautta: järjestelmien yhteensopimattomuus, asiakasyritysten tietoturvallisuuden hallinnoinnin ja toteutuksen ongelmat. Nämä voivat olla riski IT-palveluyritysten omallekin tietoturvallisuudelle.

Ohjelmistokehitystä tekevät yritykset ovat kehittäneet tietoturvallisuuden hallintamenetelmiään. Myös näille yrityksille merkittävin tietoturvallisuuden osa-alue on henkilöstöturvallisuus, jonka kehittämiseen on panostettu.

4.3.3.3 *Rahoitussektori ja kauppa*

Pankkien verkkopalvelut ovat Suomessa eräs kaikkein laajimmin käytetyistä verkkopalveluista. Paitsi käyttäjämäärissä, myös tietoturvallisuudessa suomalaiset verkkopankit edustavat maailman kärkeä.

Asiakkaiden palveluun tarkoitetun verkon lisäksi pankeilla on sisäisiä ja pankkien välisiä verkkoja, joiden tietoturvallisuus ei kuitenkaan kuulu tämän tarkastelun piiriin.

Keskeinen uhka kohdistuu loppuasiakkaille suunnattuihin Internet-palveluihin. Näiden käytettävyyden lasku vaikuttaa tuhansien ihmisen elämään. Sen sijaan onnistunut tietomurto rajoittuisi ilmeisesti niin pieneksi, ettei pankin riskinkantokyky siitä vaarantuisi.

Kaupan alalla perinteisen tukku- ja vähittäistoiminnan osalta tietoturvariskit ovat hallinnassa melko hyvin. Kaupan alalla riskienhallinnalla on pitkät perinteet (myymäläturvallisuus, logistiikan riskit). Kaupan alalla käytetään tiedonvälitykseen laajalti EDI:ä¹⁷, joka ei hyödynnä Internetiä. Erityisesti pienissä kaupan alan yrityksissä sähköisen kaupankäynnin palveluiden tarjoaminen voi kuitenkin tuoda uusia riskejä.

Kaupan bonusohjelmat keräävät tietoa asiakkaiden ostokäyttäytymisestä. Näissä järjestelmissä olevan tiedon väärinkäyttö tai joutuminen väriin käsiin olisi vakava yksityisyyden loukkaus.

4.3.3.4 *Teollisuus*

Teollisuusyritysten kannalta ongelmia aiheuttavat ympäristön nopea muutos ja tarve verkostoitua. Muutokset ovat olleet nopeimpia korkean teknologian yrityksissä. Sopeu-

¹⁷ EDI (electronic data interchange) eli OVT (organisaatioiden välinen tiedonsiirto) tarkoittaa määrämuotoista tiedonsiirtoa kahden eri organisaatiossa oleva tietojärjestelmän välillä.

tuminen ei ole aina sujunut ongelmitta tilanteessa, jossa uusien tekniikoiden ja uusien uhkien hallinta vaatii perinteisen tuotantotoiminnan yrityksissä uutta yrityskulttuuria, valmiuksia ja resursseja tietoturvallisuuden kehittämiseen. Tyypillisesti nämä yritykset eivät ole mieltäneet tietoturvallisuuden kasvavaa merkitystä itselleen eivätkä ole aiemmin tottuneet jatkuviin ympäristömuutoksiin. Molemmat seikat ovat altistaneet varsinaisille tietoturvallisuushille.

Tuotannonohjauksen ja tuotantoautomaation järjestelmät integroituvat keskenään ja muihin yritysten muodostamien arvoketjujen tietojärjestelmiin, minkä seurauksena tietoturvan merkitys kasvaa entisestään. Tietoturvallisuusasioissa tiedostamisen ja toiminnan taso vaihtelee merkittävästi yrityksestä toiseen. Verkostoitumisen myötä edellytetään kaikilta verkostoon osallistuvilta hyvää tietoturvallisuuden tasoa sekä ymmärrystä siitä, että oma tietoturvallisuus saattaa ratkaisevasti vaikuttaa muiden tietoturvaluuteen.

Riskitaso nousee huomattavasti tuotantotoiminnan integroitua yleisten verkkojen välityksellä toimiviin tietojärjestelmiin. Tietoturvatilat saattavat johtaa erittäin korkeisiin riskeihin, etenkin mikäli kompleksista järjestelmää ei kokonaisuudessaan täysin hallita. Erityisen tärkeä on tunnistaa tietoturvatilat niissä toimittajan ja asiakkaan integroiduissa järjestelmissä, jotka sisältävät mahdollisuuksia kontrolloida tehdastasoisia prosessijärjestelmiä tai kriittistä infrastruktuuria.

4.3.3.5 PK-sektorin uhat

Pienissä ja keskisuurissa yrityksissä tietoturvatietoisuuden ja tietoturvaluustoiminnan taso vaihtelevat. Tietoturva saatetaan ymmärtää vain erilaisten verkkoihin asennettavien laitteiden tai ohjelmistojen hankinnalla hoidettavaksi. Laitteiden, ohjelmistojen ja integrointipalvelun tarjoajat toimivat samalla alan konsultteina, jolloin ongelmaksi saattaa muodostua toimittajien liiallinen halu omien, mahdollisesti kapea-alaisen ratkaisujen kauppaamiseen ilman, että asiakkaan todelliset tarpeet otetaan huomioon.

Tietoturvallisuuden merkitys vaihtelee merkittävästi yrityksestä toiseen. Tietotekniikkaa vain vähäisessä määrin hyödyntävän palvelualan yrityksen tarpeet poikkeavat merkittävästi suunnittelu- ja ohjelmointialan yrityksistä.

Neljässä kymmenestä pk-yrityksestä kaikilla työntekijöillä on käytössään tietokone ja kahdeksassa kymmenestä pk-yrityksestä on Internet-yhteys, joten tietotekniikkaan ja tietoverkkoihin liittyvä tietoturva koskettaa useimpia yrityksiä.

Pk-yrityssektorin ja kunnallishallinnon välillä on nähtävissä analogiaa: suurten yksiköiden edellytykset tietoturvaluustoimintoihin ovat paremmat kuin pienten yksiköiden. Silti toimijan koolla ja tietoturvaluustoiminnan tasolla ei välttämättä ole suoraa suhdetta.

Pienissä ja keskisuurissa yrityksissä tietoturvarikkeiden syiksi arvioidaan yleisimmin käyttäjän tekemää virhettä. Tavanomaisia ovat myös ohjelmien ja laitteistojen anastus, järjestelmien luvaton käyttö ja järjestelmävirheet. Havaituista tietoturvaongelmista ehdottomasti yleisin on tietokonevirukset.

Uhkien aiheuttajia ovat omat työntekijät, satunnaiset hakkerit, entiset työntekijät ja kilpailevan yrityksen työntekijät.

Pienissä ja keskisuurissa yrityksissä erityisesti sähköisen liiketoiminnan tietoturvallisuusuhkien merkityksen arvioidaan muodostuvan merkittäväksi liiketoiminnan kehittymistä haittaavaksi tekijäksi. Epäilyt yritysvakoilusta ja muusta rikollisuudesta, epäselvyys sopimusten sitovuudesta sekä epävarmuus maksun saamisesta verkkopalvelun asiakkailta ovat yleisiä verkkopalveluiden kehittämisessä havaittuja riskejä.¹⁸

Kokonaisuutena suurimmat ongelmat ovat pienyrityksissä, joissa ei ole tietohallinnon asiantuntemusta.

Toisaalta pienyrityskentässä verkostoituminen saattaa parantaa tilannetta siltä osin, että verkostoon liittyessään pienyritykset yleensä pääsee verkoston tietoturva- ja laaturjestelmien piiriin, mikäli tällaisia verkostossa on.

Keskeisiä keinoja tietoturvallisuusuhkien vähentämiseksi pienyrityksissä ovat tietoturvallisuuden merkityksen tiedostaminen, vastuiden tunnistaminen ja selkiyttäminen, koulutus sekä selkeästi määritellyt toimintatavat ja toimintapolitiikat. Vasta näiden ollessa kunnossa on realistista hallita riskejä teknisten ratkaisujen avulla.

4.3.4 Yksityishenkilöihin käyttäjinä kohdistuvat uhat

Enemmistö käyttäjistä ei tiedosta uuden teknologian riskejä, tai joissain tapauksissa yliarvioi niitä. Esimerkkejä jälkimmäisestä ovat tilaamisen ja maksamisen pelot verkko-kaupassa.

Päätelaitteiden merkitys tietoturvan kannalta voi jäädä käyttäjälle epäselväksi. Laitteita ja Internet-liittymiä hankittaessa ei tunneta niiden tietoturvallisuusvaikutuksia, eikä tietoturvallisuusominaisuuksia arvosteta riittävästi. Tämä lienee tärkein yksityishenkilöön kohdistuva tietoturvallisuusuhka, etenkin koska sillä on vaikutuksia yrityksiin: kadotettu laite saattaa sisältää työnantajan yrityssalaisuuksia, salasanoja tai muuta luottamuksellista tietoa.

Tavanomainen ja edellistä selväpiirteisempi tietoturvaongelma ovat tietokonevirukset. Lisääntynyt sähköpostin käyttö yhdistettynä puuttuviin tai vanhentuneisiin virustorjuntaohjelmistoihin luo haittaohjelmille kasvualustaa. Sähköpostin kautta ja suoraan Internetistä ladattavissa ohjelmissa oleva virusriski on yleensä käyttäjien tiedossa, mutta vahingon mahdollisuus on silti suuri.

Internetin käyttö erityisesti kiinteiden yhteyksien (ADSL, kaapelimodeemi) kautta aiheuttaa uuden tietoturva-uhkan. Jatkuvasti IP-verkkoon kytketyt tietokoneet ovat usein huonosti suojattuja. Esimerkiksi kaapelimodeemiyhteyksillä tiedonsiirto on perusmuodossaan suojaamatonta ja mahdollistaa saman kiinteistön sisällä kaikkien käyttäjien tietoliikenteen salakuuntelun ja tietokoneiden tarkkailun. Tämän uhan merkityksen arvioidaan lisääntyvän kiinteiden yhteyksien yleistymisen myötä.

Yritysten ja yksityisten kansalaisten kannalta yhteinen muutos on työn ja yksityiselämän rajan hämärtyminen: etätöiden myötä kodista on tullut toimiston jatke. Kodin tietoturvallisuus vaikuttaa siten myös yrityksen tietoturvaluuteen.

¹⁸ PK-yritykset Internetin hyödyntäjinä. LVM ja Otso Consulting, 2000.

Kansalaisilla ja pienyrityksillä ei useinkaan ole kykyä uuden teknologian hallintaan, joten palveluntoimittajien tulisi ottaa vastuuta tarjoamiensa palveluiden tietoturvasuudesta entistä laajemmin. Internet-yhteyksien tietoturvapalveluiden jatkuva kehittäminen ja automatisointi on esimerkki tämän kaltaisesta toiminnasta.

Tietoturvasuusioiden uutisointi ja esille tuonti tiedotusvälineissä on lisännyt tietoturvasuusioiden tietoisuutta, joskin voittopuolisesti riskien näkökulmasta. Erilaisia apuaineistoja käyttäjille on saatavilla: TIEKE:n tekemä kansalaisen tietoturvaopas, valtiovarainministeriön myös käyttäjille suunnatut ohjeet (sähköposti, virustorjunta ym.), operaattorien ja virus torjuntayritysten käyttäjilleen jakama sähköinen ja kirjallinen aineisto sekä erilaiset tietoturvasuuteen liittyvät kurssit ja muu koulutustoiminta.

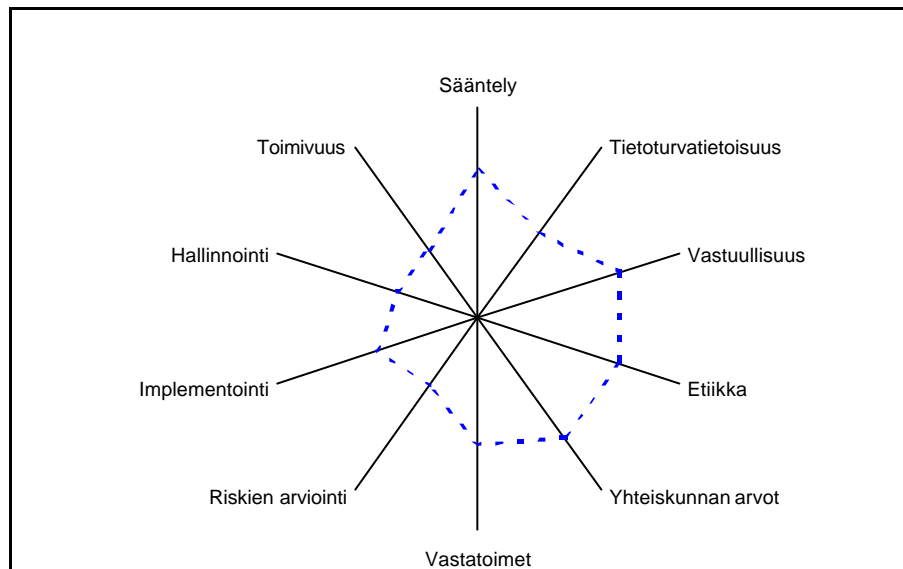
Kokonaisuutena yksityishenkilöihin kohdistuvat uhkat ovat lisääntymässä ja tilanne on kehittymässä käyttäjän kannalta huonompaan suuntaan.

Keskeisiä tietoturvasuusiuhkia

- liike- ja muun toiminnan turvasuuden vaarantuminen tietoturvasuuden puutteiden vuoksi
- johdon asenteet tietoturvasuutta kohtaan ja tietoturvasuuden toimeenpanon puutteet
- toiminnan keskeytymisen vaikutusten puutteellinen analysointi
- yritysverkostojen epäselvät vastuut ja vähäinen tietoturvasuuden valvonta
- tietojärjestelmien yhteensopimattomuus
- yhteiskunnan kriittiseen infrastruktuurin kohdistuvat uhkat
- tietoon kohdistuvat oikeuden loukkaukset (varkaus, tuhoaminen, muuttaminen)
- luvaton tunkeutuminen tietojärjestelmiin
- virukset ja muut nopeasti leviävät haittaohjelmat
- organisaation riippuvuus erityisosaamisesta ja resurssipula tietoturvasuuden toimeenpanossa
- yksityishenkilöiden asenteet ja kyvyttömyys hallita uusia palveluita ja uutta tekniikkaa
- tahattomasti tehdyt vahingot

5 TOTEUTUNEET TOIMENPITEET TIETOTURVALLISUUDEN EDISTÄMISEKSI

Jokainen verkostoituneeseen toimintaan osallistuva organisaatio ja yksilö on olennainen osa yhä laajemmassa verkossa. Tietoturvallisen toiminnan kannalta kaikkien osapuolten on sisäistettävä tietoturvalähtöinen ajattelu sekä toimintakulttuuri, johon sisältyy jatkuvaa parantamista.



Kuva. Neuvottelukunnassa syntynyt näkemys tietoturvallisuuden edistämiseksi toteutuneiden toimenpiteiden tasosta suomalaisessa yhteiskunnassa (selitetään tekstissä tarkemmin). Tilanne on sitä parempi, mitä kauempana keskipisteestä katsottuna käyrä leikkaa kunkin akselin.

5.1 Tietoturvallisuuteen liittyvä sääntely

Tietoturvaratkaisuihin liittyvää lainsäädäntöä ja pelisääntöjä kehitetään sekä kansallisesti että kansainvälisenä yhteistyönä. Ajankohtaisista aiheista on lukuisia: sähköisen kaupankäynnin vastuut, tunnistamisen ja sähköisen allekirjoituksen kysymykset, julkisen avaimen infrastruktuurin luominen ja siihen liittyvä sääntely sekä palveluntarjoajille ja operaattoreille asetettavat tietoturvavelvoitteet. Paraikaa uudistetaan Euroopan unionin sähköisen viestinnän tietosuojadirektiiviä. Direktiivin vaikutukset ulottuvat kansalliseen lainsäädäntöön ja tietoturvakulttuurin koko EU:ssa.

Suomessa ei ole erillistä tietoturvallisuuslakia, vaan tietoturvallisuuteen liittyviä säädöksiä on useassa eri laissa. Tästä huolimatta Suomen säädöspohja kattaa kokonaisuutena varsin hyvin tietoturvallisuuden eri osa-alueet. Useat perustuslain takaamat oikeudet edellyttävät toteutuakseen hyvää tietoturvallisuutta. Näistä mainittakoon viestinnän salaisuuden suoja, omaisuuden suoja ja velvoitteet hyvästä hallinnosta.

Monet tietoturvaan liittyvät lait on kohdistettu tietyille ryhmälle, kuten teleoperaattoreille, terveydenhuollolle tai julkiselle hallinnolle. Sääntely on pääosin tekniikkariippuma-

tonta ja keskittyy olennaisimpaan: tietoon ja sen turvaamiseen. Uutta sääntelytarvetta luovat lainsäädännön harmonisointi EU:ssa sekä eräät kansainväliset sopimukset.

Valtiovarainministeriön ja Lapin yliopiston yhteistyönä tehtiin jo vuonna 1997 tietoturvallisuutta koskevan mahdollisen lainvalmistelun perusselvitys¹⁹. Vuonna 1998 tehtiin päätös siitä, että ei ole tarvetta erilliseen tietoturvallisuuslain säätämiseen. Tietoturvallisuutta säätelevällä yleislailla olisi kuitenkin joitain etuja. Lain säätäminen nostaisi tietoturvallisuuden yhteiskunnallista asemaa ja siihen kohdistuvaa yleistä mielenkiintoa. Mahdollisesta yleislaista riippumatta tietoturvallisuus näkökulman tulisi olla esillä kaikessa lainsäädännössä.

Tietoyhteiskuntapalveluiden tarjonnasta²⁰ annettavan lain tavoitteena on, että palveluntarjoajat eivät voi välttää valvontaa toimimalla toisessa sijoittautumisvaltiossa. Laki myös edellyttää, että kaupallisessa viestinnässä, kuten mainonnassa ja suoramarkkinoinnissa, on noudatettava avoimuusvaatimuksia. Tällä tulee olemaan myös käyttäjien luottamusta lisäävä vaikutus.

Tietoturvallisuusrikokset on sanktioitu rikoslain 38 luvussa, mutta myös muita rikoslain kohdat saattavat tulla kyseeseen. Näin erityisesti silloin, kun tietoturvarikos aiheuttaa haittaa tai vahinkoa.

5.2 Tietoturvatietoisuus

Yksityisten ihmisten tietoturvaosaaminen on yleensä melko heikkoa. Osaltaan tähän vaikuttaa tiedon ja yksityisyyden suojan merkityksen nopea muuttuminen. Tiedotusvälineet ovat viime aikoina uutisoineet näkyvästi tietoturvallisuusrikoksista, mikä on havahduttanut monet ymmärtämään tietoturvallisuuden merkityksen. Toisaalta tiedotusvälineiden uutisointi ei aina anna riittävän selkeää kuvaa kokonaisuudesta, vaan saattaa keskittyä yksittäisiin helposti uutisoitaviin tapauksiin.

Suurissa yrityksissä tietoturvallisuuskysymyksiin on yleensä paneuduttu. Osaamisen taso on vielä varsin vaihtelevaa: eri henkilöillä on erilainen näkökulma tietoturvallisuuteen, tietoturvallisuuden osa-alueiden osaaminen on pirstoutunut, joten kokonaisuuden hallinta voi olla heikkoa.

Pienissä ja keskisuurissa yrityksissä tietoturvallisuuden kehittäminen riippuu usein merkittävästi näiden asiakkaina olevien suurten yritysten ja päämiesten asettamista tietoturvallisuusvaatimuksista. Toimittajilla ja alihankkijoilla on entistä useammin pääsy asiakkaiden ja päämiesten järjestelmiin. Toisaalta monissa pienissä yrityksissä ei ole merkittäviä turvallisuustoimenpiteitä edellyttävää tietoa lukuun ottamatta lakisääteisesti suojattavia henkilötietoja. Tällöin ei tietoturvallisuustietouteenkaan ole tarvetta merkittävästi panostaa.

Kuntasektori on heterogeeninen ja vaihtelu tietoturvallisuusasioiden hoidossa on suurta. Tietosuojaan on kiinnitetty paljon huomiota erityisesti sosiaali- ja terveydenhuollossa.

¹⁹ Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. Lapin Yliopisto 1997.

²⁰ HE 194/2001; laki implementoi vastaavan EU:n direktiivin.

Erilaista yleisesti ohjeistavaa aineistoa on runsaasti saatavilla. Valtionhallinnossa tietoturvatietoisuutta on merkittävästi parannettu Vahti:n tuottamien, myös yksityisellä ja kuntasektorilla hyödynnettävien ohjeiden ja suositusten avulla.

Tietoturvatietoisuutta on yrityksissä yleensä parannettu luomalla niiden tietoturvallisuustyötä ohjaava tietoturvapolitiikka. Jotkin yritykset ovat lisäksi sertifioineet oman tietoturvallisuustoimintansa BS7799-standardin mukaisiksi. Mahdollisten tietoturvallisuussertifikaattien julkituonnilla kehitetään tietoturvatietoisuutta laajemminkin.

Suomessa on vuoden 2002 alussa aloittanut toimintansa Viestintäviraston alainen CERT-FI -yksikkö, jonka tehtävänä on koota ja jalostaa tietoturvaan liittyvää informaatiota, välittää sitä suomalaisille, havainnoida tietoturvallisuusloukkauksia ja ehkäistä ennalta uhkia sekä osallistua tietoturvarikkomusten selvittämiseen.

Yleisesti saatavilla olevien telepalvelujen tarjoajat ovat sekä EU:n että Suomen lainsäädännön nojalla velvollisia tiedottamaan tilaajilleen erityisistä verkon turvallisuusriskeistä ja mahdollisista korjauskeinoista²¹. Internet-operaattorit ovat velvollisia kertomaan asiakkailleen tietokoneviruksista, tietomurroista ja muista Internetiin liittyvistä tietoturvallisuusriskeistä. He ovat velvoitettuja myös kertomaan, miten riskeiltä voi suojautua ja mitä se maksaa²².

Kokonaisuutena teknistä tietoturvaosaamista Suomessa on melko paljon, mutta laaja-alaista, organisaatioiden ja käyttäjien toimintaedellytyksiä parantavaa tietoturvaosaamista tulisi lisätä.

5.3 Vastuullisuusnäkökulma

Vastuullisuudella tarkoitetaan tietoverkossa toimivien vastuullisuutta omasta toiminnastaan ja sen vaikutuksista muiden tietoturvallisuuteen. Osaamiseen liittyy vastuu, ja vastuullisuuden ymmärtäminen toisaalta edellyttää riittävää osaamista. Erityisesti sähköisen tiedon epäsopeva tai laitton käyttö on teknisesti helppoa, joten käyttäjältä edellytetään myös moraalista vastuuta.

Käyttäjän tulee tuntea vastuunsa tietoverkkojen ja vuorovaikutteisten palvelujen käyttäjänä. Laitonta tai hyvän tavan vastaista on käyttää tele- tai tietoverkkoa toisia vahingoittavalla tai häiritsevällä tavalla, esimerkiksi tunkeutumalla luvatta toisen tietokoneeseen, levittämällä tietoisesti tietokoneviruksia, lähettämällä tarpeettomia viestejä tai käyttämällä verkkoa ja siihen kytettyjä resursseja tavalla, johon resurssien tarjoaja ei ole niitä tarkoittanut.

Vaikka sananvapauteen sisältyy oikeus lähettää ja vastaanottaa verkon välityksellä viestejä kenenkään sitä ennalta estämättä, ei viestissä kuitenkaan saa loukata toista henkilöä tai hänen yksityiselämäänsä.

Suomessa keskeiset toimijat, kuten pankit, perusinfrastruktuurista vastaavat yritykset ja teleoperaattorit tuntevat vastuunsa ja pyrkivät toimimaan sen mukaisesti. Käyttäjätasolla tietoisuuden puute voi vaikeuttaa vastuullista toimintaa.

²¹ Direktiivi 97/66/EY, 4. artikla

²² Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)

Yrityksissä tietoturvallisuuteen liittyvät asiat on tyypillisesti säilytetty tietohallinnolle. Vasta suurissa yrityksissä on tiedostettu, että yritysjohto on viime kädessä vastuussa tietoturvallisuuden kokonaisuudesta. Samalla käsitys tietoturvallisuudesta puhtaasti teknisenä asiana on väistynyt, ja tietoturvallisuutta pidetään yhtenä liiketoiminnan jatkuvuuden turvaajana.

Koska tietoturvallisuuden tason nostaminen on myös kustannuskysymys, toimijat saattavat pyrkiä toteuttamaan tietoturvallisuusveloitteensa minimitasolla. Kaikissa yrityksissä ei ole tietoturvapoliittikkaa, tai sitä ei ole viety käytännön toimintaan. Tällöin yrityksen tietoturvallisuus toiminnan päälinjat eivät ole selvillä tai ne eivät vaikuta riittävästi käytännön toimintaan. Myös toteuttamisvastuut saattavat jäädä epäselviksi.

5.4 Eettiset periaatteet

Voimassa oleva lainsäädäntö ilmentää yhteiskunnan eettistä normistoa. Suomalaisessa kulttuurissa ihmisten moraalit on Euroopan mittapuun mukaan korkealla tasolla, mikä näkyy mm. siinä, että yhteiskunnan normeja noudatetaan melko hyvin.

Melko yleisesti arvioidaan, ettei haittaohjelmia kehitetä Suomessa merkittävässä määrin. Esteenä ei suinkaan ole puuttuva tietotaito, sillä yksinkertaisten virusten tekeminen ei ole erityisen vaativaa, vaan ilmeisesti moraalinen käsitys virusten aiheuttamasta haitasta muille tietokoneen käyttäjille.

Useat yritykset ovat laatineet yhteistyössä henkilöstön edustajien kanssa sähköpostin ja Internetin käytön ja valvonnan pelisäännöt.

Tietoyhteiskunnassa ja tietoverkoissa eettiset normit muuttuvat nopean murroksen mukana. Erityisiä ongelmia ovat suhtautuminen tietoturvaan ja uhat yksityisyydelle, mutta myös tietoverkoissa käyttäytyminen, tekijänoikeudet ja piratismi. Myös tietoturvan ja luottamuksen synnyttämiseksi on tiedon totuudellisuus arvokasta. Totuudellisuus riippuu luonnollisesti tiedonlähteen oikeellisuudesta, mutta myös tiedon eheyden säilymisestä.

5.5 Demokratiaperiaatteet

Demokraattisessa yhteiskunnassa tietoturvalliseen toimintaan liittyviä arvoja ovat hallinnon avoimuus, julkisuus, vapaa tiedon välittäminen ja henkilöiden tietosuojat.

Viranomaisten asiakirjojen julkisuudesta annettu laki ohjaa merkittävästi hallinnon julkisuutta. Lain edellyttämää tietojen luokittelua julkishallinnon tietojärjestelmissä ollaan toteuttamassa.

Monissa kunnissa on kunnanvaltuuston ja lautakuntien toiminnan julkisuutta on lisätty tietoverkkojen avulla. Pöytäkirjoja ja esityslistoja voi lukea Internetin kautta, joten kuntalaisten mahdollisuus vaikuttaa kotikuntansa asioihin voi parantua merkittävästi.

Henkilötietolaki (523/1999) on merkittävin yksityisyyden suoja turvaava säädös. Laissa edellytetään, että henkilötiedot kerätään pääsääntöisesti vain henkilöltä itseltään. Henkilötietorekisteriin rekisteröidyllä on oikeus tarkastaa hänestä tallennetut tiedot ja vaatia virheelliset tiedot oikaistavaksi. Yksityisyyden suojaan liittyvää toimintaa valvoo ja siitä antaa ohjeita tietosuojavaltuutetun toimisto.

5.6 Vastatoimet

Tietoturvallisuustyö on pääasiassa etukäteen tapahtuvaa uhkiin varautumista. Tietoturvallisuuden rikkoonnuttua tapahtuneiden vahinkojen määrää voidaan rajoittaa oikein suunnitelluilla, nopeilla ja oikein kohdennetuilla vastatoimilla. Verkottumisen myötä tapahtuman havainnoinnin ja etukäteisvarautumisen kehittämisessä on yhteistoiminnalla merkittävä rooli.

Viestintäviraston alainen CERT-FI auttaa tietoturvaongelmien ehkäisyssä ja tietoturvaongelmien ratkaisussa.

5.6.1 Ennakoiva työ

Kaiken ennakoivan tietoturvatyön perustana on organisaation toiminnan ymmärtäminen ja sen pohjalta tapahtuva riskianalyysi. Riskianalyysin tärkeyden vuoksi se käsitellään omana kohtanaan.

Teknologiapanostuksia on tehty etupäässä tietoturvallisuuden teknisiin osa-alueisiin kuten virusurva, palomuurit ja tietojärjestelmien käytön seuranta. Tämä ei kuitenkaan yksinomaan riitä, vaan lisäksi tarvitaan tietoturvallisen toiminnan saamista organisaation normaaliksi toimintataivaksi.

Yrityksissä tietoturvallisuuskoulutus liittyy lähinnä henkilöiden työtehtäviin. Laajamittaista koulutusta peruskouluissa tai muissa oppilaitoksissa ei ole järjestetty sen enempää oppilaille kuin opetushenkilöstöllekään. Luontevaa olisi tuoda tietoturvallisuus osaksi kaikkien kansalaisten tietoyhteiskuntavalmiuksien kehittämistä.

Henkilöiden tunnistaminen ja tietoliikenteen salaaminen voidaan tehdä varmenteisiin liittyvillä julkisen avaimen salaustekniikoilla. Varmenteiden käyttöönottamiseksi on Suomessa tehty merkittävästi työtä, ja varmenneinfrastruktuuri tulisi saada laajaan käyttöön.

Valtionhallinnossa valtion tietoturvallisuuden johtoryhmä (Vahti)²³ on julkaissut runsaasti ohjeita ja suosituksia, joilla pyritään edistämään virastojen ja laitosten tietoturvalisuutta. Vahti:n ohjeet hyödyntävät myös yleisiä tietoturvaohjeita ja -käytänteitä sekä levittävät näitä edelleen. Ohjeiden soveltamista voitaisiin lisätä myös valtionhallinnon ulkopuolisella julkisella sektorilla. Valtionhallinnossa on myös laajasti tietoturvalisuutta edistäviä yhteishankkeita.

Teollisuus ja työnantajat (TT) on aktiivinen tietoturvallisuuden edistäjä jäsenkunnassaan. TT on julkaissut oppaita ja koulutusmateriaalia sekä antanut tietoturvalisuus koulutusta yritysten johdolle.

Kuluttajajärjestöjen rooli luotettavan tiedon tuottajana, jakajana ja oikeuksien valvojana on lisääntymässä. Tätä tulisi hyödyntää myös tietoturvatietoisuuden lisäämiseksi. Järjestöjen toimintaa tulisi laajentaa kattamaan tietoturvalisuus perinteisten kuluttajansuojakysymysten lisäksi.

Kuluttajatuotteiden ja palveluiden tietoturvalisuudessa pätevät pitkälti samat asiat kuin niiden tuoteturvalisuudessa: kumpikaan ei ole kuluttajalle ilmeisiä, vaan niiden

²³ <http://www.vn.fi/vm/julkaisut/tietoturvalisuus/index.html>

todentaminen vaatii tietoja ja taitoja, joita normaalilla kuluttajalla ei voida kohtuudella olettaa olevan. Myös EU:n tasolla korostetaan kattavaa kuluttajan suojaa²⁴.

Kokonaisuutena arvioiden ennakoivia toimenpiteitä on mahdollista parantaa huomattavasti. Esimerkiksi tietoturvaluuskoulutusta tulee lisätä osana muuta koulutusta ja mahdollisesti itsenäisinä koulutusohjelminä. Olemassaolevien ohjeiden kattavuutta tulee lisätä ja varmistaa, että niitä kyetään pitämään ajan tasalla nopeasti muuttuvassa ympäristössä.

5.6.2 Havainnointi ja seuranta

Tietoturvallisuuden edistämiseksi kansainvälisellä yhteistyöllä on suuri merkitys uhkien kansainvälisyyden ja nopean maasta toiseen leviäminen vuoksi. Myös tapahtuneiden tietoturvaloukkausten vastakeinot toimivat usein maasta riippumatta.

Pääosa yritysten välisestä tietoturvaluusuyhteistyöstä on henkilöiden välisiin suhteisiin perustuvaa tiedonvaihtoa.

Viestintäviraston alaisuudessa toimiva CERT-FI -yksikkö edistää tietoturvaluusua seuraamalla tilannetta Suomessa ja ulkomailla. CERT-FI kerää tietoa, analysoi sitä, antaa suosituksia, neuvontaa ja ohjeita tietoturvaluusua kehittämiseksi. Myös kansalaiset voivat CERT-FI:stä hakea verkon kautta tietoa ja ilmoittaa havaitsemistaan tietoturvaongelmista. FUNET-CERT tekee vastaavaa toimintaa korkeakouluille, tutkimuslaitoksille ja yli 50 valtion virastolle, jotka toimivat FUNET:n tietoliikenneverkossa. Eri maiden CERT-toimijoiden verkosto koostuu itsenäisistä, toisensa kanssa yhteistyötä tekevästä organisaatioista.

Valtiovarainministeriö ja valtiontalouden tarkastusvirasto (VTV) tekevät tietoturvaluusua pitkäaikaisseuranta, jota ei ole kaupallisilla toimijoilla eikä kunnallisella sektorilla.

Viranomaisyhteistyön rinnalla on eri toimijoiden välistä yhteistyötä, joiden muodot vaihtelevat. Esimerkiksi tietokonevirustorjuntaa tekevillä on tehokkaasti toimiva yhteistyöverkosto, jonka kautta vaihdetaan lähinnä uusiin tietokoneviruksiin liittyvää tietoa.

Epävirallista yhteistyötä tapahtuu täysin avoimien Internet-keskustelulistojen avulla. Suomalaiset tietokonevirustutkijat, salakirjoitusmenetelmien kehittäjät sekä muiden erityisalojen tutkijat ja tuotekehittäjät kokoontuvat omiin konferensseihinsä.

5.6.3 Reagointi

Yrityksissä ja virastoissa on vaihtelevasti sisäisiä yksiköitä ja vastuuhenkilöitä, joiden tehtävänä on tietoturvaloukkausten havainnointi, seuranta ja tapahtuneiden tietoturvaloukkausten vastaisten toimien johtaminen. Pienillä yrityksillä ei tähän yleensä ole taloudellista mahdollisuutta.

Ympäri vuorokautinen päivystys tietoturvaluusuasioissa tulee kuulumaan CERT-FI:n tehtäviin.

²⁴ Green Paper on Consumer Protection, COM (2001) 531 of 2 October 2001.

Tiedot tietokonevirushyökkäyksistä leviävät verkossa nopeasti. Virustorjuntaohjelmistoja tarjoavat globaalisti toimivat yritykset pystyvät parhaimmillaan antamaan päivitetyn torjuntaohjelman muutamien tuntien kuluessa viruksen havaitsemisesta.

Keskusrikospoliisin tietokonerikoksiin erikoistunut yksikkö selvittää tietoverkkoihin liittyviä rikoksia. Kynnys rikosilmoituksen tekoon tietoturvarikkomuksissa on kuitenkin usein korkea. Yleisesti arvioidaan, että suurin osa rikoksista jää edelleen tutkimatta. Toisaalta pienehköjen ja tavanomaisten tietoturvarikkomusten kuten tietokonevirusten ja tunkeutumisyritysten rutiininomainen torjunta on organisaatioissa jokapäiväistä toimintaa, jonka ei katsota aiheuttavan tarvetta rikosilmoituksen tekoon.

Koko yhteiskuntaan ulottuvaa nopeaa tiedotusta ei Suomessa ole, lukuun ottamatta satunnaisia uutisluonteista mediatiedottamista.

5.7 Riskien arviointi

Organisaation riskiarvioinnin on perustuttava kokonaistoiminnan ja siihen kohdistuvien uhkien tuntemiseen. Tämän pohjalta laadittu tietoturvallisuuspolitiikka ohjaa tietoturvallisuustoimintaa.

Pisimmällä tietoturvallisuuden riskiarvioinnissa ovat suuryritykset ja kriittisen infrastruktuurin toimittajat, jotka ovat valmiuslain ja muiden säädösten nojalla velvoitetut varautumaan ydintoimintansa turvaamiseen kaikissa oloissa.

Riskiarvioissa saatetaan tarkastella yksittäisiä uhkia, vaikka uhat ja niiden torjunta kytkeytyvät usein laajemmiksi kokonaisuuksiksi, joissa useilla toimijoilla on oma roolinsa. Riskien ja toteutuneiden vahinkojen arvioinnin vaikeutta kuvaa sekin, että suomalaiset vakuutusyhtiöt ovat todenneet, etteivät ne voi tarjota kattavia tietoturvakatuksia.

Riskianalyysi ulotetaan harvoin kattamaan organisaatioon kohdistuvan vahingon vaikutukset muihin yrityksiin ja koko yhteiskuntaan.

5.8 Teknisten tietoturvallisuustoimenpiteiden implementointi

Tietojen suojausten onnistumiselle olisi tärkeää, että tietoturvallisuus otetaan huomioon tietojärjestelmien ja verkkojen suunnittelussa ja toteutuksessa. Näin ei kuitenkaan yleensä toimita, vaan tietoturvallisuusominaisuuksia yritetään liittää järjestelmiin myöhemmin. Tällöin toiminta voi jäädä irrallisiksi tietoturvallisuusratkaisuiksi eikä muodosta eheää kokonaisuutta.

Yrityksissä tehtyjen tietoturvallisuuspolitiikkojen ja tietoturvatietoisuuden paranemisen myötä toimintatavat ovat muuttumassa. Tietojärjestelmien pitkistä elinkaarista johtuen tietoturvallisuus on heikosti toteutettu merkittävässä osassa vanhoja tietojärjestelmiä. Erityisesti pienissä yrityksissä tulisi olla selkeä vastuunjako teknisten muutosten (kuten uudet tietojärjestelmät ja päivitykset) aiheuttamista muutoksista tietoturvallisuuteen.

5.9 Tietoturvallisuuden hallinnointi

Valtionhallinnossa tietoturvallisuuteen liittyvät asiat on jaettu useille tahoille. Sektoreiden välillä on monen tasoista yhteistyötä.

Kuntasektorilla tilanne on hajanainen, mutta kokonaisuutena arvioiden tietoturvallisuuden kehittämisen vastuut eivät ole riittävän selkeitä. Mikäli kunnan tietojärjestelmillä on yhteyksiä valtionhallinnon tietojärjestelmiin, on myös sisäasiainministeriöllä ohjaamismahdollisuuksia tältä osin. Myös Juhta ja Kuntaliitto tekevät tietoturvallisuuteen liittyvää ohjaavaa työtä, mutta muuten kunnat toimivat itsenäisesti.

Elinkeinoelämässä tietoturvallisuuden hallinnointi tapahtuu yrityskohtaisesti. Menetelmät ovat yrityksittäin vaihtelevia, mutta tietoturvaluussertifiointien kautta yhtenäiset toimintatavat ovat alkaneet vähitellen yhtenäistyä. Suurissa yrityksissä tehdään usein tietoturvaluusauditointia esimerkiksi tilintarkastustoiminnan yhteydessä. Esimerkiksi tilitoimistoilla olisi merkittävä mahdollisuus vaikuttaa PK-yritysten tietoturvaluusuteen, mutta nämä eivät vielä yleisesti ole riittävästi tiedostaneet mahdollisuuksiaan asiakkaitensa tietoturvaluusuden parantamisessa.

Tietoturvaluus on vasta muotoutumassa osaksi organisaatioiden laatutyötä ja toimintaprosesseja. Laatutyö edesauttaa tietojärjestelmien ja prosessien koko elinkaaren kattavien tietoturvaratkaisujen kehittämistä. Monet nykyisistä ratkaisuista ovat yksittäisten tietoturvaluuhkien estämiseksi tehtyjä erillISRatkaisuja.

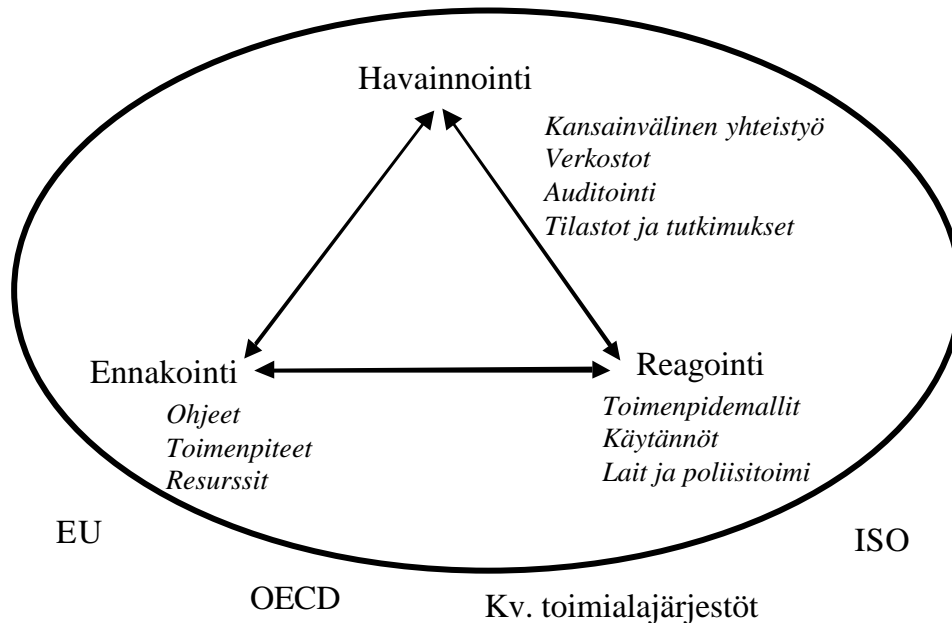
Tietoturvaluusustyön toteutuneita toimenpiteitä ja tarpeita

- Tietoturvatyö on Suomessa ja kansainvälisesti sektorikohtaista.
- Tarve laaja-alaiseen ja kokonaisvaltaiseen eri osapuolten tietoturvaluusuyhteistyöhön on ilmeinen.
- Neuvottelukunnan rooli on toimia laaja-alaisena tietoturvaluusustyön foorumina.
- Tietoturvaluusuden merkitys on lisääntynyt liike-elämän toiminnan, verkostoitumisen ja tietoyhteiskunnan palveluiden kehittymisen myötä.
- Tietoturvaluusutta säännellään useilla laeilla ja säädöksillä, mutta myös kokoavaa tietoturvaluualakia tulisi harkita.
- CERT-FI on aloittanut toimintansa ja lisää yleistä tietoisuutta tietoturvaluuhista ja auttaa ongelmatilanteiden ratkaisussa.
- Tietoturvaluusuden kehittäminen on otettu osaksi organisaatioiden laatutyötä.
- Valtion tietoturvaluusuden johtoryhmä on antanut runsaasti erilaisia ohjeita.
- Tietoturvaluusuden taso vaihtelee sektoreittain ja toimijoittain suuresti.
- Yksityisten ihmisten tietoturvaluusustietoisuus ei ole tyydyttävällä tasolla.
- Kansalaisten edellytyksissä vaikuttaa omaan tietoturvaluusuteensa on puutteita.
- Koulutusta ja tiedotusta tietoturvaluusuasioissa tarvitaan lisää.

5.10 Keskeiset toteutuneet tietoturvaluustoimenpiteet sektoreittain

5.10.1 Tietoturvaluustoiminta yhteiskunnassa

Tietoturvaluisuuden kehittämiseen on panostettu ja sitä tukevia hankkeita on käynnistetty jopa koko yhteiskunnan tietoturvaluisuutta edistävällä tasolla. Näistä yksi on tietoturvaluisuusasioiden neuvottelukunnan perustaminen.



Kuva. Tietoturvaluisuuden hallintajärjestelmä yhteiskunnassa. Sisäkehällä on esitetty keskeisiä toteutuneita kansallisia toimenpiteitä.

Tietoturvaan liittyvää tutkimustoimintaa sekä erityiskohderyhmille soveltuvaa tietoturvakoulutusta on yliopistoissa ollut tarjolla koko 1990-luvun ajan. Koulutusta on suunnattu turvallisuusjohdolle, asiantuntijoille ja päättäjille ja sitä on annettu niin ammatti- kuin korkeakoulutasoisena.

Julkiset tutkimus- ja tuotekehitysprojektien rahoittajat ja aktivoijat ovat ryhtyneet tekemään ja edistämään tietoturvatyötä. Useat edunvalvontajärjestöt ovat käynnistäneet tietoturvaluus toimintatapoja ja ammatillista osaamista lisäävää toimintaa.

Viestintäviraston CERT-FI -yksikkö on aloittanut toimintansa. Yksikkö tiedottaa ja ohjeistaa sekä julkishallinnon organisaatioita että erityisesti yrityksiä ja yksityisiä kansalaisia tietoturvaluisuusasioissa. Viranomaisyhteistyö Viestintäviraston ja poliisin kanssa on myös tiivistymässä. Tähän liittyy myös CERT-toimijoiden kansainvälisen yhteistyö.

Tieto- ja telejärjestelmissä siirrettävien tietojen luottamuksellisuus, eheys ja käytettävyys on kyetty pitämään varsin korkeana. Suo messa on myös käynnistetty tietoturvasertifiointia ja sertifiointielinten akkreditointia.²⁵

Yritysten ja julkisen sektorin valmiudet toteuttaa tietoturvallisia palveluja tietoverkoissa ovat lisääntyneet, ja tätä edistää Suomessa tehty PKI-infrastruktuurin pystyttäminen. Suomessa sähköinen tiedonsiirto on saavuttanut merkittävän laajuuden, ja sille on kehitetty tietoturvallisia menettelyitä, jotka kattavat myös Internetissä välitettävän tietoliikenteen.

Internetin aiheuttamia uhkia, muutoksia ja niihin varautumista on selvitetty, ja niistä on annettu ohjeita 90-luvun jälkipuolelta lähtien.

Kansainvälinen toimintaan kuuluu Suomen osallistuminen kansainväliseen standardointi-, tietoturvallisuus- ja muuhun yhteistyöhön, joista tärkeimpiä ovat standardointielimet, Euroopan Unioni ja OECD. Tietoturvan, tietosuojan, sähköisen allekirjoituksen ja varmennepalveluiden standardointiin liittyvää työtä tehdään laajasti ETSI:ssä, EESSI:ssä, ITU:ssa ja niihin läheisesti liittyvissä foorumeissa. Näissä Suomen rooli on ollut varsin aktiivinen.

5.10.2 Julkinen hallinto

Suurin osa julkisesta hallinnosta on jonkinasteisen tietoturvallisuuspolitiikan piirissä. Edistyneimmissä yksiköissä tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden keskeiset osa-alueet tietoturvallisuuden suunnittelusta toteutukseen ja valvotaan. Eräät organisaatiot ovat jo saaneet BS7799-tietoturvallisuussertifikaatin.

Valtioneuvoston periaatepäätös vuodelta 1999 korostaa vaatimusta laajapohjaiselle ja koko henkilöstöön kohdistuvalle tietoturvatyölle, joka etenee eri toimintasektoreilla.

Valtiovarainministeriö vastaa valtionhallinnon tietojärjestelmiä koskevan tietoturvallisuuden ohjauksesta. Valtionhallinnon tietoturvallisuuden johtoryhmä (Vahti) ja valtiovarainministeriö ovat julkaissut tietoturvallisuus suosituksia ja muuta tietoturvallisuusmateriaalia jo 20 vuoden ajan. Materiaalia on ollut saatavissa sähköisesti vuodesta 1997 lähtien. Vuosina 2000-2001 Vahti julkaisi yli 10 nidettä tietoturvallisuusjulkaisuja. Itse julkaisujen lisäksi merkittävää on, että valtionhallinnossa on luotu eri osapuolten erityisosaamista hyödyntävä menettelytapa tietoturvallisuusjulkaisujen toimittamiseksi.

Kuntaliitto on julkaissut kuntien tietoturvallisuutta käsittelevää tietoutta ja koulutusmateriaalia. Kuntaliitto on käynnistänyt tai käynnistämässä lukuisia tutkimus- ja muita projekteja, jotka sivuavat tietoturvallisuutta. Näistä mainittakoon palvelukanavasta riippumaton tietotekniikka sekä tunnistuksen ja allekirjoituksen ratkaisut sähköisessä asiointissa.

Terveystieteidenhuoltoon liittyvää sähköistä toimintaa, tietoturvaa ja tietosuojaa on kehitetty erilaisissa kärkihankkeissa ja -projekteissa. Käyttöön on otettu sähköisiä potilaskortteja, käyttäjien vahvaa tunnistamista sekä tietoliikenteen salausta.

²⁵ SFS on käynnistänyt tietoturvasertifioinnin Suomessa vuonna 2001. Mit tatekniikan keskus (MIKES) puolestaan akkreditoi eli toteaa päteväksi sertifiointielimiä.

Julkisen hallinnon tietoturvatietoisuus on jo varsin hyvä, mutta yleinen ongelma tietoturvallisuuden kehittämisessä on niin henkilö- kuin taloudellisten resurssien puute.

5.10.3 Yritykset

Suurissa ja keskisuurissa yrityksissä on yleensä tietoturvallisuuspolitiikka, mutta tyypillinen ongelma on, ettei yrityksen johto ole täysin ymmärtänyt tietoturvallisuuden merkitystä, vaan pitää sitä liiketoiminnasta erillisenä alueena.

Useat merkittävät yritykset ovat ryhtyneet kehittämään sisäistä ns. crisis management-toimintaansa, jonka yksi osa on häiriötilanteisiin liittyvien tietoturvauhkien hallinta.

Suurissa organisaatioissa tietoturvallisuusvastuu on tyypillisesti tietohallintopäälliköllä tai turvallisuuspäälliköllä. Edistyneissä yrityksissä on erillisiä tietoturvallisuusryhmiä tietoturvallisuuden johtamiseen, hallinointiin ja tietoturvarikkeiden vastatoimiin²⁶. Yritysten tietoturvallisuuden hallinnan suurimpia ongelmia on toimivan tietoturvallisuusprosessin luominen. Tarvittavia teknisiä välineitä on saatavilla, mutta niitä ei aina käytetä, käytetään väärin tai välineitä käyttävä organisaatio ei ole ajan tasalla tehtävistään.

Rahoitussektorilla on riskienhallinnassa pitkät perinteet ja riittävät resurssit. Valtiovalta asettaa rahoitussektorin tietoturvallisuudelle minimitason ja valvoo sen toteutumista. EMV²⁷-määrityksen mukaisten luotto- ja pankkikorttien liikkeeseenlasku myös Suomessa on muodostumassa kansallisesti merkittäväksi rahoitussektorin tietoturvallisuutta edistävaksi toimeksi. Rahoitussektoriin kohdistuvat uhat ovat merkittävät, mutta vastatoimien arvioidaan olevan riittäviä.

Vakiintuneiden telekommunikaatioyritysten tietoturvan taso sisäisen toiminnan osalta on ilmeisen hyvä. Pirstoutuneilla markkinoilla tietoturvan taso kuitenkin vaihtelee eri operaattorien ja palveluntarjoajien verkoissa ja järjestelmissä. Tällöin tietoturvan taso määräytyy tarjoaman alimman tietoturvallisuustason mukaiseksi.

Verkkojen ja verkossa tarjottavien palveluiden käytettävyyden alenemisen vaikutus voi olla suuri operaattorien omalle sekä erityisesti heidän asiakkaittensa liiketoiminnalle. Yritysten ja jopa yhteiskunnan tasolla esimerkiksi sähköpostipalvelujen laajamittaisen lamaantumisen vaikutukset näkyisivät nopeasti: sähköposti on jo monen yrityksen tärkein tietojärjestelmä.

Hallinnoitujen tietoturvapalveluiden markkinoiden arvioidaan kasvavan lähivuosina voimakkaasti ja korvaavan yritysten ja kansalaisten omia ratkaisuja. Suuret Internet-operaattorit ovat aloittaneet tietoturvapalveluiden tarjonnan, johon sisältyy virustorjunta ja hajautettu palomuuripalvelu.

Yritysten laatutyö on johtanut sertifioituihin laatujärjestelmiin, ja sama on tapahtumassa myös tietoturvallisuustyölle. Osa yrityksistä on jo saanut BS7799-tietoturvallisuussertifikaatin. Laatutyö luo hyvän pohjan tietoturvallisuuden

²⁶ ns. CSIRT-toiminta, *Computer Security Incident Response Team*. Tietoturvarikkeiden havainnoinnin jälkeisiin vastatoimiin erikoistunut organisaation sisäinen ryhmä.

²⁷ EMV-standardeilla (EMV= Europay, MasterCard ja Visa) myös Suomessa saavutetaan kansainvälinen muovikorttien yhteentoimivuus muuttamalla magneettiraitakortit toimikortteiksi samalla tietoturvallisuutta lisäten.

kehittämiseksi, joten laatusertifioituissa yrityksissä arvioidaan olevan hyvät organisatoriset valmiudet tietoturvan hallintajärjestelmän kehittämiseen.

5.10.4 Yksityishenkilöt

Yksityisten ihmisten kiinnostus tietoturvasasioihin on alkanut lisääntyä. Tätä ilmentää tietoturvasasioihin liittyvä yleisönosastokirjoittelu, sekä se, että tietoturvasasioita käsitellään myös muissa kuin tietotekniikkaa käsittelevissä julkaisuissa.

Yksityisten ihmisten tietotekniset kyvyt ovat parantuneet ja tämän voidaan olettaa parantavan heidän kykyään oman tietoturvasuutensa hallintaan. Toisaalta uhkien määrä lisääntyy ja niiden hallinta vaatii entistä enemmän tietoa.

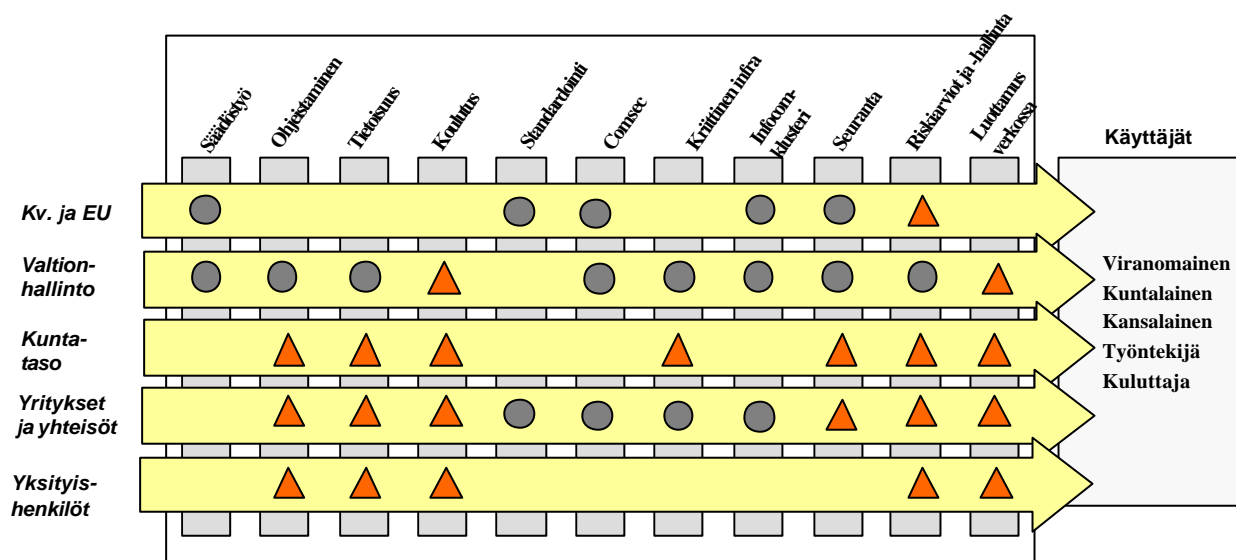
Kuluttajat ovat kritisoineet Internet-operaattoreita siitä, että nämä kykenisivät halutessaan tarjoamaan Internet-yhteyksiin ja näihin liittyviin palveluihin huomattavasti paremman tietoturvasuuden kuin mitä on tarjolla. Operaattoreiden on myös katsottu keskittyneen tuotteiden markkinoinnissa liiaksi niiden ominaisuuksiin ja jättäneen tietoturvasuustiedottamisen vain lain vaatimalle minimitasolle. Virustorjuntaa on vaadittu sähköpostipalvelimiin, jotta haittaohjelmien leviäminen saataisiin pysäytetyksi ennen asiakkaan laitteita. Myös krakkeroinnin estoon tarkoitettuja palomuuriohjelmistoja on esitetty kuuluviksi niihin Internet-yhteyden yleisiin turvallisuusominaisuuksiin, joiden kuluttaja voi olettaa sisältyvän tuotteeseen. On yleisesti esitetty, että kuluttajien vastuulle ei voi säilyttää asiaa, jota heidän ei voida olettaa hallitsevan.

Kokonaisuutena suomalaisessa koulutusjärjestelmässä puuttuu tietoturvasuuskoulutusta. Koulutus on painottunut teknisiin asioihin, eikä kursseja ole riittävässä määrin.

6 YHTEENVETO

Tietoturvaluustoiminta on sektoroitunut, ja sen taso suomalaisessa yhteiskunnassa vaihtelee suuresti. Tietoturva-asiat on hoidettu varsin hyvin operaattorien osalla, rahoitussektorilla, kaupan alalla, suurissa teollisuusyrityksissä sekä valtionhallinnossa. Heikointa on tottumattomien tietotekniikan käyttäjien ja yleisesti yksityishenkilöiden tietoturvatietämys. Pienten ja keskisuuren yritysten tilanteen arvioidaan olevan jonkin verran yksityishenkilöiden tilannetta parempi. Kuntasektorilla tilanne vaihtelee kunnittain ja lisäpanostuksia arvioidaan tarvittavan. Kansallisen tietoturvaluisuuden parantaminen edellyttää sekä kotimaista että kansainvälistä yhteistyötä ja koordinoitua.

Tietoturvaluisuuden kansallisen tilan luotettava vertaaminen muihin maihin on äärimmäisen vaikeaa. Vertailukelpoista aineistoa ei juuri ole saatavilla tai aineisto kohdistuu tietoturvaluisuuden yksittäisiin osa-alueisiin. Kattavinta on OECD:n tekemä kansainvälinen kartoitustyö.



Kuva. Työryhmätyössä tunnistettuja vahvoja aktiviteetteja (pallot) ja tarpeita tietoturvaluustyölle (kolmiot)²⁸.

Tämän katsauksen perusteella on tunnistettu seuraavia asiakokonaisuuksia. Niitä ei ole esitetty tärkeysjärjestyksessä:

1. Yhteiskunnan tietoturvaluisuus

- Kriittisen infrastruktuurin ylläpitoon osallistuvien keskinäisen yhteistyön edistäminen. Tämä voi tapahtua esimerkiksi perustamalla työryhmä, joka koostuu perusinfrastruktuurin ylläpitämisestä vastaavien organisaatioiden turvallisuudesta vastaavista henkilöistä.

²⁸ INFOCOM = telekommunikaatio ja tietotekniikkatoimiala

- Tehdään säännöllinen seurantatutkimus tietoturvallisuuden toteutumisesta. Tutkimus olisi tehtävä mahdollisimman vertailukelpoiseksi eri maissa tehtävien vastaavien tutkimusten kanssa.
- Tietoturvallisuusasioiden neuvottelukunnan roolin kehittäminen pitkäjänteinen, laaja-alaisen ja kokonaisvaltaisen tietoturvyhteistyön tekijänä.
- Organisaatioiden tietoturvallisen toiminnan ja käyttäjien kannalta keskeisten toimintojen, palveluiden ja tuotteiden sertifiointi ja standardointi, mikä lisää tietoyhteiskunnan tietoturvaa, laatua ja palveluiden saatavuutta. Lisäksi tarvitaan nykyistä tarkempaa standardien huomioonottamista erityisesti kansainvälisissä toiminnoissa.
- Julkisen sektorin pitäytyminen kilpailemasta yksityisten yritysten kanssa, mikäli markkinoilla on kaupallista tarjontaa, tai sitä voidaan olettaa syntyvän.
- Koulutus- ja tutkimustoimintaan panostaminen.
- Tietoturvallisuuden kannalta merkittävien uusien osa-alueiden tutkiminen (esim. IP-automaatio).
- Sertifiointimarkkinoiden toiminnan edistäminen.

Tausta-aineistoa:

- Saarenpää et al: Tietoturvaluus ja laki - Näkökohtia tietoturvaluuden oikeudellisesta sääntelystä, Valtiovarainministeriö ja Lapin yliopisto, Helsinki 1997
- Internet, toiminnan verkottuminen ja sen haavoittuvuus, Puolustustaloudellinen suunnittelukunta (PTS), Tietojärjestelmäjaosto, 2001
- Tietojenkäsittelyn turvaaminen tietoyhteiskunnassa, Puolustustaloudellinen suunnittelukunta (PTS), Tietojärjestelmäjaosto, 1996
- Elämänlaatu, osaaminen ja kilpailukyky: Tietoyhteiskunnan kehittämisen perustelut, Rainio, A, Kautto-Koivula, K. (toim.), Helsinki, Sitra, 1998
- Building an E-Commerce Trust Infrastructure, Verisign, 3/2002
- PK-yritykset Internetin hyödyntäjinä. LVM ja Otso Consulting, 2000
- Green Paper on Consumer Protection, Komissio 2001
- OECD:n tietoturvatyö, kts: <http://www.OECD.org>
- eEurope 2002, eEurope Benchmarking Report
- Puolustustaloudellinen suunnittelukunta: Tietojärjestelmien tietoturvaluuden hallinnolliset järjestelyt, TIHA-työryhmä, 15.5.2000
- Tietoturvaluuden hallinnointi 2 –työryhmän loppuraportti (TIHA 2)
- Hallinnon sähköisen asioinnin jaoston ehdotus julkisen hallinnon sähköisen asioinnin toimintaohjelmaksi 2002-2003 "Kohti hallittua murrosta - julkiset palvelut uudella vuosituhanalla"
- Tietoturvaa peruskäyttäjälle, Tiekien julkaisusarja, osa 6
- OECD:n neuvoston tietoturvaluussuositus, tietoturvaluusperiaatteet ja perustelu muistio, 26.11.1992. Valtio varainministeriö 5/93
- Komission tiedonanto Neuvostolle, Euroopan Parlamentille, Talous- ja Sosiaalikomitealle ja Alueiden komitealle; Verkko- ja tietoturva: Ehdotus Eurooppalaiseksi lähestymistavaksi, 2001
- VAHTI:n julkaisut, kts: <http://www.vm.fi/vahti>
 - Tietoteknisten laitetojen turvaluussuositus, Vahti 1/2002
 - Valtion tietotekniikkahankintojen tietoturvaluuden tarkistuslista, Vahti 6/2001
 - Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje, Vahti 5/2001
 - Sähköisten palveluiden ja asioinnin tietoturvaluuden yleisohje, Vahti 4/2001
 - Salauksikäytäntöjä koskeva valtionhallinnon tietoturvaluussuositus, Vahti 3/2001
 - Valtionhallinnon lähiverkkojen tietoturvaluussuositus, Vahti 2/2001
 - Valtion viranomaisen tietoturvaluusustyön yleisohje, Vahti 1/2001
 - Tietokoneviruksilta ja muilta haittaohjelmilta suojautumisen yleisohje, Vahti 4/2000
 - Valtionhallinnon tietojärjestelmäkehityksen tietoturvaluussuositus, Vahti 3/2000
 - Valtionhallinnon tietoaineistojen käsittelyn tietoturvaluusohje, Vahti 2/2000
 - Valtionhallinnon tietoturvaluuskäsitteistö, Vahti 1/2000
 - Tarpeettomaksi tulleiden tietoaineistojen hävittäminen, VM 21/01/2000, 18.4.2000
 - Valtion tietohallintotoimintojen ulkoistamisen tietoturvaluussuositus, Vahti 2/1999