OPPIMATERIAALEJA
PUHEENVUOROJA
RAPORTTEJA 167
TUTKIMUKSIA

Jarkko Paavola & Esko Vainikka (toim.)

NÄKÖKULMIA TIETOTURVAAN

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPPIMATERIAALEJA
PUHEENVUOROJA
RAPORTTEJA 167
TUTKIMUKSIA

Jarkko Paavola & Esko Vainikka (toim.)

NÄKÖKULMIA TIETOTURVAAN

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

TURUN AMMATTIKORKEAKOULUN
RAPORTTEJA 167

Turun ammattikorkeakoulu
Turku 2013

ISBN 978-952-216-398-1 (painettu)
ISSN 1457-7925 (painettu)
Painopaikka: Suomen yliopistopaino – Juvenes Print Oy, Tampere 2013
Myynti: http://loki.turkuamk.fi

ISBN 978-952-216-399-8 (pdf)
ISSN 1459-7764 (elektroninen)
Jakelu: http://loki.turkuamk.fi

441 729
Painotuote

SISÄLTÖ

ESIPUHE

Tervetuloa Turun ammattikorkeakoulun ensimmäisen tietoturvajulkaisun pariin! Tarjolla on tietoa tietoturvallisuudesta erilaisissa ympäristöissä sekä Turun ammattikorkeakoulun tarjoamista tietoturvapalveluista.

Tietoturvan merkitys kasvaa vauhdilla sitä mukaan kun yhteiskunta tulee yhä riippuvaisemmaksi ICT-palvelujen toimivuudesta. Suomessa on herätty tähän kehitykseen ja esimerkiksi Valtioneuvoston tammikuussa 2013 julkaisemassa Suomen kyberturvallisuusstrategiassa yksi keskeinen toimenpide on, että ”parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.” Myös yritysten tulee huomioida tietoturvallisuus liiketoiminnassaan. Tietoturvauhkia analysoivat organisaatiot kertovat kohdistettujen tietoturvahyökkäysten painopisteen olevan siirtymässä pieniin ja keskisuuriin yrityksiin niiden heikomman suojaustason vuoksi.

Turun ammattikorkeakoulun tutkimus-, kehitys-, ja innovaatiotoiminta (TKI) fokusoituu tutkimusryhmien ympärille. Tämän julkaisun artikkeleista valtaosa on Tietoturva ja tietosuoja -tutkimusryhmän jäsenten kirjoittamia. Tutkimusryhmämme tavoitteena on yleisen tietoturvatietoisuuden lisääminen. Erityisesti keskitymme PK-sektorin yritysten liiketoimintaedellytysten parantamiseen ICT:n avulla. Tämän lisäksi osallistumme kansallisiin ja kansainvälisiin tutkimushankkeisiin.

Tarkoituksenamme on tulevaisuudessa tarjoilla Tietoturvajulkaisu vuosittain. Se esittelee ajankohtaisia asioita tietoturvan alalta, opiskelijoiden opinnäytteissään saamia tuloksia sekä tietenkin tutkimusryhmämme saavutuksia.

Turussa 14.6.2013

Jarkko Paavola, TkT

Esko Vainikka, FL, CISSP

YRITYKSEN TIETOTURVAN PERUSTEET – LYHYT OPPIMÄÄRÄ

Matti Laakso, tradenomi
IT-suunnittelija, Turun ammattikorkeakoulu

Sana tietoturva herättää nykyään erilaisia tuntemuksia yrityksissä sekä niiden työntekijöissä. Toiset tietävät mitä sillä tarkoitetaan, toiset luulevat tietävänsä. Osaa yrityksistä koko asia ei kiinnosta laisinkaan. Todennäköisesti Suomessa on edelleen sellaisiakin yrityksiä joita tietoturva-asiat kiinnostavat, mutta asiakokonaisuus tuntuu liian monimutkaiselta.

Tähän artikkeliin on koottuna tiiviisti yleisimpiä yrityksen tietoturvan perusteisiin liittyviä käsitteitä, toimintaohjeita ja vinkkejä, joiden avulla PK-yrittäjän on helppo lähteä kehittämään oman yrityksensä tietoturvaa. Liiketoiminnan muodosta ja laajuudesta huolimatta perusteet kannattaa aina kerrata, oli kyseessä sitten IT-alalla tai urheiluvälinekauppiaana toimiva yrittäjä.

MITÄ EROA ON TIETOTURVALLA, TIETOTURVALLISUUDELLA JA TIETOSUOJALLA?

Nämä kolme termiä, tietoturva, tietoturvallisuus ja tietosuoja tarkoittavat kaikki eri asioita, mutta arkikielessä ne menevät helposti sekaisin ja niitä käytetään rinnakkain toistensa kanssa. Kun näistä aiheista puhutaan, tulisi osapuolten aina ensin selvittää toisilleen, mistä oikeasti ollaan puhumassa.

Tietoturva

Tietoturva on moniulotteinen asia ja eri tahot käsittävät sen eri tavoin. Esimerkiksi IT-asiantuntijat saattavat puhua aiheesta teknisestä näkökulmasta kun taas organisaation tietoturvavastaavan näkemys saattaa olla enemmän hallinnollinen.

Kirjallisuudessa ja sähköisissä lähteissä termillä *tietoturva* tarkoitetaan kuitenkin tiedon ominaisuuksia. Esimerkiksi Viestintävirasto määrittelee nämä tiedon ominaisuudet seuraavasti:

- Luottamuksellisuus – tietoihin on pääsy vain niillä, jotka ovat siihen oikeutettuja eikä tieto ole paljastunut muille.
- Eheys – tiedon sisältö ei ole muuttunut esimerkiksi ihmisen tai IT-järjestelmän toiminnan takia.
- Käytettävyys – tiedot ja järjestelmät ovat hyödynnettävissä tarvittaessa. (Viestintävirasto 2012.)

Miten tiedon ominaisuudet sitten liittyvät esimerkiksi urheiluvälineyrittäjän arkeen? Luottamuksellisuus on olennaista sopimusten ja muiden tärkeiden asiakirjojen osalta. Eheys on tärkeää esimerkiksi kirjanpidossa ja tietojärjestelmissä: jos varastojärjestelmä väittää, että tiettyjä urheiluvälineitä on saatavilla tietyssä hyllyssä, mutta oikeasti niitä ei ole, niin kaupat jää tekemättä ja yrittäjä menettää asiakkaan. Mikäli koko varastojärjestelmä ei ole esimerkiksi viasta johtuen saatavilla (käytettävyys), niin yrittäjä ei edes näe varastotietoja ja liiketoiminta kärsii jälleen.

Tietoturvallisuus

Termiä tietoturvallisuus käytetään joskus rinnakkain tietoturvan kanssa, mutta pitää huomioida että nämä ovat eri asioita. Tietoturva keskittyy tiedon ominaisuuksiin, kun taas esimerkiksi Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) määrittelee tietoturvallisuuden seuraavasti:

> *Tietoturvallisuus – järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus (VAHTI 2008).*

Tietoturvallisuus on iso kokonaisuus. Sen hallitsemiseksi aihetta lähestytään yleensä pienempien osa-alueiden kautta. Karkeasti jaoteltuna osa-alueet ovat seuraavat: hallinnollinen, tekninen ja henkilöstö. Usein nähdään myös yksityiskohtaisempia jaotteluita, esimerkiksi Viestintävirasto käyttää kahdeksan kohdan jaottelua: hallinnollinen tietoturva, fyysinen turvallisuus, henkilö-, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus. (Viestintävirasto 2012.)

Tietosuoja

Tietoturvallisuuden ja tietoturvan lisäksi puhutaan usein myös tietosuojasta. Se on kuitenkin kahteen edelliseen verrattuna täysin oma kokonaisuutensa. VAHTI määrittelee tietosuojan seuraavasti:

> *Tietosuoja – ihmisen yksityisyyden suoja ja muut sitä turvaavat oikeudet, henkilötietoja käsiteltäessä (VAHTI 2008).*

Tietosuoja keskittyy siis henkilöiden yksityisyyden suojaan, kun taas tietoturvallisuus sisältää paljon muutakin. Tietosuoja-asiat perustuvat vahvasti lakiin, joten esimerkiksi henkilötietolain (1999/523) sekä sähköisen viestinnän tietosuojalain (2004/516) tunteminen on olennaista.

Tietosuojalait ovat muutenkin ajankohtaisia, sillä EU:n toimielin Euroopan komissio on ehdottanut kattavaa uudistusta tietosuojalainsäädäntöön. Uudistuksen tarkoituksena on esimerkiksi vahvistaa kansalaisten oikeuksia internetissä sekä luoda yhteisiä toimintamalleja EU:n alueelle. Tutkimuksen mukaan noin 70 prosenttia eurooppalaisista on huolestuneita siitä, miten yritykset käsittelevät kansalaisten tietoja internetissä. Lakimuutoksille on siis selkeä tarve. (European Commission 2012a, 2012b.)

TIETOTURVALLISUUS OSANA LIIKETOIMINTAA

Jokaisella yrityksellä on liiketoiminnan kannalta olennaisia tietoja, jotka eivät saa paljastua ulkopuolisille. Niitä ovat esimerkiksi erilaiset liikeideat, tuotesuunnitelmat, sopimukset ja asiakastiedot. Tietoturvallisten toimintatapojen avulla näiden tietojen paljastumisriskiä voidaan vähentää.

Onko yrityksessä maksupäätteitä? Niiden käyttö edellyttää myös tiettyjen tietoturvavaatimusten täyttämistä (Luottokunta 2012). Hyvin nopeasti huomaa, että tietoturvallisuus on osa liiketoimintaa, vaikka sitä ei ihan ensimmäiseksi näin ajattelisikaan.

Tietoturvallisuutta ei myöskään tule ajatella erillisenä asiana, jonka avulla kriittisten tietojen luottamuksellisuus, eheys ja saatavuus varmistetaan. Oli yrityksen liiketoiminta sitten tuotteiden valmistusta tai palveluiden tuottamista, tulee tietoturvallisuus huomioida osana liiketoimintaprosessia alusta loppuun asti.

Käyttääkö yritys liiketoiminnassa alihankkijoita tai ulkoistaako se jotain toimintoja? Tietoturvallisuus tulee huomioida myös näissä tapauksissa. Jonain päivänä mahdollinen asiakas voi kysyä, miten yrityksen tuottaman palvelun tietoturva on hoidettu alihankkijoiden osalta. Tässä kohtaa valveutunut yrittäjä voi todeta esimerkiksi, että tietoturvallisuudesta on sovittu sopimuksissa. Todennäköisemmin asiakas ostaa palvelun sellaiselta yritykseltä, joka huolehtii tietoturvasta.

Tietoturvallisten toimintatapojen käyttöönotto ei ole yhdessä yössä hoidettu asia. Tietoturvakulttuurin luominen vaatii tahtoa, aikaa ja resursseja. Kaikki tietoturvallisuuden parantamiseksi tehdyt toimenpiteet eivät välttämättä ole ilmaisia, mutta pienilläkin investoinneilla voidaan ehkäistä suuria ongelmia tulevaisuudessa. Yrittäjän ei kuitenkaan pitäisi nähdä tietoturvallisuutta ylimääräisenä kustannuksena, vaan osana liiketoimintaa ja toiminnan laatua.

YRITYKSEN TIETOTURVALLISUUDEN PARANTAMINEN

Moni yritys varmasti pohtii onko tietoturvaa syytä lähteä parantamaan. Onhan maalaisjärjellä pärjätty tähänkin asti, joten miksi lähteä muuttamaan hyviä toimivia käytäntöjä?

Tutkimusten mukaan tietoturvallisuuden parantaminen on todella ajankohtaista erityisesti verkkopalveluiden osalta. Tietosuojavaltuutetun toimisto toteutti kesällä 2012 kymmeniin yrityksiin ja yhteisöihin tarkastuksen, jonka perusteella havaittiin, että henkilötietojen käsittelyyn ja suojaamiseen tulisi kiinnittää enemmän huomiota. Esimerkiksi tarkastuksen kohteista alle puolet tunsivat henkilötietolain vaatimukset tarpeeksi kattavasti. (Tietosuojavaltuutetun toimisto 2012.)

Toinen tutkimus osoittaa, että verkkohyökkäysten määrä on yli kaksinkertaistunut viimeisen kolmen vuoden aikana ja niiden taloudelliset kustannukset ovat kasvaneet melkein 40 prosenttia. (HP Newsroom 2012.) Ei ole mitään syytä olettaa, että nämä luvut lähtisivät laskemaan rajusti lähitulevaisuudessa.

Miten yritysten tulisi aloittaa tietoturvallisuuden parantaminen? Koko prosessin tarkoituksenahan on varmistaa liiketoiminnan jatkuvuus, parantaa sen laatua ja minimoida sitä uhkaavia riskejä. Näin ollen tietoturvallisuuden kehittäminen voidaan aloittaa riskienhallinnasta tutuilla keinoilla esimerkiksi nykytilanteen kartoituksella ja riskianalyysillä. (PK-RH 2012.)

Tilanteen kartoittaminen

Ensimmäiseksi selvitetään mitkä ovat ne tiedot, joiden luottamuksellisuus, eheys ja käytettävyys on varmistettava. Kannattaa aloittaa niistä tiedoista, jotka ovat lain mukaan suojattavia. Yrittäjän on tunnettava liiketoimintaa ohjaava lainsäädäntö. Esimerkiksi henkilötietojen käsittelystä on säädetty henkilötietolaissa (523/1999).

Seuraavaksi kartoitetaan niitä tietoja, joita ei missään tapauksessa haluta ulkopuolisten tietouteen. Näitä ovat esimerkiksi liikesalaisuudet ja -suunnitelmat. Kaikki tiedot kannattaa dokumentoida sekä luokitella niiden liiketoimintakriittisyyden mukaan, jotta asioihin voi palata myöhemmin riskianalyysin yhteydessä.

Internetissä on tarjolla lukuisia tietoturvallisuuden lähtötason kartoitukseen tarkoitettuja työkaluja. Niitä kannattaa käyttää, koska ne auttavat mahdollisten liiketoimintaa uhkaavien riskitekijöiden löytämisessä. Kartoitustyökaluja löytyy esimerkiksi osoitteista tietoturvaopas.fi sekä tietoturvapaiva.fi (Tietoturvaopas.fi 2012a; Tietoturvapaiva.fi 2012).

Riskianalyysin kautta tietoturvallisuuden kehittämiseen

Kun yrityksessä on toteutettu lähtötason kartoittaminen sekä liiketoiminnalle kriittisten tietojen luokittelu, kannattaa seuraavaksi toteuttaa riskianalyysi. Sen tarkoituksena on löytää ja analysoida tietoturvallisuutta sekä liiketoimintaa uhkaavia riskejä. (PK-RH 2012.)

Riskejä voi tarkistella esimerkiksi liiketoimintaprosessien näkökulmasta tai kolmen tietoturvallisuuden osa-alueen kautta: tekniset, hallinnolliset ja henkilöstöstä johtuvat riskit.

Kriittisimmiksi luokiteltuja tietoja ja järjestelmiä uhkaavat riskit kannattaa minimoida ensimmäisenä.

Jatkuvan parantamisen periaate

Vaikka tietoturvallisuutta voidaan kehittää asteittain esimerkiksi projektien avulla, tulee yrityksen kuitenkin muistaa, että tietoturvallisuus itsessään ei ole kertaluontoinen projekti, joka päättyy jossain vaiheessa. Sen sijaan tietoturvallisuutta tulee arvioida ja tarvittaessa kehittää jatkuvasti, kuten muutakin liiketoimintaa.

Yleisesti käytetty PDCA-malli on eräs keino tietoturvallisuuden parantamiseksi. Sen mukaisesti ensimmäiseksi suunnitellaan (Plan) jotakin tietoturvan kehittämiskohdetta. Tämän jälkeen toteutetaan (Do) suunnitelma ja tarkistetaan sen toteutumista (Check). Lopuksi toteutetaan mahdolliset korjaavat toimenpiteet (Act) ja aloitetaan suunnitteluvaihe alusta jonkin toisen kehittämiskohteen osalta.

YLEISIÄ TIETOTURVAHAASTEITA

Tietoturvallisuuden monipuolisuus asettaa sille erilaisia haasteita eri organisaatioissa. Siinä missä toiset pohtivat kehittyneiden teknisten turvallisuusratkaisujen käyttöönottoa saattavat toiset vasta miettiä mitä tietoturva oikeastaan on. Tässä luvussa on kuvattuna neljä yleistä tietoturvahaastetta, joita yritys saattaa kohdata huolimatta siitä, millä toimialalla se on.

”Tietoturva ei koske meitä”

Pienet ja keskisuuret yritykset saattavat todeta, että tekniset tietoturvahyökkäykset eivät kosketa heitä, vaan se on isompien yritysten ongelma. Tämä on kuitenkin täysin väärä lähtökohta. Itse asiassa suuret yritykset parantavat tietoturvallisuuttaan tällä hetkellä siinä määrin, että rikollisten toimijoiden päivittäinen työ hankaloituu. Rikollisten sanotaankin mukautuvan tilanteeseen siirtämällä verkkohyökkäyksiään pieniä toimijoita vastaan. (SANS 2012.)

Kaikilla yrityksillä ei tietysti ole tällaista ongelmaa, koska ne eivät välttämättä käytä tietotekniikkaa. Yleisen sanonnan mukaan tietoturvasta on kuitenkin vain 20 prosenttia tekniikkaa ja loput 80 prosenttia ovat hallinnollisia asioita. Tämä kannattaa muistaa seuraavalla kerralla, kun joku puhuu tietoturvasta pelkkänä teknisenä asiana.

Henkilöstön tietoturva-asenteet

Yksi iso osa yrityksen tietoturvallisuutta ovat työntekijät. Heidän asenteillaan ja toimintatavoillaan on suuri rooli koko yrityksen tietoturvallisuudessa. Varsinkin yksityishenkilöiltä kuulee usein lauseen ”minulla ei ole mitään salattavaa” kun heidän kanssaan puhuu tietoturvasta. Tämän ei pitäisi olla yrityksen

ongelma, mutta jos kyseinen asenne kulkeutuu mukana työpaikalle, niin siitä voi tulla isokin ongelma. Yrityksen pitää varmistua siitä, että työntekijät tietävät vastuunsa ja velvollisuutensa myös tietoturvallisuuden näkökulmasta.

Yritysjohdon tuen puute tietoturvatyölle

Tietoturvaopas.fi -sivusto kiteyttää yritysjohdon tuen merkityksen tietoturvatyölle yhdessä lauseessa: ”Johto on suunnan näyttäjä” (Tietoturvaopas.fi 2012b). Mikäli yrityksen johto ei ole kiinnostunut tietoturvallisuudesta eikä näytä mallia päivittäisissä toimissaan, on tietoturvakulttuurin levittäminen hankalaa. Tämä ei tarkoita sitä, että yritysjohdon tulisi olla tietoturva-alan ammattilaisia vaan riittää, että johto toimii yhteisten tietoturvallisten toimintatapojen mukaisesti ja osallistuu tietoturvariskien hallintaan. Tarvittavien resurssien osoittaminen tietoturvasta vastaaville henkilöille on myös olennainen osa yritysjohdon osallistumista.

Johdon sitoutuminen ilmaistaan usein kirjallisesti dokumentissa nimeltä tietoturvapolitiikka. Se on yrityksen julkinen asiakirja, jossa otetaan kantaa yleisellä tasolla yrityksen tietoturvallisuuteen ja tietoriskien hallintaan. Tietoturvapolitiikkaa kirjoitetaan sellaiseen muotoon, että se voidaan esittää esimerkiksi tarjousten yhteydessä tai yrityksen verkkosivuilla.

Tietoturva huomioidaan liian myöhään

Asiantuntijaorganisaatio KPMG toteaa Tietoturvaraportti 2012 -julkaisussaan, että tietoturva ajatellaan valitettavan usein irrallisena asiana, joka voidaan myöhemmin liimata palveluihin ja järjestelmiin. Valitettavasti tämä on väärä lähestymistapa, joka ei toimi nykymaailmassa. (KPMG 2012.)

Käytännön esimerkkinä tästä on varmuuskopiointi. Niiden ottaminen on suunniteltava ja toteutettava etukäteen, jälkeenpäin se on myöhäistä. Jos urheiluvälineyrittäjän varastotietojärjestelmä hajoaa ja varmuuskopiointia ei ole huomioitu jo järjestelmän hankintavaiheessa, niin liiketoiminta taatusti häiriintyy. Jälkeenpäin toteutettava tietoturvaratkaisu maksaa tietysti erikseen, mutta jos se olisi huomioitu jo aikaisemmin, niin kustannukset ja muut tietoon liittyvät menetykset olisivat voineet olla olennaisesti pienemmät.

Toinen esimerkki on verkkokauppa. Yrittäjä X myy tuotteitaan pelkästään internetin välityksellä. Eräänä päivänä tapahtuu vesivahinko, jossa verkkokaupan tietotekniset laitteet vahingoittuvat. Jos tietoturvaa ja toiminnan jatkuvuutta ei ole suunniteltu etukäteen, pysähtyy liiketoiminta kunnes verkkosivut on saatu palautettua toimintaan. Yrittäjä haluaa tietysti parantaa laitetilojen turvallisuutta tekemällä tiloihin fyysisiä muutoksia. Kaikki maksaa erikseen ja huomattavasti enemmän, kuin jos ne olisi huomioitu rakennusvaiheessa.

TIETOTURVALLISUUS ALKAA ASENTEESTA

Työskentely paremman tietoturvan sekä tietoturvakulttuurin aikaansaamiseksi kannattaa aloittaa heti. Yritykselle on suositeltavaa toteuttaa selkeä etenemissuunnitelma vaikkapa vuodeksi eteenpäin. Kaikki prosessin aikana tuotettu materiaali kannattaa dokumentoida. Jonain päivänä asiakkaat vaativat todisteita tietoturvallisuuden hallinnasta ja yrittäjä voi hyvillä mielin todeta niiden olemassaolon.

Vuosi saattaa kuulostaa pitkältä ajalta, mutta tietoturvakulttuuria ei luoda hetkessä. Sen tulee varmasti moni yrittäjä huomaamaan. Tulevaisuudessa on todennäköisesti edessä monia hallinnollisia ja teknisiä tietoturvahaasteita, hieman toimialasta riippuen. Tämä ei ole ongelma, sillä tietoturvasta on kirjoitettu monia hyviä kirjoja ja internet on täynnä aiheeseen liittyviä sivustoja. Ei pidä myöskään epäröidä pyytää apua, ohjausta tai koulutusta alan toimijoilta.

Yrityksen tietoturvakulttuuria rakennettaessa tulee pitää mielessä muutama asia. Ensimmäiseksi on ymmärrettävä se, että tietoturvallisuus on yrityksen elinehto. On vain ajan kysymys koska liiketoiminnalle aiheutuu haittaa, jos ei huolehdi tietoturvasta. Toinen olennainen asia on aiheen elinkaari: tietoturvatyö ei lopu koskaan, mutta kaikki alkaa oikeasta asenteesta.

LÄHTEET

European Commission 2012a. Viitattu 28.11.2012 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

European Commission 2012b. Viitattu 28.11.2012 http://europa.eu/rapid/press-release_IP-11-742_en.htm?locale=en

HP Newsroom 2012. HP Research: Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles. Viitattu 28.11.2012 http://www.hp.com/hpinfo/newsroom/press/2012/121008a.html

KPMG 2012. Tietoturvaraportti 2012. Viitattu 26.11.2012 http://www.kpmg.com/FI/fi/Ajankohtaista/Uutisia-ja-julkaisuja/Neuvontapalvelut/Documents/KPMG-Tietoturvaraportti-2012.pdf

Luottokunta 2012. Korttimaksamisen turvallisuus. Viitattu 28.11.2012 http://www.luottokunta.fi/Kaupoille/Korttimaksamisen_turvallisuus/

PK-RH 2012. Pk-yrityksen riskienhallinta. Viitattu26.11.2012 http://www.pk-rh.com/tyovalineet/haavoittuvuusanalyysi-1/haavoittuvuusanalyysi-avuksi-riskienhallintaan.html

SANS 2012. Small Business: The New Target What can they Do? SANS Reading Room 2012. Viitattu 26.11.2012 http://www.sans.org/reading_room/whitepapers/hsoffice/small-business-target-do_33974

Tietosuojavaltuutetun toimisto 2012. Lehdistötiedote: Tietosuojavaltuutettu vaatii yrityksiä panostamaan tietoturvaan. Viitattu 28.11.2012 http://www.tietosuoja.fi/59848.htm

Tietoturvaopas.fi 2012a. Tilanteen kartoitus – riskianalyysi. Viitattu 26.11.2012 http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/tilanteen_kartoitus.html

Tietoturvaopas.fi 2012b. Suunnittelu – johto on suunnan näyttäjä. Viitattu 26.11.2012 http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/johto_on_suunnan_nayttaja.html

Tietoturvapäivä.fi 2012. Viitattu 27.11.2012 http://www.tietoturvapaiva.fi/

VAHTI 2008. Valtionhallinnon tietoturvasanasto. VAHTI 8/2008. Viitattu 26.11.2012 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/name.jsp

Viestintävirasto 2012. Tietoturva ja -suoja. Viitattu 26.11.2012 http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html

PK-YRITYSTEN ULKOISTAMIEN PALVELUJEN TIETOTURVA

Esko Vainikka, FL, CISSP
Yliopettaja, Tietojenkäsittelyn koulutusohjelma, Turun ammattikorkeakoulu

TIETOTURVA-UHAT

Nykyaikainen yritystoiminta perustuu yhä enemmän tietoon. Tieto on yrityksen keskeistä pääomaa ja usein tärkein kilpailutekijä, joten sen suojaamiseen on kiinnitettävä erityistä huolta. Yrityksillä on usein myös lakisääteisiä velvoitteita tietojen suojaamiseen, kuten on laita esim. henkilötietojen osalta. Erityisesti on huomioitava, että yrityksille tärkeä tieto kiinnostaa hyvin usein myös muita tahoja ansaitsemistarkoituksessa.

Tietosuojavaltuutetun toimisto teki kesällä 2012 tarkastuksen 74 suomalaiseen yritykseen ja organisaatioon, joihin oli kohdistunut tietoturvaloukkaus tai sen uhka ajanjaksolla loka-joulukuu 2011 (Tietosuoja 2012). Syynä tähän tarkastukseen oli vuoden 2011 aikana suomalaisiin organisaatioihin kohdistuneet lukuisat tietomurrot, joiden yhteydessä tunkeutujien saaliiksi päätyi myös huomattavia määriä henkilötietoja. Tarkastuksessa kävi ilmi, että vain 46 % tarkastuksen kohteena olleista organisaatioista tunsi henkilötietolain vaatimukset rekisterinpitäjälle. Erityisen huolestuttavaa on se, että suuressa osassa organisaatioita (30 %) tietoturvaloukkaus tai -uhka ei ollut johtanut minkäänlaisiin toimenpiteisiin. Tarkastuksessa kävi myös ilmi, että organisaatioilla oli ongelmia tunnistaa omaa rooliaan henkilötietojen käsittelyn ulkoistamistilanteissa. Lisäksi tarkastus paljasti, että useat pienet yritykset tai organisaatiot olivat päätyneet lopettamaan tietoturvaloukkauksen kohteeksi joutuneet verkkopalvelunsa kokonaan. (Tietosuoja 2012.)

Oikeuspoliittinen tutkimuslaitos toteutti vuonna 2010 kansallisen yritysuhritutkimuksen suomalaisiin kaupan ja teollisuuden alan yrityksiin. Tutkimuksen otos muodostui 1500 kaupan ja 1500 teollisuuden toimipaikasta. Vastauksia tutkimuksessa saatiin 1197 kaupan ja 1230 teollisuuden toimipaikasta. (Salmi ym. 2011, 7.) Tästä tutkimuksesta kävi ilmi, että tietojärjestelmiin kohdistunut hyökkäys oli teollisuustoimipaikoissa yleisimmin koh-

dattu rikollinen teko. Kaupan alalla muut rikolliset teot ovat yleisempiä, mutta tälläkin alalla esiintyi tietojärjestelmiin kohdistuneita hyökkäyksiä. (Salmi ym. 2011, 13–20.)

Keskusrikospoliisin mukaan yritysten tietopääoman kaappaamiseen tähtäävien havaittujen hyökkäysten määrä kasvaa edelleen (Keskusrikospoliisi 2011, 11). Tämän tilannekuvan mukaan kohdistettujen tietoturvahyökkäysten toteuttaminen on rikollisille taloudellisesti kannattavaa, sillä kiinnijäämisriski ja hyökkäysten toteuttamiskustannukset ovat pienet. Yritys tai organisaatio ei voi todellisuudessa suojautua erilaisilta tietojen kaappauksilta, ellei se ymmärrä sekä omaa tietopääomaansa että siihen kohdistuvien tietoturvauhkien ilmenemismuotoja. Erityisesti, jos yrityksen tietojenkäsittely-ympäristö on ulkoistettu, on tietoturvallisuuteen kiinnitettävä erityistä huomiota, muun muassa erilaisin sopimuksin. (Keskusrikospoliisi 2011, 12.) Syksyn 2011 tilannekuva korostaa yritysten puutteellista tietojenkäsittely-ympäristöjen hallintaa, joka mahdollistaa tietoon kohdistuvien rikosten tekemisen. Jos yritys suojaa nykyisen tietoturvamallin mukaisesti tietonsa vain ulkomaailmalta, sisäverkkoon päässyt hyökkääjä pystyy varsin vapaasti keräämään kaiken haluamansa tiedon. (Keskusrikospoliisi 2011, 12.)

Erityisesti sähköisessä muodossa olevan tiedon fyysiseen suojaamiseen, tiedon syöttämisen suojaamiseen, laitteiden ja tiedon käsittelyoikeuksiin sekä tietojenkäsittely-ympäristön erilaisten haavoittuvuuksien toteamiseen ja nopeaan korjaamiseen on syytä kiinnittää erityisesti huomiota (Keskusrikospoliisi 2011, 13). Hyvän käsityksen globaalissa internetissä esiintyvistä tietoturvauhista saa muun muassa Symantec Corporationin raportista Internet Security Threat Report, 2012 Trends (Symantec 2013).

Tietoturvan laiminlyöminen voi pahimmillaan johtaa koko liiketoiminnan loppumiseen. Tästä hyvänä esimerkkinä on alankomaalaisen varmenneyhtiön DigiNotarin ajautuminen konkurssiin syyskuussa 2011 (VASCO Data Security International, Inc. 2011). Nykyään luottamus perustuu yhä enemmän yrityksen maineeseen, ja hyvin hoidettu tietoturva on osa yrityksen maineenhallintaa.

TIETOTURVAN PERUSPERIAATTEET

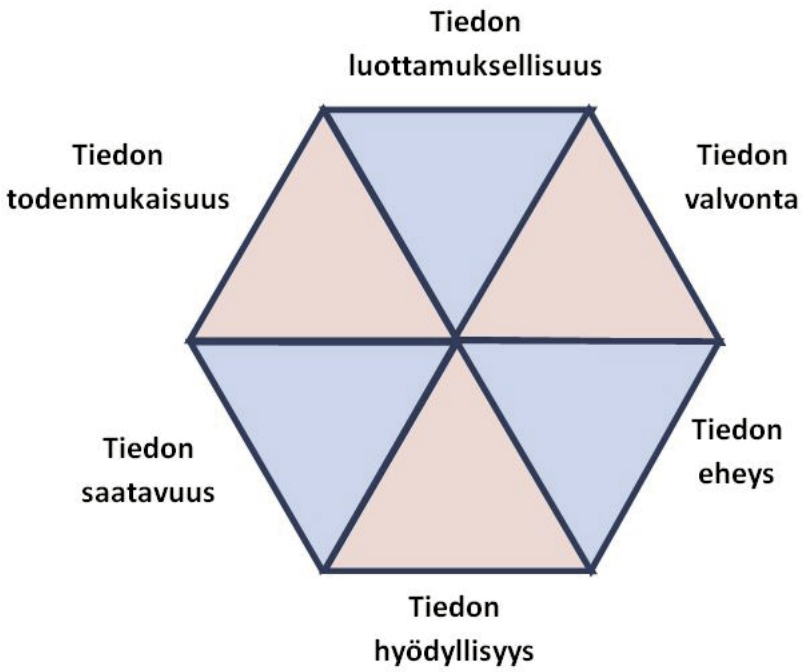
Tietoturvan perinteiset peruspilarit ovat Luottamuksellisuus (Confidentiality), Eheys (Integrity) ja Saatavuus (Availability), joista käytetään usein englanninkielistä termiä CIA-triadi (Harris 2005, 55–57). Luottamuksellisuus tarkoittaa, että suojattavat tiedot ja tietojärjestelmät ovat vain niiden käyttöön oikeutettujen saatavilla. Eheys tarkoittaa, että tietoja ja tietojärjestelmien sisältöjä ei voida muuttaa muiden kuin siihen oikeutettujen toimesta sekä että em. asiat ovat totta. Saatavuus tarkoittaa puolestaan, että tiedot ja niitä sisältävät tietojärjestelmät ovat vain niiden käyttöön oikeutettujen hyödynnettävissä aina tarvittaessa.

Peruspilareihin lisätään usein myös pääsynvalvonta (Access Control) ja kiistämättömyys (Non-repudiation), mutta pääsynvalvonta on todellisuudessa keino huolehtia CIA-triadin määrittelemistä asioista. Kiistämättömyyden voidaan puolestaan katsoa sisältyvän CIA-triadin Eheys-peruspilariin (tiedon pitää olla totta sen alkuperää myöten).

Pääsynvalvonta koostuu puolestaan neljästä vaiheesta: Käyttäjän tunnistamisesta (Identification), käyttäjän todentamisesta (Authentication), käyttäjän valtuuksien tarkastamisesta (Authorization) ja käyttäjän tekemien toimenpiteiden kirjaamisesta (Accounting). Näitä neljää vaihetta kutsutaan yhteisellä nimellä IAAA-periaatteeksi. On huomioitava, että käyttäjällä tarkoitetaan tässä yhteydessä, kuten tietoturvallisuudessa yleensäkin, ihmistä, toista tietojärjestelmää, jotain prosessia, jne. Pääsynvalvonnan johtoajatuksena on niin kutsuttu niukkuuden periaate (need-to-know tai need-to-have-access) (Harris 2005, 148).

Tietojen luottamuksellisuuden, eheyden ja saatavuuden säilyttämisen välisestä tasapainosta on huolehdittava oikein mitoitetuilla suojatoimenpiteillä. Esimerkiksi tietojen luottamuksellisuuden säilyttämisen liiallinen korostaminen saattaa vaikuttaa haitallisesti tietojen saatavuuteen. On huomioitava myös, että läheskään kaikki yrityksen tiedot eivät vaadi samanlaisia suojatoimenpiteitä. Yrityksellä on usein tietoa, joka on täysin julkista, mutta sen pitää olla totta ja saatavilla. Tällöin luottamuksellisuuden säilyttämiseen ei tietenkään pidä keskittyä. Suojatoimenpiteiden oikea valinta ja mitoittaminen vaatii yrityksen tietojen ja tietojärjestelmien luokittelua sekä niihin kohdistuvien tietoturvauhkien ja -riskien arviointia sekä hallintaa.

Donn Parker lisäsi vuonna 2002 CIA-triadiin kolme lisäominaisuutta, jolloin siitä tuli kuusikulmio, niin kutsuttu Parkerin heksadi (kuvio 1). Nämä lisäominaisuudet ovat tiedon valvonta (Possession, Control), tiedon todenmukaisuus (Authenticity) ja tiedon hyödyllisyys (Utility). (Bosworth ym. 2009, 3-1 – 3-10.)



KUVIO 1. *Parkerin heksadi.*

Parkerin heksadin tuomista hyödyistä on keskusteltu siitä lähtien varsin vilkkaasti; osa tietoturvallisuuden ammattilaisista kokee nämä lisäykset hyödyllisiksi, osa taasen ei. Donn Parker perustelee näitä lisäominaisuuksia muun muassa sillä, että perinteisessä CIA-triadissa tarkastellaan asioita liiaksi tekniikan kannalta ja jätetään ihmisten toiminta vähemmälle huomiolle (Parker 2010, 13). Parkerin heksadin tiedon valvonta tarkoittaa muun muassa sitä, että estetään valtuuttamattomien tahojen fyysinen kontakti tietoon tai ohjelmistosovellusten luvaton kopiointi tai käyttö (vrt. pääsynvalvonta). Tiedon todenmukaisuudella pyritään varmistumaan esimerkiksi siitä, että jokin sovellus ei sotke muuttujien arvoja (hinnat ovat hintoja eivätkä päivämää-

riä) tai että tiedon alkuperä on oikea (vrt. eheys). Hyödyllisyydellä puolestaan pyritään varmistumaan tiedon käyttökelpoisuudesta kuten esimerkiksi tilanteessa, jossa työntekijä salakirjoittaa (kryptaa) lähdekoodin ja unohtaa salauksen purkuavaimen (vrt. saatavuus). Edellä olleen perusteella Parkerin lisäominaisuudet eivät tuo oikeastaan mitään lisää alkuperäiseen CIA-triadiin. Ne ovat kuitenkin hyödyksi hahmotettaessa suojattaviin kohteisiin kohdistuvia uhkia. Esimerkiksi mietittäessä, mitä saattaa tapahtua, kun menetetään kontrolli johonkin tietoon tai tietoa sisältävään suojattavaan kohteeseen ja miten tieto pitäisi suojata.

TIEDON ELINKAARI

Tiedolla kuten monella muullakin asialla on elinkaari. Tiedon elinkaari voidaan jakaa seuraaviin kuuteen vaiheeseen tiedon luomisesta sen tuhoamiseen asti:

- **Luonti/päivitys.** Tämä vaihe käsittää tiedon luomisen ja olemassa olevan tiedon päivittämisen
- **Talletus.** Tieto talletetaan esim. levyjärjestelmään. Myös tiedon varmuuskopioiden ottamisen voidaan katsoa sisältyvän tähän vaiheeseen
- **Käyttö.** Tiedon tarkasteleminen, käsitteleminen ja muunlainen tiedon prosessointi
- **Jako.** Tietoa jaetaan ja siirrellään käyttäjien, asiakkaiden ja yhteistyökumppanien kesken
- **Arkistointi.** Tieto siirretään pitkäaikaiseen säilytyspaikkaan
- **Poisto.** Tieto tuhotaan pysyvästi. (Cloud Security Alliance 2011a, 53.)

On huomioitava, että tieto ei välttämättä etene lineaarisesti vaiheesta toiseen vaan ennemmin sarjana peräkkäisiä pienempiä syklejä. CIA-triadin määrittelemät asiat on otettava huomioon kaikissa tiedon elinkaaren vaiheissa. Jotta tämä onnistuisi, on tiedot ja tietoa sisältävät suojattavat kohteet luokiteltava ja kullekin luokalle on määriteltävä käsittelysäännöt (Harris 2005, 94–99). Toki ennen kuin luokittelu voidaan tehdä, on organisaation selvitettävä, mitä tietoja ja tietoa sisältäviä suojattavia kohteita sillä on. Tiedon luokittelu perustuu

useimmiten tiedon luottamuksellisuuteen ja tiedon merkitykseen organisaatiolle. On otettava huomioon myös, että tiedon luokka muuttuu hyvin usein elinkaaren eri vaiheissa.

TIETOVUODOT

IBM X-Force on nimittänyt vuotta 2011 tietovuotojen vuodeksi (IBM X-Force 2012, 12). Vuonna 2011 tapahtui useita erittäin laajoja tietovuotoja, kuten esimerkiksi Sony Playstation Networkin tietovuoto. Hyökkäykset ovat edelleen jatkuneet vuonna 2012. Hyökkäysten vaikutukset ovat olleet jonkin verran pienempiä, mutta niiden lukumäärä on kasvanut huomattavasti vuonna 2012. (IBM X-Force 2013, 12.)

Perinteisesti suurin uhka yrityksille tärkeälle tiedolle on ollut oma henkilöstö. Tämä tilanne on kuitenkin muuttunut jo useita vuosia sitten johtuen järjestäytyneen rikollisuuden toimintatavoista. Verkkorikollisten toiminnan motiivina on rahan ansaitseminen. Järjestäytyneen rikollisuuden kohteina ovat myös esimerkiksi yksityisten ihmisten henkilötiedot, verkkopankkitunnukset ja luottokorttitiedot, joita rikolliset myyvät eri verkkosivuilla. Myös monet aktivistiryhmät pyrkivät saamaan käsiinsä erilaisia luottamuksellisia tietoja, jotka ne pääsääntöisesti julkistavat omilla www-sivuillaan. Aktivistien motiivina on useimmiten erilaisten protestien esittäminen. Edellä mainittujen lisäksi tietyt valtiot pyrkivät saamaan haltuunsa niille kuulumattomia tietoja muun muassa poliittisiin tarkoituksiin. Tietyt valtiot harjoittavat jopa yritysvakoilua.

Verizonin vuoden 2012 maailmanlaajuisista tietomurroista tekemän selvityksen mukaan 92 % niistä oli yritysten ja organisaatioiden ulkopuolisten tahojen tekemiä. Selvityksessä analysoitiin 621 tietomurtoa, jotka koskivat vähintään 44 miljoonaa tietuetta. (Verizon 2013, 11–19). Taulukossa 1 on esitetty yhteenveto Verizonin analysoinnin tuloksista.

TAULUKKO 1. *Yhteenveto vuoden 2012 tietomurroista (Verizon 2013, 5–6).*

Ketkä tekevät tietomurtoja?	**Miten tietomurrot tapahtuvat?**	**Mitä yhteistä tietomurroissa esiintyy?**
92 % organisaatioiden ulkopuoliset tahot	52 % hakkeroinnin avulla	75 % taloudelliset motiivit
14 % organisaatioiden omat työntekijät	76 % tunkeutumalla tietoverkkoon hyödyntämällä anastettuja tai heikkoja tunnistautumistietoja	71 % kohdistuu käyttäjien laitteisiin
1 % yhteistyökumppanit	40 % haittaohjelmilla	54 % tunkeutumalla palvelimiin
7 % useat eri tahot yhteistyössä	35 % fyysisten hyökkäysten avulla	75 % onnistuu hyvällä onnella
19 % eri valtioihin liittyvät tahot	29 % erilaisilla social engineering -tavoilla	78 % vaikeusasteeltaan helppoja
	13 % käyttämällä pääsyoikeuksia väärin	69 % ulkopuolisten tahojen havaitsemia
		66 % havaitseminen kestänyt useita kuukausia

Vaikka eniten tietomurtoja tekevät yritysten ja organisaatioiden ulkopuoliset tahot, voidaan näihin asioihin vaikuttaa oman henkilöstön tietoturvatietoisuuden parantamisella erityisesti koulutuksen avulla. Henkilöstön on ymmärrettävä, miten heidän oma toimintansa vaikuttaa tietoturvallisuuteen. Hyvänä esimerkkinä tästä on alkuvuonna 2011 tapahtunut RSA Securityn tietomurto. Tämän tietomurron aluksi hyökkääjä lähetti kaksi sähköpostiviestiä kahdelle pienelle ryhmälle RSA Securityn työntekijöitä. Sähköpostin otsikko oli hyvin houkutteleva ”2011 Recruitment Plan” ja yksi työntekijä poimi kyseisen sähköpostin roskapostien kansiosta sekä avasi liitteenä olevan Microsoft Excel -tiedoston ”2011 Recruitment plan.xls”. Tämä tiedosto sisälsi ohjelmakoodin, joka hyödynsi Adobe Flash -ohjelman niin kutsuttua 0-päivä haavoittuvuutta ja asensi työntekijän tietokoneeseen takaporttiohjelman. (Rivner 2011.) Tämän jälkeen hyökkäys jatkui tunnetuin seurauksin, joihin voi perehtyä muun muassa CERT-FI:n tiedotteesta (CERT-FI 2011).

Kohdistetut hyökkäykset lisääntyvät jatkuvasti. Niiden kohteina ovat tietyt yritykset, organisaatiot ja jopa eri maiden kriittiset infrastruktuurit, kuten esimerkiksi energianjakeluverkot. Kohdistetut hyökkäykset hyödyntävät räätälöityjä haittaohjelmia ja erilaisia, hyvin tarkkaan suunniteltuja sosiaalisen kanssakäymisen muotoja. Symantecin mukaan kohdistettujen hyökkäysten keskimääräinen lukumäärä oli vuonna 2010 77 hyökkäystä/päivä ja vuonna 2011 82 hyökkäystä/päivä (Symantec 2012, 14). Vuonna 2012 tämä luku oli jo kivunnut 116 hyökkäykseen/päivä (Symantec 2013, 14).

Erityisen huolestuttavaa on, että PK-sektorin yrityksiin kohdistuu yhä enemmän hyökkäyksiä. Yhtenä syynä on, että hyökkääjät ovat havainneet PK-sektorin yritysten tietoturvallisuuden ja tietoturvatietoisuuden osittain heikohkon tason. Hyvin usein PK-sektorin yritystä käytetään eräänlaisena porttina kyseisen yrityksen suurempaan yhteistyökumppaniin kohdistuvassa hyökkäyksessä. PK-sektorin yrityksillä on myös usein virheellinen käsitys, että heillä ei ole mitään hyökkääjää kiinnostavaa tietoa. Symantecin raportin mukaan vuonna 2012 kaikista kohdistetuista hyökkäyksistä 31 % kohdistui yrityksiin, joilla oli alle 250 työntekijää (Symantec 2013, 16). Vielä huolestuttavammaksi asian tekee se, että Verizonin mukaan 1–100 henkilöä työllistävillä PK-sektorin yrityksillä oli globaalisti eniten tietovuotoja vuonna 2012 (Verizon 2013, 13).

Kohdistettujen hyökkäysten käyttämiä haittaohjelmia ovat Stuxnet (havaittiin vuonna 2010) ja Duqu (havaittiin lokakuussa 2011) (Symantec 2012, 14). Uusimpana tulokkaana on toukokuun lopussa 2012 havaittu Flame (CERT-FI 2012a), jota pidetään tällä hetkellä kaikkien aikojen monimutkaisimpana haittaohjelmana (Laboratory of Cryptography and System Security 2012, 3). Erityisen ikäväksi asian tekee se, että tämänkaltaiset haittaohjelmat ovat usein peräisin joidenkin valtioiden kybersodankäynnin asearsenaalista. Esimerkiksi Stuxnet on mitä todennäköisimmin kehitetty USA:n johdolla niin kutsutussa Operation Olympic Games'issa (Sanger 2012a). Laajemmin tätä toimintaa David Sanger käsittelee kirjassaan Confront and Conceal, Obama's Secret Wars and Surprising Use of American Power (Sanger 2012b).

ULKOISTUS

Yritykset ulkoistavat toimintojaan ja palvelujaan yhä enemmän. Syynä tähän on pyrkimys keskittyä omaan ydinliiketoimintaan ja -osaamiseen. Toisaalta ulkoistamisella pyritään myös löytämään kustannussäästöjä.

Ulkoistamisella tarkoitetaan liiketoiminnan tiettyjen aktiviteettien siirtämistä jonkin 3. osapuolen hoidettavaksi. Ulkoistaminen on yrityksen toimintojen ja mahdollisesti niihin liittyvän henkilöstön sekä assettien siirtämistä näihin asioihin erikoistuneelle palveluntarjoajalle. Ulkoistava yritys (ulkoistaja) vastaanottaa palveluntarjoajan palveluja ulkoistussopimuksen keston ajan sovitun palvelutasosopimuksen (SLA, Service Level Agreement) mukaan ja maksaa niistä sopimuksen mukaisen korvauksen. (Wijers & Verhoef 2009, 1.) Ulkoistamisen kohteena voi olla muun muassa jokin liiketoimintaprosessi tai erilaisia tietoteknisiä toimintoja, kokonaan tai osittain (Wijers & Verhoef 2009, 3). Ulkoistettavia liiketoimintaprosesseja voivat olla esimerkiksi laskutus, kirjanpito, tilausten käsittely, Contact Center -palvelut, henkilöstöasioiden hoito ja toimitilakiinteistön hoitoon liittyvät asiat (Solli-Saether & Gottschalk 2009, 7). Ulkoistuksen kohteena olevia tietoteknisiä toimintoja ovat muun muassa Help Desk -toiminnot, erilaiset tietotekniseen infrastruktuuriin liittyvät palvelut (muun muassa verkkoyhteydet, palvelimet ja työasemat sekä niiden hallintapalvelut ja lähituki), tietoturvapalvelut, sähköpostipalvelut ja liiketoimintasovelluksiin liittyvät palvelut.

Yrityksen liiketoimintaprosessit voidaan jakaa kolmeen luokkaan: ydinprosesseihin, liiketoiminnalle kriittisiin ei-ydinprosesseihin ja ei-kriittisiin prosesseihin. Ydinprosesseja ei yleensä ulkoisteta. Sen sijaan kahteen jälkimmäiseen luokkaan kuuluvat prosessit ovat usein ulkoistamisen kohteina. (Solli-Saether & Gottschalk 2009, 7.)

Ulkoistamisella tavoiteltavat hyödyt voidaan jakaa taulukossa 2 esitettyihin taloudellisiin, strategisiin ja teknologisiin hyötyihin.

TAULUKKO 2. *Ulkoistamisella tavoiteltavat hyödyt (Dibbern ym. 2004, 70).*

Taloudelliset hyödyt	Strategiset hyödyt	Teknologiset hyödyt
Kustannussäästöt	Ydinliiketoimintaan keskittyminen	Teknologian ajantasaisuus
Kustannusjoustavuus	Tietojärjestelmien kilpailukyky	Osaava henkilöstö
	Riskien jakaminen	Huippuluokan tietojärjestelmät
	Laadun ja luotettavuuden parantuminen	
	Joustavuus	

Ulkoistamista on tapahtunut jo paljon ennen tietotekniikan aikakautta. Voidaankin ajatella, että jo antiikin kreikkalaiset hyödynsivät tätä toimintaa. Tietojärjestelmien todellisen ulkoistamisen voidaan katsoa alkaneen vuonna 1963, jolloin Electronic Data Systems -niminen yritys (EDS) ryhtyi tuottamaan tietojenkäsittelypalveluja yhdysvaltalaiselle terveydenhoitoalan yritykselle Blue Cross of Pennsylvania (Dibbern ym. 2004, 7).

Ulkoistusliiketoiminta on lisääntynyt vuosi vuodelta. Gartnerin raportin mukaan tietojärjestelmien ulkoistusliiketoiminnan maailmanlaajuinen liikevaihto oli vuonna 2011 246.6 miljardia USA:n dollaria; kasvua vuodesta 2010 oli 7,8 % (Marketvisio 2012). Tämän raportin mukaan eniten liikevaihtoaan kasvattivat intialaiset palveluntarjoajat ja erilaisten pilvipalvelujen tarjoajat (Marketvisio 2012).

Ulkoistaminen on mahdollista toteuttaa monin eri tavoin. Sopivan ulkoistamistavan valinta riippuu muun muassa yrityksen koosta, toimialasta, toimialan kilpailutilanteesta, kansainvälistymisen tasosta, sijainnista sekä yrityksen tietoteknisen tason kypsyydestä. Yrityksen strategia on ehkä tärkein peruste ulkoistamistyypin valitsemiselle. Ulkoistaminen voidaan jakaa Schaafin mukaan taulukossa 3 esitetyllä tavalla neljään lohkoon (Schaaf 2004, 3).

TAULUKKO 3. *Ulkoistamistyypit (Schaaf 2004, 3).*

	Kotimainen	**Kansainvälinen**
Ulkoistaminen (ulkoinen)	Kotimainen ulkoistaminen (Onshoring)	Ulkomainen ulkoistaminen (Offshoring)
Oma järjestely (sisäinen)	Sisäinen kotimaan järjestely	Sidottu ulkoistaminen

Kotimainen ulkoistaminen (Onshoring) tarkoittaa järjestelyä, jossa tietty palvelu tai toiminto ulkoistetaan samassa maassa toimivalle palveluntarjoajalle. Ulkomainen ulkoistaminen (Offshoring) tarkoittaa puolestaan järjestelyä, jossa ulkoistaminen tapahtuu ulkomailla toimivalle palveluntarjoajalle. Sisäinen kotimaan järjestely ja sidottu ulkoistaminen ovat molemmat ulkoistamismuotoja, joissa ulkoistaminen tapahtuu organisaation sisäisesti. Sisäisessä kotimaan järjestelyssä ulkoistaminen tapahtuu organisaation sisällä jollekin muulle yksiköllе tai vastaavalle. Sidottu ulkoistaminen eroaa sisäisestä kotimaan järjestelystä siten, että ulkoistaminen tapahtuu yrityksen ulkomailla toimivalle tytäryhtiölle tai jonkin toisen yrityksen kanssa muodostetulle yhteisyritykselle. (Schaaf 2004, 3–6.) Usein sisäiseen kotimaan järjestelyyn liittyy niin kutsutun spin-off-yrityksen perustaminen, esimerkiksi Sonera Oyj:n 2000-luvun alussa perustama Juxto Oy tai Suomen Posti -konsernin aikoinaan perustama Atkos Oy (nimi juontuu termistä ATK-osasto). Alun perin Juxto Oy:n piti olla Sonera Oyj:n, HP:n Suomen tytäryhtiön ja Cisco Systemsin Suomen tytäryhtiön yhdessä muodostama yritys (sidottu ulkoistaminen), mutta kaksi viimeksi mainittua yritystä vetäytyi pois hankkeesta. Muutamien toimintavuosien jälkeen Juxto Oy sulautettiin kannattamattomana takaisin emoyhtiöön Sonera Oyj:hin.

Han, Lee & Seo ovat tutkineet ulkoistavan yrityksen ja palveluntarjoajan välisen vuorovaikutuksen merkitystä ulkoistuksen onnistumiseen. Tämän tutkimuksen tuloksena oli, että ulkoistajan ja palveluntarjoajan välinen vuorovaikutus on äärimmäisen tärkeää ulkoistusprosessin aikana onnistuneeseen lopputulokseen pääsemiseksi (Han ym. 2007, 40). Haasteelliseksi tämän tekee PK-yritysten osalta usein heikohkot mahdollisuudet neuvotella räätälöidyistä palvelusopimuksista palveluntarjoajan kanssa, erityisesti käytettäessä pilvipalveluja.

PILVIPALVELUT

Erilaisten pilvipalvelujen käyttö lisääntyy vuosi vuodelta. Forrester Researchin ennusteen mukaan pilvipalvelujen liikevaihto on vuonna 2020 241 miljardia USA:n dollaria, josta julkisten pilvipalvelujen osuus on yli puolet (Zdnet.com 2011).

Termille pilvipalvelut (cloud computing) ei ole yhtä yleisesti hyväksyttyä määritelmää. Käsite pilvi (cloud) on kielikuva, joka viittaa internetiin ja pilvipalveluilla tarkoitetaan toimintamallia, jossa erilaisia tietoteknisiä resursseja (muun muassa tietoliikenneyhteydet, laskenta- ja tallennuskapasiteetti, sovellukset ja tietoturva) tarjotaan käyttöön tietoliikenneverkon välityksellä ilman, että käyttäjän tarvitsee tietää, missä nämä resurssit sijaitsevat tai huolehtia niiden toiminnasta ja ylläpidosta. (Salo 2012, 16.)

Yleisimmin käytetty pilvipalvelujen määritelmä on NIST:n (National Institute of Standards and Technology) määritelmä: ”Pilvipalvelut on toimintamalli, joka mahdollistaa pääsyn vapaasti konfiguroitaviin ja skaalautuviin, jaettuihin tietotekniikkaresursseihin, jotka voidaan ottaa käyttöön tai poistaa käytöstä nopeasti käyttäjän tai palveluntarjoajan pienin toimenpitein” (NIST 2011a, 2; NIST 2012, 2–1).

NIST:n pilvipalvelujen malli koostuu viidestä ominaispiirteestä, kolmesta palvelumallista ja neljästä käyttöönottomallista.

Ominaispiirteet

- **Itsepalvelullisuus:** Asiakas saa tarvitessaan tietotekniikkaresursseja käyttöönsä ja voi lopettaa niiden käytön itsepalveluna eli ilman tarvetta olla yhteydessä palveluntarjoajaan.
- **Pääsy palveluihin:** Palvelut ovat käytettävissä verkkoyhteyden kautta eri päätelaitteilla, kuten mobiililaitteilla ja työasemilla.
- **Resurssien yhteiskäyttö:** Palvelun resurssit ovat useiden asiakkaiden yhteiskäytössä. Asiakkaalla ei yleensä ole tietoa, missä ja millä tavoin palvelut toteutetaan. Tietyissä palveluissa asiakkaan on kuitenkin mahdollista tietää, missä maassa resurssit fyysisesti sijaitsevat. Yhteiskäyttö tuo mukanaan tiettyjä ongelmia, kuten asiakkaiden eristämisen toisistaan tai jonkin käyttäjän vahingollisen toiminnan eristämisen.

- **Palvelujen nopea joustavuus:** Palvelut skaalautuvat helposti ja nopeasti sekä ylös- että alaspäin asiakkaan tarpeiden mukaan. Asiakkaan näkökulmasta resurssit vaikuttavat rajattomilta.
- **Käytön mittaaminen:** Resurssien käyttöä valvotaan ja mitataan tarkasti. Asiakas maksaa vain resursseista, joita hän käyttää. (NIST 2012, 2-1.)

Palvelumallit

- **Infrastruktuuri palveluna (Infrastructure-as-a-Service, IaaS):** IaaS -palvelulla tarkoitetaan tietojärjestelmäinfrastruktuurin hankintaa palveluna sen sijaan, että organisaatiolla itsellään on omassa hallussaan tämä infrastruktuuri. Tästä käytetään usein nimitystä virtuaalinen konesali pilvessä.
- **Sovellusalusta palveluna (Platform-as-a-Service, PaaS):** PaaS -palvelulla tarkoitetaan organisaation tarvitsemien sovellusten alustan hankintaa palveluna. Tässä palvelussa organisaatio voi kehittää itse tai hankkia joltakin toiselta osapuolelta toiminnassaan tarvitsemansa sovellukset. On huomattava, että PaaS-palvelun tarjoaja tukee vain tiettyjä ohjelmointikieliä ja työkaluja.
- **Sovellukset palveluna (Software-as-a-Service, SaaS**): SaaS -palvelulla tarkoitetaan sovellusten käyttöä palveluna perinteisen sovelluksen ostamisen, asentamisen, ylläpitämisen ja omistamisen sijasta. SaaS -palveluja on ollut markkinoilla jo pitkään, sillä ne ovat tavallaan perinteisen sovellusvuokrauspalvelun (ASP) uusi ilmenemismuoto. Yhtenä perinteisenä esimerkkinä näistä palveluista on www-selaimella käytettävä sähköpostipalvelu. (NIST 2012, 2-1 – 2-2.)

Käyttöönottomallit

- **Yksityinen pilvi:** Yksityinen pilvi on organisaation omassa käytössä ja sen käyttäjinä voivat olla esimerkiksi eri liiketoimintayksiköt. Sen voi omistaa ja sen hallinnoinnista sekä operoinnista voi vastata organisaatio itse, kolmas osapuoli tai niiden yhdistelmä. Palvelun infrastruktuuri voi sijaita muualla kuin organisaation omissa tiloissa.

- **Yhteisöpilvi:** Yhteisöpilvessä palveluinfrastruktuuri on useamman organisaation yhteisomistuksessa ja -käytössä (organisaatiot muodostavat yhteisön, jolla on esimerkiksi samat tavoitteet). Sen voi omistaa ja sen hallinnoinnista sekä operoinnista voi vastata yksi tai useampi yhteisön organisaatio, kolmas osapuoli tai niiden yhdistelmä. Palvelun infrastruktuuri voi sijaita muualla kuin organisaatioiden omissa tiloissa.
- **Julkinen pilvi:** Julkisen pilven palvelut ovat tarjolla kaikille halukkaille maksua vastaan tai jopa ilmaiseksi. Sen omistaa ja sen hallinnoista sekä operoinnista vastaa palveluntarjoaja. Palvelun infrastruktuuri sijaitsee palveluntarjoajan tiloissa.
- **Hybridipilvi:** Se on yhdistelmä yllä mainituista. Infrastruktuurista osa voi olla yksityistä tai yhteisöllistä ja osa julkista. (NIST 2012, 2-2.)

Pilvipalveluissa palveluntarjoaja vastaa palvelustaan ja sen tarvitsemasta infrastruktuurista, tiloista ja sovelluksista palvelumallista riippuen. Palveluun liittyvästä henkilöstöstään se vastaa aina. Myös vastuiden jakautuminen palveluntarjoajan ja palvelun asiakkaan kesken riippuu palvelumallista (NIST 2011b, 5).

On huomioitava, että palvelumallista riippuen asiakkaan vastuu tietoturva-asioista vaihtelee. IaaS -palveluissa vastuu infrastruktuurin tietoturvasta on palveluntarjoajalla, mutta asiakas vastaa kaikkien muiden kerrosten tietoturvasta (Cloud Security Alliance 2011a, 22).

Kansainvälinen tietoturvastandardi ISO/IEC 27001:2005

Tietoturvastandardi ISO/IEC 27001:2005 määrittelee standardin kohdassa 6.2 ’Ulkopuoliset tahot’ ja kohdassa 10.2 ’Ulkopuolisten palvelujen toimittamisen hallinta’ kummassakin kolme alakohtaa, joiden sisältämien asioiden pitää olla kunnossa noudatettaessa tätä standardia (ISO/IEC 27001:2005). Nämä alakohdat ovat

- **Ulkopuolisiin tahoihin liittyvien riskien tunnistaminen (6.2.1):** Organisaation on tunnistettava tietoon ja tietojen käsittelyyn kohdistuvat riskit, jotka aiheutuvat liiketoimintaprosesseissa mukana olevista ulkopuolisista tahoista. Organisaation on myös toteutettava asianmukaiset turvamekanismit ennen pääsyn sallimista.

- **Turvallisuudesta huolehtiminen asiakassuhteissa (6.2.2):** Organisaation on huolehdittava kaikista tunnetuista turvallisuusvaatimuksista ennen pääsyn sallimista organisaation tietoon tai suojattaviin kohteisiin.
- **Turvallisuudesta huolehtiminen kolmansien osapuolten sopimuksissa (6.2.3):** Organisaation on huolehdittava, että kolmansien osapuolten kanssa tehtävät sopimukset, jotka liittyvät organisaation tietojen tai tietojen käsittelyn käyttöoikeuksiin, käsittelyyn, hallintaan tai niistä viestimiseen tai tuotteiden tai palvelujen lisäämiseen tietojen käsittelyn piiriin, kattavat kaikki olennaiset tietoturvavaatimukset.
- **Palvelujen toimittaminen (10.2.1):** Organisaation tulee varmistaa, että ulkopuolinen palveluntoimittaja toteuttaa, käyttää ja ylläpitää sopimuksessa mainittuja turvamekanismeja, palvelumäärittelyjä ja palvelutasoja.
- **Ulkopuolisten palvelujen tarkkailu ja katselmointi (10.2.2):** Organisaation on seurattava ja katselmoitava säännöllisesti ulkopuolisen tahon toimittamia palveluja ja niihin liittyviä raportteja sekä eri tapahtumien tallenteita. Tarkastuksia on suoritettava säännöllisesti.
- **Ulkopuolisen palvelun muutosten hallinta (10.2.3):** Organisaation on hallittava palvelun tarjoamista koskevia muutoksia ottaen huomioon asianomaisten liiketoimintajärjestelmien ja -prosessien kriittisyys ja riskien uudelleenarviointi. Lisäksi organisaation on hallittava olemassa olevien tietoturvapolitiikkojen, menettelytapojen ja turvamekanismien ylläpitoa ja parantamista.

Standardi ISO/IEC 27002:2005 antaa tarkempia ohjeita näiden kohtien toteuttamiseksi (ISO/IEC 27002:2005). Kaikkien ulkoistuspalveluja käyttävien organisaatioiden on syytä perehtyä näihin ohjeisiin, vaikkakin ne ovat varsin yleisluonteisia. Cloud Security Alliance on laatinut erittäin hyvän taulukon pilvipalveluihin liittyvistä suojatoimenpiteistä. Tässä taulukossa on esitetty, mitä muiden tietolähteiden suojatoimenpiteitä ne vastaavat, kuten esimerkiksi ISO/IEC 27001:2005-standardia. (Cloud Security Alliance 2011b.)

ULKOISTETTUIHIN PALVELUIHIN LIITTYVIÄ HUOLENAIHEITA JA OHJEITA

Kuten edellä on todettu, kaikki alkaa tietoturvariskien tunnistamisesta. Ulkoistusta harkitsevan organisaation on arvioitava, millaisia riskejä eri toimintojen ulkoistamiseen liittyy. Organisaation on selvitettävä erittäin tarkasti, millaisia tietoja sen eri toiminnoissa käsitellään ottaen huomioon tiedon elinkaarimalli. Samoin organisaation on selvitettävä, kuinka kriittisiä eri toimintojen tarvitsemat tietojärjestelmät ovat sen omalle toiminnalle. Vasta näiden selvitysten perusteella se voi tehdä päätöksiä, millaisia toimintoja sen kannattaa tai se voi edes ulkoistaa.

Tietoturvariskien tunnistaminen ja arvioiminen ovat osa tietoturvariskien hallintaa, joka muodostaa perustan koko tietoturvallisuudelle. Tietoturvariskien hallintaan kuuluvat myös tarvittavien suojatoimenpiteiden käyttöönotto ja niiden toimivuuden seuraaminen sekä tietoturvariskien jatkuva tarkkailu ja niistä viestiminen. Tästäkin asiasta on oma ISO-standardinsa, ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management (ISO/IEC 27005:2008). On erityisen tärkeää ymmärtää, että tietoturvariskien hallinta on jatkuva prosessi eikä kertaluontoinen projekti.

Erinomaisen käsityksen ulkoistukseen liittyvistä huolenaiheista saa Kimmo Rouskun blogikirjoituksesta 'Tietoturvallisuus palvelujen tuottamisessa' (Rousku 2012). Tässä 4-osaisessa kirjoituksessa hän tarkastelee asioita hyvin monesta näkökulmasta käyttäen usein käytettyä termiä XaaS, joka on yhteisnimitys IaaS-, PaaS- ja SaaS -palveluille sekä muille vielä tarkemmin määrittelemättömille pilvipalveluille.

Ulkoistusta harkitsevan organisaation on tiedettävä tai selvitettävä etukäteen, millaisia vaatimuksia lainsäädäntö ja toimialakohtaiset määräykset asettavat ulkoistukselle. Esimerkiksi millaisia ovat kirjanpitolain vaatimukset aineiston säilyttämiselle? Erityisen paljon keskustelua on herättänyt henkilötietojen käsittely ulkoistetuissa palveluissa ja erityisesti käytettäessä pilvipalveluja. Tästä on oivana esimerkkinä aiemmin mainittu vuonna 2011 Suomessa tapahtuneiden lukuisten tietomurtojen ja niiden yritysten aiheuttama Tietosuojavaltuutetun toimiston kesällä 2012 tekemä tarkastus. EU:n Tietosuojadirektiivin 95/46/EC Artikla 29:n mukainen tietosuojatyöryhmä on esittänyt oman kannanottonsa henkilötietojen käsittelyyn pilvipalveluissa (Article 29 Working

Party 2012). Tämän kannanoton mukaan pilvipalveluissa tapahtuvaan henkilötietojen käsittelyyn liittyviä palvelun asiakkaan omien, riittävän hyvien valvontamahdollisuuksien puutteesta aiheutuvia riskejä ovat:

- Tietojen saatavuuden menettäminen johtuen liiallisesta toimittajariippuvuudesta (tietoja ei voi siirtää vaihdettaessa palveluntarjoajaa)
- Tietojen eheyden menettäminen johtuen palvelun resurssien ja infrastruktuurin jakamisesta usean asiakkaan kesken
- Tietojen luottamuksellisuuden menettäminen johtuen jonkin EU:n ulkopuolisen maan viranomaisten palveluntarjoajalle esittämien vaatimusten johdosta
- Liian monimutkainen ulkoistuspalvelujen ketju, jossa osan palveluista tuottaakin jokin toinen palveluntarjoaja, joka puolestaan on ulkoistanut osan toiminnoistaan kolmannelle palveluntarjoajalle, jne.
- Tietojen kohteiden (henkilöt, joiden henkilötiedoista on kyse) riittävien oikeuksien puute, mm. pääsy tietoihin, tietojen poistaminen tai korjaaminen
- Tietojen yhdistämismahdollisuus johtuen palveluntarjoajan henkilöstön liian suurista käyttöoikeuksista (Article 29 Working Party 2012, 5–6.)

Saman kannanoton mukaan henkilötietojen käsittelyn läpinäkyvyyden puutteesta aiheutuvia mahdollisia uhkia ovat:

- Ketjutettu tietojen käsittely (useita käsitteleviä tahoja ja alihankkijoita)
- Henkilötietoja käsitellään eri maissa Euroopan talousalueella, jolloin on hankalaa varmistaa, minkä maan lainsäädäntöä noudatetaan.
- Henkilötietoja voidaan mahdollisesti siirtää jopa Europan talousalueen ulkopuolelle maihin, joissa ei ole riittäviä tietoturvakäytäntöjä. (Article 29 Working Party 2012, 6.)

Ulkoistaminen ei kuitenkaan läheskään aina tarkoita pilvipalvelujen käyttämistä. Esimerkiksi organisaation oman lähiverkon tai työasemien ylläpito tai asiakaspalvelu voidaan ulkoistaa jonkin palveluntarjoajan hoidettavaksi. Näissäkin tilanteissa organisaation on ehdottomasti tehtävä tietoturvariskien arviointi ja mietittävä, millaiset toimintatavat on otettava käyttöön. Tästä on hyvänä esimerkkinä entisen pääministeri Matti Vanhasen valokuviin liittynyt tapaus, jossa ulkopuolisen palveluntarjoajan palveluksessa oleva tietokoneen korjaaja kopioi Matti Vanhasen yksityisen valokuvan hänen virkasähköpostistaan valtioneuvoston linnassa vuonna 2007. Tapaus tuli ilmi, kun kyseinen henkilö yritti myydä kyseistä valokuvaa lehdistölle. (Iltalehti 2010.)

USA on ollut henkilö- ja henkilökohtaisten tietojen tietovuotojen ilmoitusvelvollisuutta koskevassa lainsäädännössä EU:n edellä. Tässä lainsäädännössä ei kuitenkaan ole tarkkaa, yksikäsitteistä määritelmää henkilö- ja henkilökohtaisille tiedoille. Näistä tiedoista käytetään engl. kielistä termiä Personally Identifiable Information (PII) ja riippuen osavaltiosta ne voivat käsittää EU:ssa käytössä olevan henkilötietojen määritelmän lisäksi myös erilaisia henkilön rahatalouteen liittyviä tietoja kuten esim. pankkitilin tai luottokortin numeron. Ensimmäinen näiden tietojen vuotamisen ilmoittamiseen velvoittava laki astui voimaan Kaliforniassa jo vuonna 2002. Tällä hetkellä tällainen laki on voimassa 46 USA:n osavaltiossa, Columbian piirikunnassa, Guamissa, Puerto Ricossa ja Neitsytsaarilla. (Stevens 2012, 1–4.) Tämä lainsäädäntö velvoittaa eri organisaatioita ilmoittamaan henkilö- ja henkilökohtaisten tietojen kohteille heidän tietojaan koskevista tietovuodoista. Erinomainen tietolähde USA:ssa tapahtuneista eri syistä johtuneista tietovuodoista on Privacy Rights Clearinghousen www-sivusto (Privacy Rights Clearinghouse 2012). On kuitenkin huomattava, että läheskään kaikki organisaatiot eivät noudata tätä lainsäädäntöä eivätkä ilmoita tapahtuneista tietovuodoista ennen kuin asia paljastuu jotain muuta kautta. Esimerkiksi toistaiseksi maailman laajimman tietovuodon kokenut Heartland Payment Systems ilmoitti tammikuussa 2009 joutuneensa tietomurron kohteeksi. Tämä tietovuoto käsitti lähes 130 miljoonan pankki- ja maksukortin tiedot. Tietomurto paljastui alun perin väärennettyjen maksukorttien perusteella. Tarkempi selvitys on paljastanut, että tietomurto oli alkanut jo 18 kuukautta aikaisemmin. (Kitten 2012.)

Euroopan komissio julkaisi vuoden 2012 alussa ehdotuksen uudeksi henkilötietojen suojaa koskevaksi sääntelyksi (Euroopan komissio 2012a). Tämän uuden sääntelyn tarkoituksena on korvata vuonna 1995 voimaantullut henkilötietodirektiivi (95/46/EY), joka on osoittautunut riittämättömäksi teknologi-

sen kehityksen ja henkilötietojen käsittelyn globalisoitumisen vuoksi. Tämän sääntelyn yhtenä tavoitteena on yhtenäistää henkilötietojen käsittely EU:ssa nykyisen, erittäin hajanaisen sääntelyn sijasta. Yhtenä merkittävänä uudistuksena tulee olemaan henkilörekisterinpitäjien ilmoitusvelvollisuus viranomaisille ja henkilötietojen kohteille henkilötietojen tietovuodoista 24 tunnin kuluessa tapahtumasta (Euroopan komissio 2012b, 62–63). Lisäksi henkilötietojen käsittelijätahojen on ilmoitettava tällaisista tietovuodoista rekisterinpitäjälle välittömästi (Euroopan komissio 2012b, 62). Uutta on myös tämän sääntelyn mukanaan tuoma seuraamuskäytäntö, joka yritysten osalta voi olla jopa 2 % niiden vuotuisesta maailmanlaajuisesta liikevaihdosta riippuen tapahtuman vakavuudesta (Euroopan komissio 2012b, 94–95). Uusi sääntely tulee vahvistamaan myös henkilötietojen kohteiden (rekisteröityjen) niin kutsuttua oikeutta tulla unohdetuksi, jonka mukaan rekisteröidyillä on oikeus saada henkilötietonsa poistettua henkilörekistereistä, mikäli niiden tallentamiseen ei ole perusteltua syytä (Euroopan komissio 2012b, 53). Tavoitteena on, että tämä sääntely astuu voimaan vuonna 2014 kahden vuoden siirtymäajalla, mutta nopeampikin voimaantulo on mahdollista.

Ulkoistettuja palveluja ja toimintoja käyttävien tai niitä harkitsevien yritysten ja organisaatioiden on perehdyttävä hyvissä ajoin tähän uuteen henkilötietojen sääntelyyn. Niiden on myös luonnollisesti tunnettava nykyinen henkilötietojen käsittelyyn liittyvä lainsäädäntö ja toimittava sen mukaisesti. Muun muassa tilanteet, joissa henkilötietojen käsittelyyn liittyy aiemmin mainittu ketjutettu tietojen käsittely, tulevat olemaan hyvin haasteellisia.

Tietoverkkojen ja tietojärjestelmien tietoturvallisuudella on yhä suurempi merkitys liike-elämälle ja koko yhteiskunnalle. Tämän johdosta Euroopan komissio julkisti 7.2.2013 EU:n kyberturvallisuusstrategian ja ehdotuksen Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa (Euroopan unioni 2013). Direktiiviehdotus velvoittaisi kaikki EU:n jäsenvaltiot perustamaan tietotekniikan kriisiryhmiä (CERT) ja vahvistamaan kansallisia verkko- ja tietoturvastrategioita sekä tietoturvan yhteistyösuunnitelmia ja kansallisten toimivaltaisten viranomaisten tekemään yhteistyötä. Lisäksi ehdotus velvoittaisi kriittisillä sektoreilla (muun muassa pankkitoiminta, pörssit, energian tuotanto, siirto ja jakelu, lento-, rautatie- ja meriliikenne, terveydenhuolto, internetpalvelut sekä julkishallinnot) toimivien yritysten ja julkishallinnon arvioimaan niihin kohdistuvat tietoturvariskit, toteuttamaan asianmukaiset toimenpiteet verkko- ja tietoturvan varmistamiseksi sekä raportoimaan toimivaltaisille vi-

ranomaisille kaikista turvapoikkeamista, jotka vaarantavat vakavasti niiden verkot ja tietojärjestelmät ja vaikuttavat merkittävästi kriittisten palvelujen ja hyödykkeiden toimitusten jatkuvuuteen. Direktiiviehdotuksen 14 artiklan 3. kohdan mukaan näitä vaatimuksia sovelletaan kaikkiin EU:ssa palveluja tarjoaviin markkinatoimijoihin lukuun ottamatta mikroyrityksiä. Saman artiklan 4. kohdan mukaan toimivaltainen viranomainen voi tiedottaa yleisölle tai vaatia julkishallintoja ja markkinatoimijoita tiedottamaan yleisölle, jos se katsoo turvapoikkeaman julkistamisen olevan yleisen edun mukaista. Direktiiviehdotus ei sen sijaan vaadi palveluntarjoajaa ilmoittamaan turvapoikkeamista asiakkailleen, joten ulkoistusta harkitsevan PK-sektorin yrityksen pitää ottaa tämä huomioon neuvotellessaan palvelutasosopimusta palveluntarjoajan kanssa.

Ovatko palveluntarjoajien palvelut immuuneja verkkohyökkäyksille, erilaisille haittaohjelmille tai toimintahäiriöille? Vastauksena tähän kysymykseen on, eivät ole. Ohessa muutamia esimerkkejä Suomesta ja muualta.

Kesällä 2008 uutisoitiin Finanssialan keskusliiton verkkopalvelun tietoturvaongelmista. Palvelu levitti haittaohjelmia www-sivustolla käyneiden tietokoneisiin. Kyseessä oli niin kutsuttu troijalainen, joka tarttui tartunnan saaneen tietokoneen Microsoft IE 7-selaimen tilapäistiedostojen hakemistoon. Kyseessä oli hyvin todennäköisesti laajempi hyökkäys, joka käytti sql injection -tekniikkaa (Tietoviikko 2008). Ajantasaisella virustorjuntaohjelmistolla suojatut tietokoneet olivat immuuneja näille tartunnoille. Hyvin arveluttavaksi asian teki se, että tätä www-sivustoa hoitavan toimittajakumppanin raportin mukaan hyökkäysten ei olisi edes pitänyt olla mahdollisia, mutta palveluntarjoaja suoritti kaikki puhdistus- ja korjaustoimenpiteet saatuaan tiedon ongelmasta. (Tietoviikko 2008.) Tässä tapauksessa ei palveluntarjoaja ollut huolehtinut tietoturvavelvoitteistaan juuri ollenkaan. Asiakas kuitenkin uskoi, että nämä asiat olivat kunnossa. Toisenlainen tapaus oli kyseessä toukokuussa 2012 ilmenneessä verkkohyökkäyksessä muun muassa Suomen Lääkäriliiton www-sivuille. Tässä tapauksessa hyökkäys perustui tapahtumahetkellä vielä tuntemattoman haavoittuvuuden (0-päivä hyökkäys) hyväksikäyttöön, johon palveluntarjoaja ei ollut mitenkään voinut varautua etukäteen. (CERT-FI 2012b.)

OP-Pohjolan pankkijärjestelmissä oli vakava toimintahäiriö tammikuussa 2011. OP-Pohjola käyttää Tieto Oyj:n konesalipalveluja. Palvelujen turvaamiseksi ne on hajautettu kahteen konesaliin. Tässä häiriössä konesalien välinen tietoliikenne ei kuitenkaan toiminut johtuen väärin konfiguroidusta kytkimestä. (IT-viikko 2011.) Kyseessä oli siten inhimillinen erehdys.

Marraskuussa 2011 Tieto Oyj:llä oli vakavia ongelmia yhdessä Ruotsissa sijaitsevassa konesalissaan. Kyseessä oli levyjärjestelmävika, jonka vuoksi noin 50 asiakkaan keskeiset tietotekniset palvelut eivät olleet käytettävissä yli kahteen viikkoon. (Tieto Oyj 2012a, 4.) Kustannukset tästä häiriöstä Tieto Oyj:lle olivat vähintään 5 miljoonaa euroa (Tietoviikko 2012). Syyksi tähän häiriöön paljastui EMC:n toimittama uusi tallennusjärjestelmä (Tieto Oyj 2011), jossa ilmeni hyvin epätodennäköinen laitteistovika. Tällaisten tapahtumien estämiseksi vastaisuudessa laitteistokonfiguraatiota on muutettu. (Tieto Oyj 2012b.)

Globaaleissa pilvipalveluissa on esiintynyt niiden olemassaolon aikana erittäin suuria saatavuusongelmia. Hyvän käsityksen näistä häiriöistä saa muun muassa InfoWorld:in artikkelista (Infoworld 2011) sekä Gina Stevensin raportista USA:n kongressille (Stevens 2012, 2–3), joissa käsitellään muun muassa Amazonin EC2-palvelun, Googlen Gmail -palvelun, Microsoftin Sidekickin ja Hotmail-palvelun, Salesforcen ja PayPalin häiriöitä.

YHTEENVETO

Mikä tekee ulkoistuksesta houkuttelevan vaihtoehdon? Useimmiten syynä ovat kustannustehokkuuden etsiminen ja pyrkimys keskittyä omaan ydinliiketoimintaan. Ulkoistaminen voidaan nähdä jopa nykyajan muoti-ilmiönä eli ulkoistetaan siksi, että muutkin ulkoistavat. On olemassa myös hyvin paljon esimerkkejä vastakkaisesta toimintatavasta, jolloin organisaatiot ovatkin luopuneet ulkoistettujen palvelujen käytöstä.

Ulkoistusta mietittäessä on ulkoistettaviin toimintoihin liittyvien tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat tietoturvariskit aina arvioitava etukäteen. Samoin ulkoistettavien tietojärjestelmien tärkeys organisaation liiketoiminnalle on arvioitava etukäteen. Vasta tämän jälkeen organisaatio voi vakavasti harkita ulkoistamista. On kuitenkin aina muistettava, että vastuuta ei voi ulkoistaa.

LÄHTEET

Article 29 Working Party 2012. WP 196 Opinion 05/2012 on Cloud Computing. Viitattu 8.10.2012 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

Bosworth, S.; Kabay, M. E. & Whyne, E. (toim.) 2009. Computer Security Handbook. 5th Edition. Hoboken: Wiley.

CERT-FI 2011. RSA:lta varastettuja tietoja käytetty tietomurrossa, RSA vaihtaa SecurID:t uusiin. Viitattu 3.6.2012 www.cert.fi > Tietoturva nyt! > 2011 > Kesäkuu.

CERT-FI 2012a. Tietoja varastava haittaohjelma löytyi idästä. Viitattu 31.5.2012 www.cert.fi > Tietoturva nyt! > 2012 > Toukokuu.

CERT-FI 2012b. OpenX-mainosalustan haavoittuvuutta hyväksikäytetään Suomessa. Viitattu 3.6.2012 www.cert.fi > Tietoturva nyt! > 2012 > Toukokuu.

Cloud Security Alliance 2011a. Security guidance for critical areas of focus in cloud computing V3.0. Viitattu 31.5.2012 https://cloudsecurityalliance.org/.

Cloud Security Alliance 2011b. Cloud Controls Matrix V1.2. Viitattu 4.6.2012 https://cloudsecurityalliance.org/.

Dibbern, J.; Goles, T.; Hirschheim, R. & Jayatilaka, B. 2004. Information Systems Outsourcing: A Survey and Analysis oft he Literature. The DATA BASE for Advances in Information Systems. Vol. 35, No 4, 6–102.

Euroopan komissio 2012a. Lehdistötiedote – Tietosuojasääntöjen kattava uudistus parantaisi käyttäjien mahdollisuuksia valvoa tietojaan ja vähentäisi yritysten kustannuksia. Viitattu 30.10.2012 http://europa.eu/rapid/press-release_IP-12-46_fi.htm.

Euroopan komissio 2012b. EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta

liikkuvuudesta (yleinen tietosuoja-asetus). Viitattu 30.10.2012 http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fi.pdf.

Euroopan unioni 2013. EU:n kyberturvallisuusstrategia. Viitattu 27.8.2013 http://eeas.europa.eu/policies/eu-cyber-security/index_fi.htm.

Han, H., Lee, J. & Seo, Y. 2007. Analyzing the impact of a firm's capability on outsourcing success: A process perspective. Information & management. Vol. 45, No 1, 31–42.

Harris, S. 2005. All-In-One CISSP Exam Guide. 3rd Edition. New York: McGraw-Hill/ Osborne.

IBM X-Force 2012. IBM X-Force 2011 Trend And Risk Report. Viitattu 28.5.2012 https:// www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_ PKG=xforce-trend-risk-report.

IBM X-Force 2013. IBM X-Force 2012 Trend And Risk Report. Viitattu 23.5.2013 https:// www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-WW_Security_ Organic&S_PKG=ov12250.

Iltalehti 2010. Viitattu 7.10.2012 http://www.iltalehti.fi/uutiset/2010012110969708_ uu.shtml.

Infoworld 2011. The 10 worst cloud outages (and what we can learn from them). Viitattu 3.6.2012 http://www.infoworld.com/d/cloud-computing/the-10-worst-cloud-outages-and-what-we-can-learn-them-902.

ISO/IEC 27001:2005. Information Technology. Security techniques. Information security management systems. Requirements.

ISO/IEC 27002:2005. Information technology. Security techniques. Code of practice for information security management.

ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management.

IT-viikko 2011. OP-pankin viat johtuivat Tiedon konesalista. Viitattu 3.6.2012 http://www.itviikko.fi/ratkaisut/2011/01/25/op-pankin-viat-johtuivat-tiedon-konesalista/20111138/7.

Keskusrikospoliisi 2011. Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva, Syksy 2011. Viitattu 28.5.2012 http://www.poliisi.fi/krp > Yritysturvallisuus.

Kitten, T. 2012. A Tale of Two Breaches. What Heartland's Story Says About Global Payments' Future. Viitattu 26.10.2012 http://www.bankinfosecurity.com/tale-two-breaches-a-4658/p-1.

Laboratory of Cryptography and System Security 2012. sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks. Viitattu 31.5.2012 http://www.crysys.hu/ skywiper/skywiper.pdf.

Marketvisio 2012. Gartner Says Worlwide IT Outsourcing Market Grew 7.8 Per Cent in 2011. Viitattu 10.6.2012 http://www.marketvisio.fi/fi/ajankohtaista/uutiset-gartner/1343-gartner-says-worldwide-it-outsourcing-market-grew-7-8-per-cent-in-2011.

NIST 2011a. The NIST Definition of Cloud Computing. Special Publication 800–145. Viitattu 8.6.2012 http://csrc.nist.gov/publications/PubsSPs.html.

NIST 2011b. Guidelines on Security and Privacy in Public Cloud Computing. Special Publication 800–144. Viitattu 13.6.2012 http://csrc.nist.gov/publications/PubsSPs.html.

NIST 2012. Cloud Computing Synopsis and Recommendations. Special Publication 800–146. Viitattu 8.6.2012 http://csrc.nist.gov/publications/PubsSPs.html.

Parker, D. 2010. Our Excessively Simplistic Information Security Model and How to Fix It. ISSA Journal. Vol. 8, Issue 7, 12–21.

Privacy Rights Clearinghouse. 2012. Viitattu 25.10.2012 https://www.privacyrights.org/.

Rivner, U. 2011. Anatomy of an Attack. Viitattu 3.6.2012 http://blogs.rsa.com/rivner/anatomy-of-an-attack/.

Rousku, K. 2012. Tietoturvallisuus palveluiden tuottamisessa. Viitattu 7.10.2012 http://www.tietoviikko.fi/blogit/turvasatama/.

Salmi, V.; Lehti, M. & Keinänen, A. 2011. Kauppa ja teollisuus rikosten kohteena, Vuoden 2010 yritysuhritutkimuksen tuloksia. Oikeuspoliittisen tutkimuslaitoksen tutkimuksia 254.

Salo, I. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo.

Sanger, D. 2012a. Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times. Viitattu 23.10.2012 http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all.

Sanger, D. 2012b. Confront and Conceal, Obama's Secret Wars and Surprising Use of American Power. New York: Crown Publishers.

Schaaf, J. 2004. Offshoring: Globalisation wave reaches service sector. Deutsche Bank Research. Nro 45, 1–16.

Solli-Soether, H. & Gottschalk, P. 2009. Managing IT Outsourcing Performance. Hershey: IGI Global.

Stevens, G. 2012. Data Security Breach Notification Laws. CRS Report for Congress, R42475. Viitattu 25.10.2012 http://www.fas.org/sgp/crs/misc/R42475.pdf.

Symantec Corporation 2012. Internet Security Threat Report, 2011 Trends. Volume 17. Viitattu 28.5.2013 http://www.symantec.com/threatreport/.

Symantec Corporation 2013. Internet Security Threat Report, 2012 Trends. Volume 18. Viitattu 28.5.2013 http://www.symantec.com/threatreport/.

Tietosuoja 2012. Tietosuojavaltuutettu vaatii yrityksiä panostamaan tietoturvaa. Viitattu 15.10.2012 http://www.tietosuoja.fi/59848.htm.

Tietoviikko 2008. Pankkialan sivusto levitti haittaohjelmia. Viitattu 1.6.2012 http://www.tietoviikko.fi/kaikki_uutiset/pankkialan+sivusto+levitti+haittaohjelmia+paivitetty/a133598.

Tietoviikko 2012. Konesalin ongelmat maksoivat Tiedolle miljoonia. Viitattu 1.6.2012 http://www.tietoviikko.fi/cio/konesalin+ongelmat+maksoivat+tiedolle+miljoonia/a772842.

Tieto Oyj 2011. I stort sett alla tjänster åter I drift – Tieto utreder den bakomliggande orsaken. Viitattu 3.6.2012 http://www.tieto.se > Nyhetsarkiv > I stort sett alla tjänster åter i drift – Tieto utreder den bakomliggande orsaken.

Tieto Oyj 2012a. Osavuosikatsaus 4/2011.

Tieto Oyj 2012b. Viitattu 3.6.2012 http://www.tieto.se > Nyhetsarkiv > Tieto: Slutsatser och lardomar efter driftstorningen den 25 november 2011.

VASCO Data Security International, Inc. 2011. Viitattu 23.5.2012 http://www.vasco.com/company/about_vasco/press_room/news_archive/2011/news_vasco_announces_bankruptcy_filing_by_diginotar_bv.aspx.

Verizon 2013. 2013 Data Breach Investigations Report. Viitattu 28.5.2013 http://www.verizonenterprise.com/DBIR/2013/.

Wijers, G. & Verhoef, D. 2009. IT Outsourcing, Part I: Contracting the Partner, A Management Guide. Amersfoort: Van Haren Publishing.

Zdnet.com 2011. Cloud computing market : $241 billion in 2020. Viitattu 12.6.2012 http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702.

KAUKANA KAVALA MAAILMA – VAIN YHDEN KLIKKAUKSEN PÄÄSSÄ?

Virpi Raivonen, FM
Lehtori, Tietojenkäsittelyn koulutusohjelma, Turun ammattikorkeakoulu

Sinikka Leino, merkonomi
Projektipäällikkö, Turun ammattikorkeakoulu

Maailman talousfoorumin WEF:n vuonna 2013 tekemän tutkimuksen mukaan suomalaisista kotitalouksista 85 prosenttia omistaa tietokoneen ja 89 prosenttia suomalaisista käyttää internetiä säännöllisesti. Liikkuvan laajakaistan omistaa 87 % suomalaisista.

Tietotekniikan yleistyminen on synnyttänyt kasvavan tarpeen asiantuntevalle opastukselle, joka olisi kaikkien saatavilla. Kansalaisen Mikrotuki on Turun ammattikorkeakoulun kehittämishanke, jonka tehtävänä on madaltaa tietoyhteiskunnan kynnystä Turun seudun asukkaille. Opiskelijavoimin ylläpidettävä toimipiste Lemminkäisenkadun kampuksella tarjoaa kansalaisille maksutonta opastusta tietokoneiden ja oheislaitteiden käyttöön ja tietoturvaan. Kansalaisen Mikrotuki palvelee vuosittain noin 1400 asiakasta. Pääministerin Parhaat käytännöt -kisassa Matti Vanhanen antoi kunniamaininnan Kansalaisen Mikrotuelle ”Tietoturvan edistäminen ja soveltaminen”-sarjassa 23.11.2006.

Kansalaisen Mikrotukeen tulee lähes päivittäin tapauksia, joissa henkilökohtaisessa tietoturvassa on puutteita. Tietoturvariskejä on monenlaisia, joista suurin osa johtuu tietämättömyydestä tai huolimattomuudesta.

Suomalaisiakin kohdanneet salasanavuodot ovat paljastaneet suomalaisten heikon osaamisen tai välinpitämättömyyden tietoturvaosaamisessa; mm. Älypääpelin 127 000 salasanan vuotaminen (vuonna 2010), Hotmail (käyttäjätilin salasanan kaappaaminen vuonna 2012), LinkedIn (salasanojen vuoto 2012), Facebook/Twitter (2013). Tietokoneen käyttäjiä pitää muistuttaa säännöllisesti tietoturvariskeistä. Pelottelu ei ole se tapa, jolla ihmiset saadaan toimimaan, vaan tiedotus, opastaminen ja koulutus.

Kansalaisen Mikrotuki opastaa ihmisiä tietoturvassa, ohjelmien käytössä, sekä tietokoneen yleisessä käytössä. Vuodesta 2004 toiminut hanke on auttanut tuhansia ihmisiä henkilökohtaisesti ja saatu palaute on ollut erinomaista. Hankkeen konsepti on olla joustava ja ajan hengessä toimiva palvelu, joka pystyy vastaamaan tietoyhteiskunnan muuttuviin tarpeisiin. Kansalaisen Mikrotuessa asiakkaina ovat etenkin korkeakoulujen vaihto-opiskelijat sekä Turun lähialueiden senioriasukkaat.

Eläkeläisille suunnattujen kurssien ja kerhojen määrä on kasvanut huimasti viime vuosien aikana. Monet Mikrotuen asiakkaista ovat osallistuneet mm. Auralan tai työväenopiston kursseille. Kurssin aikana on asioita käsitelty nopealla tempolla tai asia on alun perin ollut vaikeasti ymmärrettävissä. Omaan osaamiseen ei vielä kerran kurssituksen jälkeen luoteta. Kerran Kansalaisen Mikrotukeen tullut senioriasiakas tuleekin todennäköisesti uudestaan, jopa useamman kerran. Aluksi apua haetaan samaan ongelmaan kuin ensimmäisellä kerralla. Tämän jälkeen asia, johon apua toivotaan, alkaa enemmän fokusoitua koneen toimivuuden sijaan ohjelmien opastukseen. Toistot henkilökohtaisessa ohjauksessa auttavat luottamaan omaan taitoon.

Mikrotuessa hoidetut ongelmat vaihtelevat paljon. Huolta saattaa aiheuttaa mm. arveluttavana pidetty kuvake työpöydällä. Yleisin ongelma on hidastunut kone ja virustorjuntaohjelma, joka pitää joko päivittää, vaihtaa, poistaa tai asentaa asiakkaan puolesta. Koneen puhdistamiseen kuluu usein tunteja tai pahimmissa tapauksissa jopa päiviä.

Syyskuun ensimmäisenä päivänä 2007 Suomessa siirryttiin pelkästään digitaalisiin televisiolähetyksiin. Tämä näkyi Kansalaisen Mikrotuen toimipisteessä. Digiboksien ostamiseen ja asentamiseen liittyvät ongelmat toivat ihmiset toimipisteeseen.

TAULUKKO 1: *Yleisimpiä asiakkaiden esille tuomia asioita.*

2007	2008
Digiboxin käytön opastus	Digiboxin viritys
Kone on hidas	Käyttöjärjestelmäongelmia
Viiruksia	Tietoturvaohjelmassa ongelmia
	Kone hidas
	Kovalevy rikki

2010	2011
Mokkulat	valokuvat talteen
Printterit	miniläppärit
Tietoturvaohjelmat	verkkoyhteydessä ongelmia
Linux	haittaohjelmat/viirukset
Facebook opastus	käytön opastus

Vuosi 2010 toi mukanaan uuden aallon oheislaitteita. Etenkin mokkulat ja niiden asentaminen nousivat esiin. Facebook-opastukset yleistyivät etenkin vanhemman väestön parissa. Koneiden hitaus ja virusepäilyt ovat pysyneet kestosuosikkeina läpi toimintavuosien.

Kansalaisen Mikrotuessa on järjestetty mm. Facebook-päivä, jossa asiakkaita on opastettu tietoturvalliseen sosiaalisen median käyttöön. Keväällä 2012 pidetyssä Skype -päivässä oli osallistujilla mahdollisuus kokeilla yhteyden saamista turvallisessa ympäristössä. Vieressä oleva tuki antaa uskallusta ylittää tietotekninen, usein korkeakin kynnys.

Vaikka Microsoftin tuoreen tutkimuksen mukaan suomalaiset kuuluvat Euroopan eliittiin tietoturva-asioissa, on meillä vielä paljon opittavaa yksilötasolla. Äärimmäisenä esimerkkinä yhdestä asiakaskoneesta löydettiin 256 erilasta haittaohjelmaa.

Syksyllä 2011 suurin osa asiakkaista käytti Avast-virustorjuntaohjelmaa. Asiakkaita, joilla ei ollenkaan ollut virusturvaa tai se oli vanhentunut, opastettiin virusohjelmien käyttöön ja näytettiin mistä maksuttomia virusohjelmia löytää.

Ongelmalliseksi on osoittautunut rekisteröiminen, joka pitää tehdä aina vuoden välein. Asiakkaiden osaaminen ei usein riitä tämän toiminnan suorittamiseen. Tieto päivitystarpeesta tuo asiakkaat uudemman kerran pisteeseen. Jos asiakas varaa ajan, voidaan päivittäminen tehdä hänen kanssaan, jolloin uskallus itsenäisesti tehtävään päivittämiseen lisääntyy.

Kansalaisen Mikrotuessa on huomattu asiakkaiden tietotason kasvu. Jos aiemmin asiakkaan ilmoittama vika oli niinkin epämääräinen kuin ”kone ei toimi” tai ”kone on hidas”, nykyisin toivelistalta löytyy jo muun muassa käyttöjärjestelmän uudelleenasennusta, tiettyjen ohjelmien asennusta, peruspuhdistusta koneelle, haittaohjelmien tarkistus ja poisto sekä mahdollisesti kovalevyn eheytys. Lisäksi asiakirjojen ja kuvien talteenottojen määrä rikkoutuneelta kovalevyltä on kasvanut.

Yksi useimmin esiintyvistä ongelmista löytyy ohjelmistosta, kuten käyttöjärjestelmän oikuista tai päällekkäin asennetuista virustorjuntaohjelmista. Myös laitevikoja löytyy asiakkaiden koneista melkein kaikista komponenteista; rikkoutuneista virtalähteistä muistikampojen kautta emolevyihin. Ohjelmistopuolen ongelmat vaihtelivat vähintään yhtä paljon kuin laiteviat.

Yleisimmät riskit voivat aiheutua esimerkiksi päivitysten laiminlyönnistä. Uusia viruksia luodaan jatkuvasti, joten torjuntaohjelman tunnisteet on syytä pitää myös ajan tasalla. Yksi perinteisimmistä tavoista levittää virusta on ollut sähköpostien liitetiedostojen kautta. Asiakkaat ovat avanneet viestejä ilman että ovat olleet varmoja lähettäjistä.

Hyvä ohjenuora turvalliseen verkkoselaukseen on tietysti pysyä tutuilla ja turvallisiksi todetuilla verkkosivuilla. Uudet, vähänkään epäilyttävät verkkosivut, voi tarkistuttaa erinäisillä työkaluilla, joista moni toimii automaattisesti selaimen liitännäisenä. Selain kannattaa myös pitää ajan tasalla.

Käyttäjätunnusten ja salasanojen tallennusta selaimeen ei suositella, varsinkaan ilman pääsalasanaa. Tallennettuina ne ovat erittäin helposti saatavissa kenelle tahansa, joka pääsee fyysisesti tietokoneelle tai jopa etäyhteydellä. Salasanat ovat myös usein liian lyhyitä ja täten helppoja arvata tietokoneelle. Vastoin yleistä käsitystä, 8-merkkinen salasana, joka sisältää erikoismerkkejä, isoja kirjaimia ja numeroita on tietokoneelle helpompi arvata, kuin 20-merkkinen helposti muistettava lause tai sarja sattumanvaraisia sanoja.

Tietojen kalastelu eli ”phishing” on lähivuosina tullut hyvin suosituksi huijauskeinoksi. Tämän takia kannattaa aina miettiä kahteen kertaan, mihin sivustolle on syöttämässä luottokorttitietojaan tai mihin sähköpostiin lähettää vastauksena tilinumeronsa. Usein phishing -sivustot ovat taitavasti naamioitu näyttämään alkuperäiseltä sivustolta, kuten vaikka pankin kotisivulta. Eron useimmiten huomaa sivuston web-osoitteesta ja sivuston salauksesta. Kaikkien pankkien sivustot ovat suojattuja.

Henkilökohtaisia tietoturvariskejä on paljon, mutta niin on myös keinoja välttää ne. Samalla kun rikolliset kehittävät uusia keinoja hyväksikäyttää uusimmat tietoturva-aukot, sovelluskehittäjät tekevät töitä niiden paikkaamiseen ja estämiseen. Paras yksittäinen vinkki tietoturvan säilyttämiseen on maalaisjärjen käyttö ja jos internetissä on jotain liian hyvää ollakseen totta, se on useimmiten huijausyritys. Etenkin pankki- tai viranomaisasiointeihin liittyviä tunnuksia ja salasanoja ei kannata säilyttää sähköpostissa tai puhelimessa jossa on nettiyhteys.

Kotikoneet ovat alttiita hyökkäyksille, koska ihmiset joko uskovat että heidän koneidensa tietoturva on riittävä tai että heidän koneillaan ei ole mitään hakkereita kiinnostavaa. Tutkija Rick Walls toteaa kirjoituksessaan *Folk Models of Home Computer Security*, että kansalaiset löytävät useita tapoja siirtää vastuun tietoturvasta jollekin ulkoiselle taholle. Taho voi olla tekninen väline kuten palomuuri tai sosiaalinen kuten toinen ihminen tai IT-henkilöstö tai instituutio kuten pankki. Käyttäjät tekevät näin koska he kokevat, että heillä ei ole riittäviä taitoja kunnollisen tietoturvatason ylläpitämiseksi.

Microsoftin tutkimuksen mukaan (Microsoft Oy, Lehdistötiedote 7.2.2012) suomalaiset ovat Euroopan priimuksia tietoturvassa. Alla on koottuna tutkimuksen tuloksia Suomesta ja suluissa koko Euroopan tulos:

- 85 prosenttia (57) päivittää tekee ohjelmistopäivityksiä ja/tai pitää automaattipäivitystä päällä
- 76 prosenttia (61) käyttää vahvoja salasanoja
- 64 prosenttia (51) tekee ostoksia vain luotettavista sivustoista
- 52 prosenttia (31) luo jokaiselle käyttäjätililleen oman salasanan
- 36 prosenttia (27) toimii verkkomaineensa suojelemiseksi
- 24 prosentilla (18) on virustorjuntaohjelma mobiililaitteessaan.

Yritysten henkilökunta koostuu yksilöistä, joista monet käyttävät työkoneitaan myös muissa kuin työtehtävissään. Vastaavasti kotikoneissa käytettyjä siirrettäviä tallennusvälineitä saatetaan tuoda työkoneisiin. Yhteiskunnan ja yritysten kannalta on tärkeää että yksilöiden tietoturvaosaamista lisätään. Tähän henkilökohtaisen tietoturvan parantamiseen tähdätään Kansalaisen Mikrotuessa.

Kansalaisen Mikrotuessa yleisimmin asiakkaille suositeltuja toimintoja ja ohjeita ovat:

- Tunnetuimmilta sivuilta harvemmin tulee viruksia.
- Virukset tulevat koneille useimmiten itse ladatuista tiedostoista.
- Virustunnisteet ja Windowsin päivitykset pidettävä ajan tasalla.
- Sähköpostien linkkien kanssa kannattaa olla varovainen, jos ei tunne lähettäjää tai viesti vaikuttaa epänormaalilta. Myös sähköpostien kuvien kautta voi saada viruksia.
- Oltava varovainen sähköpostien liitetiedostojen kanssa.
- Virukset voivat levitä myös pdf-tiedostoista.
- Säännölliset virustarkistukset auttavat.
- Salasanojen tallentaminen selaimeen ei suositeltavaa, jos useita käyttäjiä.
- Jos salasanat ovat muistissa lapulla, pidä lappu piilossa.
- Kannettavaa ei näkyville autossa.

LÄHTEET

Pietikäinen, Rami, Salko, Severi, 2011. Kansalaisen Mikrotuen loppuraportti.

Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective; Journal of the Association for Information Systems Vol. 11 Issue 7 pp. 394–413 July 2010.

Rick Wash, 2010. "Folk Models of Home Computer Security" Proceedings of the Symposium on Usable Security and Privacy.

Rick Wash and Jeff MacKie-Mason, 2008. "A Social Mechanism for Home Computer Security." Workshop on Information Systems and Economics (WISE). December 2008.

Microsoft, 2012. http://blogs.technet.com/b/tiedotteet/archive/2012/02/07/suomalaiset-euroopan-priimuksia-tietoturva-asioissa.aspx Viitattu 26.8.2013.

Kansalaisen Mikrotuen kevään 2012 projektipäällikkö Patrik Birkströmin haastattelu (26.4.2012). Julkaisematon.

World Economic Forum. The Global Information Technology Report 2013. http://reports.weforum.org/global-information-technology-report-2013/ Viitattu 26.8.2013.

Vulnerability Laboratory, 2012. http://www.vulnerability-lab.com/get_content.php?id=529 Viitattu 26.8.2013.

Viestintävirasto, 2012. http://www.cert.fi/tietoturvanyt/2012/06/ttn201206061430.html Viitattu 26.8.2013.

MTV3, 2013.http://www.mtv3.fi/uutiset/it.shtml/facebookissa-vakava-haavoittuvuus---zuckerbergin-profiiliin-murtauduttiin/2013/08/1793179 Viitattu 26.8.2013.

Jonathan Rudenberg, 2012. http://titanous.com/posts/twitter-facebook-venmo-sms-spoofing Viitattu 26.8.2013.

TIKOTRAIN-PROJEKTIPAJAN PALVELUT PK-YRITYKSILLE

Jana Pullinen, FM
Lehtori, Tietojenkäsittelyn koulutusohjelma, Turun ammattikorkeakoulu

TiKoTrain-projektipaja on Turun ammattikorkeakoulun tietojenkäsittelyn koulutusohjelman projektipaja, jossa opiskelijalla on mahdollisuus suorittaa projektimuotoisia opintoja. TiKoTrainiin haetaan virallisen hakuprosessin kautta, jolloin opiskelija saa myös oppia työn hakemisesta. Projekteja käynnistyy sujuvasti syyskuusta toukokuuhun, joten tehtävien suorittaminen ei ole välttämättä sidottu mihinkään opintojaksoon. Näin pystymme palvelemaan alueen PK-yrityksiä läpi vuoden, lukuun ottamatta kesäkuukausia. Projekteja pystytään kuitenkin myös integroimaan opetussuunnitelmassa oleviin opintojaksoihin tarpeen mukaan.

Opiskelijat tekevät projekteja projektipäälliköinä. Isomman projektin ollessa työn alla, projektipäälliköt voivat hakea resursseja muista opiskelijoista. Projektipäälliköt ovat mukana TiKoTrainissa 1–2 vuotta, jotkut jopa koko opintojensa keston ajan ja he työstävät projekteja itsenäisesti ohjaavan opettajan avulla.

TiKoTrainin toimii tärkeänä linkkinä koulun ja alueen yritysten välillä. Projektien myötä ammattikorkeakoulu saa arvokasta informaatiota alueen tämänhetkisistä tarpeista ja opiskelija saa tuntumaa aidossa ympäristössä tehtävästä projektista. Näin pystytään muokkaamaan koulutustarjontaa yritysmaailmaa yhä paremmin palvelevaksi. Projektien olleessa laajoja opiskelija voi halutessaan jatkaa työtään aina opinnäytetyövaiheeseen saakka ja näin laajentaa sekä syventää osaamistaan aiheeseen liittyen. Aina niin tärkeä tietoturva on läsnä kaikessa opetuksessa aina määrittelystä dokumentointiin saakka.

TIKOTRAIN-WWW-OHJELMOINTIPROJEKTIT

TiKoTrainissa opiskelijat voivat suorittaa erityyppisiä projekteja. Suosituimpia ovat olleet www-ohjelmointiprojektit, jossa PK-yritykselle luodaan kotisivut markkinoimaan yrityksen toimintaa. Tietoturva-asiat ovat erityisen tärkeässä roolissa näissä projekteissa. Myös tietoturvasta tiedottaminen asiakkaalle on jatkuvasti läsnä eli projektipäällikkö ei lähde suin päin toteuttamaan asiakkaan vaatimuksia vaan valistaa asiakasta eri mahdollisuuksista sekä seurauksista mahdollisuuksiin liittyen. Kotisivujen työstäminen aloitetaan aina vaatimusmäärittelyllä. Vaatimusmäärittelyn avulla projektipäällikkö pystyy myös arvioimaan projektin laajuuden sekä keston.

TIETOTURVAPÄIVÄ PK-YRITYKSILLE

Tietojenkäsittelyn koulutusohjelma järjestää vuosittain tietoturvapäivän PK-yrityksille. Projekti kestää noin 7 kuukautta ja työllistää 4–6 opiskelijaa. Projekti aloitetaan heti syyskuussa kesälomien jälkeen ja projekti päättyy helmikuisen päivän jälkeen. Tietoturvapäivä on laajentunut vuosi vuodelta ja projektin myötä pyrimme saattamaan tietoturva-asioita niin PK-yrittäjän kuin tavallisen kansalaisenkin tietoisuuteen. Projektin tärkeimmät osa-alueet ovat esiintyjien varmistaminen ja markkinointi yrityksille ja yhteisöille. Itse päivässä on mukana myös nuorempia opiskelijoita auttamassa käytännön järjestelyiden kanssa. Aiheet on pyritty valitsemaan siten, että kuulijat saisivat mahdollisimman paljon käytännönläheistä tietoutta. Tulevaisuudessa tietoturvapäivää tullaan edelleen kehittämään aina ajankohtaisten asioiden suuntaan.

TIETOTURVASIVUSTO PK-YRITYKSILLE

Tietoturvapäivän ohella tarjoamme tietoturvatietoutta www.tietoturvapäivä.fi-sivustomme kautta. Tietoturvasivustoa ylläpidetään viikoittain kahden opiskelijan toimesta. Projekti miehitetään helmikuisen tietoturvapäivän jälkeen ja opiskelijat työstävät projektia aina seuraavaan tietoturvapäivään saakka. Tässä projektissa opiskelijat saavat kokemusta siitä, mitä pitkäkestoinen projekti pitää sisällään. Tietoturvasivusto-projektin hektisimmät hetket ovat, kun ilmoittautumissivusto avataan ja sivusto valmistellaan seuraavaa tietoturvapäivää varten. Esiintyjien yritysten logot ja esitysten aiheet julkaistaan sivustolla

syksyn aikana ja näitä tarkennetaan aina viimeiseen hetkeen saakka. Itse tietoturvapäivän aikana sivustolle viedään esitysmateriaalit. Tietoturvasivustolta PK-yrittäjä löytää paitsi esitysmateriaalit tietoturvapäivistä myös nettilinkkejä, joista on hyötyä yrittäjän arjessa. Emme kirjoita asioita uusiksi vaan olemme luoneet sateenvarjoportaalin tietoturva-asioiden löytymisen helpottamiseksi.

TIETOTURVATESTI

Tietoturvasivuston www.tietoturvapäivä.fi yhteydessä on myös tietoturvatesti, jonka jokainen voi käydä tekemässä useampaankin otteeseen. Testi on anonyymi eli mitään henkilötietoja tai yrityksen tietoja ei tarvitse antaa eikä testin tuloksia talleteta mihinkään. Testin avulla testin tekijä havahtuu miettimään tietoturvaa omassa toiminnassaan. Kysymykset tulevat tietokannasta ja tietoturvapäiväsivuston ylläpitäjät huolehtivat siitä, että kysymyksiä tulee kantaan jatkuvasti lisää.

TIETOTURVA-AUDITOINTI

Jotta tietokantaan saadaan lisää kysymyksiä, tarvitsemme apua tietoturva-auditointeja tekevältä projektiryhmältä. Tietoliikenteen opiskelijat työstävät PK-yritykselle tietoturva-auditointiprojektia, jossa laaditaan kysymyspatteristoa yrittäjälle. Samaiset kysymykset viedään myös tietokantaan, josta ne arvotaan tietoturvatestiin. Itse tietoturva-auditointi tehdään PK-yrityksessä ja tämän auditoinnin tarkoitus on herättää henkilökuntaa miettimään yrityksen tietoturva-asioita. Auditointi on luottamuksellinen ja tietoa siitä ei viedä muille kuin projektiryhmän jäsenille ja ohjaavalle opettajalle. Mikäli PK-yrittäjä sallii, tuloksia voidaan analysoida tiimityönä seuraavan projektin yhteydessä.

TiKoTrain-projektipaja kannustaa opiskelijoita miettimään projektien jatkumoa sekä asiakaspalvelua PK-yritykselle. Ohjaavana opettajana pidän tärkeänä sitä, että aina ei lähdetä luomaan uutta ja romuteta vanhaa olemassa olevaa. Usein työelämään astuessa opiskelija pääsee ensimmäisenä työstämään ylläpitoa johonkin projektiin oman uuden ja ihmeellisen tuotoksen sijaan. Toisen tuotoksen lukeminen, ymmärtäminen ja muuttaminen ovat käytännössä vaativaa työtä, jopa vaativampaa kuin uuden luominen.

TIETOTURVALLISUUS – TEKNIIKKAA VAI IHMISEN TOIMINTAA?

Esko Sillanpää, Ins. (AMK), LuK
IT-pääsuunnittelija, tietoturvavastaava, IT-toiminta,
Turun ammattikorkeakoulu

”Tietoturvallisuudesta tehdään jatkuvasti uusia tutkimuksia. Niiden tulokset viestivät karkealla tasolla ongelman olevan ihmisissä ja heidän toiminnassaan, ei niinkään tekniikassa, ohjelmistoissa tai resurssien vähyydessä. Kun toisaalta seurataan organisaatioiden omia päätelmiä siitä, miten tietoturvallisuuden tasoa voidaan nostaa, ovat vastaukset hyvin teknologiaorientoituneita. Tyypillisiä vastauksia ovat: tarvitsemme palomuurin, virustorjunnan tai kassakaapin”. (Jaakohuhta, 2001.) Mutta onko asia todella näin yksinkertainen?

Tiedetään, että ihmisen toiminta on suuri resurssi tietoturvallisuuden toteuttamiselle, mutta samalla se on myös mahdollinen uhka. Niin organisaatiot kuin tietoverkot ja -järjestelmät tarvitsevat toimiakseen ihmisen, jolloin ihmisestä tulee erottamaton osa tietoturvallisuutta. Todennäköisimmät tietoturvauhat ja niistä aiheutuvat riskit ovat sekä käyttäjälähtöisiä että tietoverkkojen ja -tietojärjestelmien ylläpitäjälähtöisiä. Tietoturvaongelmat voivat syntyä tahattomasti tai tahallisesti. Käyttäjät voivat toimia varsin itsenäisesti ja sivuuttaa organisaation tietoturvallisuuden hallinnolliset ja tekniset ratkaisut. Näin toimiessaan he saattavat luoda haavoittuvuuksia organisaation tietoverkkoon ja -järjestelmiin. Tietoverkkojen ja -tietojärjestelmien ylläpitäjältä voi jäädä huomaamatta vakavimmat tietoturvauhat. Näitä haavoittuvuuksia ja tietoturva-uhkia verkkorikolliset osaavat käyttää hyväksi ja toisaalta yhä useammin tekijä voi olla kuka tahansa kaupallisen tuotteen internetkäyttäjä.

Väitetään, että organisaation johdon tehtävänä on osoittaa henkilöstölle ja muille sidosryhmille selvä suunta ja näyttää tukensa ja sitoutumisensa tietoturvallisuuteen luomalla koko organisaatiota koskeva tietoturvallisuuspolitiikka ja -strategia sekä ylläpitämällä sitä. Tietoturvapolitiikkaan sisältyvät periaatteet ovat organisaation toiminnasta lähteviä vaatimuksia, jotka ovat teknisistä to-

teutustavoista tai järjestelmistä riippumattomia. Tietoturvapolitiikka ja niistä seuraavat käyttäjien ja ylläpitäjien tietoturvaohjeet ovat keskeinen lähtökohta tietoturvallisuuden kehittämiselle organisaatiossa.

”Mutta miten organisaatio voi toteuttaa tietoturvallisuutta, jos organisaation jäsenillä ei ole aavistustakaan, mihin tekijöihin pitäisi kiinnittää huomiota?” (Jaakohuhta, 2001)?

ORGANISAATION TIETOTURVALLISUUDEN UHAT

Tietoturvauhkia voi aiheuttaa tietojärjestelmien hankintaan, suunnitteluun ja kehittämiseen liittyvät haasteet, tietojärjestelmien ja tietoverkon infrastruktuuriin liittyvät haavoittuvuudet, käyttäjien toiminta sekä näiden ehkäisemisessä käytettävät tietoturvallisuusmenetelmät ja tietoturvateknologiat.

Yksittäisiä tietoturvallisuuteen kohdistuvia tietoturvauhkia, jotka liittyvät minkä tahansa organisaation päivittäiseen toimintaan, on rajattomasti. Uusia uhkia syntyy koko ajan ja osa vanhoista poistuu. Jotta uhkiin voidaan varautua, on ne tunnettava. Nykyisin tyypillisimpiä ja tavallisimpia tietoturvauhkia aiheutuu seuraavista:

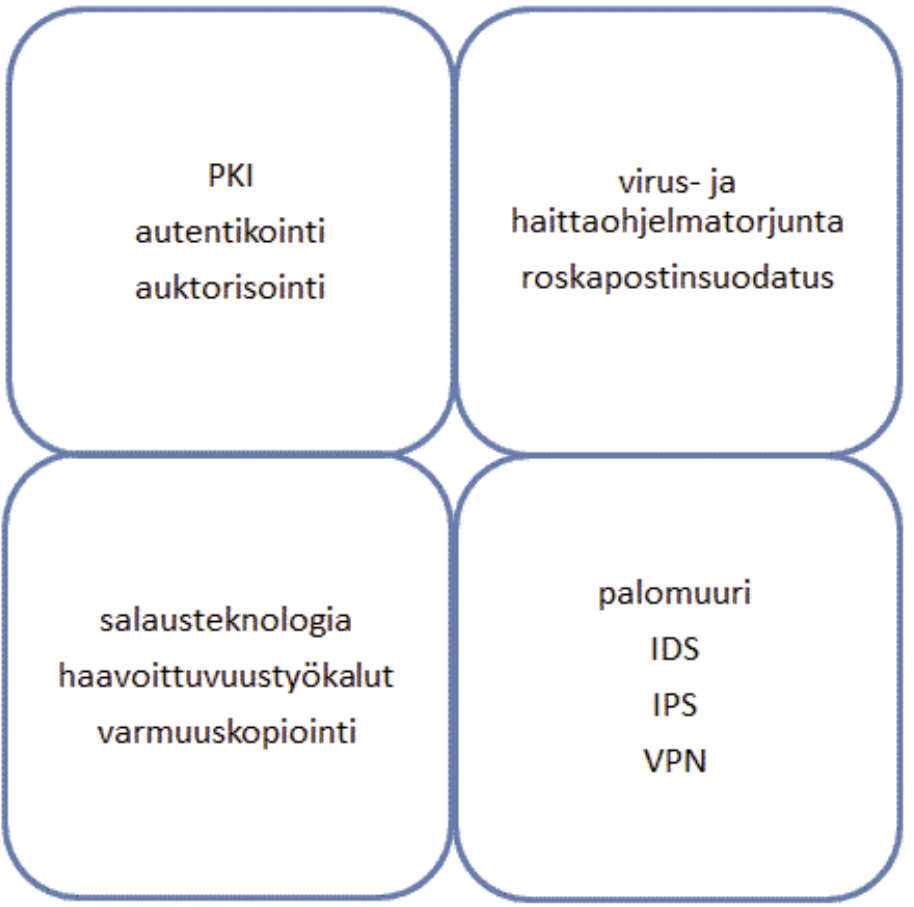
- internetin käyttämisestä ilman ajantasaista virustorjuntaa
- puutteellisista haittaohjelmien ja virusten torjuntajärjestelmistä
- nettiselaimen tietoturva-aukoista
- langattomien verkkojen käyttämisestä ilman salausta
- ohjelmistotuen saatavuusongelmista
- käyttöympäristön työskentelyolojen turvattomuudesta
- pääsyoikeuksien ja käyttövaltuuksien puutteellisesta hallinnasta ja valvonnasta
- puutteellisista tietojenkäsittelylaitteistojen ja käyttöjärjestelmien päivityksistä
- tahallisista ja tahattomista virheistä tai rikkomuksista
- perehdytyksen ja koulutuksen puutteista

- heikkojen salasanojen käytöstä
- käyttäjätunnusten ja salasanojen luovuttamisesta ulkopuolisille
- järjestelmien toiminnallisten ja teknisten vaatimusten määrittelyn puuttumisesta tai puutteista
- tulostamisesta
- mobiililaitteiden, sovellusten ja pilvipalveluiden käyttämisestä
- sosiaalinen hakkerointi, ”kalasteluviesteistä”
- sosiaalisen median tietoturva-aukoista
- vertaisverkkojen sovelluksista
- virtuaalikoneympäristöstä.

Organisaation toiminta tulee arvioida järjestelmällisesti ja kaikki uhkat on käytävä läpi. Tähän tarkoitukseen on olemassa erityisiä menetelmiä, jotka pyrkivät varmistamaan kaikkien uhkien mukaantulon kartoitukseen. Kun tiedetään, miten hyvin jotakin tietoa halutaan suojata, voidaan valita sille asianmukainen säilytystapa ja riittävät suojaustoimenpiteet.

TIETOTURVATEKNOLOGIA VIE?

Tietoturvallisuus ja sen teknologia on vaikea ja monimutkainen alue. Tietoturvateknologiaan liittyy monenlaisia osa-alueita (kuva 1), kuten virus- ja haittaohjelmatorjunta, autentikointi (todennus), auktorisointi (valtuutus), julkisten avainten järjestelmä (Public Key Infrastructure, PKI), salausteknologiat, haavoittuvuustyökalut, VPN (VirtualPrivateNetwork) -ratkaisut, palomuurit, tunkeutumisen havainnointi (Intrusiondetectionsystem, IDS) ja tunkeutumisen esto (Intrusion prevention system, IPS), roskapostinsuodatus ja varmuuskopiointi. Organisaatio, joka haluaa suojata tietoverkkonsa ja sen palvelut sekä turvata liiketoimintansa jatkuvuuden, joutuu arvioimaan näistä jokaisen osa-alueen merkitystä omalle toiminnalleen ja tietoturvallisuudelleen.



KUVIO 1. *Tietoturvateknologian yhteentoimivuus ja hallinta.*

Usein tietoturvallisuus nähdään teknisenä ongelmana, johon on löydettävissä tekninen ratkaisu. Siksi useimmat organisaatiot aloittavatkin tietoturvallisuuden kehittämisen erilaisilla teknisillä suojaus-menetelmillä. Tällöin teknologian hankintaa saattaa ohjata usko teknologian kaikkivoipaisuuteen, teknologinen determinismi. Teknisen kehityksen uskotaan suojaavan organisaation toimintaa ja toimintaprosesseja ihmisen puutteellisista tiedoista ja taidoista aiheutuvilta uhkilta tai jopa vaikuttaa ihmisen asenteisiin ja tietoisuuteen omasta toiminnastaan ja niiden vaikutuksesta tietoturvallisuuteen.

Vaikka tietoturvatietoisuus on osa tietoturvallisuutta, ei tietoisuudesta ole hyötyä ilman tehokasta tietoturvan teknistä ja toiminnallista toteutusta. Teknologinen muutos pitäisi käsittää pelkkää teknistä muutosta laajemmaksi prosessiksi. Hyvän tietoturvallisuuden toteuttamisessa ihmisten rooli on keskeinen ja vain osa voidaan hoitaa teknologian avulla.

IHMISEN TOIMINTA – UHKA JA MAHDOLLISUUS

Tietoturvan loukkaukset johtuvat varsin usein inhimillisistä tietojärjestelmän käyttöön tai ylläpitotehtäviin liittyvistä toimista. Tiedon häviäminen ja muuttuminen johtuvat useimmiten käyttäjän tai ylläpitäjän tahattomista teoista, vahingoista, tietämättömyydestä tai osaamattomuudesta. Monet tietojärjestelmät ovat lopulta murtuneet järjestelmiä käyttäneiden tai ylläpitäneiden ihmisten taholta.

Ihmisen toimenpiteet perustuvat vastuiden, velvollisuuksien ja ohjeiden hyödyntämiseen tietoturvallisuuteen liittyvissä toimissa. Työntekijöille on opetettava tietoturvallisuuden peruskäsitteet ja tietototurvallisuuden merkitys organisaatiolle. Heidän on ymmärrettävä, millainen vaikutus heidän toiminnallaan on ja kuinka se vaikuttaa organisaation tietoturvallisuuteen. Käyttäjät on koulutettava hallitsemaan ne taidot, joita he tarvitsevat työnsä turvalliseen suorittamiseen, ja turvallisuudesta huolehtivat on koulutettava toteuttamaan ja ylläpitämään tarvittavat turvavalvontamekanismit.

ORGANISAATION TIETOTURVALLISUUDEN KEHITTÄMINEN

Tarkastelen Turun ammattikorkeakoulun tietoturvallisuuden kehittämistä havainnoimalla ihmisen toimintaa, normaalia päivittäistä tietoverkon ja sen palveluiden käyttöä, mittaamalla haittaohjelmien määrää sekä tulkitsemalla tietoturvapoikkeamista tehtyjä raportteja. Tavoitteena on etsiä näiltä osin vastausta kysymykseen, kumpi voi toteuttaa parempaa tietoturvaa: tekniikka vai ihminen?

Tietoturvallisuustehtävät ulottuvat ammattikorkeakoulun johdosta, sovellusten vastuuhenkilöistä ja järjestelmien ylläpitäjistä aina järjestelmien peruskäyttäjiin saakka. Ylin johto vastaa tietoturvallisuuden toteutumisesta laatimansa tietoturvapolitiikan mukaisesti. Teknisten asiantuntijoiden tehtävänä on sovel-

taa ja toteuttaa tietoturvapolitiikkaa omaa erikoisasiantuntemustaan hyödyntäen ja vastata tietoturvallisuustoimenpiteiden huomioon ottamisesta omalla vastuualueellaan noudattaen hyvää tietoturvallisuus- ja ylläpitotapaa. Käyttäjien tehtävänä on tuntea annetut ohjeet ja noudattaa niitä sekä raportoida havaitsemistaan ongelmista, uhkista ja ohjeiden vastaisista menettelyistä.

Nimetyt tietoturvavastaavat ja jokainen työntekijä oman toimintaympäristönsä osalta valvovat ja seuraavat, että tietoturvaohjeistus on käytössä ja sitä noudatetaan sekä ylläpidetään tietoa tietoturvauhista, jotka ovat ammattikorkeakoulun kannalta merkittäviä.

Tietoturvallisuuden hallinta muodostuu toteutusteknisestä tarkastelukulmasta. Varsinainen tietoturvasuunnitelma on kehittämisen kohteena, jossa esimerkiksi tietoturvallisuuden vaikutusta arvioitaisiin ammattikorkeakoulun toimintaan, jollakin systemaattisella menetelmällä, johdon ja toimintaprosessien omistajien näkökulmasta.

YHTEISÖTILAAJA

Turun ammattikorkeakoulu toimii myös yhteisötilaajana (työnantaja), joka käsittelee viestintäverkossaan luottamuksellisia viestejä, tunnistamis- ja sidosryhmätietoja sekä henkilötietoja, joista osa voi olla arkaluontoisia. Hallinnon ja opetuksen tulosalueilla käsitellään todellisia työelämän tietoja, jotka ovat osin salassa pidettäviä, kuten potilas-, katsastus- ja tilitiedot sekä harjoittelupaikkojen ja opinnäytetöiden toimeksiantajaorganisaatioiden liikesalaisuudet. Ammattikorkeakoulu noudattaa toiminnassaan julkisuuslain (621/1999) mukaista hyvää tiedonhallintatapaa ja henkilötietolakia (523/1999). Muita tietosuojan kannalta keskeisiä säädöksiä ovat sähköisen viestinnän tietosuojalaki (516/2004) ja yksityisyyden suoja työelämässä (759/2004). Yhteisötilaajan velvollisuus on huolehtia toiminnan turvallisuuden, tietoliikenne-, laitteisto-, ohjelmisto- ja tietoaineistoturvallisuuden varmistamisesta.

Mutta onko tietoturvallisuuden haluttu taso saavutettu, kun tietoturvallisuuden organisatoriset ja hallinnolliset toimet sekä tekniset ratkaisut on määritelty ja toteutettu?

SAANKO KÄYTTÄJÄTUNNUKSESI JA SALASANASI?

Tyypillisiä käyttäjän aiheuttamia tietoturvauhkia ovat helposti murrettavat salasanat, sähköpostin ja internetin huoleton käyttö. Käyttäjätunnus ja salasana luovutetaan kovin helposti työkaverille, vierailijalle tai sähköpostilla ”kalasteluviestissä” ulkopuolisille pyytäjille.

Käyttäjälle on kerrottava ja hänen pitää ymmärtää, mitä käyttäjätunnus ja salasana merkitsevät. Käyttäjätunnus yksilöi käyttäjän ja salasana todentaa hänet. Nämä yhdessä tietojärjestelmän pääsynvalvonnan kanssa antavat käyttöoikeudet ja valtuutuksen tehdä toimenpiteitä kohdejärjestelmässä. Muun kuin oman käyttäjätunnuksen käyttäminen on allekirjoituksen väärentämistä. Käyttäjätunnus ja salasana ovat henkilökohtaisia, eikä niitä saa eikä tarvitse luovuttaa missään tilanteessa kenellekään toiselle.

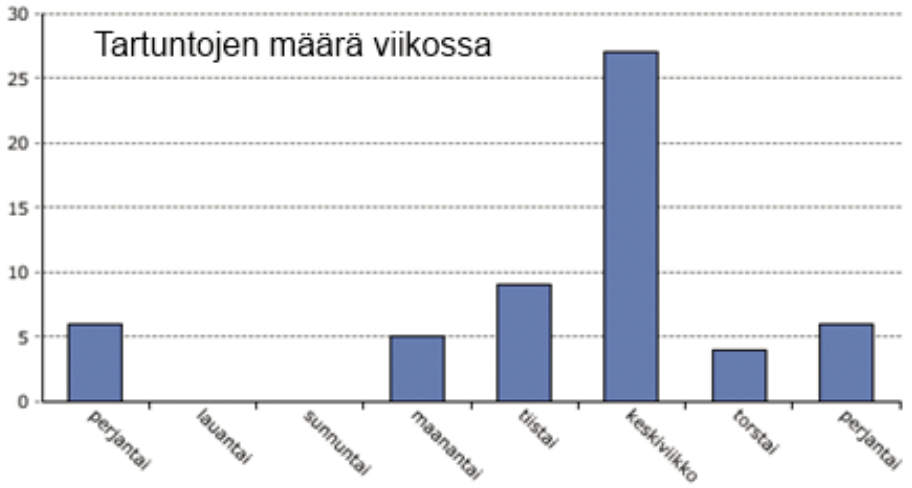
Usein kuulee väitteen: ”Ei minulla ole mitään salaista tietoa eikä meillä, koska olemme julkinen yhteisö ja meillä on vain julkista tietoa”. Kaikella tiedolla, niin julkisella, salaisella kuin arkaluontoisellakin, on samat tiedon ominaisuudet: luottamuksellisuus, eheys ja saatavuus. Tietoturva perustuu näihin tietojen ominaisuuksien väliseen tasapainoon, josta huolehditaan oikein mitoitetuilla suojaustoimenpiteillä. Julkisella tiedolla huomio keskittyy tiedon eheyteen sekä saatavuuteen ja luottamuksellisuuden vaatimusta voidaan vähentää. Tietoturvallisuustaso ja sen mukaiset tietoturvatoimenpiteet on määritelty tietoaineistojen ja tietojärjestelmien luokittelulla tietoaineistojen luottamuksellisuuden ja tietojärjestelmien tärkeyden mukaan.

HAITTAOHJELMIEN TORJUNTARAPORTTI TIETOTURVALLISUUDEN MITTARINA

Virukset ja muut haittaohjelmat muodostavat edelleen merkittävän osan tietoturvallisuuden uhkista. Erilaisten haittaohjelmien määrä ja tyypit ovat jatkuvassa kasvussa. Niiden tavoitteena on yhä enenevässä määrin yleisen haitanteon sijaan varastaa käyttäjien luottamuksellisia tietoja verkkopetoksia tai identiteettivarkauksia varten.

Haittaohjelmien hälytykset, joiden yksityiskohtaista raporttia ei esitellä salassapitovelvoitteen vuoksi, jakaantuvat troijalaisiin, matoihin, mainos- ja vakoiluohjelmiin. Tartuntahälytyksiä tarkastellaan marraskuun 2012 yhden viikon

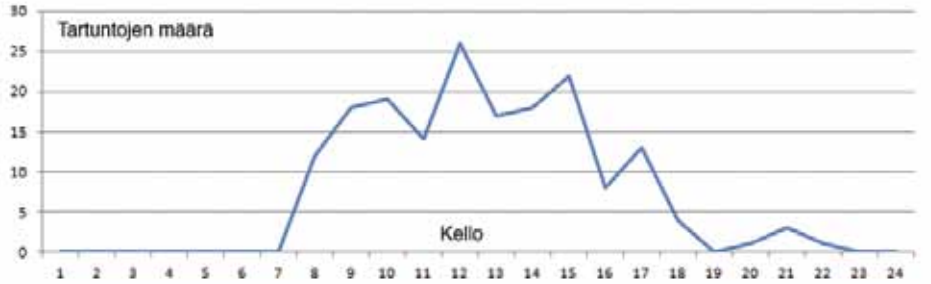
perjantaista perjantaihin (kuva 2) välisenä aikana sekä yhden vuorokauden tartuntahälytysten määrää (kuva 3) puolen vuoden ajalta. Absoluuttinen haittaohjelmien määrä vaihtelee 0–27 kappaletta tarkastelujaksojen aikana. Järjestelmä havaitsee verkossa työasemien määräksi noin 2 600. Todellinen aktiivisten käyttäjien määräksi voidaan olettaa noin 2 000 henkilöä. Haittaohjelmien määrä ei ole suuri, mutta jokainen niistä on mahdollinen uhka tietoturvalle. Suurin osa haittaohjelmista on troijalaisia. Tartuntojen lähteinä ovat sähköpostin ja internetin käyttö.



KUVA 2. *Tartuntahälytysten määrä viikon ajalta eri viikonpäivinä, marraskuu 2012.*

Erityisesti mielenkiinto kohdistuu viikkotarkastelussa (kuva 2) viikonlopun ja työpäivien väliseen tartuntahälytysten määrän eroon. Viikonloppuna, jolloin järjestelmien käyttöaste on vähäinen, ei tartuntahälytyksiäkään esiinny. Työviikon aikana järjestelmien käyttöasteen ollessa suurimmillaan tartuntahälytysten määrä kasvaa vaihtelevasti päivittäin.

Päiväkohtaisessa tarkastelussa (kuva 3) havaitaan, että tartuntahälytysten määrä kasvaa työpäivän alkaessa kello seitsemän, vähenee taukojen kello 11 ja 14 aikana ja loppuu noin kello 21 jälkeen. Käyrä kuvaa omalta osaltaan tyypillistä ihmisen toiminnan arkea, kello 7 ja 21 välisen ajan, jolloin tietoverkon ja sen palveluiden käyttöaste on suurimmillaan.



KUVA 3. *Tartuntahälytysten määrä vuorokauden aikana puolen vuoden ajalta.*

Troijalaiset ja nykyisin myös madot tulevat yleensä viestien mukana, ja niissä hyödynnetään sosiaalisen hakkeroinnin keinoja. Viesteissä on myös linkkejä verkkosivuille, joilta käyttäjän koneelle latautuu tietoja varastelevia haittaohjelmia, tai huijaussivustoille, jotka ovat samankaltaisia kuin tietojenkalastelu-hyökkäyksissä käytetyt. Molemmat tyypit, troijalainen ja näissä tilanteissa myös mato, vaativat toimiakseen käyttäjän aktiivista toimintaa, joko tietoista tai tahatonta.

Usein kuulee käyttäjältä ja jopa järjestelmien ylläpitäjiltä kommentin: ”Onhan meillä palomuuri ja virustorjunta, joilla nämä estetään”. Onko perusteltua olettaa, että joissakin tapauksissa usko teknologian kaikkivoipaisuuteen heikentäisi yksilön, ymmärrystä ja harkintaa, vastuullista tietoverkon ja sen palveluiden käyttämistä sekä tietoturvatietoisuutta?

Ammattikorkeakoulun toiminta pakottaa päästämään palomuurin läpi aina osan tietoliikenteestä. Näin palomuuri ei suojaa kaikelta. Esimerkiksi verkkohyökkäykset, jotka kulkevat osana normaalia sähköposti- tai webliikennettä, pääsevät palomuurin läpi ja juuri tätä heikkoutta esimerkiksi verkkorikolliset hyödyntävät tarkoituksenaan kaapata tai huijata luottamuksellisia tietoja omiin rikollisiin käyttötarkoituksiinsa.

Haittaohjelmien torjuntajärjestelmä suojaa tietoja ja tietojärjestelmiä sekä ammattikorkeakoulun ydintoimintaa vain sen mahdollistamin keinoin sekä sen mukaan mitä ihminen on sille määritellyt.

YHTEENVETO

”Kun tarkastellaan tietoturvallisuudesta käytävää julkista keskustelua, se on kovin tekniikkapainotteista. Keskusteluissa esiintyvissä ongelmissa harvoin viitataan muuhun kuin aineellisiin ongelmiin. Perusteluina ongelmille on usein tiettyjen laitteiden, ohjelmistojen sekä rahan ja henkilöstön puute”. (Jaakohuhta, 2001.) Tyypillinen ratkaisu organisaation tietoturvallisuutta parannettaessa on hankkia joukko teknisiä ratkaisuja. Usein nämä tekniset ratkaisut ovat oikeissa paikoissa ja oikein käytettynä hyviä, mutta voiko organisaation tietoturvallisuuden parantamisen lähtökohtana olla suunnittelemattomasti ostetut tietoturvatuotteet? Tietoturvallisuus ei ole tuote, se ei myöskään ole palvelu, jonka voi sellaisenaan ostaa ilman organisaation omaa panostusta.

Tietoturvallisuus on pohjimmiltaan hallinnollinen ongelma. Halutun tietoturvallisuustason saavuttamiseksi ja ylläpitämiseksi on otettava kattavasti huomioon organisatorisia asioita. Tietoturvallisuudelle voidaan luoda hallinnolliset ja tekniset ratkaisut, mutta tärkeintä on saada kaikki käyttäjät: organisaation johto, toimintaprosessien ja tietojärjestelmien omistajat ja ylläpitäjät, suojausmenetelmien ylläpitäjät ja toteuttajat sekä järjestelmien käyttäjät tietoturvallisuuden ylläpitoon.

Turvallisuustietoisuuden lisäämisellä voidaan vaikuttaa henkilökunnan asenteisiin ja käyttäytymiseen. Ihmisen toiminta on usein tietoturvallisuuden suurin uhka ja usein juuri siksi, että heitä ei ole koulutettu tai he eivät tiedä, mitä tietoturvallisuus merkitsee organisaation toiminnalle. Työntekijöiden on ymmärrettävä, millainen vaikutus heidän toiminnallaan on, ja kuinka ne vaikuttavat tietoturvallisuuteen. Organisaation johdon sitoutuminen on tärkeää: jos johto ei noudata laatimaansa tietoturvapolitiikka ja tietoturva-ohjeistusta, ei se voi sitä vaatia muiltakaan.

Organisaation tietoturvallisuuden tason subjektiivisella arvioinnilla sekä käyttäjien ja ylläpitäjien tietoturvatietoisuuden asteen objektiivisella mittaamisella voi saada informaatiota siitä, mihin tekijöihin pitäisi kiinnittää huomiota, jotta organisaatio voi toteuttaa ja kehittää määrittelemäänsä tieto-turvallisuuden tasoa haluttuun suuntaan.

Haittaohjelmien torjuntaraportin mittaustulokset ovat helppotajuisia ja yksiselitteisiä eikä niiden tulkinnasta synny epäselvyyksiä tai ristiriitoja. Sen sijaan käyttäjätunnusta ja salasanaa ei aina mielletä henkilökohtaiseksi ja salaiseksi

tiedoksi, joita ei saa luovuttaa toiselle missään tilanteessa. Havaintoja voidaan käyttää käytännön esimerkkeinä, joiden avulla henkilöstölle avautuisi mitä politiikoilla, ohjeilla ja toimintamalleilla todellisuudessa tarkoitetaan.

Haittaohjelmien torjuntaraportit ja tulkintani tietoturvapoikkeamaraporteista osoittavat osaltaan sen, että ihmisen toiminta tai tekniikka ei yksin riitä hyväksytyn tietoturvallisuuden toteuttamiseen. Hyvän tietoturvallisuuden toteuttamisessa ihmisten rooli on keskeinen ja vain osa voidaan hoitaa teknologian avulla. Kaiken muun voi ulkoistaa, mutta vastuuta tietoturvasta ei voi, se on aina itse organisaatiolla. Parasta tietoturvaa voi toteuttaa ihminen ja tekniikka yhdessä.

LÄHTEET

Jaakohuhta H. 2001. Tietoturva on ilmaista – vai onko? ITNetPlus 1, 14.

Krutz R. L., Vines R. D. 2003. Tietoturvasertifikaatti – CISSP. Helsinki: Edita Prima.

Laaksonen, M., Nevasalo T., Tomula K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Nordprint.

Miettinen J. E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Jyväskylä: Gummerus Kirjapaino.

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. VAHTI 3/2007.

KORKEAKOULUN TIETOTURVA, JAKAMINEN JA STRATEGISET VERKOSTOT

Mauri Kantola, VTM
Koulutuspalvelupäällikkö, Turun ammattikorkeakoulu

Korkeakoulun tietoturva-osaaminen ja tietoturvatarpeet ovat toisensuuntaista ja lähtökohdiltaan erilaisia kuin useimmilla muilla organisaatioilla. Korkeakoulun toiminnan lähtökohtia ovat avoimuus, vapaa pääsy, tiedon jakaminen ja verkostoiminen. Tällöin vuorovaikutus- ja verkostoitumistaidot, yksilön tietoturvavastuu, medialukutaito ja pyrkimys mielekkääseen sisällöntuotantoon nousevat merkittäviksi tietoturvan osa-alueiksi. Korkeakoulutusta suunnitellaan ja kehitetään avoimissa verkostoympäristöissä, jotta muun yhteiskunnan kehittämispaineet havaittaisiin ja niihin voitaisiin reagoida. Tavoitteena on rohkaista opiskelijoita, opettajia ja tutkijoita soveltamaan ja luomaan uutta tietoa, joka mahdollistaa innovaatioiden syntymistä moninaisissa työelämän organisaatioissa (Penttilä 2012). Korkeakouluja ei nähdä muista irrallisina vaan niitä pidetään sosiaalisten verkostojensa ympäröiminä aktiivitoimijoina. Siksi tietoturvaakin pohdittaessa tietoympäristöjä koskeva kokonaisuuksien analysointi ja tietoisen ohjauksen merkitys on kasvanut, samoin kuin tarve kehittää systemaattisia malleja, analyysitapoja ja tarkastelukehikkoja. Korkeakouluissa pyritään sidosryhmätarpeiden huomioinnin lisäksi myös itsenäisesti suunnittelemaan tulevaisuutta samoin kuin arvioimaan ja raportoimaan omaa toimintaa ottamalla toki huomioon paikallinen ja globaali sosiaalinen vastuu (Kantola 2009).

Erityisesti langattoman viestinnän alueella tapahtuva nopea kehitys ja innovaatiot luovat uusia mahdollisuuksia ja haasteita. Internetin palveluiden ja viestinnän siirtyessä yhä vahvemmin mobiilille puolelle, langattomille verkoille asetettavat vaatimukset kasvavat. Samanaikaisesti kuitenkin epävarmuus eri langattomien verkkojen teknologioiden, palveluntarjoajien ja käyttäjienkin roolista erilaisissa verkkoympäristöissä kasvaa. Päätöksenteko ja ennustaminen eri ulottuvuuksilla tässä ympäristössä vaativat kokonaisvaltaista lähestymistapaa, jossa huomioidaan sekä teknologisten näkökulmien lisäksi muitakin näkökulmia. (Smura 2012).

Korkeakoulut testaavat ja koettelevat rajoja sen suhteen kuinka avoimia tietojärjestelmät voisivat olla maksimissaan vielä toimiakseen. Epäilemättä rajat tulevat vastaan jossakin vaiheessa, mutta näistä rajoista ei välttämättä ole yhteiskunnan muilla instituutioilla tietoa, koska ne usein liikkuvat tiedon maksimaalisen turvaamisen urilla eikä koetteluun ole mahdollisuuksia yhtä vapaasti kuin korkeakouluilla.

Kunkin yksityisen ja julkisen sektorin organisaation tietoturvaa tarkasteltaessa on siis mielekästä ottaa lähtökohdaksi oman organisaation luonne ja sen strategiset tehtävät. Korkeakoulujen perustehtäviä on määritelty lainsäädännössä, opetus- ja kulttuuriministeriön laatimissa kehittämissuunnitelmissa ja myös ammattikorkeakoulujen yhteisissä kuten rehtorineuvosto Arenen julkilausumissa. Lisäksi korkeakoulut autonomisina toimijoina määrittelevät tavoitteitaan itsenäisesti. Yleisesti ottaen suomalainen koulutuspolitiikka ja lainsäädäntö edellyttävät korkeakoulutuksen vastaavan työelämän tarpeisiin ja kehittävän sitä. Yliopistoja ja ammattikorkeakouluja jopa usein arvostellaan niiden hitaudesta vastata yhteiskunnassa tapahtuviin muutoksiin. Yhteiskunta ja globaali talous ovat laajasti pakottamassa koulutusta reagoimaan nopeammin mitä erilaisimpiin muutoksiin. Toiminnalta vaaditaan lisättyä joustavuutta ja liikkuvuutta. Tällöin avainsanoiksi nousevat nopeus, muutosvalmius ja tilanneherkkyys (Penttilä 2012). Tämä kaikki merkitsee uusien ratkaisumallien etsimistä myös tietoturvan näkökulmasta.

Korkeakoulun tietoturvan vaikuttavuuden arviointi merkitsee yleisen kokonaisviitekehyksen kuvaamista sisältäen organisaation kiinnittymistavat toimintaympäristöönsä ja myös ulkoiset vaikutukset. Mallinnuksessa olisi hyvä samanaikaisesti huomioida niin verkostoyhteiskuntakeskustelu, strateginen suunnittelu, yhteiskuntavastuu kuin laadunvarmistuksen elementitkin. Tässä artikkelissa esitettävää kehikkoa voidaan käyttää ja edelleen kehittää tietoturvaan liittyvän päätöksenteon apuvälineeksi korkeakoulun ollessa sidoksissa paikallisiin, valtakunnallisiin ja kansainvälisiin tehtäviinsä.

Strategisella suunnittelulla tähdätään tulevaisuuteen ja se pohjautuu kokonaiskäsitykseen organisaation toiminnasta sisältäen mahdollisimman selkeästi ilmaistun toiminta-ajatuksen, vision, strategiset valinnat ja organisaation arvot (Kettunen 2006). Strategiaprosessin tarkoituksena on siten suunnittelun lisäksi tuottaa selkeitä toiminnallisia tavoitteita. Kattavalla strategisella suunnittelulla on myös mahdollista tuottaa perusteltuja näkemyksiä kuinka organisaatio voi tukea alueellista kehitystä ja yhteistä tulevaisuutta. Korkeakoulun tavoit-

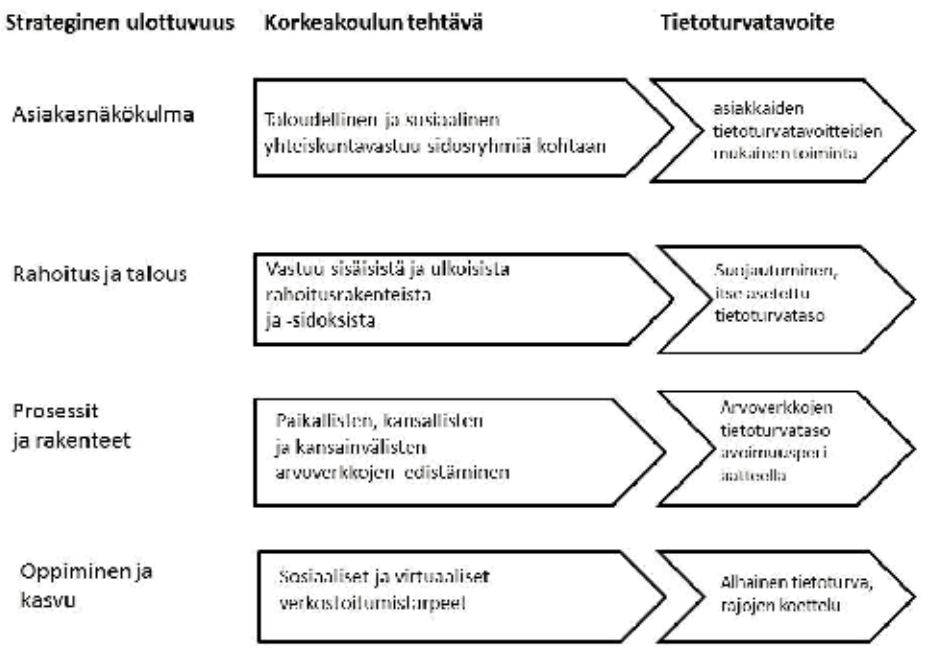
teena tulisi olla tehokas reagointi muuttuvaan ympäristöön, markkinoihin ja sidosryhmien tarpeisiin sekä näitten ennakointi (Johnson & Scholes 2002, Steiss 2003). Korkeakoulut ovat siirtyneet perinteisestä julkisorientaatiosta kohti ympäristöorientoituneita toimintatapoja, joissa korostetaan sitoutumista nimenomaisesti omaan toimintaympäristöön ja vaikutusalueen kehittämiseen (Kettunen & Kantola 2006).

Turun ammattikorkeakoulussa käytetään Kaplanin ja Nortonin (2004) kehittämää tasapainotettua tuloskortistoa (Balanced Scorecard, BSC) strategisen suunnittelun tukena. Tämän tasapainoisen lähestymistavan avulla voidaan suunnittelun lisäksi myös kommunikoida sidosryhmien kanssa ja kortistoa voidaan lisäksi käyttää varsinaisen toimenpanon apuvälineenä. Tuloskortilla kuvatut ulottuvuudet Turun ammattikorkeakoulussa ovat

- alueellinen ja kuluttajanäkökulma: aluekehitys ja asiakastyytyväisyys
- rahoitusnäkökulma: valtiovallan rahoitus, ulkoinen rahoitus, kustannustehokkuus
- sisäisten prosessien näkökulma: opetus ja oppiminen, tutkimus ja kehitys ja sisäistäminen
- oppimisen ja kasvun näkökulma: opettajien kouluttautuminen, tutkimus ja kehitys ja kansainväliset mahdollisuudet.

Edellä kuvatun pohjalta on mahdollista Kaplanin ja Nortonin strategisen suunnittelun lähestymistapaa hyödyntäen rakentaa korkeakoululle sopiva kokonaisviitekehys tietoturvan suunnittelua varten. Kaplanin ja Nortonin strategiakartta voi yksinkertaisimmillaan olla graafinen pelkistys organisaation perustavoitteista. Strategialla tavoitellaan johdon, henkilöstön ja sidosryhmien ymmärryksen lisäämistä siitä miksi ja miten organisaation tavoitteet ovat rakentuneet ja kuinka tavoitteisiin päästäisiin. Strategiakarttaa puolestaan käytetään kuvaamaan strategisia teemoja ja tavoitteita eri perspektiiveistä ja valottamaan teemojen keskinäisiä suhteita (Kettunen & Kantola 2006). Tässä artikkelissa kyseistä konseptia alustavasti sovelletaan siis tietoturvasuunnittelun alueelle. Keskeisenä tavoitteena on ei-materiaalisten aktiviteettien kuvaaminen olennaisimpien elementtiensä osalta, välttäen liiallisia yksityiskohtia. Viitekehyksellä tavoitellaan johdon tukemista tehtäväsään tulkita ja operationalisoida korkeakoulun yleisiä strategisia tavoitteita tietoturvan näkökulmasta.

Kuviossa 1. kuvataan verkostomaisen yhteistyön ja aluekehitykseen tähtäävän toiminnan kokonaisuutta korkeakoulussa Nortonin ja Kaplanin BSC-ulottuvuuksien avulla liittäen ne tietoturvatavoitteisiin. Vapaiden tietovyöhykkeiden (oppiminen ja kasvu) lisäksi korkeakouluilla on tietoturvatarpeita myös suljetuissa maksimaalisen tietoturvaamisen (rahoitus ja talous) vyöhykkeissä. Tällaisia ovat esimerkiksi talous-, henkilöstö, ja opiskelijahallinnon tietojärjestelmät. Näiden osa-alueiden väliin jää eräänlaisia vaihettumisalueita, joiden tietoturvan taso ja toimenpiteet voidaan määritellä osittain itse kumppaneista ja ulkoisista verkostoista riippumattomasti.

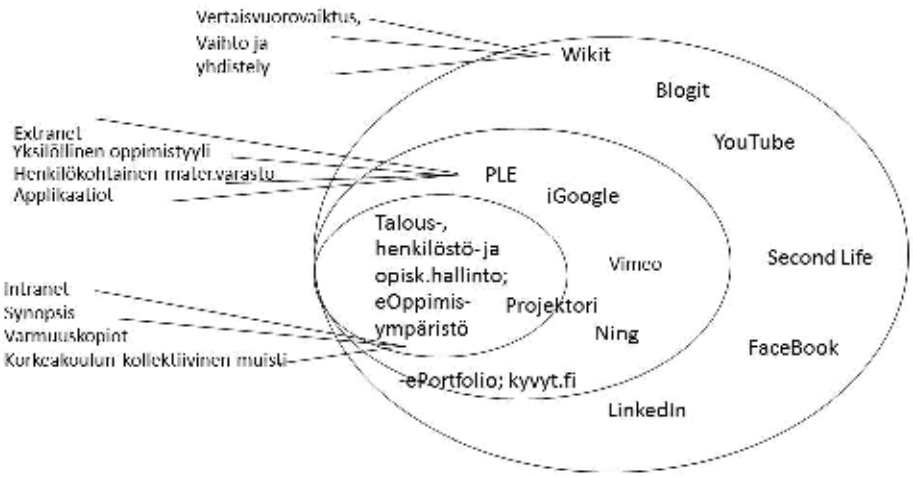


KUVIO 1. *Tietoturvaamisen strategiakartta.*

Vaikka opiskelijoiden henkilökohtaisia tietoja ei tietoverkoissa voida vapaasti välittää ja niitä pitää ehdottomasti suojata, niin heidän kanssaan toimitaan edellisen lisäksi useissa sellaisissakin yhteyksissä, joissa tarvetta korkean tason tietoturvaamiseen ei lainkaan ole olemassa. Itse asiassa juuri tässä kyseisessä opiskelijarajapinnassa on mahdollista yhteistyössä heidän kanssaan harjoittaa avoimen rajojen ja ”tietoturvattomuuden” koettelua. Osittain tämä

sama tilanne koskee myös osaa muita korkeakoulun prosesseja (prosessit ja rakenteet). Näillä alueilla on toki kuitenkin löydettävissä myös omia suljettuja alueitaan.

Edellistä ajatuskulkua edelleen jatkamalla voidaan muodostaa seuraavanlainen mallinnus. Kuvion 2 avulla nimittäin pyritään seuraavaksi yksinkertaistaen mallintamaan koko tietojärjestelmäkenttää korkeakoulun näkökulmasta sisältäen kuviossa 1 esitetyt strategiset niin asiakasnäkökulmat, talouden, prosessien ja rakenteiden kuin oppimisenkin ulottuvuudet. Vaikka kaikkia mahdollisia käytössä olevia tietojärjestelmiä ei kuvioon yritetä mahduttaa, niin tärkeimmät toiminnalliset vyöhykkeet siitä pääpiirteissään ilmenevät.



KUVIO 2. *Sosiaalinen media ja ammattikorkeakoulun tietoturva.*

Suljettujen järjestelmien, kuten opiskelijahallinto ja e-oppimisympäristö, tarkoituksena on henkilökohtaisten yksityistietojen turvaamisen lisäksi tarjota yhteisön jäsenille jäsennelty ja tietosisältöjä säilyttävä tietoympäristö. Voidaan puhua myös organisaation kollektiivisesta muistista, jota myös pyritään turvaamaan yhdessä toiminnallisten jäsennyksien (synopsis) kanssa. Monet korkeakouluyhteisön jäsenet ovat kuitenkin halukkaita hyödyntämään myös täysin avoimia tietoympäristöjä, joita tarjotaan kenen tahansa käyttöön internetin välityksellä erilaisina pilvipalveluina. Näihin avoimiin ympäristöihin voidaan suljetuista ympäristöistä siirtyä linkkien avulla. Käyttäjä ei useissa tapauksissa

siirtymää nykyisin edes huomaa. Tietoturvan näkökulmasta joustavuus nousee keskiöön eikä perinteisillä tietoturvapolitiikoilla päästä pitkälle. Yksilön vastuu toimijana tällöin korostuu, kuten myös kyky lukea mediaa ja verkkotilanteita.

Erilaisten tietoympäristöjen yhteiskäyttö on perusteltua sosiaalisen interaktion kasvattamisen lisäksi siis myös taloudellisesta näkökulmasta. Pohjolan (2012) mukaan tietoliikennepalvelut ovat edullisia kun palveluita voidaan siirtää alhaisin kustannuksin verkossa. Enää ei ole tarvetta sille, että kullakin toimijalla olisi omat ympäristönsä ja ohjelmistonsa, vaan suurtuotannon edut ovat hyödynnettävissä pilvipalvelujen kautta samoin kuin näihin etuihin on toisaalla päästy esimerkiksi sähkötuotannossa voimaloiden kautta. Tämä vapauttaa henkilöt ja organisaatiot myös paikkasidonnaisuudesta, aivan kuten sähkö vapautti esimerkiksi metsäteollisuusyritykset toimimasta koskien läheisyydestä. Edelleen Pohjolan mukaan pilvipalvelulla voidaan työ järjestää sinne, missä se on työnteon kannalta järkevintä. Tästä koituvat yhteiskunnalliset säästöt voivat olla merkittäviä. Nykyisten palveluiden myötä myös nuorison toimintatapa ja elämä on muuttunut ja sen mukana myös työelämä tulee muuttumaan. (Pohjola 2012).

Edellisten näkökulmien lisäksi viimeaikaisissa korkeakoulujen toimintaa koskevissa keskusteluissa on korostunut rajoja ylittävien virtuaalisten oppimistilojen tarve osana työ-elämän ja korkeakoulujen välistä mentorointia ja valmentamista. Tämä suhde on nähty vuorovaikutteisena eli vähintään kaksisuuntaisena. Ensisijaisesti jatkuvasti muutoksen alainen tietoyhteiskunta luo kysyntää jatkuvalle ammatilliselle kehittämistoiminnalle niin aktiivityössä oleville kuin sen ulkopuolellakin. Kompetenssista on tullut kilpailuväline tiukentuvilla työmarkkinoilla. Tämä edellyttää uudenlaisten yhteistyömuotojen kehittelyä koulutuksen ja työ-elämän välille, kuten esimerkiksi niin kutsuttu e-mentorointi. Tietoturvan näkökulmasta tämäkin luo korkeakoululle uusia haasteita eikä perinteinen suljettujen järjestelmien suojautumisen strategia ole mahdollinen. (Leppisaari & Tenhunen 2012). Tässäkin yksilön vastuu toimijana institutionaalisten kokonaisratkaisujen sijaa korostuu yksilön itse toiminnallaan vastatessa työhönsä liittyvästä tietoturvasta.

Digitalisaation peräkkäiset aallot läntisissä tietoyhteiskunnissa muuttivat työelämän aiempaa liikkuvammaksi. Uusien digitaalisten ympäristöjen ilmestyminen nosti esiin vaatimuksen semanttisen älyn hyödyntämismahdollisuuksista rakenteellisesti jäsennellyin kokonaisuuksin kaoottisten datatulvien sijaan. Modernissa mobiilielämässään yksilöt tarvitsevat vaivattoman

pääsyn helposti käsiteltävissä olevaan ja jäsentyneeseen informaatioon. Uusi joka paikan tietojenkäsittely on alkanut määrittää digitaalisaation viimeisintä vaihetta. Olemme siirtyneet massojen portaaleista yksilöllisen tietojenkäsittelyn aikaan kunkin yksilön tukeutuessa hiljaiseen teknologiaan, jossa teknologia vetäytyy taka-alalle arkielämän eri tilanteissa. Tietoteknologian tarkoituksena on auttaa yksilöä keskittymään muihin asioihin kuin itse tietotekniikkaan (Weiser 1997). Weiserin (1997) mukaan paras teknologia on hiljainen ja näkymätön palvelija. Mitä enemmän ihmiset kykenevät käyttämään intuitiotaan, sitä älykkäämpään toimintaan he yltävät tietotekniikan laajentaessa heidän alitajuntaansa. Siten teknologia voi olla edistämässä myös jopa niin kutsuttua downshiftaamista. Muotoilleessaan hiljaisen teknologian määritelmää, Weiser ja Brown (1995) kirjoittivat hiljaisen teknologian (calm technology) olevan jotakin sellaista joka informoi, mutta ei lainkaan vaadi huomiotamme. Näin määriteltynä hiljaisen teknologian idea lähestyy Polanyin (1967) konseptia äänettömästä tietämyksestä tai osaamisesta (tacit knowledge). Tietoturvatoimintaan sovellettuna yksilön näkökulmasta organisaatioiden tietohallinnon määrittelemät käyttäytymisnormit joutuvat uuteen valoon. Yksittäinen asiantuntija tarvitsee taustalle jäävää hiljaista tietoturvatukea, ei niinkään tietoturvaa koskevia eksplisiittisiä rajoituksia ja normeja. Korkeakoulun tulee rakentaa näkymätön tietoturvallisuuden konsepti, joka perustuu tietoturvarajojen koetteluun ja automatisoituun ongelmien poistamiseen ristiriitatilanteissa yksilön vastuuta korostaen.

JOHTOPÄÄTÖKSET

Korkeakoulun tietoturvatoiminnan on hyvä perustua sen omaan strategiaan. Tietoturvaa on syytä tarkastella strategisista lähtökohdista käsin ja strategisen suunnittelun välinein. Tähän soveltuu hyvin välineeksi tasapainotettu tuloskortisto, Balanced Scorecard. Tietoturvan tulisi tukea korkeakoulun perustehtävää eikä sen tulisi haitata tiedonjakamis- eikä verkostoitumistehtävää. Keskeisimpiä tekijöitä yhteiskuntavastuullisen tietotyön kehittämisessä ovat verkostoituminen ja strateginen suhtautuminen siihen. Käytännön yhteistyö olemassa olevien ja potentiaalisten kumppanien kanssa toteutuu avoimesti verkostoissa ja niiden tukemana. Verkostomainen toiminta vahvistaa korkeakouluja niiden pyrkimyksissä edesauttaa positiivisten ulkoisten vaikutusten kasvua, kuten myös kommunikaatiota ja ulkoista arviointia. Tästä johtuen myös tietoturvaa ja tietoympäristöjä koskeva kokonaisuuksien analysointi ja

tietoisen ohjauksen merkitys on kasvanut, samoin kuin tarve kehittää systemaattisia malleja, analyysitapoja ja tarkastelukehikkoja. Asiantuntijat tarvitsevat taustalle jäävää hiljaista tietoturvatukea, ei niinkään tietoturvaa koskevia eksplisiittisiä rajoituksia ja normeja.

LÄHTEET

Inkinen, S. 2009. Kaaos ja Kosmos. Vaasa.

Johnson, G. ja Scholes, K. 2002. Exploring Corporate Strategy, Prentice Hall, Englewood Cliffs, NJ.

Kantola, M. 2009. Verkostostrategia ja strategiset verkot. KeVer-verkkolehti, vol 8, No 3 (2009). http://ojs.seamk.fi/index.php/kever/article/viewArticle/1122

Kantola, M., Kettunen, J. & Helmi, S. 2010. Strategic regional networks in higher education. Teoksessa Patricia Ordóñez de Pablos, W.B. Lee & Jingyuan Zhao, toim. Regional Innovation Systems and Sustainable Development: Emerging Technologies. Hersey: IGI Global.

Kaplan, R., & Norton, D. 2004. The strategy maps. Boston, Massachusetts: Havard Business School Press.

Kettunen, Juha 2006. Strategic planning of regional development in higher education. Baltic Journal of Management, 1(3),259–269.

Leppisaari, I. & Tenhunen M.-L. 2012. Establishing virtual learning places between higher education and working life through e-mentoring. Teoksessa Ahola, S. & Hoffman, D. (toim.): Higher education research in Finland – emerging structures and contemporary issues. Jyväskylä: Finnish institute for educational research in co-operation with Consortium of Higher Education Researchers in Finland (CHERIF), s. 421–440.

Penttilä, Taru 2012. Environmental Issues in Business Education Curricula at Finnish Universities of Applied Sciences – Towards a Postmodern Curriculum? Väitöskirja. Itäsuomen yliopisto.

Polanyi, Michael 1967. The Tacit Dimension, New York: Anchor Books.

Pohjola, M. 2012. Haastattelu. Logican asiakas- ja sidosryhmälehti Ratkaisu 1/2012 . s.11.

Smura, T. 2012. Techno-economic modelling of wireless network and industry arhcitectures. Helsinki: Aalto University publication series: doctoral dissertations 23/2012. UnicrTimes New Romanafia Oy.

Steiss, A.W. 2003. Strategic Management for Public and Nonprofit Organizations. London: Taylor and Francis, CRC Press.

Weiser, M. 1997: Organizational Memory: Reducing Source-Sink Distance. In: HICSS 1997. pp. 271–280.

Weiser, M. & Brown, J. 1995. Designing Calm Technology. Xerox Parc. http://www.ubiq.com/hypertext/weiser/calmtech/calmtech.htm

JOUSTAVA TAAJUUKSIEN KÄYTTÖ TUO UUSIA TIETOTURVAHAASTEITA LANGATTOMAAN VIESTINTÄÄN

Jarkko Paavola, TkT
Yliopettaja, Tietojenkäsittelyn koulutusohjelma, Turun ammattikorkeakoulu

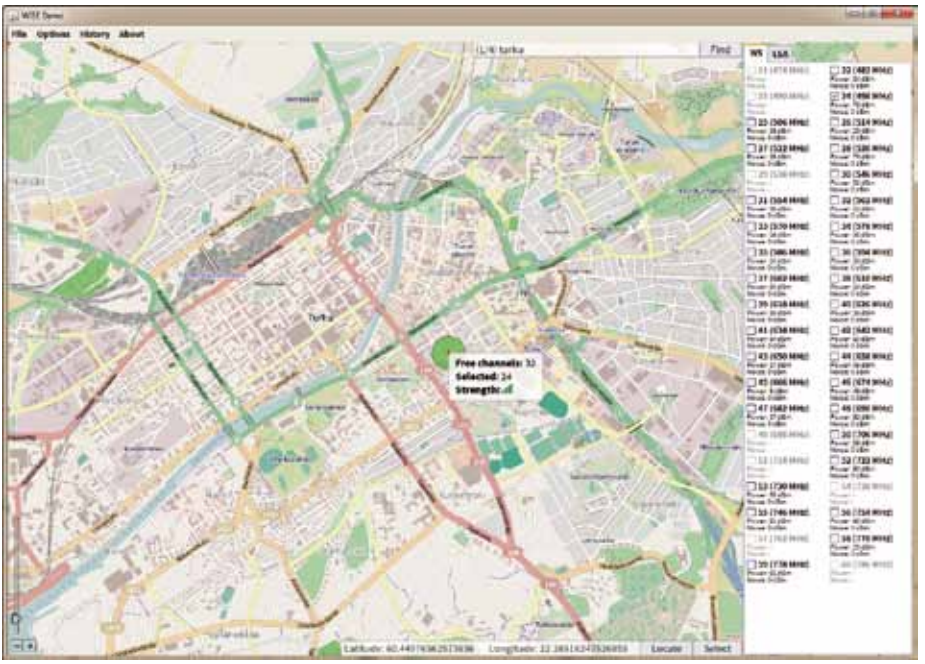
Mobiilidatan käytön yleistyessä radiotaajuuksia käyttävät langattomat verkot ruuhkautuvat nopeasti. Tarve tehokkaammalle taajuuksien käytölle on suuri, koska valtaosa käyttökelpoisista taajuuksista on jo käytössä. Kuitenkin samaan aikaan osa näistä taajuuksista on vajaakäytössä tietyissä maantieteellisissä kohdissa. Turun ammattikorkeakoulu kehittää joustavan taajuuksien käytön menetelmiä Tekes-rahoitteisessa *White Space Test Environment for Broadcast frequencies* (WISE) -hankkeessa (WISE 2013, Paavola ym. 2011), joka kuuluu Tekesin Trial-teknologiaohjelmaan (Tekes 2013). Langattomien tietoliikennejärjestelmien peittoaluekartoissa hyödyntämätön alue näytetään usein valkoisella värillä. Tästä johtuen joustavaan taajuuksien käyttöön kykeneviä laitteita kutsutaan *White Space* -laitteiksi (WS).

Suomessa taajuuksien käyttöä määrää ja valvoo Viestintävirasto, joka pitää myös yllä taajuusjakotaulukkoa (Viestintävirasto 2013, 1). Maailmanlaajuisesti ensimmäiseksi WS-taajuusalueeksi on suunniteltu televisio-käytössä olevia taajuuksia 470–790 MHz. TV-lähetysten digitalisoinnin johdosta näillä taajuuksilla on teoreettisesti paljon WS-alueita käytössä. Kuva käytössä olevista TV-taajuuksista on saatavilla Viestintäviraston verkkosivuilta (Viestintävirasto 2013, 2). WS-taajuuksia voidaan käyttää hyvin moniin erilaisiin tarpeisiin, kuten esimerkiksi haja-asutusalueiden langattomaan laajakaistaan, nykyisten matkapuhelinverkkojen lisäkapasiteetiksi, langattoman lähiverkon lisätaajuuksiksi tai vaikkapa laitteiden väliseen kommunikaatioon. Suomessa WS-käyttö on huomioitu myös Liikenne- ja viestintäministeriön uudessa Sähköisen median viestintäpoliittisessa ohjelmassa.

WS-laitteiden toiminnalliset haasteet nousevat kahdesta suunnasta: ne eivät voi vaatia suojausta muiden järjestelmien aiheuttamilta häiriöiltä, eivätkä ne saa aiheuttaa häiriöitä muille järjestelmille. Mahdollisessa häiriötapauksessa WS-järjestelmän tulee väistää ensisijaista käyttöä ja tämä tuo WS-liiketoiminnalle merkittäviä haasteita. WS-käytön tulisi siis samaan aikaan olla väistävä ja pystyä tarjoamaan luotettavaa laatua siten, että WS-toiminta on myös liiketaloudellisesti kannattavaa. TV-taajuuksilla häiriöiltä täytyy TV-lähetysten lisäksi suojella langattomien radiomikrofonien käyttö, jotka tulevaisuudessa käyttävät samoja taajuuksia.

WS-laitteiden täytyy selvittää ns. geolokaatiotietokannasta GPS-koordinaattien perusteella, mitkä ovat vapaana olevat taajuudet ja mitkä ovat maksimaaliset lähetystehot kyseisillä taajuuksilla. Ainakin alkuvaiheessa WS-verkko muodostuu normaalisti tukiaseman avulla. Tällöin tukiasema on yhteydessä tietokantaan ja jakaa saadun vastauksen eteenpäin langattomille laitteille.

Turun ammattikorkeakoulu on kehittänyt WISE-hankkeessa ohjelmiston, joka toimii kuten WS-laite ja mahdollistaa geolokaatiotietokannan toiminnan testauksen. Esimerkki ohjelman toiminnasta on esitetty kuvassa 1. Ohjelmassa hiiren painallus kartalla tarkoittaa WS-laitteen sijoittamista kyseiseen kohtaan. Ohjelma lähettää pyynnön geolokaatiotietokannalle, joka vastaa listalla vapaista taajuuksista kyseisessä kohdassa. Laite (ohjelma) pystyy varaamaan yhden kahdeksan megahertsin taajuuskaistan itselleen valitsemalla sen ruudun oikeasta reunasta.



KUVA 1. *Turun AMK:n kehittämän WS-ohjelman käyttönäkymä. Kuvan oikeassa reunassa näkyvät vapaat taajuudet kartalla näkyvän vihreän ympyrän alueella.*

TIETOTURVAHAASTEET

Geolokaatiotietokanta sijaitsee internetissä, joka luo omanlaisensa toiminnalliset haasteet tietoturvan kannalta. Ensimmäistä kertaa kokonaisen langattoman tietoliikennejärjestelmän toiminta nojautuu tukiaseman internetyhteyden luotettavuuteen. WS-laitteen ja tietokannan tulee esimerkiksi pystyä molemminpuoliseen autentikointiin, jotta tietokanta tietää onko WS-laite sallittu ja vastaavasti laitteen täytyy pystyä varmistumaan tietokannan aitoudesta. Tiedonsiirto tukiaseman ja tietokannan välillä täytyy olla salattu eikä tietokannan sisältöä pitäisi voida muuttaa kuin tietokannan ylläpitäjä. Tietokantaan voi kohdistua myös palvelunestohyökkäyksiä. Jos tietokannan tietoturva vaarantuu, se voi WS-verkon lamautumisen lisäksi aiheuttaa voimakkaita häiriöitä TV-signaalille, koska WS-laitteilla on väärää tietoa sallituista alueista ja maksimaalisista lähetystehoista.

Tiedeyhteisö on analysoinut jonkin verran joustavaan taajuuksien käyttöön liittyviä tietoturvauhkia. Tutkimus on keskittynyt lähinnä palvelunestohyökkäyksiin WS-järjestelmää vastaan sekä WS-järjestelmällä tehtävällä palvelunestohyökkäyksellä pääkäyttöä vastaan (Brown,T. Sethi, A. 2007; Arkoulis ym. 2008; Anand ym. 2011; Chen ym. 2011; Newman ym. 2010; Chaczko ym. 2010). Newmanin ja kumppaneiden artikkelissa analysointiin myös WS-järjestelmän alttiutta ns. *man-in-the-middle*-hyökkäykselle. TV-lähetysten häiriintyminen on ollut huolenaiheen erityisesti Yhdysvalloissa, sillä siellä TV on pääasiallinen kriisitilanteiden tiedotuskanava. Joustavaa taajuuksien käyttöä on myös analysoitu siltä kannalta miten järjestelmä takaa WS-taajuuksien käytön reilusti kaikkien käyttäjien välillä (Arkoulis ym. 2008).

TIEDONSIIRTOPROTOKOLLAN MÄÄRITTELYPROSESSI

Internetissä kaikille avoimien protokollien määrittely tapahtuu IETF:ssä (Internet Engineering Task Force) (IETF 2012), joka julkaisee valmiit protokollat RFC-dokumentteina. IETF:ssä on tämän artikkelin kirjoitushetkellä käynnissä PAWS-protokollan (Protocol to Access White Space) määrittely WS-tukiaseman ja tietokannan väliseen viestintään. Turun ammattikorkeakoulu osallistuu prosessiin Tekes-rahoitteisen ReWISE-hankkeen (Reliability Extension to WISE) puitteissa, joka on kansainvälinen laajennus WISE-hankkeen geolokaatiotietokantaasioista. Hankkeessa on mukana partnereita myös Kanadasta ja Yhdysvalloista.

PAWS-protokollan määrittelyprosessissa on ensin kuvattu protokollan käyttötapaukset ja näistä on johdettu uhkamalli (*threat model*), joka kuvaa tilanteita, joissa protokollaa voitaisiin käyttää WS-järjestelmän vahingoksi. Uhkamallin avulla on vuorostaan määritelty protokollan tietoturvavaatimukset. PAWS-protokollan määrittelyssä on identifioitu seuraavanlaisia uhkia:

- WS-järjestelmän luvaton käyttö hyödyntäen joko tukiaseman tai tietokannan haavoittuvuuksia
- Tukiaseman ja tietokannan välisen viestiliikenteen väärentäminen
- WS-laitteiden sijainnin ja identiteetin paljastuminen viestiliikenteen salakuuntelussa
- Tietokantayhteyden puuttuminen, joka lamauttaa WS-järjestelmän toiminnan.

Ylläkuvatusta uhkamallista on johdettu protokollalle tietoturvavaatimukset, jotka ovat pääosin perinteisiä internetissä tapahtuvalle tiedonsiirrolle. Protokollan täytyy mahdollistaa molemminpuolinen tunnistautuminen (*authentication*), varmistautua viestiliikenteen aitoudesta (*integrity*), turvata tietojen yksityisyys ja salaus (*confidentiality*, *encryption*) sekä varmistaa tietokantapalvelun saatavuus (*availibility*). Protokollamäärittelyssä tietoturvauhkia on kuvattu vielä hieman yksityiskohtaisemmin kunkin tietoturvavaatimuksen kohdalta:

Autentikointi:

- Käyttäjä modifioi laitettaan niin, että tietokanta uskoo laitteen olevan sertifioitu. Ilman kunnollista suojausta ulkopuolinen laite saattaa tallentaa rekisteröitymisprosessin ja myöhemmin tehdä niin sanotun replay-hyökkäyksen.
- WS-laitteen tulee varmistua siitä, että tietokanta jolta vastaus tulee, on aito. Väärennetyn tietokannan avulla pystyttäisiin WS-laitteelle syöttämään informaatiota, joka aiheuttaisi häiriöitä primaarikäyttäjille.
- Ulkopuolinen taho voi esiintyä PAWS-protokollaprosessin osana. Tällöin esimerkiksi tietokantana esiintyvä taho voi lähettää WS-laitteelle viestin, joka aiheuttaa sen pois päältä kytkeytymisen.

Tietojen muuttumattomuus:

- Väärennetty WS-laitteen tietokantapyyntö voisi aiheuttaa potentiaalisesti häiriöitä pääasialliselle käytölle. Toisaalta tämä voi aiheuttaa WS-järjestelmälle palvelunestohyökkäyksen.
- Tietokantavastauksen väärentämisen vaikutukset ovat samat kuin edellisessä kohdassa.

Tietojen salaus:

- Jos laite pystyy salakuuntelemaan liikennettä, niin se pystyy käyttämään taajuuksia luvatta.
- Kolmas osapuoli pystyy seuraamaan WS-laitteen paikkatietoja ja selvittämään sen identiteetin jos yhteys on salaamaton.

Saatavuus:

- Esimerkiksi luonnonkatastrofi voi estää taajuustietojen saannin hätätapauksissa.

Huomionarvoista on, että taajuussäätelystä vastaavat tahot saattavat asettaa tiukempia tietoturvavaatimuksia kuin mihin PAWS-protokollakehityksessä on tällä hetkellä varauduttu.

LOPUKSI

Tässä artikkelissa on kuvattu joustavan langattomien taajuuksien käytön tuomia tietoturvahaasteita. Tietojen salaukseen, niiden muuttumattomuuden tarkastamiseen sekä palvelujen saatavuuteen liittyvät haasteet ovat perinteisiä internetpohjaisten palvelujen kohdalla. Tästä syystä Turun ammattikorkeakoulun tietojenkäsittelyn koulutusohjelmassa on pyritty vastaamaan erityisesti autentikointihaasteeseen, johon ei vielä ole ratkaisumalleja esitetty. Tähän ongelmakenttään liittyy myös analyysi siitä, kuinka varmistetaan, että WS-laitteet eivät varaa taajuuksia käyttöönsä yli oman tarpeen.

Aika näyttää miten joustava taajuuksien käyttö tulee yleistymään. Yhdysvalloissa on jo muutama geolokaatiotietokantaoperaattori saanut luvan aloittaa kaupallisen toiminnan rajatuilla maantieteellisillä alueilla. Euroopassa Iso-Britannia on ilmoittanut aloittavansa kaupallisten toimilupien myöntämisen mahdollisimman pian. Todennäköisesti tämä tapahtuu vuoden 2014 aikana. Muu Eurooppa jää odottamaan harmonisoitua EU-standardia, mutta työ senkin aikaansaamiseksi on alkamassa. Myös PAWS-protokollan standardoinnin pitäisi valmistua vuoden 2013 aikana, mikä omalta osaltaan nopeuttaa prosessia poistamalla yhteensopivuusongelmia eri geolokaatiotietokantojen välillä.

Suomessa lainsäädäntö mahdollistaa jo WS-viestinnän ja Viestintävirasto on myöntänyt WISE-projektin puitteissa täyden radioluvan taajuusalueelle 470 MHz–790 MHz Turkuun. Trial-teknologiaohjelma jatkuu vielä vuoden 2014 loppuun. WISE-hankkeessa on tarkoitus laajentaa WS-testausta ja keskittyä erityisesti erilaisten langattomien palvelujen tekniseen pilotointiin. Samalla pyritään esittämään luotettavat tietoturvaratkaisut, jotta toimilupia voitaisiin myöntää jo lähitulevaisuudessa. Käytössä oleva WS-ohjelmisto ja geolokaatiotietokanta mahdollistavat järjestelmän yksityiskohtaisen tietoturvatestauksen.

LÄHTEET

Anand, S.; Hong, K.; Sengupta, S.; ChandramouliIs, R. 2011. Is Channel Fragmentation/ Bonding in IEEE 802.22 Networks Secure?, IEEE International Conference on Communications 2011 (ICC 2011), Kyoto, Japan, 2011.

Arkoulis, S.; Kazatzopoulos, L.; Delakouridis, C.; Marias, G.F. 2008. Cognitive Spectrum and its Security Issues, The Second International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST 2008), Cardiff, Wales, 2008.

Brown,T.; Sethi, A. 2007. Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment, 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2007), Orlando, USA, 2007.

Chaczko, Z.; Wickramasooriya, R.; Klempous, R.; Nikodem, J. 2010. Security Threats in Cognitive Radio Applications, 14th International Conference on Intelligent Engineering Systems (INES 2010), Canary Islands, Spain, 2010.

Chen, S.; Zeng, K.; Mohapatra, P. 2011. Hearing is Believing: Detecting Mobile Primary User Emulation Attack in White Space, The 30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011), Shanghai, China, 2011.

IETF 2012. http://www.ietf.org/, Viitattu 19.5.2012.

Newman, T.R.; Clancy, T.C.; McHenry, M.; Reed, J.H. 2010. Case Study: Security Analysis of a Dynamic Spectrum Access Radio System, IEEE Global Communications Conference 2010 (GLOBECOM 2010), Miami, USA, 2010.

Paavola J. ym. 2011. Hyödyntämättömät TV-taajuudet käyttöön, Prosessori-lehti, Nro 11–12, 2011.

Tekes 2013. http://www.tekes.fi/ohjelmat/trial. Viitattu 13.6.2013.

Viestintävirasto 2013, 1. https://www.viestintavirasto.fi/taajuudet/radiotaajuuksienkaytto/taajuusjakotaulukko.html. Viitattu 13.6.2013.

Viestintävirasto 2013, 2. https://www.viestintavirasto.fi/taajuudet/radiotaajuuksienkaytto/tv-asematsuomessa/valtakunnalliseentv-toimintaanvaratuttaajuudet.html. Viitattu 13.6.2013.

WISE 2013. http://wise.turkuamk.fi. Viitattu 13.6.2013.