OPPIMATERIAALEJA
PUHEENVUOROJA
RAPORTTEJA 179
TUTKIMUKSIA

Jarkko Paavola (toim.)

NÄKÖKULMIA TIETOTURVAAN 2

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPPIMATERIAALEJA
PUHEENVUOROJA
RAPORTTEJA 179
TUTKIMUKSIA

Jarkko Paavola (toim.)

NÄKÖKULMIA TIETOTURVAAN 2

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

TURUN AMMATTIKORKEAKOULUN
RAPORTTEJA 179

Turun ammattikorkeakoulu
Turku 2014

ISBN 978-952-216-443-8 (painettu)
ISSN 1457-7925 (painettu)
Painopaikka: Suomen Yliopistopaino – Juvenes Print Oy, Tampere 2014
Myynti: http://loki.turkuamk.fi

ISBN 978-952-216-444-5 (pdf)
ISSN 1459-7764 (elektroninen)
Jakelu: http://loki.turkuamk.fi

441 729
Painotuote

SISÄLTÖ

OPPIMISYMPÄRISTÖJÄ JA OPISKELIJAPROJEKTEJA

ESIPUHE

Tervetuloa järjestyksessään toisen Turun ammattikorkeakoulun tietoturvajulkaisun pariin. Ensimmäinen julkaisu saatiin valmiiksi syyskuussa 2013. Julkaisujen välille jää siis vain noin kuusi kuukautta, mutta uutta asiaa on saatu mukaan yhdentoista artikkelin verran. Hyvä osoitus siitä, kuinka nopeasti asiat muuttuvat ja menevät eteenpäin tietoturvallisuuden tai kyberturvallisuuden kannalta. Kyberturvallisuus on määritelty Valtioneuvoston julkaisemassa Suomen kyberturvallisuusstrategiassa tavoitetilana, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristö puolestaan on sähköisessä muodossa olevan informaation käsittelyyn tarkoitettu tietojärjestelmistä muodostuva toimintaympäristö.

Turun ammattikorkeakoulun tutkimus-, kehitys-, ja innovaatiotoiminta (TKI) fokusoituu tutkimusryhmien ympärille. TKI-toiminnan tavoitteena on tuottaa uutta tietoa yritysten hyödynnettäväksi. Tämän julkaisun kirjoittaminen kuuluu yhtenä osana tutkimusryhmän Tietoliikenne ja tietoturva tehtäviin. Suomen kyberturvallisuusstrategiassa korostetaan kaikkien yhteiskunnan toimijoiden kyberosaamisen ja -ymmärryksen kehittämistä. Tämän julkaisun lisäksi tutkimusryhmämme järjestää vuosittain PK-yrityksille suunnatun tietoturvapäivän. Kaikkia turkulaisia tietotekniikka- ja tietoturvaongelmissa palvelee Kansalaisen mikrotuki.

TKI-projektit ja oppimisympäristöt, kuten Kansalaisen mikrotuki, pyrkivät ottamaan opiskelijat täysivaltaisesti mukaan työelämälähtöisten kehitysongelmien ratkaisuun. Tämä julkaisu esittelee myös opiskelijoiden saavutuksia ja Turun ammattikorkeakoulun tarjoamia palveluja alueen yrityksille.

Turussa 13.12.2013

Jarkko Paavola, TkT
Yliopettaja ja tutkimusryhmän vetäjä

AJANKOHTAISTA TIETOTURVASTA

TIETOTURVAVUOSI 2013

Jarkko Paavola, TkT
Yliopettaja, tietojenkäsittelyn koulutusohjelma,
Turun ammattikorkeakoulu

Tietomurtojen määrä, laajuus ja niistä julkaistavien uutisten määrä ovat edelleen kasvussa. Vuotta 2011 kutsuttiin suurten tietomurtojen vuodeksi (IBM X-Force 2012, 12). Esimerkiksi Anonymous- ja LulzSec-hakkeriryhmät olivat aktiivisia (PCMag.com 2013). Vuoden 2012 tietoturvakatsauksessa (Vainikka 2013) keskeisiksi teemoiksi nousivat tietoturvahyökkäysten keskittyminen pieniin ja keskisuuriin yrityksiin (Symantec 2013, 16; Verizon 2013, 13). Yksi syy tietomurtojen jatkuvaan kasvuun on se, että niistä on tullut oma liiketoiminta-alueensa, jossa räätälöidyn hyökkäyksen voi tilata palveluna. Vaihtoehtoisesti internetistä voi tilata ohjelmiston, jossa on automatisoitu tunnettujen haavoittuvuuksien hyödyntäminen. Näistä yksi tunnetuimmista on ollut Blackhole-ohjelmisto (Arstechnica 2012), jonka kehittäjä kuitenkin pidätettiin Venäjällä lokakuussa 2013 (Computerworld 2013). Toimiva liiketoimintamalli takaa, että uusia yrittäjiä on tulossa. Osa hyökkäystyökaluista vaatii käyttökohteesta riippuen pientä räätälöintiä (Business Insider 2013), mutta ohjelmointitaitoja ei tarvita graafisten käyttöliittymien yleistyttyä hyökkäystyökaluissakin. Huomionarvoista on se, kuinka hyvin ylläpidettyjä hyökkäysohjelmistot ovat verrattuna niihin tuotteisiin, joiden haavoittuvuuksia hyökkäyksissä hyväksikäytetään. Suomessa keskusrikospoliisi julkaisee kahdesti vuodessa yrityksiin kohdistuvan ja yrityksiä hyödyntävän rikollisuuden tilannekatsauksen. Tietomurroista todetaan seuraavaa (KRP 2013, 6):

> *Rikoksen tekeminen ei välttämättä vaadi erityistaitoja. Tapaukset ovat lisääntyneet myös, koska rikollisten verkottuminen on yhdistänyt kohdistettujen hyökkäystyökalujen valmistajat ja niistä kiinnostuneet käyttäjät. Vielä vuosikymmen sitten henkilötietojen kaappaus satunnaisilta kotikoneilta edellytti huomattavaa hyökkäysohjelmistojen kehitystyötä. Samat hyökkäystyökalut voidaan nyt ostaa pienin räätälöidyin muutoksin myös yritysvakoilun kaltaisten tiettyyn uhriin kohdistettujen rikosten toteuttamista varten.*

Vuosi 2013 tulee jäämään historiaan tieto- tai kyberturvallisuuden kannalta eräänlaisena poliittisen päätöksenteon heräämisen vuotena ja myös vuotena, jolloin suuren yleisön tietoisuuteen tuli, kuinka laajamittaista tietojen kerääminen ja verkkovakoilu on.

NSA:N PROJEKTIT PRISM JA BULLRUN ESIMERKKEINÄ

Eniten kansainvälistä julkisuutta sai varmastikin alun perin kesäkuussa 2013 Guardian-lehden paljastama Yhdysvaltojen harjoittama verkkourkinta (Guardian 2013a). National Security Agency (NSA) vastaa Yhdysvaltojen kybervalvonnasta (NSA 2013). NSA:lla on henkilökuntaa 35000 henkilöä ja vuosibudjetti 11 miljardia dollaria (Washington Post 2013). Tästä 440 miljoonaa dollaria käytetään tutkimustyöhön. Täten NSA on epäilemättä parhaiten resursoitu tietoturva-asioiden tutkimuslaitos maailmassa. Guardianin uutisessa kerrottiin NSA:n PRISM-ohjelmasta, jonka budjetti on 20 miljoonaa dollaria vuodessa ja jossa suurimmat verkkotoimijat kuten Microsoft, Apple, Facebook ja Google ovat luovuttaneet NSA:lle suoran yhteyden kaikkiin käyttäjien tietoihin. Tietojen vuotaja Edward Snowden tuli uutisten julkaisun jälkeen julkisuuteen kertomaan motiiveistaan paljastaa Yhdysvaltojen toiminta. Tämän jälkeen Snowden on ollu maanpaossa, sillä Yhdysvalloissa häntä uhkaa tuomio vakoilusta. Tietoturvan kannalta huolestuttavinta ovat väitteet, että NSA olisi onnistunut ujuttamaan internetissä yleisesti käytössä oleviin salausmenetelmiin ja tietoturvaohjelmistoihin takaportteja, joiden avulla salaus pystytään purkamaan (Guardian 2013b). Tämän projektin nimi on Bullrun ja sen budjetti on vuositasolla 250 miljoonaa dollaria. Jos tällaisia takaportteja ohjelmistotuotteista löytyy, niin teoriassa on mahdollista muidenkin tahojen ne löytää. Bullrun-ohjelma on toiminut vuodesta 2000 eteenpäin.

Oman osansa valtioiden välisestä verkkovakoilusta sai myös Suomi. Ulkoministeriön viestintää oli seurattu jo useiden vuosien ajan (Ulkoministeriö 2013). Kyseessä oli niin kutsuttu APT-verkkohyökkäys (Advanced Persistent Threat). APT-hyökkäykseen liitetään termit kehittynyt ja pitkäkestoinen. Tyypillisesti hyökkääjällä on käytössään suuret resurssit ja useita erilaisia työkaluja, ja yleensä kyseessä onkin valtiollinen toiminta (Dell 2013).

POLIITTINEN HERÄÄMINEN TIETOTURVAUHKIIN

Kansallisesti ja EU-tasolla tietoturvauhkiin on varauduttu strategioiden luomisella ja lakimuutosten valmistelulla. Näistä tässä artikkelissa esitellään tarkemmin ensin Suomen kyberturvallisuusstrategia. Edellinen valtioneuvoston ICT-ympäristöä koskeva strategia oli Kansallinen tietoyhteiskuntastrategia 2007–2015 (Valtioneuvoston kanslia 2006), jonka tavoitteena oli tuoda kaikki suomalaiset verkkopalvelujen piiriin. Siinä yksi peruspilareista oli luottamus tietoyhteiskunnan toimijoihin ja palveluihin. Suomi on monella tasolla tietoyhteiskunta, vaikkakin tietyt ihmisryhmät tuntuvat syrjäytyvän kuten tämän julkaisun artikkelissa *Asiakkaan tietoturvatietoisuuden vahvistaminen – case Kansalaisen mikrotuki* kerrotaan. Nyt kun tietoyhteiskunnan luomisessa on onnistuttu kohtuullisen, hyvin huoleksi ovat nousseet tietoturvauhat. Osaavatko tietoyhteiskunnan asukkaat toimia tietoturvallisesti? Mielenkiintoista on myös kyber-termin nousu poliittisen puheen ykköstermiksi. Alun perin tieteiskirjallisuudesta liikkeelle lähtenyt termi on nyt keihäänkärkenä ajamassa poliittista päätöksentekoa eteenpäin. Termiin on ladattu sekä tieteellisestä että populaarikulttuurin eri puolilta uhkakuvia ja sodankäynnin konnotaatioita.

Jo ennen viimeisimpien tietoturvahyökkäysten tapahtumista uhkiin on reagoitu EU-direktiivin valmistelulla ja Suomessa julkaistiin Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategia tammikuussa 2013 (Valtioneuvosto 2013). Dokumentissa: ”Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. ” Kybertoimintaympäristö määritellään seuraavasti:

> *Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Tästä keskinäisriippuvaisesta ja moninaisesta sähköisessä muodossa olevan tiedon käsittelyyn tarkoitetusta ympäristöstä on kansainvälisesti ryhdytty käyttämään termiä kybertoimintaympäristö.*

Kyberturvallisuus perustuu koko yhteiskunnan tietoturvallisuuden järjestelyihin. Strategiassa on määritelty kymmenen linjausta, joilla suomalaista kyberturvallisuutta parannetaan. Varsinainen strategian toimeenpano-ohjelma julkaistaan keväällä 2014. Turun ammattikorkeakoulussa toimivalla tutkimusryhmällä Tietoliikenne ja tietoturva on käynnissä aktiviteetteja liittyen erityi-

sesti strategiseen linjaukseen *Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä*. Tähän toimintaan liittyy esimerkiksi vuosittainen tietoturvajulkaisu.

EU:n kyberturvallisuusstrategia julkaistiin helmikuussa 2013 (European Commission 2013). Sitä on valmisteltu samaan aikaan kuin kansallista strategiaa. Strategiassa ohjeistetaan EU:n alaisia organisaatioita ja jäsenvaltioita sekä esitetään komission sitoumukset sen toteutumiseen. Strategiassa nostetaan esiin viisi korkean tason päätavoitetta:

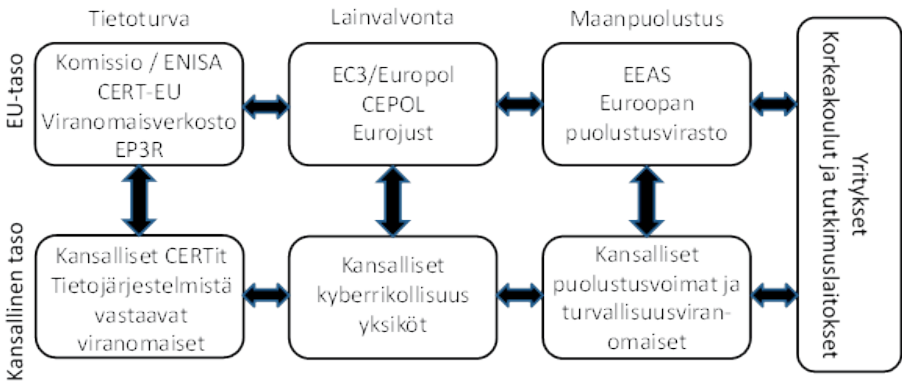
- Kyberkestävyyden saavuttaminen (achieving cyber resilience). Tällä toiminnalla pyritään julkisen ja yksityisen sektorin yhteistyöllä parantamaan EU:n sisäistä kyberkestävyyttä. Kestävyydellä tarkoitetaan kaikkien yhteiskunnan toimijoiden kyvykkyyttä toimia kyberympäristössä. EU:n alaisen The European Network and Information Security Agencyn (ENISA) roolia vahvistetaan. ENISAn tehtävänä on toimia Euroopanlaajuisena osaamiskeskittymänä tietoturvan saralla. Tämän lisäksi EU-lainsäädäntöä esitetään kehitettäväksi ja jäsenvaltioita patistetaan toteuttamaan EU-direktiivien toimeenpano. Tietoturvatietoisuutta pitää lisätä kaikilla tasoilla jäsenvaltioissa.

- Vähennetään kyberrikollisuutta (drastically reducing cybercrime). Lainsäädäntöä kehitetään ja rahoitusta lisätään tutkimukseen verkkorikollisuuden estämiseksi esimerkiksi Horizon 2020 -ohjelman kautta. Erityisenä tavoitteena on pyrkiä estämään lasten hyväksikäyttöä internetin välityksellä. Tavoitteena on vahvistaa yhteistyötä eurooppalaisten lainvalvontayksiköiden välillä kuten Europolin European Cybercrime Centre (EC3) ja Eurojust.

- Kehitetään kyberpuolustusvalmiuksia (developing cyberdefence policy and capabilities related to the Common Security and Defence Policy - CSDP) osana yleistä uhkien torjuntaa.

- Kehitään kyberturvallisuusteollisuutta ja sen teknologisia resursseja (develop the industrial and technological resources for cybersecurity). Tuetaan aihealueen teollisuutta saamaan kyberpuolustustuotteet markkinoille laajasti EU:n alueella.

- Huolehditaan, että tietoturva otetaan huomioon EU:n päätöksenteossa kaikilla tasoilla (establish a coherent international cyberspacepolicy for the European Union and promote core EU values). Parannetaan koordinaatiota organisaatioiden välillä ja varmistetaan, että tietoturvakäytänteet leviävät EU:n alueella.



KUVA 1. *Eri toimijoiden vuorovaikutussuhteet EU:n kyberstategiassa.*

Kuvassa 1 on esitelty, miten eri toimijat EU:n sisällä liittyvät kyberturvallisuusstrategiaan, joka jakaantuu EU- ja kansalliseen tasoon. Alla on selitetty kuvassa mainitut lyhenteet, joita ei vielä tekstissä ole esitelty.

- CERT on lyhenne sanoista Computer Emergency Response Team. Kyseisiä ryhmiä toimii jäsenmaissa ja EU:n laajuinen tiimi perustettiin vuonna 2012. Ne ovat vastuussa EU:n alaisten instituutioiden IT-järjestelmien tietoturvallisuudesta. Suomessa CERT-FI on ”viestintävirastossa toimiva kansallinen tietoturvaviranomainen, jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen” (CERT-FI 2013). Vuoden 2014 alusta CERT-FI:n tehtävät liitetään perustettavaan Kyberturvallisuuskeskukseen (Viestintävirasto 2013).

- The European Public-Private Partnership for Resilience (EP3R) on julkisen ja yksityisen sektorin yhteistyöfoorumi, joka pyrkii valmistautumaan laajamittaisiin häiriöihin sähköisessä viestinnässä ja niistä palautumiseen.

- European Police Collegen (CEPOL) rooli strategiassa on suunnitella koulutuksia lainvalvonnasta vastaaville tahoille.

- EEAS tarkoittaa Euroopan unionin ulkosuhdehallintoa eli yhteistyötä EU:n ulkopuolisten tahojen kanssa.

EU ohjaa jäsenvaltioiden lainsäädäntöä direktiivien avulla. Euroopan parlamentti ja neuvosto antoivat 12.8.3013 direktiivin 2013/40/EU *tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta*, jossa linjataan miten kansallisen lainsäätäjän tulee suhtautua tietoturvarikoksiin. Tämän direktiivin tavoitteina on yhtenäistää jäsenvaltioiden rikosoikeutta tietojärjestelmiin kohdistuvien hyökkäyksien osalta ja vahvistaa puitteet rikosten määrittelylle ja sovellettaville seuraamuksille. Tarkoitus on lisäksi parantaa yhteistyötä toimivaltaisten viranomaisten välillä jäsenvaltioiden poliisi- ja muut erikoistuneet lainvalvontaviranomaiset mukaan luettuina. Näiden lisäksi koordinaatiota kehitetään EU:n toimivaltaisten erityisvirastojen ja -elinten, kuten Eurojust, Europol (Euroopan verkkorikostorjuntakeskus), sekä Euroopan verkko- ja tietoturvaviraston (ENISA) välillä.

Myös tietosuojadirektiivi on uudistusten kohteena (European Commission 2012). Direktiivi-ehdotus on myötätuulessa ja se tulee varmistamaan, että yritysten on pakko ottaa tietosuoja- ja tietoturva-asiat vakavasti. Sakko huolimattomuudesta johtuvista tietomurroista voi olla jopa 5 % yrityksen vuosittaisesta liikevaihdosta tai maksimissaan 100 miljoonaa euroa. Direktiivissä tullaan säätämään myös henkilön oikeudesta poistaa tietonsa verkosta niin halutessaan. Tämä tulee vaikuttamaan erityisesti sosiaalisiin medioihin ja verkkomainostamiseen.

Suomen laissa on oma lukunsa tieto- ja viestintärikoksille. Rikoslain 38 luku (Rikoslaki 19.12.1889/39) käsittelee näitä asioita. Lain kehittymistä vuosien varrella on esitelty pro gradu -työssä *Tieto- ja viestintärikokset rikoslain 38 luvussa* (Jounio 2011). Kyseinen rikoslain luku uudistui vuonna 1995 käsittämään tieto- ja viestintärikokset. Sitä on muutettu lakimuutoksin viisi kertaa vuoden 1995 jälkeen. Kuitenkin KRP:n mukaan tällä hetkellä ”tietomurtorikosnimikkeen soveltamisala on hyvin kapea. Sitä voidaan soveltaa lähinnä vain silloin, kun tekijä on paljastunut ja epäonnistunut tavoitteessaan” (KRP 2013, 4). Suomessa oikeusministeriö on käynnistänyt direktiivin 2013/40/EU toimeenpanon (Oikeusministeriö 2013). Direktiivin edellyttämät kansalliset täytäntöönpanotoimet on tehtävä viimeistään 4.9.2015.

LÄHTEET

Arstechnica 2012 BlackHole 2.0 gives hackers stealthier ways to pwn. Viitattu 8.12.2013 http://arstechnica.com/security/2012/09/blackhole-2-0-gives-hackers-stealthier-ways-to-pwn/.

Business Insider 2013 This Diagram Shows How A Recent String Of Hacking Attacks Came From One Cyber Arms Dealer. Viitattu 8.12.2013 http://www.businessinsider.com/hacking-attacks-came-from-cyber-arms-dealer-2013-11.

Computerworld 2013 Hackers move to create next Blackhole after 'Paunch' arrest. Viitattu 8.12.2013 http://www.computerworld.com/s/article/9243070/Hackers_move_to_create_next_Blackhole_after_Paunch_arrest.

Dell 2013 Advanced Threat Resource Center. Viitattu 8.12.2013 http://go.secureworks.com/advancedthreats.

European Commission 2012 Commission proposes a comprehensive reform of the data protection rules. Viitattu 8.12.2013 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

European Commission 2013. Join(2013) 1 FINAL: joint communication to the european parliament, the council, the european economic and social committee and the committee of the regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta

Guardian 2013a NSA Prism program taps in to user data of Apple, Google and others. Viitattu 8.12.2013 http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Guardian 2013b Revealed: how US and UK spy agencies defeat internet privacy and security. Viitattu 8.12.2013 http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

IBM X-Force 2013. IBM X-Force 2012 Trend And Risk Report. Viitattu 8.12.2013. https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov12250.

IBTimes 2013 EU Votes in Data Protection Directive More Than Doubling Potential Fines. Viitattu 8.12.2013 http://www.ibtimes.co.uk/articles/516305/20131023/eu-data-protection-directive-approved-raising-fines.html.

Jounio, Anu 2011. Tieto- ja viestintärikokset rikoslain 38 luvussa, Lapin yliopisto.

KRP 2013. Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus. KRP 2400/2013/2121. Viitattu Viitattu 8.12.2013 http://www.poliisi.fi/poliisi/krp/home.nsf/files/82BCC556598FEBB7C2257C240024DB24/$file/Yritysturvallisuuden%20tilannekuva_Syksy_2013_nro14.pdf.

NSA 2013 About NSA - Mission. Viitattu 8.12.2013 http://www.nsa.gov/about/mission/index.shtml.

Oikeusministeriö 2013. Tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan EU:n direktiivin kansalliset täytäntöönpanotoimet. Viitattu 8.12.2013. http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/rikosoikeus/tietojarjestelmiinkohdistuvathyokkaykset.html.

PCMag.com 2013 LulzSec? Anonymous? Know Your Hackers. Viitattu 8.12.2013 http://www.pcmag.com/article2/0,2817,2387396,00.asp.

Symantec Corporation 2013. Internet Security Threat Report, 2012 Trends. Volume 18. Viitattu 8.12.2013 http://www.symantec.com/threatreport/.

Ulkoministeriö 2013. Tietoturvaloukkaus Suomen ulkoasiainhallinnossa. Viitattu 8.12.2013 http://formin.finland.fi/public/default.aspx?contentId=291701&nodeId=23&contentlan=1&culture=fi-FI.

Vainikka, Esko 2013. PK-yritysten ulkoistamien palvelujen tietoturva. Teoksessa Paavola J. & Vainikka E. (toim.) Näkökulmia tietoturvaan, Turun ammattikorkeakoulu, 14–38.

Valtioneuvoston kanslia 2006 Kansallisen tietoyhteiskunnan strategia 2007-2015. Viitattu 8.12.2013 http://vnk.fi/julkaisukansio/2006/tietoyhteiskuntaneuvosto/tietoyhteiskuntastrategia/fi.pdf.

Verizon 2013. 2013 Data Breach Investigations Report. Viitattu 8.12.2013. http://www.verizonenterprise.com/DBIR/2013/.

Viestintävirasto 2013. Kyberturvallisuuskeskus vahvistaa Viestintäviraston nykyisiä tietoturvatehtäviä. Viitattu 8.12.2013 https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2013/kyberturvallisuuskeskusvahvistaaviestintavirastonnykyisiatietoturvatehtavia.html.

Washington Post 2013 U.S. spy network's successes, failures and objectives detailed in 'black budget' summary. Viitattu 8.12.2013 http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html.

MURTAUTUMISTESTAUS – MITÄ SE TARKOITTAA JA MIKSI SITÄ TARVITAAN

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

KYBERSODANKÄYNTIÄ VAI KYBERPUOLUSTUSTA?

Elämme tietointensiivisessä maailmassa, jossa yritysten ja eri organisaatioiden toiminta perustuu yhä enemmän tietoon. Olemme erittäin riippuvaisia tietoverkkojen ja erilaisten tietojärjestelmien häiriöttömästä toiminnasta ja siten myös erittäin haavoittuvia. Suomen kyberturvallisuusstrategian (2013, 1) mukaan ”kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Suomi on osa globaalia maailmaa, jolle on ominaista muun muassa lähes kaikkialle ulottuvan, kaikille avoimen internetin ja erilaisten verkkopalvelujen käyttö sekä eri toimintojen ulkoistaminen.

Toimintaympäristöömme kohdistuu vaikutuksiltaan yhä vakavampia tietoturvauhkia sekä yksittäisten ihmisten että yritysmaailman ja eri organisaatioiden kannalta. Näiden uhkien aiheuttajat ovat nykyisin suurimmaksi osaksi täysin ammattimaisia sekä järjestäytyneitä. Suurimpana motiivina näillä kyberrikollisilla on rahan ansaitseminen eri tavoin. Tästä toiminnasta saa hyvän käsityksen Raj Samanin ja Francois Pagetin tuoreesta artikkelista Cybercrime Exposed, Cybercrime-as-a-Service (Samani & Paget 2013). Europolin mukaan kyberrikollisuus tulee yhä vain lisääntymään potentiaalisten kohteiden määrän ja niin kutsutun hyökkäyspinta-alan kasvaessa (Europol 2013, 28). Tämä ilmiö koskee myös Suomea Keskusrikospoliisin uuden raportin Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus mukaan (KRP 2013). Toisenlaiseen toimijajoukkoon kuuluvat eri haktivistiryhmät, joiden tärkeimpänä motiivina on erilaisten mielenilmausten esittäminen, mutta suoranaista sabotaasiakaan ei voida jättää ottamatta huomioon. Muun muassa paljon julkisuutta saanut Anonymous-ryhmä on hyvä esimerkki hak-

tivistiryhmistä. Oman lukunsa muodostavat valtiolliset tai niiden alaisuudessa toimivat tahot, joiden motiivina on useimmiten toisten valtioiden vakoilu, eri terroristijärjestöjen tai omien kansalaistensa toiminnan seuraaminen sekä teollisuusvakoilu. Yhtenä motiivina on lisäksi toisten valtioiden tiettyjen toimintojen häiritseminen, kuten oli laita Stuxnetin yhteydessä (Sanger 2012).

Yritykset ja organisaatiot joutuvat puolustautumaan sellaisia tahoja vastaan, jotka ilman valtuuksia yrittävät päästä käsiksi yritysten suojattuihin tietoihin ja tietojärjestelmiin. Tätä voidaan pitää suorastaan kybersodankäyntinä. Varsinaisesta valtioiden välisestä kybersodankäynnistä tämä eroaa siinä, että kyseessä on puolustustaistelu, jonka tavoitteena on hyökkäysten torjunta. On huomattava, että kaikki hyökkääjät eivät ole ulkopuolisia tahoja, vaan ne voivat olla myös yritysten tai organisaatioiden omia työntekijöitä.

Sodankäyntitaidossa yksi tärkeimmistä asioista on vihollisen taktiikan tunteminen. Lähes 2500 vuotta sitten eläneen mystisen kiinalaisen kenraalin Sun Tsun uskotaan kirjoittaneen: ”Tunne itsesi ja tunne vihollinen, sadassakaan taistelussa et ole vaarassa. Kun et tunne vihollista, mutta tunnet itsesi, ovat mahdollisuutesi voittaa tai hävitä yhtäläiset. Jos et tunne sen paremmin vihollista kuin itseäsi, häviät varmasti jokaisen taistelun.” (Sun Tsu 2012.) Nämä Sun Tsun lauseet pätevät erinomaisesti nykyisessä kyberpuolustustaistelussa, sillä yritysten ja organisaatioiden on tunnettava oma toimintaympäristönsä ja sen suojaamiseen tarvittavat tietoturvakontrollit, joiden toimivuutta on testattava säännöllisesti. Samoin niiden on tunnettava hyökkääjän toimintavat ja välineet mahdollisimman hyvin pystyäkseen puolustautumaan mahdollisimman tehokkaasti tunkeutumisyrityksiä vastaan. Hankalaksi tämän tekee se, että tietoturva-asiantuntijoiden mukaan aukotonta tietoturvaa ei ole olemassa. Riittävillä resursseilla ja osaamisella varustettu hyökkääjä pystyy tunkeutumaan kaikkien tietoturvakontrollien läpi niin halutessaan. Puolustautuja voi kuitenkin tehdä oikein valituilla tietoturvakontrolleilla hyökkääjän toiminnan mahdollisimman vaikeaksi ja aikaa vieväksi, jolloin tunkeutumisyrityksiin pystytään reagoimaan.

MURTAUTUMISTESTAUS – MITÄ JA MIKSI?

Murtautumistestauksella (Penetration testing) on pitkät perinteet tietoturva-alalla. Penetration testing -termi lienee esiintynyt ensimmäisen kerran 2000-luvun taitteessa. Siitä on pidetty lukuisia esityksiä eri foorumeilla, ku-

ten esimerkiksi Black Hat-, DEF CON- ja RSA-konferensseissa. Nyttemmin myös yksi suurimmista tietoturvallisuuden koulutusorganisaatioista, SANS.org, on ottanut tämän koulutuksen tarjontaansa. Murtautumistestauksesta keskustellaan alan asiantuntijapiireissä ja siitä sekä siihen liittyvistä asioista kirjoitetaan yleistajuisissa julkaisuissa yhä enemmän (mm. Tietoviikko 9/2013). Sen toteuttamiseen tarvittavat työkalut kehittyvät koko ajan, ja osa niistä on vapaasti saatavilla internetissä, kuten BackTrack 5 R3, ja nyttemmin sen korvannut Kali Linux -työkalukokoelma. Hyvän käsityksen Kali Linux -työkalupakin ohjelmista ja niiden käytöstä murtautumistestaukseen saa PenTest Magazine -lehden erikoisnumerosta 05/2013 (PenTest Magazine 2013).

Perinteisesti murtautumistestauksella ei ole ollut formaalia toteuttamistapaa, mutta nykyisin on toisin. Muun muassa PTES-standardi (Penetration Testing Execution Standard) (PTES 2013), NISTin Special Publication 800–115 *Technical Guide to Information Security Testing and Assessment* (NIST 2008) ja ISECOMin *OSSTMM* (the Open Source Security Testing Methodology Manual) (OSSTMM 2010) kuvaavat murtautumistestauksen prosessia ja antavat ohjeita sen suorittamiseen. Näistä PTES-standardi on yksityiskohtaisin. Se julkistettiin DerbyCon-konferenssissa Luisvillessä, USA:ssa, vuonna 2011. Tällä hetkellä käytössä on vuonna 2012 julkistettu PTES-standardin betaversio. (PTES 2013.)

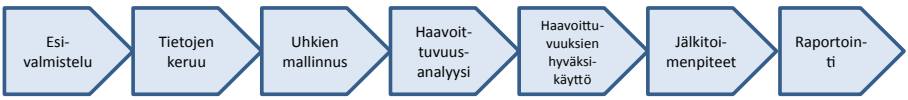
Murtautumistestaajasta käytetään usein nimitystä eettinen hakkeri (ethical hacker) tai White Hat -hakkeri (Walker 2012, 6). Tämän vastakohta on pahantahtoinen hakkeri, niin kutsuttu Black Hat -hakkeri, josta käytetään myös nimitystä krakkeri (cracker) (Walker 2012, 6). Näiden välimaastossa toimivasta henkilöstä käytetään puolestaan nimitystä Gray Hat -hakkeri (Walker 2012, 6). Hakkeri-termiin suhtaudutaan kuitenkin nykyisin varsin negatiivisesti, joten sen käyttöä kannattanee välttää ja käyttää sen sijaan varmuuden vuoksi termiä murtautumistestaaja.

Murtautumistestaajalla on oltava kohdeorganisaation lupa tehdä testaustaan. On huomattava, että hänellä on oltava lupa toimintaansa myös kaikilta asiaan liittyviltä palveluntarjoajilta, kuten esimerkiksi kaikilta testaajan ja kohteen välisistä verkkoyhteyksistä vastaavilta verkkopalvelujen tarjoajilta sekä ulkoistamistilanteissa myös asianomaiselta palveluntarjoajalta.

Miksi tällaisia lupia sitten tarvitaan? Viestintäviraston internet-yhteyspalveluja koskevan määräyksen 6 §:n johdosta verkkoyhteyksistä vastaavien palveluntarjoajien on seurattava omassa verkossaan tapahtuvaa liikennettä, jotta ne ha-

vaitsevat tietoturvaa vaarantavan verkkoliikenteen. Saman määräyksen 8 §:n mukaan palveluntarjoajan on kytkettävä asiakkaan verkkoliittymä irti internetistä, jos palvelun tietoturva vaarantuu oleellisesti liittymään kohdistuvan tai liittymästä lähtevän liikenteen johdosta. (Viestintävirasto 2011.) Rikoslain 38 luku (Rikoslaki 19.12.1889/39) käsittelee tieto- ja viestintärikoksia, joista ainakin tietoliikenteen ja tietojärjestelmän häirintään sekä tietomurtoihin liittyvien rikosnimikkeiden vuoksi testaajalla pitää olla tarvittavat luvat. Euroopan parlamentti ja neuvosto antoivat 12.8.2013 direktiivin 2013/40/EU Tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta, jonka mukaan myös tietotekniikkarikosten tekemiseen käytettävien välineiden tuottaminen, myynti, käyttöön hankkiminen, tuonti, levittäminen tai muu saataville asettaminen on rangaistavaa (Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, 7. artikla). Direktiivi korostaa kuitenkin, että edellä mainitut asiat eivät ole rikosoikeudellisesti rangaistavia tekoja, jos nämä välineet on alunperin tehty laillisia tarkoitusperiä varten, kuten tietojärjestelmien turvallisuuden testaamiseksi. Samoin tietojärjestelmien luvallinen testaaminen, kuten tietoturvakontrollien toimivuuden testaaminen, ei ole rangaistavaa. Direktiivissä määrätään myös jo osittain rikoslain 38. luvussa olevista asioista, joten kyseisen luvun sisältö tullee muuttumaan, sillä direktiivin määräämien seikkojen on oltava toteutettuina kansallisessa lainsäädännössä viimeistään 4.9.2015. Oikeusministeriö onkin asettanut 5.11.2013 työryhmän valmistelemaan edellä mainitun direktiivin täytäntöönpanoa (Oikeusministeriö 2013). Edellä mainitut asiat pätevät Suomessa ja tietyin osin koko Euroopan unionissa, mutta jos testaustilanteeseen liittyy EU:n ulkopuolisia toimijoita, on asianomaisten valtioiden lainsäädäntö ja muut määräykset otettava ehdottomasti huomioon.

Murtautumistestaus voidaan jakaa kolmeen päävaiheeseen: valmisteluun, testaukseen ja johtopäätösten tekemiseen (Walker 2012, 8). Valmisteluvaiheen ehkä tärkein tehtävä on määritellä ja sopia testauksen tarkka kohde kohdeorganisaatiossa (Harper ym. 2011, 158). Testauksen kohde voi olla esimerkiksi kohdeorganisaation kaikki tietojärjestelmät ja koko toiminta, tai se voi olla jokin yksittäinen tietojärjestelmä tai prosessi tai jopa henkilöstö. PTES-standardi jakaa murtautumistestauksen yksityiskohtaisemmin 7 vaiheeseen (kuvio 1) ja antaa yksityiskohtaisia ohjeita kunkin vaiheen toteuttamiseen.



KUVIO 1. *Murtautumistestauksen vaiheet (PTES 2013).*

NISTin Special Publication 800–115 määrittelee tietoturvatarkastuksen (Information Security Assessment) prosessiksi, jolla selvitetään, kuinka hyvin tarkastuksen kohteessa on toteutettu vaadittavat tietoturvatavoitteet. Tarkastuksen kohteena voi olla esimerkiksi yksittäinen tietojärjestelmä, sovellus, tietoverkko, jokin prosessi tai jopa joku henkilö. Tietoturvatarkastus voidaan toteuttaa kohteesta riippuen muun muassa testaamalla, perehtymällä dokumentaatioon tai haastattelemalla. (NIST 2008.) Tässä julkaisussa (NIST 2008) esitetään myös NISTin näkemys murtautumistestauksesta, joka noudattaa varsin hyvin edellä mainittua PTES-standardia. PenTest Magazinen numeron 05/2015 artikkeli Mapping Kali Usage to NIST 800–115 käsittelee hyvin mielenkiintoisella tavalla Kali Linuxin työkalujen käyttöä NISTin murtautumistestausprosessin eri vaiheissa (PenTest Magazine 2013).

Tietoturvatarkastus on ymmärretty aiemmin pelkäksi mahdollisten haavoittuvuuksien etsimiseksi tai olemassa olevien tietoturvakontrollien tarkastamiseksi tarkastuslistojen avulla. Joskus sillä on tarkoitettu pelkästään tarkastusta, jossa selvitetään noudattaako kohdeyrityksen tai -organisaation henkilöstö kohteen tietoturvapolitiikkaa sekä muita annettuja ohjeita. Se mitä tarkastuksella tarkoitetaan, mitä siinä tehdään, miten toimitaan tarkastuksen aikana ja miten tulokset raportoidaan, pitää aina sopia etukäteen.

Murtautumistestaus sekoitetaan usein haavoittuvuustarkastukseen, mutta kyseessä ei ole sama asia (Northcutt ym. 2006; Rapid7 2013). Suurin ero niiden välillä on, että murtautumistestauksessa pyritään käyttämään hyväksi löydettyjä haavoittuvuuksia ja murtautumaan kohteeseen niiden kautta. Toinen merkittävä ero on, että yleensä murtautumistestaus pyritään suorittamaan siten, että kohdeorganisaatio ja sen erilaiset valvonta- ja hälytysjärjestelmät eivät huomaa tietojen keruuta eivätkä varsinaista testausta. Englanninkielinen termi under the radar kuvaa osuvasti tätä toimintaa. Vasta raportointivaiheessa testauksen suorittaminen ja tulokset tulevat julki.

On olemassa useita syitä, miksi murtautumistestauksen tekeminen on välttämätöntä. Yksi tärkeimmistä syistä on löytää mahdolliset haavoittuvuudet ja korjata ne ennen kuin hyökkääjä hyödyntää niitä. Joissakin organisaatioissa

on esiintynyt tilanteita, joissa olemassa olevista haavoittuvuuksista on tiedetty, mutta joiden korjaamiseksi ei ole saatu organisaation johdon taholta riittävää tukea. Onnistuneen murtautumistestauksen jälkeen tilanne on useimmiten korjaantunut. Tietoturvakontrollien toimivuus voidaan luonnollisesti todentaa murtautumistestauksen avulla samoin kuin uusien tietojärjestelmien, sovellusten ja toimintatapojen turvallisuus ennen niiden ottamista tuotantokäyttöön. (Northcutt ym. 2006; Rapid7 2013.) Tietyillä toimialoilla murtautumistestaus on pakollista. Kaikkien yritysten ja organisaatioiden, jotka ottavat vastaan luottokorttimaksuja, on noudatettava kansainvälistä PCI DSS -standardia (Luottokunta 2013). Tasolla 1 olevien tahojen on teetettävä vuosittain valtuutetulla PCI-arvioijalla murtautumistestaus. Tälle tasolle kuuluvat myös tietomurron kohteeksi viimeisen vuoden kuluessa joutuneet tahot. (Luottokunta 2013; PCI DSS 2.0 2010.) On huomioitava, että uusi PCI DSS -standardin versio 3.0 hyväksyttiin marraskuun alussa 2013 ja se tarkentaa entisestään murtautumistestauksen suorittamista (PCI DSS 3.0 2013).

Murtautumistestaus voi olla luonteeltaan niin kutsuttu white box-, black box- tai gray box -testaus (Harper ym. 2011, 157). White box -testauksessa testaajalla on käytössään paljon ennakkotietoa kohteesta, kuten esimerkiksi verkkokaaviot, tietojärjestelmien käyttöjärjestelmät ja käytössä olevat sovellukset sekä niiden versiotiedot ja niin edelleen. Black box -testauksessa hänellä sen sijaan ei ole käytössään mitään ennakkotietoja kohdeorganisaation nimen lisäksi. Tämän tyyppisessä testauksessa tietojen keruuvaihe on äärimmäisen tärkeä (vrt. kuvio 1), jotta varsinainen testaus olisi mahdollisimman todenmukainen ja vastaisi erityisesti ulkopuolisten tunkeutujien toimintaa. Gray box -testaus puolestaan on kahden edellisen testaustyypin välimaastossa, ja siinä testaajalla on käytössään jo alkuvaiheessa jonkin verran etukäteistietoa kohteesta. Erityisen tehokas tapa toimia on tehdä murtautumistestaus kahteen kertaan: ensin black box -testaus ja sen jälkeen gray box -testaus tiettyihin organisaation tai yrityksen toiminnalle erittäin tärkeisiin kohteisiin.

MURTAUTUMISTESTAUKSEN KOULUTUS

Useat yritykset ja koulutusorganisaatiot järjestävät nykyisin koulutusta murtautumistestauksesta, ja niistä tunnetuimmat ovat SANS.org ja EC-Council. Myös KPMG tarjoaa nykyisin tämän alueen kursseja. Murtautumistestaajan on myös mahdollista hankkia esimerkiksi CEH (Certified Ethical Hacker)

-sertifikaatti EC-Council -järjestöltä (EC-Council 2013). Toinen tunnettu murtautumistestauksen sertifikaatti on GIAC:in (Global Information Assurance Certication) GPEN (GIAC Penetration Tester) -sertifikaatti, johon SANS.orgin järjestämät tämän alueen kurssit tähtäävät (SANS.org 2013, GIAC.org 2013).

Helmikuussa 2013 julkaistun ICT 2015 -työryhmän raportin 21 polkua kitkattomaan Suomeen (ehdotus vuodeksi 2013, polku 8 Tietoturva) mukaan tietoturva-alan koulutusta ja tutkimusta ehdotetaan lisättäväksi. Lisäksi raportissa ehdotetaan, että alan korkeakoulut lisäävät resursseja tietoturvaosaamisen koulutukseen ja liiketoimintalähtöiseen tutkimukseen. (Työ- ja elinkeinoministeriö 2013.)

Suomen kyberturvallisuusstrategian (2013, 5) mukaan ”kyberturvallisuuteen tähtäävän tutkimuksen, kehittämisen ja koulutuksen toteuttaminen eri tasoilla vahvistaa kansallista osaamista ja Suomea tietoyhteiskuntana. Kyberturvallisuuden kehittämisessä panostetaan voimakkaasti kybertoimintaympäristön tutkimukseen, koulutukseen, työllistymiseen ja tuotekehitykseen, jotta Suomi voisi kehittyä yhdeksi kyberturvallisuuden johtavista maista”. Saman strategian mukaan ”kyberturvallisuuden perustutkimuksen, soveltavan tutkimuksen ja innovaatiotoiminnan edellytyksiä vahvistetaan yliopistoissa ja tuotekehitystyön edellytyksiä vahvistetaan ammattikorkeakouluissa. Lisätään mahdollisimman nopeasti kyber-/tietoturvakursseja korkeakouluihin ja ammattikorkeakouluihin. Lisätään tietoturva-alan aloituspaikkoja alan koulutusta antavissa oppilaitoksissa sekä lisätään sivuainekursseja kyberturvallisuudesta.” (Suomen kyberturvallisuusstrategia 2013, 31–32.)

Turun ammattikorkeakoulussa on aloitettu murtautumistestaukseen liittyvä perusopetus syksyllä 2012, jolloin tutustuttiin muutamiin BackTrack 5 R5 -järjestelmän työkaluihin. Huolimatta varsin vähäisestä tämän aihealueen kokemuksesta Turun ammattikorkeakoulun opiskelijat menestyivät kohtalaisesti helmikuussa 2013 University of Ontario Institute of Technologyn järjestämässä CTF- (Capture The Flag) kilpailussa (Digitoday 2013). Tarkemmin kilpailusta opiskelijan näkökulmasta kerrotaan tämän julkaisun artikkelissa *Tietoturvakilpailu oppimisen vauhdittajana*.

Kesällä 2013 tietojenkäsittelyn koulutusohjelman opiskelija teki opinnäytetyönään oppimisympäristön (Penetration Testing Learning Environment) murtautumistestauksen opetusta ja opiskelua varten. Tässä oppimisympäristössä tärkeimpänä työkaluna on toistaiseksi Kali Linux -työkalupakki, mutta

muita työkaluja tullaan lisäämään siihen lähitulevaisuudessa. Oppimisympäristöä käytettiin ensimmäisen kerran syksyn 2013 Tietoturva-opintojakson laboratoriotyöskentelyssä. Erilaisia tietoturvatarkastuksia ja murtautumistestauksia tietojenkäsittelyn koulutusohjelman opiskelijat ovat tehneet kohdeyrityksiin tarkastuslistojen, haavoittuvuusskannerien ja testaustyökalujen avulla.

Murtautumistestauksen ja siihen liittyvien asioiden opiskelu on osa laajempaa Turun ammattikorkeakoulun tietoturva-alan opiskelua. Lisäksi Turun ammattikorkeakoulussa toimii Tietoturva ja tietosuoja -tutkimusryhmä, jonka toimintaan opiskelijat osallistuvat erilaisissa tutkimusprojekteissa.

YHTEENVETO

Yritysten ja organisaatioiden ainoa keino selviytyä puolustustaistelusta tunkeutujia vastaan on suojautua mahdollisimman hyvin ja murtotestata suojaustensa toimivuus. Tunkeutujat muuttavat jatkuvasti toimintatapojaan ja työkalujaan ja puolustautujan pitää tuntea ne. Erityisesti PK-sektorin yrityksille tämä on erittäin haastavaa johtuen niiden käytössä olevista resursseista ja usein myös riittävän osaamisen puutteesta. Tähän voidaan vaikuttaa kouluttamalla lisää tietoturva-asiantuntijoita ja perehdyttämällä yritysten ja organisaatioiden omaa henkilöstöä näihin asioihin.

LÄHTEET

Digitoday 2013. Suomalaisopiskelijat hakkeriharjoituksessa: Selvittivät Yhdysvaltojen sotilastukikohdat. Viitattu 22.11.2013 http://www.digitoday.fi/tietoturva/2013/04/16/suomalaisopiskelijat-hakkeriharjoituksessa-selvittivat-yhdysvaltojen-sotilastukikohdat/20135453/66.

EC-Council 2013. Viitattu 9.11.2013 http://www.eccouncil.org/.

Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU.

Europol. 2013. SOCTA 2013. Viitattu 8.11.2013 https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf.

GIAC.org. 2013. Viitattu 9.11.2013 http://www.giac.org/.

Harper, A.; Harris, S.; Ness, J.; Eagle, C.; Lenkey, G. & Williams, T. 2011. Gray Hat Hacking. The Ethical Hacker's Handbook. McGraw-Hill: New York.

KRP 2013. Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus. KRP 2400/2013/2121. Viitattu 15.11.2013 http://www.poliisi.fi/poliisi/krp/home.nsf/files/82BCC556598FEBB7C2257C240024DB24/$file/Yritysturvallisuuden%20tilannekuva_Syksy_2013_nro14.pdf.

Luottokunta 2013. Kauppiaan raportointivelvollisuudet. Viitattu 22.11.2013 http://www.luottokunta.fi/Kaupoille/Korttimaksamisen_turvallisuus/Raportointi/.

NIST 2008. NIST SP800-115 Technical Guide to Information Security Testing and Assessment. Viitattu 15.11.2013 http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Siles, R. & Mancini, S. 2006. Penetration Testing: Assessing Your Overall Security Before Attackers Do. SANS. org. Viitattu 22.11.2013 http://www.sans.org/reading-room/analysts-program/PenetrationTesting-June06.

Oikeusministeriö 2013. Tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan EU:n direktiivin kansalliset täytäntöönpanotoimet. Viitattu 15.11.2013 http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/rikosoikeus/tietojarjestelmiinkohdistuvathyokkaykset.html.

OSSTMM. 2010. Open Source Security Testing Methodology Manual. Viitattu 16.10.2013 http://www.isecom.org/research/osstmm.html.

PCI DSS 2.0. 2010. Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures Version 2.0. Viitattu 22.11.2013 https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

PCI DSS 3.0. 2013. Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures Version 3.0. Viitattu 22.11.2013 https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

PenTest Magazine 2013. Kali Linux. Vol. 3, No. 5.

PTES. Penetration Testing Execution Standard. Viitattu 16.10.2013 http://www.pentest-standard.org/index.php/Main_Page.

Rapid7. 2013. What is Penetration Testing. An Introduction for IT Managers. Viitattu 12.10.2013 http://information.rapid7.com/what-is-penetration-testing-whitepaper.html?LS=1138726.

Rikoslaki 19.12.1889/39.

Samani, R. & Paget, F. 2013. Cybercrime Exposed, Cybercrime-as-a-Service. Viitattu 8.11.2013 http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf.

Sanger, D. 2012. Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times. Viitattu 8.11.2013 http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all.

SANS.org. 2013. Viitattu 9.11.2013 http://www.sans.org/.

Sun Tsu. 2012. Sodankäynnin taito. Tietosanoma Oy: Porvoo.

Suomen kyberturvallisuusstrategia. 2013. Viitattu 8.11.2013 http://www.yhteiskunnanturvallisuus.fi/fi/component/search/?searchword=kyber&ordering=&searchphrase=all.

Työ ja elinkeinoministeriö. 2013. ICT-2015 työryhmän raportti. 21 polkua Kitkattomaan Suomeen. Työ- ja elinkeinoministeriön julkaisuja 4/2013.

Viestintävirasto 2011. Määräys Internet-yhteyspalvelujen tietoturvasta 13 B/2011M. Viitattu 15.11.2013 https://www.viestintavirasto.fi/ohjausjavalvonta/lainsaadanto/maaraykset/maarays13internet-yhteyspalvelujentietoturvasta.html.

Walker, M. 2012. CEHTM Certified Ethical Hacker All-In-One Exam Guide. McGraw-Hill: New York.

TIETOSUOJA JA TUNNISTAUTUMINEN

VERKKOPALVELUN TARJOAJA – KUNNIOITATKO KÄYTTÄJÄN YKSITYISYYTTÄ?

Matti Laakso, Tradenomi
IT-suunnittelija, Turun ammattikorkeakoulu

Verkkopalveluiden käyttäjien tietosuojaa – henkilön itsemääräämisoikeutta omiin tietoihin – käsitellään eri medioissa aina silloin tällöin. Kansalaisille uutisoidaan, miten heidän liikkeitään eri verkkopalveluissa seurataan. Samoissa uutisissa käyttäjää valistetaan digitaalisen jalanjäljen pienentämisestä ja siitä, miten seurannalta voi suojautua teknisten keinojen avulla. Vastuu suojautumisesta jätetään kuitenkin aina käyttäjälle itselleen. Harvemmin mainitaan siitä, että suomalaiset verkkopalvelut keräävät käyttäjän toiminnasta automaattisesti tietoja ja siirtävät niitä suoraan ulkomaalaisten pörssiyhtiöiden hyödynnettäviksi. Verkkopalvelun tarjoaja ei aina ymmärrä, että näin tapahtuu.

Tämän artikkelin tarkoituksena on kääntää ajattelumalli toisin päin. Verkkopalveluiden tarjoajien tulisi pohtia sivustojensa toteutusta uudelleen sellaiseksi, että niissä huomioitaisiin paremmin käyttäjien yksityisyys ja tietosuoja. Alan lehdissä on puhuttu, että Suomesta voisi tulla tiedon turvasatama (Tietotekniikan liitto ry 2013). Mutta miten suomalaiset voivat herättää luottamusta muualla maailmassa, elleivät he kunnioita edes omien kansalaistensa tietosuojaa?

MIKSI VERKKOPALVELUT HALUAVAT KERÄTÄ KÄYTTÄJÄSTÄ TIETOJA?

Suurin motiivi erilaisten tietojen keruulle ja hyödyntämiselle on rahan ansaitseminen. Esimerkiksi yritysten ensisijaisena tavoitteena on saada verkkopalvelun vierailijat asiakkaiksi. Seuraamalla ja keräämällä tietoa asiakkaiden toiminnasta sivustolla voidaan päätellä, millaiset palvelut ja tuotteet kiinnostavat eniten, mitä tietoja käyttäjät etsivät sivustolta ja millaista sisältöä sivustolle kannattaa tuottaa.

Verkkokauppojen asiakkaat halutaan saada ostamaan mahdollisimman paljon ja usein. Kun seurataan asiakkaan ostokäyttäytymisiä ja kiinnostuksen kohteita, niin jatkossa hänelle voidaan tarjota juuri häntä kiinnostavia tuotteita ja palveluita. Tietyille asiakasryhmille kannattaa tarjota tuotteita erityistarjouksilla, koska todennäköisyys ostamiselle on suurempi.

Osa verkkopalveluista tuottaa rahaa mainostulojen avulla. Mainokset saattavat olla kaikille samoja tai vaihdella vierailijan mukaan. Mitä tarkemmin sivuston tarjoaja tietää vierailijoiden kiinnostuksen kohteet, sitä tarkemmin mainoksia pystytään kohdentamaan tietylle käyttäjäryhmälle. Verkkopalvelun tarjoaja hyötyy mainospaikkojen myynnistä, ja mainostajan hyöty puolestaan näkyy tuotteiden tai palveluiden myynnin kasvuna.

TIETOJEN KERÄÄMISEN HAITTAPUOLET

Suomalaisen IT-palveluyhtiö Descomin tutkimuksen mukaan yli 90 % suomalaisista hyväksyy verkkokauppojen tekemän kävijöiden seurannan ja tietojen analysoinnin, mikäli käyttäjä hyötyy tästä parempana palveluna ja tarjouksina (Descom 2013). Alennetut hinnat ovat käyttäjän näkökulmasta hyvä asia, joten miksi tietojen kerääminen olisi haitallista?

Lähtökohtaisesti eri verkkopalveluissa tapahtuvasta tietojen keruusta ei ole haittaa, jos käyttäjä voi etukäteen selvittää, mitkä tiedot hänestä kerätään, missä tietoja säilytetään, kuka tietoja käsittelee, ja lopuksi vielä päättää, haluaako hän sallia keräämisen vai ei. Valitettavasti tämä selvittäminen ei aina ole mahdollista. Sen sijaan käyttäjästä kerätään tietoa jatkuvasti hänen tietämättään, ja kyseistä materiaalia käytetään kauppatavarana eri yritysten välillä. Tietoja siirtyy myös ulkomaille täysin ulkopuolisten yritysten hyödynnettäviksi. On olemassa liiketoimintaa, jonka tarkoituksena on myydä käyttäjien tietoja eteenpäin.

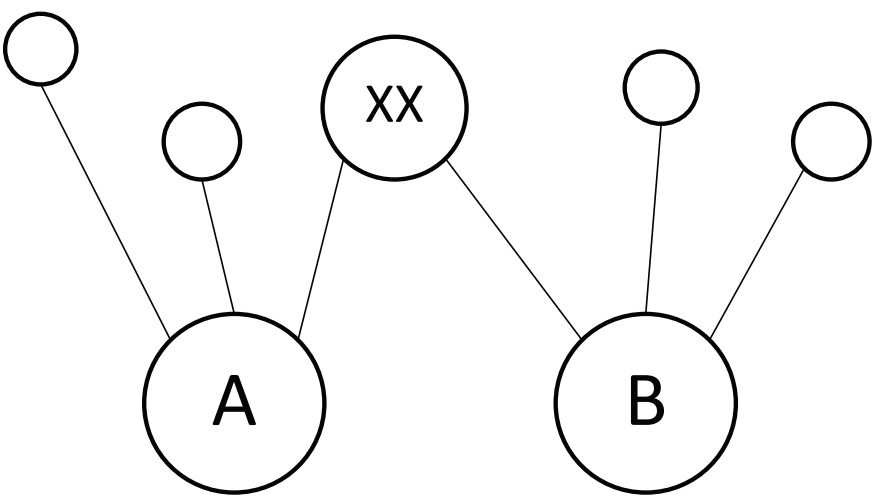
Jokainen internetiä paljon käyttänyt on varmasti huomannut tämän ilmiön: tietyt verkkosivustot ja sosiaalisen median palvelut mainostavat käyttäjälle juuri sellaisia tuotteita, joita hän on hetki sitten verkosta etsinyt. Tämä on mahdollista, koska eri verkkopalvelut ovat muodostaneet käyttäjästä ja hänen kiinnostuksen kohteistaan kattavan profiilin, jota sitten myydään eteenpäin halukkaille ostajille.

Harva kansalainen tulee kuitenkaan ajatelleeksi, että samalla tavalla kaikki esimerkiksi terveyteen liittyvät verkkohaut ja -selailut tallentuvat seurantaprofiileihin. Kukaan ei voi tietää, mihin tällaisia tietoja käytetään tulevaisuudessa – tai kuka tietoja hyödyntää. On pelottavaa ajatella, että jokin kaupallinen taho tietää mielenkiinnon kohteistamme enemmän kuin esimerkiksi puolisomme.

YHDET KÄYTTÄJÄTIEDOT – MONTA HYÖDYNTÄJÄÄ

Verkkopalveluiden käyttäjien tiedot voidaan kerätä automaattisesti eri tekniikoiden avulla tai manuaalisesti käyttäjältä itseltään esimerkiksi kommenttikenttien sekä palaute- ja rekisteröintilomakkeiden avulla. Automaattinen tietojen keräys on usein käyttäjälle täysin näkymätöntä, koska kerääminen tapahtuu verkkosivujen selaamisen yhteydessä.

Kävijöiden seurantaan tarkoitetut ohjelmistot on yleensä helppo ottaa käyttöön. Verkkopalveluiden ylläpitäjien tarvitsee vain lisätä seurantapalvelun tarjoama ohjelmistokoodi omille verkkosivuilleen. Aina kun vierailija käy seurantaa harjoittavalla verkkosivustolla, lataa käyttäjän selain sivujen lisäksi myös seurantakoodin.



KUVA 1. *Sivustojen A ja B seurantakoodit ottavat yhteyttä ulkopuoliseen palveluntarjoajaan XX.*

Yksi tietojen keräämisen suurimmista ongelmista liittyy siihen, että osa seurantakoodeista ottaa suoraan yhteyden myös ulkopuoliseen palveluntarjoajaan. Kuviossa 1 havainnollistetaan seurantatapahtumaa. Jos käyttäjä vierailee verkkosivustolla A, niin seurantakoodi ladataankin ulkomaalaisen yrityksen palvelusta XX. Tällöin palveluntarjoaja XX tietää käyttäjän vierailleen sivulla A. Jos sama seurantamekanismi on käytössä sivustolla B, niin se sama ulkomaalainen yritys XX tietää käyttäjän olleen myös sivustolla B.

Kyseessä ei ole pelkästään kävijäseurantaohjelmistoihin liittyvä ongelma, sillä samaa tekniikkaa käytetään myös sosiaalisen median yhteisöliitännäisissä sekä mainostamiseen tarkoitetuissa ohjelmistoissa. Kyseiset palvelut tarjoavat samaan tapaan verkkosivuille lisättävää ohjelmistokoodia, joka on lopulta yhteydessä kolmanteen osapuoleen. Yksi suomalainen verkkosivusto saattaa siis sisältää useita yhteyksiä ulkopuolisiin järjestelmiin, jotka automaattisesti keräävät tietoa sivuston vierailijoista.

Vinkki: Mozilla Firefox -selaimeen on saatavilla lisäosa, joka havainnollistaa kuvion 1 tapaisesti verkkosivustoilla tapahtuvaa tietojen keräämistä ja siirtämistä. Löydät sen Firefoxin Add-ons-valikosta nimellä Lightbeam.

KÄYTTÄJÄN VAIKUTUSMAHDOLLISUUDET

Verkossa liikkuvien käyttäjien on mahdollisuus vaikuttaa siihen, kuinka laajasti heistä pystytään keräämään tietoja eri seurantamenetelmien avulla. Uudemmissa nettiselaimissa on olemassa niin sanottu Älä seuraa / Do not track -toiminto. Kun kyseinen toiminto on otettu käyttöön, niin nettiselain kertoo verkkopalvelulle sivua aukaistaessa, että käyttäjä ei halua tulla seuratuksi. Verkkopalvelun tarjoajan vastuulle jää päättää, kunnioittaako se käyttäjän toivetta vai ei.

Nettiselaimiin on mahdollista asentaa myös erillisiä lisäosia, joiden avulla pystyy rajoittamaan tietoja keräävien ohjelmakoodien toimintaa. Lisäosia on olemassa kymmeniä. Yksi tunnetuimmista on nimeltään NoScript. Kyseiset toimet rajoittavat käyttäjästä kerättävän tiedon määrää, mutta täydellinen keräämisen estäminen vaatii työtä. Miksi käyttäjän pitää erikseen nähdä paljon vaivaa ansaitakseen yksityisyytensä?

KÄYTTÄJÄN YKSITYISYYDEN KUNNIOITTAMINEN

Verkkopalveluiden tarjoajat ovat olennaisessa osassa yksityisyyden suojan toteuttamisessa. Tekemällä oikeat hallinnolliset ja tekniset päätökset yritys voi edelleen kerätä käyttäjästä tietoa, mutta samalla myös huolehtia hänen yksityisyydestään.

Ohessa on listattuna asioita, jotka toteuttamalla teet verkkopalvelustasi asiakasystävällisemmän tietosuojan näkökulmasta.

1. Tee päätös, että käyttäjän tahtoa kunnioitetaan. Jos verkkopalvelusi vierailijan selain kertoo, että käyttäjä ei halua tulla seuratuksi, niin älä aktivoi kävijäseurantaa.
2. Määrittele, mitä tietoja on kerättävä ja miksi. Sen jälkeen kerää vain tarvitsemasi tiedot. Jotkin keräysohjelmat voidaan käskeä tallettamaan vain halutut tilastolliset tiedot.
1. Päätä, että kerättyjä tietoja ei siirretä ulkomaille. Markkinoilla on tuotteita, joissa keräysohjelmat toimivat yrityksen omilla palvelimilla ja kerätyt tiedot jäävät vain ja ainoastaan yrityksen omaan käyttöön. Esimerkkinä tästä on avoimen lähdekoodin ohjelmisto Piwik.
2. Mieti, miten sosiaalisen median yhteisöliitännäiset otetaan käyttöön. Ladataanko ne sivuston yhteydessä vai vasta sitten, kun käyttäjä haluaa painaa kyseistä nappia.
3. Kerro avoimesti kerättävistä tiedoista ja keräämisen tarkoituksesta palvelusi tietosuojaselosteessa. Läpinäkyvä ja rehellinen toiminta herättää luottamusta.

Käyttäjän yksityisyyden kunnioittaminen ei perustu pelkästään hyvään tahtoon, vaan asiasta on säädetty myös Suomen laissa. Kun puhutaan verkkopalvelun käyttäjän tietojen keräämisestä sekä käsittelystä, on tunnettava henkilötietolaki ja sähköisen viestinnän tietosuojalaki. Euroopan unionissa on myös suunnitteilla uusi lakiasetus, jonka tarkoituksena on ottaa kantaa verkkopalveluiden käyttäjien tietosuojaan.

Lainsäädännöllisten asioiden lisäksi aihetta kannattaisi ajatella myös eettisestä näkökulmasta. Myytkö verkkopalvelusi käyttäjien yksityisyyden oman etusi nimissä?

LÄHTEET

Descom 2013. Tutkimus: Suomalaiset hyväksyvät verkkokauppojen kävijäseurannan. Viitattu 4.11.2013 http://www.descom.fi/fi/what+is+new/news/suomalaiset+hyvaksyvat+verkkokauppojen+kavijaseurannan.

Tietotekniikan liitto ry 2013. Suomesta tietoturvan turvasatama? Viitattu 4.11.2013 http://www.ttlry.fi/news/201309/suomesta-tietoturvan-turvasatama.

MITEN PARANTAA SÄHKÖISEN TENTIN TIETOTURVAA JA YKSITYISYYDEN SUOJAA?

Matti Kuikka, FM
Lehtori, Turun ammattikorkeakoulu

Sähköinen tenttiminen tuo haasteita tenttijälle ja opettajalle sekä muille järjestelmiä ja tietoja käsitteleville tahoille. Tämä artikkeli pohtii näitä haasteita ja analysoi käytettyjä ja ehdotettuja ratkaisuja käyttäen esimerkkinä Turun ammattikorkeakoululla tällä hetkellä käytössä olevaa ratkaisua – Sordino Soft Tutor (http://www.sordino.fi).

OPISKELIJAN TUNNISTAMINEN HAASTEET

Tunnistamisen tarkoituksena sähköisessä tentissä on varmistaa opiskelijan identiteetti sekä varmistaa, että opiskelija todella on se, joka hän väittää olevansa. Apampa, Wills ja Argles (Apampa et. al. 2010) tutkivat sähköisen tentin haasteita ja määrittelivät neljä toisena persoonana esiintymisen (imitoinnin) uhkaa:

- Valvoja ei huomaa tai huomioi väärinkäytöstä (tyypin A uhka).
- Opiskelija antaa tunnuksensa toiselle, joka tekee tentin (tyypin B uhka).
- Opiskelija aloittaa itse tentin, mutta tekijä vaihtuu tentin aikana (tyypin C uhka).
- Toinen henkilö auttaa opiskelijaa tentin aikana (tyypin D uhka).

YKSITYISYYDEN SUOJAN HAASTEET

Opiskelijan näkökulma

Tenttijärjestelmä kerää opiskelijasta henkilökohtaista tietoa. Opiskelijanumero, nimi, puhelinnumero tai sähköpostiosoite voidaan kerätä ilmoittautumisen yhteydessä. On myös mahdollista, että muuta henkilökohtaista tietoa tallennetaan tentin aikana. Tentin vastaukset ja tulokset tallentuvat järjestelmään. Tämän takia on tärkeää, että tietoihin pääsy on rajoitettu vain tenttivälle opettajalle ja järjestelmän pääkäyttäjille opiskelijan lisäksi.

Opiskelijan vastausten tallentaminen luotettavasti tentin aikana luo myös haasteita erityisesti, jos vastattaessa käytetään erillisiä dokumentteja. Liitteet eivät tallennu automaattisesti itse tenttijärjestelmään, vaan ne tallentuvat vasta siinä vaiheessa, kun opiskelija liittää ne vastaukseensa. Tapahtuu kuitenkin tilanteita, joissa liitettä ei ole ehditty tai muistettu tallentaa ajoissa vastaukseksi, jolloin työ menee hukkaan. Tenttien vastauksia tulee myös arkistoida: opiskelijan vastauksia ei saa poistaa järjestelmästä ennen kuin se on ohjesääntöjen mukaan sallittu.

Opettajan näkökulma

Opettajan tulee itse voida päättää, kuka käyttää hänen laatimiaan tehtäviä. Kuitenkin tehtävien jakamisen ja käyttämisen pitää olla helppoa. Järjestelmä tulee olla varmistettu myös mahdollisten opettajan tekemien virheiden varalta: tenttien ja vastausten poistaminen tulee olla joko kokonaan estetty tai varoitustekstein varmistettu.

LAITTEISTOJEN JA TIETOJÄRJESTELMIEN HAASTEET

Opiskelijan päätelaitteet

Opiskelijoilla tulee tentissä olla laite (tietokone), jonka avulla ja selaimen välityksellä tehtävät tehdään. Koulussa voi olla **tenttiakvaariotila**, jossa tentti voidaan tehdä. Tenttiakvaarioiden päätteistä ei yleensä pääse muualle kuin sähköiseen tenttijärjestelmään, mutta avoin tai rajoitettu internetyhteys voi olla sallittu akvaariosta. Tentin vastaukset tallentuvat käytettyihin päätelaitteisiin, joten akvaarion pääte on yleensä sellainen, josta tiedot hävitetään esi-

merkiksi virtuaalisointitekniikalla (Golden 2011). Virtuaalipäätteiden tekniset ongelmat voivat myös johtaa keskeneräisten tietojen häviämiseen. Tämän takia on tärkeää, että vastaukset ja niiden liitetiedostot tallennetaan tietyin väliajoin järjestelmään.

Koulun **(tietokone)luokkia** voidaan myös käyttää tenteissä. Kaikilla opiskelijoilla on tällöin samanlaiset tietokoneet, ja heillä voi olla normaali pääsy Internetiin. Tällöin opiskelijalla on myös yleensä pääsy omalle työalueelle internetin lisäksi. Opiskelija voi käyttää myös **omaa tietokonettaan** (esimerkiksi kannettavaa tai tablettia) tentin aikana, jolloin opiskelijalla on mahdollisuus käyttää muita tietovarastoja.

Opiskelijan tietokonetta voidaan myös käyttää rajoitetusti tentin aikana. Tietokone voidaan esimerkiksi **käynnistää ulkoiselta medialta** (kuten USB-tikulta), jolloin käytössä on tietty käyttöjärjestelmä (esimerkiksi Linux) ja vain tietyt ohjelmat ja sallitut ulkoiset yhteydet. Tämä toimintapa tullee olemaan yleinen sähköisissä massatenteissä. Opiskelijat ovat myös toivoneet voivansa käyttää sähköisessä tentissä paperia ja kynää ja **skannata** vastaukset tiedostoina tentin vastaukseksi.

Käyttöjärjestelmän luotettavuus on tärkeä tekijä opiskelijan päätelaitteilla. Perinteinen toimintapa ongelmatilanteissa, eli lopeta prosessi, sulje ikkuna tai uudelleenkäynnistä tietokone, ei sovellu sähköiseen tenttiin, koska tietoa ei haluta häviävän ongelmatilanteissa.

Tenttijärjestelmä

Tenttijärjestelmä voidaan toteuttaa paikallisesti tenttitilassa (omalla paikallisella palvelimella), koulun omalla palvelimella (IT-konesalissa) tai pilvipalveluna internetissä (ulkoisella palvelimella).

Tenttitilan oma palvelin on näistä turvallisin, koska mahdolliset ongelmat tilan ulkopuolella eivät vaikuta tentin suoritukseen. Sähkökatkot tosin voivat aiheuttaa ongelmia tässäkin tapauksessa. Kokeen aikana kaikki opiskelijoiden tietokoneet kommunikoivat palvelimen kanssa.

Koulu voi ylläpitää **erillistä tenttipalvelinta**, johon ollaan yhteydessä sisäisen verkon kautta. Yhteys tenttitiloista voi olla rajoitettu vain tähän palvelimeen. Tietoverkon ongelmat voivat vaikuttaa tentin suoritukseen.

Sähköinen tenttijärjestelmä voidaan toteuttaa **pilvipalveluna**, jolloin se näkyy käyttäjille palveluna internetin välityksellä ja sitä käytetään selaimen välityksellä. Pilvipalveluissa verkon ongelmat voivat aiheuttaa häiriöitä palvelun käytössä.

Vaikka oma palvelin onkin turvallisin vaihtoehto, kustannukset sen ylläpidossa ovat huomattavasti suuremmat kuin keskitetyssä mallissa. Keskitetylle palvelimelle voidaan edullisemmin toteuttaa Telecom-maailmassa käytettyjä toimintatapoja, kuten kahdennetut palvelimet (Active & Standby palvelimet), jolloin päästään jopa 99,999% luotettavuuteen itse palvelun saatavuuden kohdalla.Ne eivät kuitenkaan auta verkkohäiriöiden osalta.

Wiak, Jeske, Krasuski ja Stryjek painottivat lisäksi, että tenttijärjestelmässä tulee olla riittävästi kapasiteettia jopa tuhansia samanaikaisia käyttäjiä varten. Klusteripalvelimia tarvitaan kuorman tasaukseen (load balancing). (Wiak et. al. 2011.)

Opiskelijan tunnistamis- ja valvontajärjestelmät

Opiskelija tunnistetaan ja häntä valvotaan tentin aikana. Tyypillisesti käytössä on useampia menetelmiä samanaikaisesti, jotta eri tyypin uhat saadaan minimoitua. Tunnistamisjärjestelmät jaotellaan perinteisesti seuraavasti: 1. Tietämystekijöihin perustuvat menetelmät, 2. Omistajuustekijöihin perustuvat menetelmät, 3. Biometrisiin tekijöihin perustuvat menetelmät, jotka kattavat sekä fyysiset tekijät että käyttäytymistekijät. (Gao 2010.)

Tietämystekijät (Something user knows):

- Käyttäjänimi ja salasana, mikä on perinteisin tunnistamismenetelmä.
- Tentissä voidaan myös esittää opiskelijaan liittyviä henkilökohtaisia kysymyksiä, joihin vain opiskelija tietää vastauksen, jotta opiskelijan vaihtuminen tentin aikana voidaan huomata (Tyypin B ja C uhat).

Omistajuustekijät (Something user has):

- Älykortti (esimerkiksi SIM-kortti, sirullinen henkilökortti, pankki/luottokortti tai USB-tikku).

Biometriset Tekijät:

- Fyysiset tekijät (Something user is):
  - Sormenjälki, joka on käytetyin biometrinen menetelmä.
  - Muita tunnistamiseen soveltuvia biometrisiä menetelmiä ovat esimerkiksi: kasvojen tunnistus, verkkokalvon (iiris) skannaus, pään geometrian tunnistus, kämmenenjäljen tunnistus, käden tai sormen geometrian tunnistus ja lämpökuvaus.
- Käyttäytymistekijät (Something user does):
  - Tietokoneen näppäilytapa
  - Äänen tunnistus
  - Allekirjoitus.

Eniten tunnistamiseen käytetään ”Käyttäjätunnus ja Salasana” -menetelmää, mutta muita metodeja tarvitaan imitaatiouhkien huomaamiseen. Näistä enemmän ”Ehdotetut Tunnistamis- ja Valvontamenetelmät” -kappaleessa.

Gao esitti, että tentissä tulisi käyttää vähintään kahta reaaliaikaista biometristä menetelmää useita kertoja tentin aikana. Gao vertaili myös markkinoilla olevien ratkaisujen kustannuksia: (Gao 2010.)

- Secureexam Remote Proctor (http://www.softwaresecure.com), jossa valvonta on toteutettu käyttämällä sormenjälkitunnistusta, 360 astetta kuvaavaa videota ja mikrofonia. Kustannus on 150 $ opiskelijaa kohti.
- Webassessor (https://www.webassessor.com), jossa valvonta tapahtuu sekä web-kameralla että näppäilyn tunnistamisen avulla. Kustannus on 50–80 $ opiskelijaa kohti.
- ProctorU (http://www.proctoru.com), jossa opiskelija vastaa tentin alussa häneen liittyviin henkilökohtaisiin kysymyksiin. Opiskelijan on vastattava näihin oikein voidakseen tehdä varsinaisen tentin. Lisäksi tenttiä valvotaan web-kameralla, jota tentin valvoja seuraa. Kustannus: 10 $ opiskelijaa kohti.

Varausjärjestelmän yksityisyys

Sähköistä tenttiä varten tarvitaan yleensä kalenteri, jonka avulla opiskelija voi valita itselleen soveltuvan tenttimisajan. Kalenteri voi olla avoin, eli opiskelija näkee ketkä muut opiskelijat tulevat tenttimään samaan aikaan. Varauskalenterin anonymisointi, tai ainakin sen näkymättömyys laajemmalle yleisölle, voi lisätä opiskelijan yksityisyyden suojaa ja vähentää vilppiä. Varauskalenterissa olevien opiskelijoiden nimet voisivat olla opettajien tai vain järjestelmän tukihenkilöiden nähtävissä.

Yhteydet järjestelmien välillä

Yhteydet tentissä käytetyn päätelaitteen ja itse tenttijärjestelmän eri osien välillä on toteutettu perinteisillä verkkoteknologioille kuten esimerkiksi Ethernet, reitittimet sekä julkiset ja sisäiset tietoliikenneyhteydet. Sovellustason liikenne tulisi olla salattua, ja yhteydet tulisi olla suojattu ulkoisia uhkia vastaan.

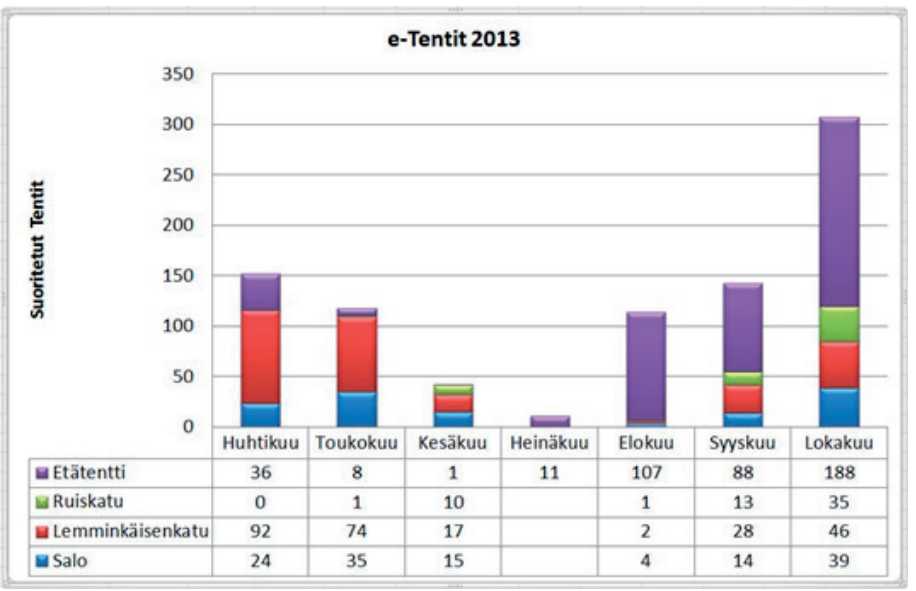
Hallinnointioikeudet

Tenttijärjestelmässä on tyypillisesti vähintään seuraavia käyttäjätyyppejä: opiskelija, opettaja ja pääkäyttäjä (administraattori). Kullakin käyttäjäryhmällä on omat oikeustasonsa, ja ylemmällä tasolla on normaalisti kaikki alemman tason oikeudet. Opiskelijalla on oikeus vain omiin tietoihinsa eli lähinnä omaan tenttiinsä. Opettajalla on pääsy omiin kursseihinsa, niiden tehtäviin ja tentteihin sekä oikeus nähdä ja arvostella omat tenttinsä. Opettajilla voi olla pääsy myös toisten opettajien tekemien kurssien tietoihin. Pääkäyttäjällä on suurimmat valtuudet ja yleensä aina pääsy kaikkiin tietoihin järjestelmässä. Järjestelmissä voi myös olla hallinnointitaso opettajien ja pääkäyttäjän välillä, mikä mahdollistaa kaikkien kurssien hallinnan. Tällaisella käyttäjällä on pääsy myös kaikkien opettajien kursseja ja tenttejä koskeviin tietoihin. Yksityisyyden suojan takia on välttämätöntä, että käyttäjätasot ja oikeudet on määritelty.

TURUN AMMATTIKORKEAKOULUN NYKYINEN JÄRJESTELMÄ

Tämä artikkeli esittelee lyhyesti Turun ammattikorkeakoululla käytössä olevan sähköisen tentin ratkaisun ja pohtii sen ominaisuuksia tietoturvan ja yksityisyyden kannalta. Tämän jälkeen esitellään käytössä olevia tietoturvaan ja yksityisyyteen liittyviä ratkaisuja, joita on esitetty aiemmissa tutkimuksissa. Lopuksi ehdotetaan keinoja parantaa Turun ammattikorkeakoulun ratkaisua.

Turun ammattikorkeakoulu valitsi Sordino Systemsin toimittaman Soft Tutor -ohjelmiston sähköisen tenttimisen järjestelmäksi 2011 lopulla. Pilotointivaihe oli pääosin vuoden 2012 aikana. Laajempi käyttö alkoi vuonna 2013, ja nykyisin tenttejä suoritetaan järjestelmällä 200–300 kuukausittain. Näistä noin 100 suoritetaan kameravalvotussa tilassa – tenttiakvaariossa. Tenttiakvaariota on kolme, joista kaksi on Turussa ja yksi Salossa kirjastojen yhteydessä. Vaihtoehtona on myös ”etätentti”, jossa tentti suoritetaan yleensä tietokoneluokassa opettajan valvonnassa, mutta se voidaan myös toteuttaa todellisena etätenttinä esimerkiksi kotoa käsin. Kuvassa 1 esitetään sähköisten tenttien jakautuminen tenttitiloihin.



	Huhtikuu	Toukokuu	Kesäkuu	Heinäkuu	Elokuu	Syyskuu	Lokakuu
Etätentti	36	8	1	11	107	88	188
Ruiskatu	0	1	10		1	13	35
Lemminkäisenkatu	92	74	17		2	28	46
Salo	24	35	15		4	14	39

KUVIO 1. *Turun AMK:n sähköiset tentit 4–10/2013.*

Tenttiakvaarioiden tietokoneista on pääsy vain e-tenttisovellukseen, joka fyysisesti sijaitsee Joensuun Tiedepuistossa. Käyttäjien kannalta kyse on pilvipalvelusta. Järjestelmässä on määritelty eri akvaariot ja niihin liittyvät rajoitukset: IP-osoite, tenttipaikkojen lukumäärä ja aukioloajat.

Opettaja määrittelee järjestelmään kurssit, niihin liittyvät kysymykset sekä tentit. Tentin suoristusajankohdan lisäksi opettaja määrittelee tenttiakvaario(t), jossa tentin voi suorittaa.

Opiskelija varaa itse tenttiajan järjestelmän kalenterista, jolloin hän tentin valinnan lisäksi tallentaa järjestelmään opiskelijanumeronsa, nimensä, sähköpostiosoitteensa sekä puhelinnumeronsa. Tenttiä varten opiskelija saa kertakäyttöiset tunnukset (käyttäjänimi ja salasana). Tentin vastauksen opiskelija tekee suoraan järjestelmään tai käyttää siihen liitetiedostoja.

Opettajilla on yleensä kurssien hallintaoikeudet, joten he voivat luoda kursseja ja näkevät kaikki järjestelmässä luodut kurssit sekä opiskelijoiden suoritukset.

Tenttiakvaariot Turun ja Salon kirjastoissa on varustettu nauhoittavalla videovalvonnalla. Videoihin ei nauhoiteta mukaan ääntä. Tenttiakvaarion tietokoneet ovat virtuaalipäätteitä, joista kaikki tieto häviää aina, kun opiskelija sammuttaa tietokoneen. Tietokoneissa on Windows 7 -käyttöjärjestelmä ja normaalit toimisto-ohjelmistot, kuten MS Office. Tenttiakvaariotilat kirjastoissa eivät ole lukittu.

Tentistä järjestelmään tallentuu lisäksi lokitietoa: tentin ilmoittautumis-, aloitus- ja päätösajat sekä käytetty IP-osoite.

EHDOTETUT TUNNISTAMIS- JA VALVONTAMENETELMÄT

Marais, Argles ja von Solms tutkivat sähköisen tentin tietoturvaa ja yksityisyydensuojaa sekä tenteissä käytettyjä metodeja. He ehdottivat julkisen avaimen salausperiaatten (PKI) käyttöä tunnistamiseen siten, että opiskelijan sormenjälki toimii yksityisavaimena ja sormenjäljen avulla luodaan julkinen avain. Julkinen avain on tallessa tenttijärjestelmässä. Julkisen avaimen periaatteesta on kerrottu enemmän tämän julkaisun artikkelissa *Autentikointiarkkitehtuuri tulevaisuuden langattomiin verkkoihin*. Opiskelija rekisteröityy ja kirjautuu

tenttiin sormenjäljellään, jota ei missään vaiheessa tallenneta järjestelmään. E-tenttijärjestelmää käyttävän opettajan ei tarvitse tietää, kenen tenttiä hän arvostelee, ja siten kaikki opiskelijat arvioidaan aina subjektiivisesti. (Marais et. al. 2006.)

Ramim ja Levy tutkivat biometrisiä tunnistusmenetelmiä, joilla estetään huijaaminen tentin aikana. He ehdottivat ratkaisua, jossa normaalin (käyttäjätunnus ja salasana) todennuksen lisäksi käytetään sormenjälkitunnistusta. Tenttijän sormenjälkitunnistus toistetaan satunnaisesti useita kertoja tentin aikana. (Ramim & Levy 2007.)

Apampa, Wills ja Argles tutkivat käyttäjän tietoturvaa sähköisessä tentissä. Tutkimus käsitteli tietoturvatekijöitä (luottamuksellisuus, eheys ja saatavuus) sekä tapoja turvallisesti tunnistaa ja todentaa käyttäjä tentin aikana ja sitä miten estää toisena persoonana esiintymisen uhkia tentissä. He totesivat, että yhtä biometrista tunnistamismenetelmää hyödyntävä ratkaisu ei ole riittävä. Sen sijaan käyttämällä useita menetelmiä samanaikaisesti voidaan minimoida imitoinnin uhkia ja parantaa käyttäjän tietoturvallisuutta. Ratkaisuksi ehdotettiin jatkuvan todentamisen käyttämistä useilla erilaisilla tunnistamismenetelmillä. Lisäksi opiskelijan sijaintia tentin aikana tarkkaillaan kameralla. (Apampa et. al. 2010.)

Balasundaram ehdotti graafisten salasanojen käyttämistä niiden monimutkaisuuden ja muistamisen helppouden takia. Tentin kysymykset ja vastaukset salataan, jotta luvattomien käyttäjien pääsy tentin tietoihin estyy. Tutkimus osoitti myös haittoja eri menetelmissä: Sormenjälkitunnistus ei yksin riitä, äänen tunnistus voi epäonnistua ikääntymisen tai kurkun infektion aiheuttamien muutosten takia, silmien sairaudet voivat vaikuttaa iiristunnistamiseen ja joidenkin tunnistamismenetelmien kustannukset ovat suuria. (Balasundaram 2011.)

Bhardwaj ja Singh tutkivat tietoturvakysymyksiä tenteissä Intiassa. He korostivat automaattisen arvioinnin ja turvallisuusuhkien vähentämisen tärkeyttä, koska tenttien käsittelyyn kuluva työaika kasvaa voimakkaasti Intiassa. Tenttien manuaalinen käsittely vaatii liikaa työtä, ja tenttipaperien käsittely ei ole niin tehokasta, luotettavaa ja tarkkaa kuin sähköisessä tentissä. Tutkimus käsitteli myös tenttimiseen liittyviä sisäisiä ja ulkoisia tietoturvauhkia, joihin ehdotettiin ratkaisuksi arkkitehtuuria, jossa eri käyttäjäryhmät on suojattu palomuurilla ja omilla auktoriteettitasoilla. (Bhardwaj & Singh 2011.)

Chiranji, Deephti ja Shetkar tutkivat, miten estää vilppiä sähköisessä tentissä ja erityisesti sen käyttöä etätenteissä. Ehdotettu ratkaisu perustuu viiteen kohtaan: 1. Web-kameralla otetaan kuva tenttijästä ilmoittautumisen yhteydessä; 2. Tenttitilanne kuvataan nauhoittavalla videolla äänen kera; 3. Videon lisäksi otetaan tietokoneen näytöstä kuvakaappauksia tentin aikana; 4. Kaikki muu kommunikointi tietokoneelta paitsi tenttiminen on estetty sulkemalla muut portit paitsi e-tenttiin käytetty; 5. Kaikkien ohjelmien käyttö, paitsi e-tenttiin vaadittu ohjelman käyttö, on estetty. Lisäksi internetselain on pakotettu toimimaan koko näytöllä ja osoiterivi sekä työkalut on poistettu käytöstä. (Chiranji et. al. 2011.)

Gao tutki, miten biometrinen tunnistusta ja IP-osoitteita voidaan käyttää mahdollisen vilpin havaitsemiseen etäopetuksessa. Hän totesi, että tyypillisesti opiskelija teki kokeita kolmessa eri IP-osoitteessa (kotona, kampuksella tai työpaikalla). IP-osoitteita käyttämällä on mahdollista havaita, jos useat opiskelijat tekevät samaan aikaan tentin lähellä toisiaan. Käytettyjen IP-osoitteiden lisäksi talletetaan aikaleimat tentin alussa, mitä pidetään Gaon mukaan tehokkaana tapana löytää vilppiyritykset tentin aikana. (Gao 2012.)

Ivy, Shalini ja Yamamuna tekivät ehdotuksen tenttijärjestelmästä, jollainen tarvitaan turvallisuuden varmistamiseen ja huijaamisen estämiseen sähköisessä tentissä. Ehdotetussa ratkaisussa – SeCOneE System – pyritään luomaan valvoja-toimintoja estämään huijaamista etätenteissä. Järjestelmässä on omat käyttäjäluokat valvojille ja tenttijöille. Järjestelmä käyttää PKI-arkkitehtuuria (julkiset ja yksityiset avaimet) kaikessa ryhmien välisessä viestinnässä sekä lisäksi symmetrisiä avaimia (Diffie-Hellman) ryhmien sisäisessä viestinnässä. Järjestelmä tunnistaa huijaamisen yritykset PKI:n avulla. Ehdotetussa ratkaisussa tentissä käytetään samoja kysymyksiä kuin perinteisten tentissä luokkahuoneessa ja tentti suoritetaan etänä samanaikaisesti. (Ivy et. al. 2012.)

Sabbah, Saroit ja Kotb tutkivat tietoturvavaatimuksia, tunnistamismenetelmiä, erityisesti sormenjälkeen ja näppäilyyn liittyviä menetelmiä sekä sähköisen tentin uhkia. He käyttivät hyväkseen Apampa, Wills ja Argles'in tutkimusta (Apampa et. al. 2010) ja esittivät teoreettinen mallin sähköisen etätentin tunnistamiseen. Ehdotetussa mallissa käytetään videovalvontaa ja kahta biometristä tunnistusmenetelmää, joita käytetään tentin eri vaiheissa: ennen tenttiä, sen aikana ja sen jälkeen. Malli on täysin automatisoitu eikä vaadi henkilöitä valvomaan tenttiä. (Sabbah et. al. 2012.)

NYKYJÄRJESTELMÄN ANALYYSI

Turun ammattikorkeakoulun nykyisen ratkaisun kannalta seuraavia kohtia tulisi muuttaa tietoturvan ja yksityisyyden parantamiseksi:

- Opiskelijoiden tietojen näkyvyys tulisi rajata vain tentin järjestävälle opettajille.
- Tentin alussa tarvitaan perinteisen käyttäjätunnuksen ja salasanan lisäksi toinen menetelmä (esimerkiksi kuva tai sormenjälki), jotta voidaan paremmin varmistaa opiskelijan identiteetti tentin aikana.
- Jokaisella tietokoneella tulisi olla oma web-kamera, joka kuvaa tenttijää koko tentin ajan, jotta tenttijän mahdollinen vaihtuminen voitaisiin paremmin huomata.
- Tenttijästä otetaan kuva (ja ääninäyte) joko siinä vaiheessa, kun tentti aloitetaan, tai jo ilmoittautumisen yhteydessä. Järjestelmä kuvaa tenttiä, ja jos huomataan tenttijän vaihtuminen (tai muita ääniä), siitä talletetaan järjestelmään ”varoitus”, jonka opettaja tai tukihenkilö voi jälkikäteen tarkistaa.
- Web-kameraa voitaisiin myös käyttää etätukeen. Opiskelija voisi tentin aikana ottaa yhteyttä ongelmatilanteissa keskusteluohjelmalla (esimerkiksi MS Lync) tukihenkilöihin. Nykyään ongelmatilanteissa otetaan yhteyttä kirjaston henkilökuntaan, joka soittaa tukihenkilölle. Tuki on tärkeä, jotta opiskelija ei menetä tentin aikana kirjoittamiaan vastauksia.
- Web-kameran käyttöön liittyvät teknologiat voivat olla vielä liian kalliita, joten tarkemman kuvakäsittelyn sijaan voidaan käyttää satunnaisia tenttijään liittyviä kysymyksiä, kuten ProctorU (http://www.proctoru.com) -järjestelmässä. Henkilökohtaisia kysymyksiä käytetään varmistamaan se, että tenttijä todella on se, joka hän väittää olevansa. Näistä kysymyksistä on hyvä mitata myös vastausaika. Tämän mittauksen tarjoaa Turun Yliopiston ViLLE-järjestelmä (http://ville.cs.utu.fi). Henkilökohtaiset kysymykset voidaan myös sisällyttää kysymyspankkiin.

- Sabbah, Saroit ja Kotb'n (Sabbah et. al. 2012) malli, jossa tentin alussa tapahtuvan biometrisen tunnistuksen lisäksi tentissä käytetään videovalvontaa tentin aikana, on varteenotettava vaihtoehto, kun luodaan järjestelmä, joka automaattisesti valvoo tentin suoritusta ilman henkilöresursseja. Ratkaisuun on kuitenkin hyvä lisätä opiskelijan paikkaan liittyvää toiminnallisuutta. IP-osoitteen käyttö ei kuitenkaan ole riittävä, vaan tarvitaan toisenlainen varmempi tapa todeta varsinainen tenttimispaikka.

- Marais, Argles & von Solms'n (Marais et. al. 2006) esittämä ratkaisu, jossa identiteetti salataan opiskelijan sormenjäljestä luodulla PKI-avaimella, parantaa opiskelijan tietoturvaa ja yksityisyyttä sekä arvostelun luotettavuutta, koska opettaja ei tiedä, ketä hän arvioi. Tämän toteutus voi kuitenkin olla liian kallis.

- Tentin suorituspaikka voidaan myös rajata tietyksi tilaksi ja sijoittaa tenttijärjestelmä samaan tilaan ja siten sulkea pois ulkoisia uhkia. Tentissä käytetty tietokone voi olla käynnistettävissä vain USB-tikulta, joka sisältää tentissä käytettävän käyttöjärjestelmän ja mahdollisesti myös vain tietylle opiskelijalle tehdyn tentin, joka on salattu opiskelijan julkisella avaimella.

Ratkaisun vaikutus tietoturvaan, yksityisyyden suojaan sekä vilpin estämiseen taulukossa 1.

Parannusten toteuttamiseksi vaaditaan todennäköisesti uusi tenttimisjärjestelmä Turun ammattikorkeakoululle. Ratkaisuun käytettävissä olevat kustannukset ja sähköisen tenttimisen hyödyt vaikuttavat järjestelmän valintaan: mikä on tietoturvan ja yksityisyydensuojan hinta?

TAULUKKO 1. *Parannusten vaikutus.*

	Opiskelija	Opettaja
Tietoturva	Opiskelija saa reaaliaikaisesti tukea ongelmatilanteissa, joten tietojen häviäminen vähenee. Identiteetin salaus arvioinnissa takaa puolueettoman arvioinnin.	Opettaja saa tiedon automaattisesti mahdollisista tietoturvaloukkauksista.
Yksityisyydensuoja	Opiskelijan tietoihin pääsevät käsiksi vain tietoja oikeasti tarvitsevat. Toisaalta enemmän henkilökohtaista tietoa tallentuu järjestelmään.	Opettajan yksityiskohtainen arvostelu pysyy opiskelijan ja opettajan välisenä tietona.
Vilpin esto	Vilppi on vaikeaa. Kuitenkaan tenttiä ei välttämättä keskeytetä heti vilpin (automaattisen) huomioinnin jälkeen: parempi oikeusturva.	Opettajan ei tarvitse käyttää omaa aikaansa vilpin havaitsemiseen.

YHTEENVETO

Sähköisen tentin käyttö laajenee, haluamme sitä tai emme. Opettajan käyttämä aika tenttien käsittelyyn vähenee, ja tentit ja muut opintoihin liittyvät rutiinitehtävät suoritetaan lähitulevaisuudessa suurelta osalta sähköisesti.

Teknologia kehittyy vauhdilla ja tietoturvaan ja yksityisyyteen liittyvät uhat lisääntyvät. Tietoturvaan ja yksityisyydensuojaan liittyvät tekijät on tärkeä ottaa huomioon sähköisessä tenttimisessä. Opiskelijan turvallisuuden ja yksityisyyden takaamiseksi tarvitaan mahdollisesti myös ratkaisuja, joissa tenttiä valvotaan ja vastaukset arvioidaan järjestelmillä, joissaopiskelijaa voidaan käsitellä anonyymisti. Ratkaisuissa on tärkeä löytää oikea balanssi tentin uhkia havaitsevien toiminteiden, ja niistä mahdollisesti seuraavien yksityisyydensuojan vaikutusten välillä. Lisäksi ratkaisun hinta suhteessa saavutettavaan suojaan määrittelee rajat halutulle turvatasolle.

Uusien langattomien teknologioiden käyttöä sähköisessä tentissä tulee myös tutkia tarkemmin, jotta tenttijän sijainti tentin aikana voitaisiin varmemmin todeta IP-osoitteen lisäksi.

LÄHTEET

Apampa, K. M.;Wills, G.;& Argles, D. 2010. User Security Issues in Summative E-Assessment Security. International Journal of Digital Society (IJDS), 135–147.

Asha, S. 2008. Authentication of e-learners using multimodal biometric technology. Biometrics and Security Technologies, (ss. 1–6). Chennai.

Balasundaram, S. R. 2011. Securing Tests in E-Learning Environment. International Conference on Communication, Computing & Security (ss. 624-627). New York: ACM.

Bhardwaj, M. & Singh, A. J. 2011. Automated Integrated Examination System: A Security Concern. Information Security Journal, 156–162.

Castella-Roca, J. 2006. A secure e-exam management system. Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on.

Chiranji, N.;Deepthi, C.;& Shekhar, T. P. 2011. A Novel Approach to Enhance Security for Online Exams. JCST, 85–89.

Gao, Q. 2010. Online teaching: Do you know who is taking the final exam? Fall 2010 Mid-Atlantic ASEE Conference (ss. -). Villanova: Villanova University.

Gao, Q. 2012. Using IP Addresses as Assisting Tools to Identify Collusions. International Journal of Business, Humanities & Technology Jan2012, Vol. 2 Issue 1, Academic Search Elite (EBSCOhost), 70–75.

Golden, B. 2011. Virtualization for Dummies. Viitattu 18.12.2013 http://www8.hp.com/de/de/pdf/virtuallisation_tcm_144_1147500.pdf.

Ivy, B. P.;Shalini, A.;& Yamuna, A. 2012. WebBased online Secured Exam. International Journal of Engineering Research and Applications (IJERA), 943–944.

Marais, E.;Argles, D.;& von Solms, B. 2006. Security Issues Specific to e-Assessments. 8th Annual Conference on WWW Applications. Bloemfontein.

Ramim, M. M.;& Levy, Y. 2007. Open University of Israel. Viitattu 1.4.2013 http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf.

Ramim, M. M.;& Levy, Y. 2007. Towards a Framework of Biometric Exam Authentication in E-Learning Environments. Managing Worldwide Operations & Communications with Information Technology, 539–543.

Sabbah, Y. 2011. An interactive and secure e-examination unit (ISEEU). Roedunet International Conference (RoEduNet), 2011 10th.

Sabbah, Y.;Saroit, I.;& Kotb, A. 2012. Synchronous Authentication with Bimodal Biometrics for e-Assessment. 2012 6th International Conference on Sciences of Electronic, Technologies of Information and Telecommunications . Sousse.

Wiak, S.;Jeske, D.;Krasuski, M.;& Stryjek, R. 2011. Modern distance examination using the latest technology - the E-matura project. 2nd World Conference on Technology and Engineering Education (ss. 27–31). Ljubljana, Slovenia: WIETE.

TIETOTURVA SOSIAALISESSA MEDIASSA

Juha Kontturi
IT -suunnittelija, Turun ammattikorkeakoulu

Sosiaalisten medioiden käyttö on lisääntynyt merkittävästi muutaman viime vuoden aikana (Wikipedia 2013). Aikaisemmin sosiaalisia medioita käyttivät lähinnä nuoret aikuiset. Nyt sen tarjoamia palveluja hyödyntävät kaiken ikäiset ihmiset sekä yhä enemmän myös yritykset ja erilaiset yhdistykset. Huomioitava kehitys palvelujen käytössä on se, että käyttö aloitetaan yhä nuorempana, vaikka moneen palveluun, esimerkkinä Facebook, on 13 vuoden alaikäraja. Suomessa on lähes kaksi miljoonaa Facebook-käyttäjää. Aktiivisimmat käyttäjät ovat iältään 25–34-vuotiaita. Palveluja ei käytetä pelkästään tietokoneilla, vaan kuukausittain noin puoli miljoonaa suomalaista käyttää Facebookia matkapuhelimellaan. Näin ollen käyttö ei siis ole rajattu tiettyyn paikkaan, vaan se tapahtuu missä ja milloin tahansa.

Yksityishenkilöt käyttävät sosiaalisia medioita lähinnä yhteydenpitoon ystävien kanssa. Viestien lähettäminen on helppoa ja nopeaa. Lisäksi käytössä olevat palvelut ovat yleensä käyttäjilleen ilmaisia, mikä tietenkin lisää käyttäjämääriä sekä palvelujen käyttöä pääsääntöisenä yhteydenpitovälineenä. Viestittämisen lisäksi palveluja käytetään myös viihdetarkoituksessa. Palvelujen yhteydessä voi esimerkiksi pelata erilaisia pelejä. Näiden lisäksi moni käyttää sosiaalisia medioita valokuvien julkaisupaikkana.

KÄYTTÄJIEN OMAN TOIMINNAN ETUJA JA HAITTOJA

Mihin yksittäisen henkilön kannattaa kiinnittää huomioita, jotta toiminta yhteisöpalveluissa olisi turvallista? Sosiaalisissa medioissa käyttäjä ei ole pelkästään tiedon hakija, vaan myös itse sisällöntuottaja ja viestittäjä. Sisältöä tuotetaan joko yksityishenkilönä tai esimerkiksi jonkin yrityksen tai yhdistyksen jäsenenä. Sisältöä voidaan tuottaa eri muodoissa: yksittäisenä viestinä, osallistumalla keskusteluihin tai julkaisemalla valokuvia. Koska palvelut

ja yhteisöt ovat pääsääntöisesti julkisia, jaetun tiedon tulisi olla luonteeltaan sellaista, joka kestää laajankin julkisuuden. Verkossa ja sosiaalisissa medioissa kannattaisi välttää omien henkilötietojen jakamista. Omalla nimellä ja kuvalla voi toki esiintyä, mutta tarkempia henkilötietoja ei kannattaisi itsestään kertoa. Tällaisia tietoja ovat esimerkiksi syntymäaika, katuosoite sekä puhelinnumero. (Valtiovarainministeriö 2010a, Valtiovarainministeriö 2010b)

Koska sosiaalisia medioita on nykyisillä teknisillä apuvälineillä (tietokone, puhelin) nopeaa ja helppoa käyttää, on sisällön ja mielipiteiden julkaisukynnys käyttäjillä matala. Netin ja palveluiden julkisuutta ei aina sisältöä tuotettaessa ajatella. Varsinkin nuorten keskuudessa tämä on todettu ongelma. Alle 17-vuotias henkilö ei tutkimustietojen perusteella ymmärrä täysin internetin julkisuusastetta. Tämä taas saattaa johtaa tietynlaisiin ylilyönteihin sisältöä tuotettaessa. Nuori paljastaa itsestään liikaa henkilökohtaisia tietoja ja kommentoi muiden käyttäjien mielipiteitä ja mieltymyksiä joskus epäasiallisestikin. Tiedossa on paljon rikosilmoituksia, jotka on tehty nimenomaan sosiaalisissa medioissa käytyjen keskustelujen perusteella. Koska yleiset keskustelut ja mielipiteiden vaihto jäävät palveluissa näkyviin, niitä saatetaan käyttää todisteena esimerkiksi kunnianloukkaussyytteissä.

Valokuvien julkaisemisessa täytyy muistaa muutama tärkeä asia. Internetiin itsestä tai perheestä julkaistu valokuva on laillisesti kaikkien internetin käyttäjien kopioitavissa, vaikka kopioija ei tietenkään saa julkaista valokuvaa missään julkisessa paikassa. Toinen huomioitava asia on se, että muita ihmisiä esittäviä kuvia ei saa julkaista ilman kuvissa esiintyvän henkilön suostumusta. Sama koskee mitä tahansa tietoa, joka liittyy toisiin henkilöihin, ei pelkästään valokuvia.

TIETOKONEENKÄYTTÄJÄN TEKNISET TIETOTURVARISKIT

Käyttäjätunnuksia ja niihin liittyviä salasanoja yritetään kaapata monella eri tavalla. Käyttäjä voi saada esimerkiksi sähköpostiviestin, jossa lähettäjä kysyy salasanaa vedoten esimerkiksi jonkin palveluntarjoajan teknisiin tietoturvapäivityksiin. Yleensä käyttäjä huomaa huijausyrityksen helposti. Viesti on kirjoitettu esimerkiksi huonolla suomen kielellä, ja se sisältää paljon kirjoitusvirheitä. Käyttäjä, joka saa haittaohjelman tai viruksen sähköpostiviestissä, lähettää usein tietämättään haittaohjelmaa eteenpäin omassa osoitekirjassaan

oleviin sähköpostiosoitteisiin. Tällöin oma tietokone toimii roskapostin edelleenvälittäjänä. Pahimmassa tapauksessa toiminta johtaa käyttäjän liittymän sulkemiseen.

Sähköpostissa yritetään myös levittää haitallisia ohjelmia käyttäjien koneille. Kaksi yleisintä haittaohjelmaa ovat erilaiset virukset sekä vakoiluohjelmat. Nämä leviävät yleisimmin sähköpostiviestien liitetiedostojen tai hyperlinkkien välityksellä. Kolmas yleinen haittaohjelmien leviämistapa liittyy tiedostojen lataamiseen suoraan verkosta omalle tietokoneelle.

Jos saapunut sähköpostiviesti on henkilöltä, jota vastaanottaja ei tunne, ja viestin aihe ei oikeastaan liity vastaanottajaan ilmeisellä tavalla, ei viestin mukana tulleita liitetiedostoja kannata avata. Sama sääntö koskee viestissä olevia hyperlinkkejä. Ladattavat tiedostot ovat usein verkossa laittomasti ladattavissa. Verkossa jaossa olevat elokuvat ovat tästä yksi esimerkki. Tällaisen latauksen yhteydessä on mahdollista saada omalle tietokoneelle jokin edellä mainituista haittaohjelmista. Kun verkosta ladataan laittomia tiedostoja, usein omalle tietokoneelle asennetaan sovellus, joka pahimmassa tapauksessa jakaa omalla tietokoneella olevia tiedostoja eteenpäin muille verkon käyttäjille (musiikkitiedostot, valokuvat jne.) Joskus kyseiset sovellukset asentuvat niin, ettei käyttäjä edes itse huomaa sen olemassaoloa omalla tietokoneellaan.

Vakoiluohjelmat keräävät tietoja siitä, mitä käyttäjä omalla tietokoneellaan tekee. Vakoiluohjelma saattaa esimerkiksi rekisteröidä jokaisen käyttäjän tekemän näppäinpainalluksen, jolloin hänen käyttäjätunnuksensa ja salasanansa paljastuvat. Lisäksi vakoiluohjelman tekijä/levittäjä pääsee tunkeutumaan käyttäjän tietokoneelle ja käyttää sitä omistajan tietämättä.

AVOIMUUS JA RISKEIHIN VARAUTUMINEN VERKOSSA

Sekä yksityishenkilöt että työyhteisön jäsenet käyttäytyvät verkossa toisinaan liian avoimesti. Koska koko sosiaalisen median perusajatus on avoimuus, yksityistietojen levittäminen ja jakaminen tuntuu liiankin helpolta. On jopa liian helppoa lähteä mukaan keskusteluihin, joissa muutkin käyttäjät kertovat avoimesti asioita. Työasioista ei välttämättä kannata keskustella ympäristössä, jossa keskustelun voi nähdä usea eri taho. Muutenkin nyrkkisääntönä voidaan pitää sitä, että ei kannata julkaista mitään, mitä ei halua tuntemattomille ihmisille itsestään kertoa. Sosiaalisissa medioissa sekä yksilöt että yritykset

törmäävät jopa niin sanottuihin identiteettivarkauksiin. Mikäli yksittäisestä henkilöstä on verkossa eri palveluissa paljon yksilöivää tietoa, on vakuuttavan valeprofiilin laatiminen helppoa. Yleensä yksittäiset henkilöt tekevät identiteettivarkauden lähinnä kiusaamistarkoituksessa.

Sekä tietokoneen että puhelimen käyttöön liittyy ulkoisia sovelluksia, jotka ovat jonkun muun tahon kuin käytettävän palvelun laatimia. Ne muodostavat merkittävän uhan yksityistietojen menettämiselle. Esimerkiksi sosiaalisissa medioissa käyttäjiä ohjataan pelaamaan jotakin peliä, yleensä kavereiden kutsusta. Jotkut tällaisista sovelluksista saattavat levittää sovelluksen käyttäjän yksityistietoja johonkin muuhun internetissä olevaan palveluun. Esimerkiksi käyttäjän kaikki henkilökohtaiset valokuvat saattavat siirtyä johonkin julkiseen ympäristöön. Viime vuonna tuhansien suomalaisten Facebook-käyttäjien tietämättä heistä tehtiin internetiin seuranhakuilmoitus. Käyttäjä oli siis avannut Facebook -kaverinsa lähettämän linkin, jonka seurauksena tiedot siirtyivät toisen palvelun käyttöön. Tämä on hyvin yleinen tietojen urkintatapa, ei vain sosiaalisissa medioissa vaan myös sähköpostin käytön yhteydessä. Kun tällainen haitallinen sovellus suoritetaan matkapuhelimella, puhelimessa olevat tiedot (esimerkiksi koko puhelimen osoitekirja) voivat päätyä jollekin internetsivustolle tai ulkopuolisten henkilöiden käsiin.

Salasanoihin tulisi kiinnittää erityistä huomiota. Salasanan pitäisi olla monimutkainen, ja sen tulisi sisältää pieniä ja isoja kirjaimia, numeroita ja joitakin erikoismerkkejä eikä sen tulisi olla mikään selkeä sana. Tällöin salasanan murtaminen on teknisesti vaikeampaa. Lisäksi salasana on syytä vaihtaa säännöllisin väliajoin. Sosiaalisissa medioissa kannattaa käyttää jotakin sellaista salasanaa, jota käyttäjä ei ole rekisteröinyt mihinkään muuhun palveluun. Tämä on hyvä sääntö myös muihin internetissä tarjolla oleviin palveluihin. Vaikka yksittäinen salasana joutuisikin muiden tietoon, ovat muut käytetyt palvelut (esimerkiksi työsähköposti tai henkilökohtainen sähköposti) tältä osin suojattu.

Oman tietokoneen tietoturva pitää olla ajan tasalla. Viruksia ja eri haittaohjelmia tunnistava torjuntasovellus on kotitietokoneen turvallisuuden kannalta välttämätön. Parhainkaan tietoturvaohjelmisto ei silti aina estä virusten ja haittaohjelmien pääsyä omalle tietokoneelle. Myös käyttäjän omalla käyttäytymisellä verkkopalvelujen asiakkaana on suuri merkitys turvallisuuden kannalta. Kun tietää, missä verkossa liikkuu – kun osaa tunnistaa niin sanotut ”viralliset” sivustot – on virusten saaminen epätodennäköisempää.

TAULUKKO 1. *Internetin ja sosiaalisen median tavallisimmat tietoturvariskit.*

Tekniset uhat	Sosiaalisen median tietoturvariskit
Käyttäjätunnuksiin kohdistuva väärinkäyttö	Liiallinen avoimuus
Haittaohjelmat	Ulkoiset sovellukset
Roskaposti	Salasanat
Vakoiluohjelmat	Oman tietokoneen tietoturva
Identiteettivarkaudet	

HUOMIOITAVIA ASIOITA SUOSITUISSA YHTEISÖPALVELUISSA

Tunnetuin ja suosituin sosiaalinen media on Facebook. Facebookin käyttäjiä on noin miljardi. Palvelun avulla on mahdollista pitää yhteyttä ystäviin viestein tai osallistumalla keskusteluihin, joissa on osallisena muitakin palvelun käyttäjiä. Moni käyttäjä kuuluu ryhmiin, jotka liittyvät johonkin kiinnostuksen kohteeseen. Ryhmissä käyttäjät ympäri maailman vaihtavat mielipiteitä yhteisen teeman ympärillä. Yksityisyydensuojan kannalta ongelmalliseksi muodostuu se, että Facebook perustuu USA:n lainsäädäntöön. Esimerkiksi eurooppalainen käyttäjä ei siten voi olla varma, kuinka laajasti Facebook tallettaa käyttäjän lähettämät viestit, keskustelut ja ladatut valokuvat.

Wikipedia on ilmainen tietosanakirja, johon jokainen käyttäjä voi toimittaa sisältöä. Tämä tietenkin tarkoittaa sitä, että lukija ei aina voi olla varma Wikipediassa olevan tiedon oikeellisuudesta. Samasta syystä artikkeleiden taso vaihtelee suuresti. Wikipediasta on käytössä myös suomenkielinen versio, josta löytyy noin 300 000 artikkelia.

Youtube-videopalvelun käyttäjä voi katsoa, ladata ja lisätä omia videoita julkiseen käyttöön. Youtubeen ei saa lisätä tekijänoikeuksilla suojattuja videoita, mutta palvelun suosion vuoksi sitä on mahdotonta täysin valvoa: uusia videoita lisätään Youtubeen yhden minuutin aikana kymmeniä tunteja.

Suomalaisia yhteisöpalveluja ovat esimerkiksi Suomi24 ja IRC-Galleria. Suomi24 sisältää keskusteluyhteisön muiden palvelujen ohella. IRC-galleria on suomalainen kuvagalleria, johon käyttäjät voivat lisätä kuvia sekä haluamiaan tietoja itsestään. Joissakin palveluissa sisällön valvontaan on kiinnitetty huomiota, ja esimerkiksi viranomaiset (Poliisi) ovat esillä tietyissä, lähinnä nuorille ja nuorille aikuisille suunnatuissa palveluissa. Mikäli käyttäjä havaitsee

häiritsevää viestittelyä, yhteydenotto viranomaisiin on mahdollista suoraan palveluiden käytön yhteydessä.

Facebookin tietoturva käyttäjien näkökulmasta katsoen on usein epäluottamusta herättävä. Muutama käytännön esimerkki: Oman profiilini suojausasetukset olivat nollaantuneet pari vuotta sitten, jolloin kuka tahansa pääsi katsomaan profiiliani. Huomasin tämän siten, että pääsin itse katsomaan tuntemattomien käyttäjien tietoja ilman mitään rajoituksia. Tämän jälkeen olen tarkastanut säännöllisesti, ovatko suojausasetukseni kunnossa. Syksyllä 2012 osalle käyttäjistä kävi niin, että yksityiset viestit olivat muuttuneet julkisiksi. Facebook selitti molemmat tapaukset melko ympäripyöreästi eikä juuri ottanut tapahtuneista mitään vastuuta.

Huolestuttavinta on se, että Facebook ja muutkin yhteisöpalvelut, kuten Google+, keräävät käyttäjien tietoja. Tietoja kerätään esimerkiksi siitä, millä www-sivuilla käyttäjä vierailee, riippumatta siitä onko käyttäjä juuri silloin kirjautuneena yhteisöpalveluun vai ei. Se, kuinka palvelut näitä tietoja hyödyntävät, ei ole tarkkaan selvillä. Voisi olettaa, että ainakin kaupallisissa tarkoituksissa käyttäjien selaushistoriasta lähetetään tietoja mainostajille. Näitä tietoja hyödynnetään esimerkiksi markkinointitarkoituksessa.

YHTEENVETO

Koska käyttäjä ei voi olla varma eri sosiaalisten medioiden tietoturvasta, on tärkeää tiedostaa se, millaista tietoa itsestään kertoo. Sosiaalisten medioiden välityksellä ei kannata kertoa asioita, joita ei halua kolmansien osapuolien tietoon tai hyödynnettäviksi. Tämä on tärkeää esimerkiksi yksityisiä viestejä lähetettäessä. Sähköposti lienee turvallisin vaihtoehto yksityiseen käyttöön tarkoitettujen viestien lähettämiseen. Sekään ei aina ole täysin turvallinen, sillä haittaohjelmat ja virukset voivat aiheuttaa myös sähköpostin käytössä tietoturvaan liittyviä ongelmia.

LÄHTEET

Valtiovarainministeriö 2010a Sosiaalisen median tietoturvaohje. Viitattu 18.12.2013 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/Sosiaalinen_media.pdf.

Valtiovarainministeriö 2010b Sosiaaliseen mediaan liittyvät tietoturvariskit. Viitattu 18.12.2013 https://www.vahtiohje.fi/web/guest/2.-sosiaaliseen-mediaan-liittyvat-tietoturvariskit.

Wikipedia 2013 Social networking service. Viitattu 18.12.2013 http://en.wikipedia.org/wiki/Social_networking_services.

AUTENTIKOINTIARKKITEHTUURI TULEVAISUUDEN LANGATTOMIIN VERKKOIHIN

Jarkko Paavola, TkT
Yliopettaja, tietojenkäsittelyn koulutusohjelma,
Turun ammattikorkeakoulu

Arto Kivinen, Tradenomi
Projektipäällikkö, Turun ammattikorkeakoulu

Tekesin Trial-teknologia-ohjelman tavoitteena on luoda Suomeen kognitiiviradioiden testausympäristöjä. Turun ammattikorkeakoulun WISE-, ReWISE- ja WISE2-projekteissa on kehitetty testausympäristö TV-taajuuksille niin kutsutun white space -tiedonsiirron tutkimiseksi. WISE on lyhenne sanoista *White Space Test Environment*. WISE-hanke toteutettiin vuosina 2011–2012. Sen kansainvälinen tietoturvalaajennus ReWISE (Reliability extension to WISE) on suoritettu 2012–2013. Työ jatkuu WISE-projektin jatkohankkeessa WISE2.

White space (WS) tarkoittaa aluetta, jossa jollekin langattomalle järjestelmälle myönnetty taajuusalue on osittain hyödyntämättä maantieteellisesti tai ajallisesti. Taajuusalueen ensisijaista käyttäjää kutsutaan usein primaarijärjestelmäksi. Ensimmäiseksi taajuusalueeksi, joka todennäköisesti tullaan ottamaan WS-käyttöön, on identifioitu TV-käyttöön osoitettu UHF-taajuusalue 470–790 MHz. Tällöin puhutuaan TVWS-taajuuksista. Tämän taajuuskaistan primaarikäyttö on TV-lähetysten vastaanotto.

WS-laite tai -tukiasema saa tiedot vapaista taajuuksista ja näillä taajuuksilla sallituista lähetystehoista internetin välityksellä geolokaatiotietokannasta, jonka tehtävänä ovat suojella ensisijaisia käyttäjiä, etsiä vapaa käytettävissä oleva taajuus WS-laitteille ja mahdollisesti tulevaisuudessa hallita niiden keskinäisiä häiriöitä. Tietokantoja kutsutaan usein geolokaatiotietokannoiksi, koska halutaan korostaa maantieteellisen informaation merkitystä radiotaajuuksien hallinnassa.

TV-lähetysten lisäksi langattomat mikrofonit siirtyvät samalle taajuusalueella vuodesta 2014 alkaen, jolloin nämäkin laitteet tulee suojella tietokannan avulla. Tämä on haastava tehtävä, sillä langattomien mikrofonien saaminen tietokantaan on vaikeaa. Suomessa langattomien mikrofonien käyttäjien pitäisi rekisteröidä laitteensa Viestintävirastolle (Viestintävirasto 2013a). Rekisteröintiaktiivisuus on ollut laimeaa, joten virallisesti tiedossa on todennäköisesti vain murto-osa kaikista Suomessa käytössä olevista mikrofoneista. Turun ammattikorkeakoulun opiskelijat ovat pyrkineet selvittämään langattomien mikrofonien käyttöä Turussa ja Dublinissa, Irlannissa. Päällimmäiseksi jäänyt kokemus on, että tietoa on vaikea löytää.

ReWISE-projektissa on suunniteltu autentikointiarkkitehtuuri nimenomaan langattomien mikrofonien automaattiseen hallintaan. Autentikoinnilla eli todennuksella tarkoitetaan laitteen, käyttäjän tai palvelun identiteetin varmentamista. Samaa periaatetta voidaan toki hyödyntää myöhemmin WS-laitteiden kohdalla. Autentikointiarkkitehtuuri pyrkii vastaamaan kahteen ongelmaan. Radiomikrofonit täytyisi saada tietokantaan, jotta niitä voidaan suojella. Ongelmallista on mikrofonien käytön satunnaisuus. Mikrofonien rekisteröimisestä tulisi tehdä automaattinen toimenpide. Toisaalta jaettuun käyttöön tarkoitetun spektrin riittävyys tulisi taata mahdollisimman monelle. Mikrofonikäyttäjien omakohtainen laiterekisteröinti antaa teoriassa mahdollisuuden varata taajuuksia yli todellisen tarpeen. Tällöin WS-laitteille käytössä olevat taajuuskaistat vähenisivät hyvin nopeasti, sillä tämänhetkiset tekniset ratkaisut eivät mahdollista yhden kahdeksan megahertsin kanavan jakamista pienempiin osiin. Täten yhden laitteen tai laiteryhmän rekisteröinti varaa kokonaisen kanavan. Tälläinen toiminta olisi tavallaan palvelunestohyökkäys (denial of service) WS-järjestelmää vastaan.

Molemmat tavoitteet ovat ratkaistavissa, jos suojattavassa laitteessa on ominaisuus, josta laite voidaan luotettavasti yksilöidä. Tällainen ominaisuus on esimerkiksi sim-kortti tai TPM-piiri. Näistä jälkimmäinen on ollut tutkimuskohteena Tekes-rahoitteisessa ReWISE-projektissa. Valinta on tehty sillä perusteella, että todennäköisimmäksi sovellusalueeksi on nähty Wi-Fi-tyyppinen ratkaisu ennemmin kuin matkapuhelinkäyttö.

TPM-piiri on mikrosiru, jonka toiminnan on spesifioinut Trusted Computing Group (TCG 2013). TPM-piiri löytyy jo monista tietokoneista ja mobiililaitteista. Nykypäivänä TPM-piiriä käytetään esimerkiksi kannettavissa tietokoneissa, palvelimissa, tablettitietokoneissa ja kännyköissä. TPM-piiriä

käytetään kannettavissa tietokoneissa muun muassa sormenjälkitunnistukseen tai kovalevyn sisällön salaamiseen. Jokainen valmistettu TPM-piiri on yksilöllinen, mikä takaa TPM-piiriä hyödyntäville sovelluksille sen, että laite on varmistettu. Tietoturvatoiminnallisuuksiin kuuluu esimerkiksi yksilöllisten salausavaimien muodostaminen, ja niiden tyypillisiä käyttötapauksia ovat tietojen salaaminen tai allekirjoittaminen. Digitaalisella allekirjoituksella voi varmistua tietojen alkuperästä. Emulointiohjelma tai toinen TPM-piiriä käyttävä laite ei pysty käyttämään omia salausavaimiaan murtaakseen salattuja tietoja.

TPM-piirikin hyödyntää siis julkisen avaimen salausperiaatetta – public key infrastructure (PKI). Tässä salausmenetelmässä salausavaimena toimii itseasiassa avainpari. Avainparin muodostaminen tapahtuu esimerkiksi RSA-algoritmin avulla. Julkinen avain voidaan ilmoittaa nimensä mukaisesti vaikkapa internetissä tai sähköpostin signature-osiossa. Yksityinen avain täytyy pysyä vain omistajansa tiedossa. Kun viestin lähettäjällä ja vastaanottajalla on käytössään oma avainpari, pystytään salaamis- tai allekirjoitusoperaatio suorittamaan (pkix 2013):

- Viestiä salattaessa lähettäjä suorittaa salauksen hyödyntäen vastaanottajan julkista avainta. Tällöin salatun viestin pystyy avaamaan vain vastaanottajan yksityisellä avaimella.
- Viestiä allekirjoitettaessa lähettäjä käyttää omaa yksityista avaintaan ja liittää näin saadun digitaalisen allekirjoituksen lähetettävään viestiin. Vastaanottaja voi tarkistaa allekirjoituksen lähettäjän julkisen avaimen perusteella.

Jokainen TPM-piiri on yksilöity siihen kiinteästi sisällytetyllä Endorsment Key (EK) RSA -avaimella. EK-avaimella muodostetaan Attestation Identity Key (AIK) RSA -avaimia, joita käytetään esimerkiksi tietojen salaamiseen ja allekirjoittamiseen. Näin TPM-piirin yksilöivää EK-avainta ei kukaan ulkopuolinen voi päätellä. (TCG 2011)

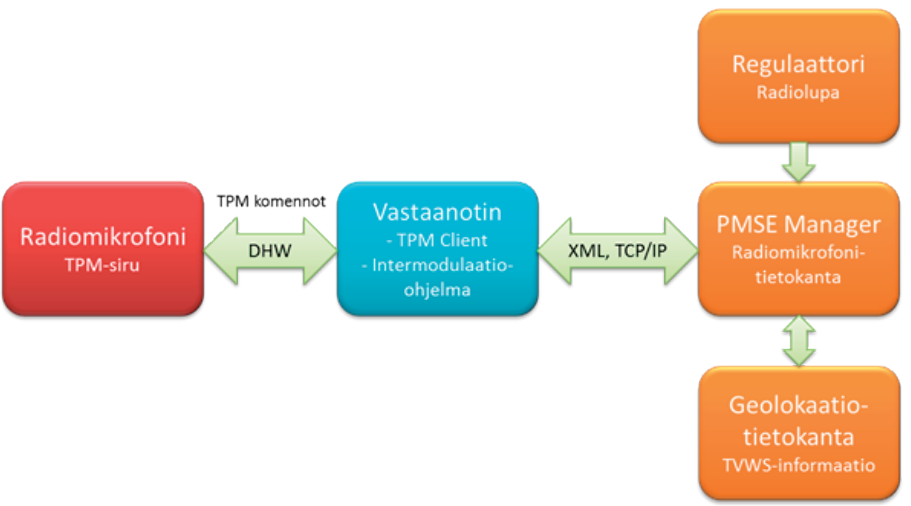
AUTENTIKOINTIARKKITEHTUURI

Radiomikrofonien käyttö vaatii radioluvan taajuuksien käytöstä vastaavalta viranomaiselta, joka Suomessa on Viestintävirasto. Vuonna 2012 suomessa oli 728 voimassa olevaa radiolupaa radiomikrofoneille. Radiolupa ei ilmaise ra-

diomikrofonien määrää, joita voi olla yhdestä tuhansiin yhtä radiolupaa kohden. Radiolupa ei myöskään sisällä tarkkaa tietoa siitä, missä radiomikrofonia käytetään, mitkä taajuudet on valittu ja milloin laite on käytössä (Viestintävirasto 2013b). Selvityksen perusteella Suomessa on alle 60 000 radiomikrofonia, jotka toimivat 800 MHz:n taajuusalueella. Vuonna 2010 radiomikrofonien vuosimyynti oli yli 7 000 kappaletta. (Liikenne- ja viestintävirasto 2013).

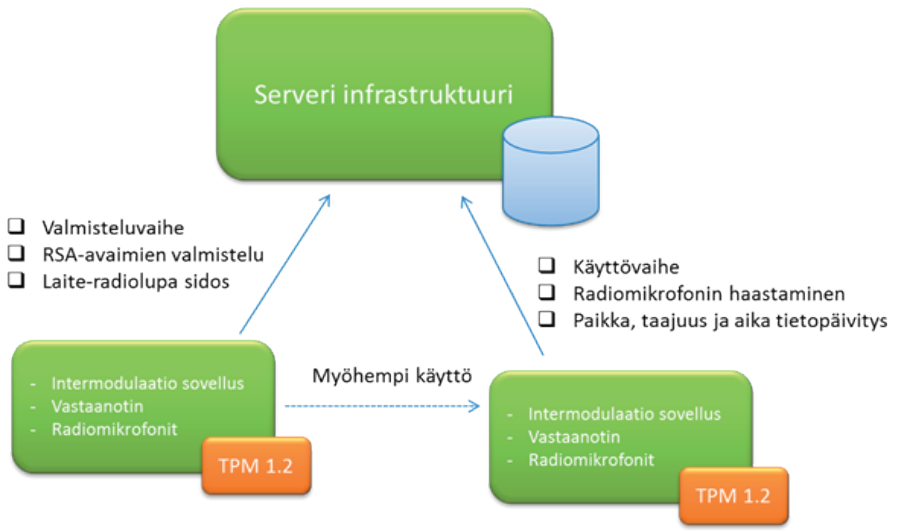
WISE-hankkeessa on kehitetty radiomikrofonitietokantajärjestelmä PMSE Manager, joka on yksinkertainen pilvipalvelu radiomikrofonien käyttäjille. Lyhenne PMSE tulee sanoista Programme and Special Event. Tällä tarkoitetaan video- ja audiolaitteita, joita käytetään esimerkiksi uutislähetyksiä tehtäessä (Viestintävirasto 2013a).

Kohderyhmänä palvelulle ovat kaikki radiomikrofonien käyttäjät. Alkuperäisenä tavoitteena oli mikrofonien rekisteröinti-innon lisääminen tuomalla moderni tapa käyttäjien saataville. Radiomikrofonitietokannalla voidaan yhdistää teknisesti Viestintäviraston myöntämät radioluvat, radiomikrofonien sijaintitiedot ja käytössä olevat taajuudet. Järjestelmällä on mahdollista automaattisesti ylläpitää taajuus- ja paikkatietoja käyttäen TPM-piiriä radiomikrofonien todentamiseen. PMSE Manager tarkistaa tietyin väliajoin, onko radiomikrofoni asetettu päälle lähettämällä autentikointikyselyn.



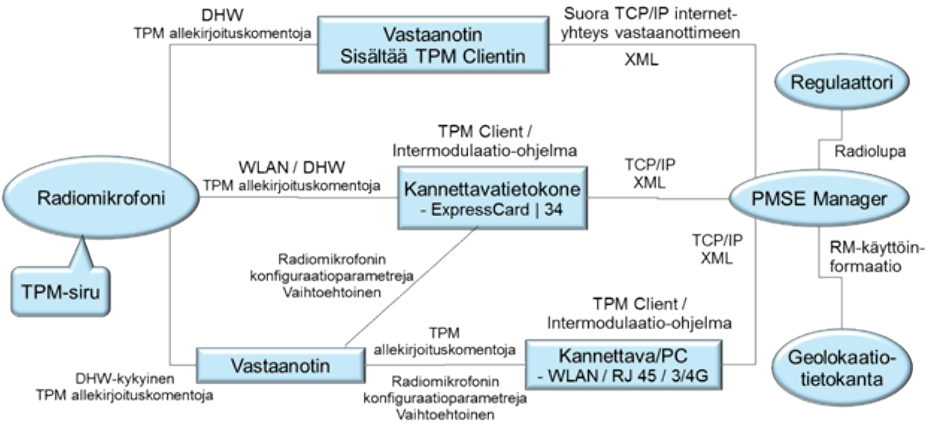
KUVA 1. *Toiminnallinen arkkitehtuuri.*

Radiomikrofonit ovat tietokoneisiin verrattuna yksinkertaisia laitteita, joten niistä ei voida olettaa löytyvän TPM-sirua. Radiomikrofonit ovat yhteydessä vastaanottimen sisältävään keskusyksikköön, joka sisältää laskentakapasiteettia. Keskusyksikkö pystyy kommunikoimaan PMSE Managerin kautta internetin välityksellä. Tilanne on esitetty kuvassa 1. Järjestelmän toimintavaiheet on esitetty kuvassa 2. Toiminnassa on kaksi vaihetta. Ensimmäisessä vaiheessa, kun laite otetaan käyttöön, tehdään sidos radioluvan ja laitteen välille.



KUVA 2. *Toiminnan vaiheet.*

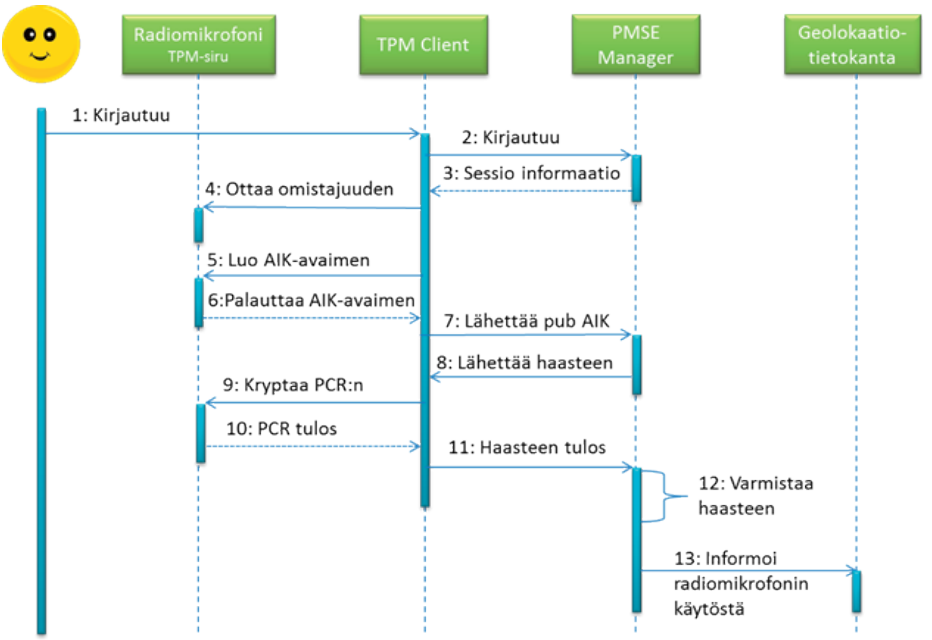
Tämän jälkeen aina mikrofonia käytettäessä otetaan ensin yhteys palvelimeen, joka tekee tarvittavan taajuusvarauksen käyttöä varten. Kuvassa 3 on esitetty käytännön toteutus kuvien 1 ja 2 kaavioiden pohjalta. Toteutuksen toimintaa on demonstroitu kansainvälisissä seminaareissa.



KUVA 3. *Demonstaattorin komponentit.*

ReWISE-hankkeessa on kehitetty protokolla kuvan 2 vaiheiden toteuttamiseksi. Laiteautentikointi PMSE Manageriin toimii seuraavasti: Radiomikrofoni tuottaa AIK RSA -avainparin (Attestation Identity Key), jonka julkinen avain lähetetään PMSE Managerille. Protokolla on challenge-response -tyyppinen. PMSE Manager lähettää radiomikrofonille haasteen, joka sisältää selkeäkielisen merkkijonon. Radiomikrofoni suorittaa allekirjoitusoperaation TPM-piirin tietystä rekisteristä löytyvän datan ja PMSE Managerilta saadun merkkijonon avulla. Radiomikrofoni lähettää PMSE Managerille tulokset. PMSE Manager varmentaa tuloksen allekirjoituksen käyttäen AIK-avaimen julkista osuutta ja radiomikrofonille haasteessa lähetettyä merkkijonoa. PMSE Manager lisää radiomikrofonin tietokantaan ja muodostaa sidoksen käyttäjän radiolupaan. Protokollan toiminta on kuvattu sekvenssikaavion avulla kuvassa 4.

Tuloksena on automaattinen ja tietoturvallinen laiterekisteröinti. Tämän avulla voidaan varmistaa, että vain luvalliset laitteet ovat käytössä. Samalla pystytään tehostamaan taajuuksien käyttöä.



KUVA 4. *Sekvenssikaavio radiomikrofonin rekisteröintioperaatiosta.*

TVWS-langattomalle teknologialle on kehitetty PAWS-protokolla (Protocol to Access White Space), joka toimii WS-laitteen ja geolokaatiotietokannan välisenä keskusteluprotokollana (IETF 2013). PAWS-protokolla mahdollistaa automatisoidun kommunikoinnin laitteen ja geolokaatiotietokannan välillä. PAWS-protokollalla laite voi rekisteröityä TVWS-järjestelmään ja pyytää geolokaatiotietokannalta TVWS-taajuuksia käytettäväksi. ReWISE-hankkeessa on laajennettu yllä esitetty protokolla siten, että sitä pystytään hyödyntämään yhdessä PAWS-protokollan kanssa WS-laitteita rekisteröitäessä. Tällöin WS-järjestelmään saadaan lisättyä laitetason autentikointi ja hallinta.

LÄHTEET

IETF 2013 Protocol to Access White-Space (PAWS) Databases. Viitattu 9.12.2013 https://datatracker.ietf.org/doc/draft-ietf-paws-protocol.

Liikenne- ja viestintävirasto 2013 800 MHz:n taajuusalueen matkaviestinkäyttö ja vapauttaminen radiomikrofonikäytöstä. Viitattu 9.12.2013 http://www.lvm.fi/c/document_library/get_file?folderId=1969043&name=DLFE-12964.doc.

pkix 2013 Public-Key Infrastructure (X.509). Viitattu 9.12.2013 http://datatracker.ietf.org/wg/pkix.

TCG 2011. Part 1 - Design Principles. Viitattu 9.12.2013 http://www.trustedcomputinggroup.org/files/static_page_files/72C26AB5-1A4B-B294-D002BC0B8C062FF6/TPM%20Main-Part%201%20Design%20Principles_v1.2_rev116_01032011.pdf.

TCG 2013. Trusted Platform Module. Viitattu 9.12.2013 http://www.trustedcomputinggroup.org/developers/trusted_platform_module.

Viestintävirasto 2013a Langattomat kamerat, videolinkit ja mikrofonit . Viitattu 9.12.2013 https://www.viestintavirasto.fi/taajuudet/radioluvat/langattomatmikrofonitjakamerat.html.

Viestintävirasto 2013b Radiolaitteet, -luvat ja tutkinnot 2012. Viitattu 9.12.2013 https://www.viestintavirasto.fi/tietoatoimialasta/katsauksetjaartikkelit/taajuudet/radiolaitteet-luvatjatutkinnot2012.html.

KÄYTTÄJÄHALLINTARATKAISUT SAP-TOIMINNANOHJAUS-JÄRJESTELMÄSSÄ

Aapo Sillanpää, tietojenkäsittelyn koulutusohjelman opiskelija, Turun ammattikorkeakoulu

Tuomo Helo, FM
Päätoiminen tuntiopettaja, tietojenkäsittelyn koulutusohjelma, Turun ammattikorkeakoulu

Toiminnanohjausjärjestelmät voivat korvata yrityksessä suurenkin määrän erillisiä toimintokohtaisia tietojärjestelmiä. Käyttäjienhallinnan näkökulmasta tarkasteltuna toiminnanohjausjärjestelmän käyttöönoton pitäisi siis yksinkertaistaa asioita. Näin suoraviivainen ajattelu voi kuitenkin johtaa harhaan. Toiminnanohjausjärjestelmät tukevat ja automatisoivat mitä moninaisimpia liiketoimintaprosesseja ja tehtäviä, minkä takia käyttäjien valtuuttamiseen liittyvät kysymykset ovat monimutkaisia. Käyttäjienhallintaan liittyvien uhkakuvien toteutumisen vaikutukset voivat myös olla laajoja ja merkittäviä. Toiminnanohjausjärjestelmä ei myöskään ole yrityksen ainoa tietojärjestelmä, vaan se usein integroidaan toimimaan yhteen monien muiden tietojärjestelmien kanssa. Tämä asettaa käyttäjienhallinnalle haasteita, jotka liittyvät integroinnin tuomaan tietoturvauhkaan ja sovelluskirjoon.

JOHDANTO

SAP on maailman johtava yritysohjelmistojen valmistaja. Se on erikoistunut yritysten toiminnanohjausjärjestelmien kehittämiseen (SAP 2013). SAP-toiminnanohjausjärjestelmä koostuu moduuleista, joita ovat esimerkiksi SAP Materials Management (MM) ja SAP Production Planning (PP).

Käyttäjienhallinta on tärkeä osa-alue yrityksen tietoturvan ja järjestelmäylläpidon näkökulmasta. Järjestelmäylläpidon tulee tietoturvan kannalta tietää, kenellä on pääsy yrityksen tietojärjestelmiin. Käyttäjähallinnan avulla ylläpito

hallinnoi yrityksen järjestelmien käyttäjätunnuksia sekä käyttäjien pääsyä järjestelmiin tai niiden osiin. (SAP AG 2011a.)

KÄYTTÄJÄHALLINNAN HAASTEET

Käyttäjienhallinnassa on nykyään monia haasteita liittyen etenkin organisaatioiden heterogeenisiin järjestelmäympäristöihin. Monien erilaisten tietojärjestelmien käyttäjien hallinta on ongelmallista, koska se joudutaan toteuttamaan usein monella erillisellä ratkaisulla. Tämä lisää ylläpidon haasteita ja heikentää tietoturvaa. Ylläpidosta tulee raskasta ja aikaa vievää.

SAP-toiminnanohjausjärjestelmän käyttäjähallinnassa on useita haasteita ja ongelmia, joista yksi suurimmista on SAP-ympäristön heterogeenisuus. Nykyisin SAP-järjestelmiin pystytään integroimaan muidenkin valmistajien järjestelmiä. SAP:n käyttäjähallinnan tulisi siis tukea myös niitä.

Ilman tukea muiden valmistajien järjestelmille SAP:n käyttäjähallinnalla voidaan hallita ainoastaan SAP:n ratkaisuja. SAP-järjestelmään liitettyjä järjestelmiä voivat olla esimerkiksi SAP Portal, erilaiset raportointityökalut ja webpohjaiset ratkaisut.

Tavoitteena on kaikkien SAP-järjestelmien ja niihin liitettyjen järjestelmien käyttäjähallinnan yhdistäminen yhteen keskitettyyn ratkaisuun. Tällainen ratkaisu nopeuttaisi ja helpottaisi SAP-ympäristön käyttäjähallintaa.

SAP-järjestelmien käyttäjähallinnan ongelmana on myös todella monimutkainen roolien luontiprosessi. Käyttäjäroolit tulisi pystyä luomaan työtehtäviin perustuen. Central User Administration -ratkaisulla roolien luonti työtehtäviin perustuen on todella haasteellista, ilman osaavaa henkilöstöä.

SAP-käyttäjähallinnan puutteena voidaan pitää myös vaarallisten työyhdistelmien muodostumista. Vaarallisella työyhdistelmällä tarkoitetaan, että sama työntekijä voi esimerkiksi tehdä laskun ja hyväksyä sen. Central User Administration -ratkaisu ei ota huomioon käyttäjärooleissa mahdollisesti olevia vaarallisia työyhdistelmiä, mikä on selkeä riski tietoturvan ja väärinkäytösten kannalta.

KESKITETTY KÄYTTÄJÄHALLINTA

Käyttäjähallinnan ratkaisuilla luodaan käyttäjärooleja ja -profiileja tietojärjestelmiin. Käyttäjärooleilla ja -profiileilla voidaan estää tai sallia loppukäyttäjien pääsy tiettyihin järjestelmiin tai niiden osiin. Rooleja voidaan luoda esimerkiksi työtehtävien perusteella. Työtehtäviin perustuvilla käyttäjärooleilla mahdollistetaan, että loppukäyttäjille annetaan tarpeeksi oikeuksia, jotta he pystyvät suorittamaan työtehtäviään. Työtehtäviin perustuvilla rooleilla pystytään myös varmistamaan se, että loppukäyttäjille annetaan juuri oikea määrä oikeuksia käyttämäänsä järjestelmään.

Heterogeenisen järjestelmäympäristön käyttäjähallinta tulisi pyrkiä ratkaisemaan keskitetyllä käyttäjähallintaratkaisulla. Keskitetty käyttäjähallinta yhdistäisi kaikkien järjestelmien käyttäjähallinnan yhteen keskitettyyn ratkaisuun (Wun-Young ym. 2008, 41). Keskitetyn ratkaisun avulla ylläpito helpottuu ja nopeutuu. Uusien käyttäjien luominen nopeutuu, koska uusi käyttäjä voidaan luoda yhdellä kerralla moneen järjestelmään. Tietoturva paranee, koska käyttäjien tiedot ovat ainoastaan yhdessä järjestelmässä. (Wun-Young ym. 2008, 41.)

SAP:N KÄYTTÄJÄHALLINNAN PROFIILIT JA ROOLIT

SAP:n autorisointikonsepti perustuu profiileihin ja rooleihin. Roolien kautta loppukäyttäjät saavat käyttöoikeudet järjestelmään. (Help SAP 2013.)

Profiilit sisältävät itse autorisointiin tarvittavan informaation. SAP-järjestelmässä voi olla erilaisia profiileja perustuen niiden luontitapaan tai ominaisuuksiin. SAP-profiileja voidaan luoda manuaalisesti tai Profile Generatorin avulla. Profiileja voi olla yksittäisiä sekä yhdistelmiä eri profiileista eli Composite-profiileja. (Help SAP 2013.)

SAP:n rooli on kokoelma käyttöoikeuksia eli profiileja. Rooli voi sisältää monia profiileja, mutta sen täytyy sisältää ainakin yksi profiili. SAP:n roolit voidaan jakaa kahteen ryhmään, Composite ja Single. Composite-rooli koostuu useista Single-rooleista. Single-rooli taas on yksittäinen rooli (Help SAP 2013a). Roolit voidaan määrittää loppukäyttäjille transaktioilla SU01 tai PFCG. SU01 transaktio käynnistää SAP Central User Administrationin maintain user -toiminnon. PFCG-transaktio käynnistää Profile Generatorin, jonka avulla pystytään luomaanja ylläpitämään rooleja. (Help SAP 2013b.)

SAP-KÄYTTÄJÄHALLINTARATKAISUT

SAP-toiminnanohjausjärjestelmän käyttäjähallintaan on saatavilla monia erilaisia ratkaisuja. Ratkaisut eroavat toisistaan lähinnä integraatiomahdollisuuksiensa ja käyttäjäprofiilien luonnin perusteella.

SAP Central User Administration

SAP Central User Administration -ohjelmisto (SAP CUA) kehitettiin vain Advanced Business Application Programming (ABAP) -ohjelmointikielellä toteutettujen sovellusten hallintaan. Sen päätehtävänä on luoda ja jakaa kaikki käyttäjätilit ja käyttäjäroolit keskitetysti yhdestä ABAP-pohjaisesta järjestelmästä. (Gergen ym. 2010, 70.)

SAP CUA:n suurimpina hyötyinä voidaan pitää käyttäjähallinnan helppoutta sekä mahdollisuutta keskittää käyttäjähallinnan toimet yhteen järjestelmään. CUA:ta suosivat useat yritykset, jotka hankkivat käyttöönsä monia ABAP-pohjaisia SAP-moduuleita. (Gergen ym. 2010, 70.)

CUA on vieläkin todella suosittu ratkaisu SAP:n käyttäjien hallintaan, vaikka se ei enää pysty tarjoamaan muuta kuin hyvät integraatiomahdollisuudet ABAP-ympäristössä. CUA:ssa ei ole rajapintoja SAP:n muille ratkaisuille kuten Workflow`lle tai Portalille, jolloin niiden integraatiot tulee toteuttaa itsenäisesti.

CUA ei myöskään huomioi roolitukseen liittyviä riskejä. Käyttäjille pystytään myöntämään rooleja, jotka voivat sisältävät vaarallisia työyhdistelmiä. Tietoturvan ja väärinkäytösten kannalta tämä on selkeä riski. SAP CUA ei myöskään tue loppukäyttäjien itsepalveluominaisuuksia salasanojen vaihtamiseen. (Gergen ym. 2010, 70.)

SAP CUA:ssa on selkeitä puutteita verrattuna esimerkiksi SAP NetWeaver Identity Management - NW IDMkäyttäjienhallintaratkaisuun. SAP on lopettanut CUA:n kehitystyön kokonaan. Korjauksia kuitenkin julkaistaan vielä. Oheinen seikka osoittaa selvästi, että SAP ei enää halua tarjota asiakkailleen CUA-ratkaisua käyttäjien hallintaan, vaan pyrkii tarjoamaan uudempia ja kehittyneempiä ratkaisuja.

SAP NetWeaver Identity Management

SAP NetWeaver Identity Management on SAP NetWeaver alustan päälle rakennettu käyttäjähallintasovellus. Se mahdollistaa keskitetyn käyttäjätietojen hallinnan ja jakelun koko organisaation järjestelmäympäristössä. (Gergen ym. 2010, 78.)

NetWeaver Identity Management -ratkaisuun pystytään integroimaan erilaisia ratkaisuja, kuten SAP Governance, Risk and Compliance -ratkaisuja ja web-palveluita. Windows-, tietokanta- ja räätälöidytsovellukset voidaan myös integroida SAP NW IDM -ratkaisun piiriin. NetWeaver tarjoaa myös avoimiin standardeihin perustuvan kehitysympäristön SAP-ohjelmistoille. (Gergen ym. 2010, 77.)

NetWeaver Identity Managementin suurimpana hyötynä voidaan pitää sen laajoja integraatiomahdollisuuksia. NetWeaver Identity Managementin käyttäjähallinnan piiriin pystytään integroimaan myös muita kuin ABAP-pohjaisia järjestelmiä.

YHTEENVETO

Nykyisin SAP:n ratkaisuihin integroidaan monia erilaisia ja eri valmistajien ratkaisuja tuomaan lisäarvoa yrityksen toimintaan.

SAP Central User Administrationiin ei voida integroida muita kuin SAP:n ABAP-pohjaisia ratkaisuja (taulukko 1). Tämä on nykyään suuri puute, jos keskitetyn käyttäjähallintaratkaisun piiriin halutaan kaikki yrityksen tietojärjestelmät.

Nykyajan vaatimuksiin parhaiten vastaa NetWeaver Identity Management -ratkaisu, jonka keskitetynkäyttäjähallinnan piiriin saadaan niin SAP:n kuin muidenkin valmistajien ratkaisut. Tämä seikka helpottaa ylläpitoa sekä parantaa tietoturvaa, koska käyttäjätiedot sijaitsevat ainoastaan yhdessä järjestelmässä. NetWeaver Identity Management -ratkaisussa käyttäjäroolien luonti on suoraviivaista ja helppoa. Roolit pystytään luomaan työtehtäviin perustuen. SAP NetWeaver Identity Management -ratkaisun avulla pystytään myös eliminoimaan vaaralliset työyhdistelmät, mikä parantaa tietoturvaa ja vähentää riskiä väärinkäytöksiin.

SAP NW IDM:n integrointimahdollisuuksien ansiosta SAP Portal -ratkaisun integroiminen keskitetyn SAP-käyttäjähallinnan piiriin olisi mahdollista. Käyttäjäroolit, käyttäjätunnukset ja käyttöoikeudet voitaisiin hallita keskitetysti yhdellä ratkaisulla.

Loppukäyttäjien itsepalveluominaisuuksien kautta käyttäjien hallintaan liittyvien muutoksien suorittaminen nopeutuisi. Ominaisuuden avulla loppukäyttäjät pystyvät tekemään tiettyjä muutoksia itsenäisesti, esimerkiksi uusimaan salasanansa ilman, että heidän tarvitsisi ottaa yhteyttä käyttäjien hallinnasta vastaavaan tahoon.

SAP NW IDM:n avulla pystytään rakentamaan todella kattava raportointi loppukäyttäjistä ja käyttäjähallinnan tilasta. Raportteihin saataisiin mukaan myös SAP Portal -ratkaisu. NW IDM:n raportointi integroituu todella hyvin Crystal Reports ja Business Warehouse -pohjaisiin raportointiratkaisuihin (taulukko 1).

TAULUKKO 2. *SAP käyttäjähallintasovellusten vertailu (SAP AG 2011b).*

Toiminnallisuus	SAP CUA	SAP NetWeaver Identity Management
Kohdejärjestelmät	Vain ABAP-pohjaiset	SAP:n ja muiden toimittajien sovellukset
Workflow (työnkulku) tuki	Ei	Kyllä
Roolihierarkian mallinnus	Ei	Kyllä
Järjestelmäriippumaton roolien jakelu	Manuaalinen	Kyllä, automaattinen
LDAP-hakemiston integraatio	Ainoastaan LDAP-synkronointi	Kyllä
Salasanojen hallinta	Kyllä, keskitetty alustavien salasanojen hallinta ja jakelu	Kyllä, käyttöliittymä mahdollistaa keskittämättömän salasanojen vaihdon
Graafinen käyttöliittymä	Kyllä, transaktion SU10:n kautta	Kyllä, tukee massamuutoksia CSV-tiedostojen kautta
Raportointi	Kyllä, transaktion SUIM:n kautta	Kyllä, standardoituja raportteja SAP Business warehousen tai SAP Crystal Reportsin kautta
Sähköposti-ilmoitukset	Ei	Kyllä

SAP NW IDM -ratkaisun avulla organisaatiot voisivat saavuttaa monia hyötyjä. SAP Portalin ja muiden ratkaisujen integrointi keskitetyn käyttäjähallintaratkaisun piiriin on mahdollista. SAP NW IDM integroituu saumattomasti SAP NW Business Warehouse ja Crystal Reports raportointiratkaisuihin. SAP NW IDM tukee automaattista käyttäjähallintaa, työnkulkuun perustuen. SAP NW IDM -ratkaisussa käyttäjärooleja hallitaan työtehtäviin perustuen.

LÄHTEET

Gergen, P.; Heilig, L. & Muller, A. 2010. Understanding SAP NetWeaver Identity Management. Boston: Galileo Press. Translator: Lemoine International.

Help SAP 2013a. AS ABAP Authorization Concept. Viitattu 5.11.2013 http://help.sap.com/saphelp_nw2004s/helpdata/en/52/671285439b11d1896f0000e8322d00/content.htm.

Help SAP 2013b. PFCG Overview. Viitattu 18.12.2013. http://help.sap.com/saphelp_nw70ehp2/helpdata/en/8b/ad5f3695c948d6b465be609da6d9f7/content.htm.

SAP AG 2011a. SAP NetWeaver ID Management Solution Details. SAP Solution in Detail 5/11.

SAP AG 2011b. SAP NetWeaver Identity Management: The Time is now. Replace CUA – Set a strategic course in user administration 11/04.

SAP 2013. About SAP AG. 1971-1981: the early years. Viitattu 20.11.2013 http://global.sap.com/corporate-en/our-company/index.epx.

Wun-Young, L.; Hirao, J.; Hirao, J.; Choi, M.; Cox, P. & Passer, L.S. 2008. SAP Security Configuration and Deployment. Burlington: Syngress.

OPPIMISYMPÄRISTÖJÄ JA OPISKELIJAPROJEKTEJA

KATSAUS TIKOTRAIN-PROJEKTIPAJAN VUODEN 2013 TOIMINTAAN

Jana Pullinen, FM
Lehtori, tietojenkäsittelyn koulutusohjelma, Turun ammattikorkeakoulu

TiKoTrain-projektipaja on Turun ammattikorkeakoulun tietojenkäsittelyn koulutusohjelman (TiKo) 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 pystytään palvelemaan alueen PK-yrityksiä läpi vuoden, lukuun ottamatta kesäkuukausia. Pienet ja keskisuuret yritykset (PK-yritykset) määritellään yrityksiksi, joiden palveluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa. (Tilastokeskus 2013). Projekteja pystytään kuitenkin myös integroimaan opetussuunnitelmassa oleviin opintojaksoihin tarpeen mukaan.

Opiskelijat toteuttavat 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.

TiKoTrain toimii tärkeänä linkkinä ammattikorkeakoulun ja alueen yritysten välillä. TiKoTrainista saa lisää tietoja Turun ammattikorkeakoulun julkaisusta Näkökulmia tietoturvaan (Pullinen 2013). TiKoTrain tekee tiivistä yhteistyötä yritysten ja alueella toimivien järjestöjen, kuten esimerkiksi Varsinais-Suomen Tietojenkäsittely-yhdistys ry:n (VSTKY), kanssa (VSTKY 2013). VSTKY järjestää laadukkaita seminaareja ja tilaisuuksia, joista hyötyvät niin opettajat kuin opiskelijatkin. Näistä mainittakoon keväällä 2013 Turussa järjestetty road show Liiketoiminnan vaatimukset tietohallinnon ja tietoturvan

haasteena. (VSTKY Roadshow 2013). Tilaisuuden järjestivät Tietotekniikan liiton jäsenyhdistykset VSTKY, Tietoturva ry (Tietoturva ry 2013) ja ICT Leaders Finland (ICT Leaders Finland 2013).

TIKOTRAININ WWW-OHJELMOINTIPROJEKTIT

TiKoTrainissa opiskelijat voivat suorittaa erityyppisiä projekteja. Suosituimpia ovat olleet www-ohjelmointiprojektit, joissa PK-yritykselle luodaan kotisivut markkinoimaan yrityksen toimintaa. Kotisivujen työstäminen aloitetaan aina vaatimusmäärittelyllä. Vaatimusmäärittelyn avulla projektipäällikkö pystyy myös arvioimaan projektin laajuuden sekä keston. Vuoden 2013 aikana on toteutettu laaja TiKon markkinointiprojekti, jossa päämääränä on ollut saada näkyvyyttä syksyn yhteishakuun (TiKo 2013). Projekti on sisältänyt niin sisällönsuunnittelua, ohjelmointia, haastatteluita, videointia kuin myös testausta ja laajaa dokumentointia. Itse markkinointisivustot toteutettiin merkintäkieli XHTML:n avulla. Projektissa oli tarkoitus hyödyntää WordPress-sisällöntuotantojärjestelmää, mutta visuaalisen ilmeen vaatimusten vuoksi tämä ei onnistunut järjestelmän osoittautuessa joustamattomaksi. Projektin loppuvaiheessa opiskelijaryhmät testasivat sivuston toimivuuden tietoturvaa silmälläpitäen. Laajaan projektiin kuului myös TiKoTrainin omien sivujen uudelleensuunnittelu vastaamaan markkinointisivustojen ulkonäköä. Markkinointisivustoista haluttiin sateenvarjo, josta asiakas tai opiskelija pääsee navigoimaan itsensä TiKon palveluihin.

TIETOTURVAPÄIVÄ PK-YRITYKSILLE

Tietojenkäsittelyn koulutusohjelma järjestää vuosittain Tietoturvapäivän PK-yrityksille. Projekti kestää noin seitsemän kuukautta ja työllistää neljästä kuuteen opiskelijaa. Vuoden 2013 projekti on aloitettu syyskuussa 2013 kesälomien jälkeen ja projekti päättyy Tietoturvapäivän jälkeen helmikuussa 2014. Tietoturvapäivä on laajentunut vuosi vuodelta, ja projektin myötä pyritään saattamaan tietoturva-asioita niin PK-yrittäjän kuin tavallisen kansalaisenkin tietoisuuteen. Projektin tärkeimmät osa-alueet ovat esiintyjien varmistaminen ja markkinointi yrityksille sekä yhteisöille. Itse päivässä on mukana myös nuorempia opiskelijoita auttamassa käytännön järjestelyissä. Aiheet on pyritty

valitsemaan siten, että kuulijat saisivat mahdollisimman paljon käytännönläheistä tietoutta. Tulevaisuudessa Tietoturvapäivää tullaan edelleen kehittämään aina ajankohtaisten asioiden mukaisesti.

Vuoden 2014 Tietoturvapäivän teema on *Tietoturva liiketoiminnan mahdollistajana*. Esiintyjälistalla ovat edustajat seuraavista yrityksistä: Anders Inno, Fujitsu, Oracle, Securitas, SSH Communications Security sekä Symantec. Puheenvuorojen lisäksi tapahtumassa esitellään tietoturvaan liittyviä demonstraatioita. Tunkeutumistestaus (engl. penetration testing) osoittaa verkkojen ja tietojärjestelmien haavoittuvuuden (vrt. Esko Vainikan artikkeli tässä julkaisussa) ja sen, kuinka tietomurtoihin liittyvät ohjelmistot ovat kaikkien saatavilla. Internetselailun tietosuojaa havainnoillistetaan ohjelmistoilla, jotka näyttävät, kuinka nopeasti ja laajalle internetin käyttötiedot leviävät (vrt. Matti Laakson artikkeli tässä julkaisussa).

PK-YRITYKSILLE SUUNNATTU TIETOTURVASIVUSTO

Tietoturvapäivän ohella tietoturvatietoutta tarjotaan erillisen sivuston kautta (Tietoturvapäivä 2013a). Kaksi opiskelijaa ylläpitää tietoturvasivustoa viikoittain. Projekti käynnistetään helmikuussa 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 kun sivusto valmistellaan seuraavaa Tietoturvapäivää varten. Esiintyjien yritysten logot ja esitysten aiheet julkaistaan sivustolla syksyn aikana ja tietoja tarkennetaan aina viimeiseen hetkeen saakka. Itse Tietoturvapäivän aikana sivustolle viedään esitysmateriaalit (Tietoturvapäivä 2013b). Tietoturvasivustolta PK-yrittäjä löytää paitsi esitysmateriaalit Tietoturvapäivistä myös nettilinkkejä, joista on hyötyä yrittäjän arjessa. Asioita ei kirjoiteta sivustolla uudelleen, vaan sivusto toimii sateenvarjoportaalina tietoturva-asioiden löytymisen helpottamiseksi. Vuoden 2013 aikana, markkinointiprojektin yhteydessä, tietoturvasivusto on uusittu noudattamaan samaa ulkoasua kuin markkinointisivusto. Opiskelija toteutti projektin erillisprojektina, mutta projektiryhmät pitivät hyvin tiiviisti yhteyttä toisiinsa.

Tietoturvasivuston yhteydessä on myös tietoturvatesti, jonka jokainen voi käydä tekemässä useampaankin otteeseen. Testi on anonyymi, eli mitään hen-

kilötietoja 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 sinne jatkuvasti lisää. Myös tietoturvatestin ulkoasu on muuttunut kuluneen vuoden aikana. Tietoturvatestin tietokantaan on lisätty huomattava määrä kysymyksiä, ja suunnitelmissa on jatkojalostaa testiä vuoden 2014 aikana.

TIETOTURVA-AUDITOINNIT

Jotta tieturvasivuston tietokantaan saadaan lisää kysymyksiä, hyödynnetään tietoturva-auditointeja tekeviä projektiryhmiä. Opiskelijat työstävät PK-yritykselle tietoturva-auditointiprojektia, jossa laaditaan kysymyspatteristoa yrittäjälle. Samaiset kysymykset viedään myös sivuston 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.

Syksyllä 2013 Raision alueen yrityksille on käynnistetty laaja kysely, jossa tavoitteena on kartoittaa PK-yrityksen tietoturva-asiat alueella. Pilottiprojekti käynnistetään yhteistyössä Raision Yrittäjien (Raision yrittäjät 2013) kanssa ja sitä laajennetaan muille alueille vuonna 2014. Kysely toteutuaan ensi vaiheessa opiskelijaprojektina, ja pyrkimyksenä on, että kaksi opiskelijaa tekisi siitä opinnäytetyön.

VERKKOKAUPPA OPISKELIJAPROJEKTINA -OPINNÄYTETYÖ

TiKoTrainiin tulee yhä enemmän kyselyitä verkkokaupan perustamisesta. Koska verkkokauppa on käsitteenä huomattavasti paljon laajempi kuin pelkät www-sivut, käynnistettiin projekti, jossa opiskelija teki aiheesta opinnäytetyön (Pakarinen 2013). Verkkokauppa on riskialtis liiketoimintamalli, ja opinnäytetyön valmistumisen myötä TikoTrainissa on mahdollisuus opastaa yrittäjiä tähän toimintaan antamalla opinnäytetyö luettavaksi, ennen kuin yrittäjä pe-

rustaa varsinaisen verkkokaupan. Opinnäytetyössä käytetään TiKoTrainia esimerkkinä, mutta tieto on hyvin sovellettavissa mihin liiketoimintaan tahansa. Opinnäytetyö lähtee liikkeelle perusasioista, kuten lainsäädäntö ja pilvipalveluiden perusteet, ja jatkuu aina itse verkkokauppajärjestelmän asentamiseen saakka. Esimerkkeinä opinnäytetyössä on käytetty Amazon EC2 pilvipalvelua (Amazon 2013) sekä Magneto-verkkokauppa-alustaa (X Commerce 2013). Opinnäytetyötä edelsi konsultointiprojekti Yrityspalvelukeskus Potkurin (Potkuri 2013) kanssa. Siellä oli noussut esiin sama problematiikka – yrittäjät eivät ole tietoisia kaikista lainsäädännöllisistä sekä tietoturvaan liittyvistä asioista.

LOPUKSI

TiKoTrain-projektipaja kannustaa opiskelijoita miettimään projektien jatkumoa sekä asiakaspalvelua PK-yritykselle. Ohjauksessa keskeisenä periaatteena on, että aina ei lähdetä luomaan uutta ja romuteta vanhaa olemassa olevaa. Usein työelämään astuessaan 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.

LÄHTEET

Amazon 2013 What is AWS?. Viitattu 11.11.2013 http://aws.amazon.com/.

ICT Leaders Finland 2013. Viitattu 11.11.2013 http://www.ilf.fi/.

Pakarinen, Hannu 2013. Verkkokauppa opiskelijaprojektina. Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Turku: Turun ammattikorkeakoulu. http://publications.theseus.fi/bitstream/handle/10024/58080/Pakarinen_Hannu.pdf?sequence=1 .

Potkuri 2013 Yrityspalvelukeskus Potkuri. Viitattu 11.11.2013 http://www.potkuri.fi.

Pullinen, Jana 2013. TiKoTrain-projektipajan palvelut PK-yrityksille. Teoksessa Paavola J. & Vainikka E. (toim.) Näkökulmia tietoturvaan, Turun ammattikorkeakoulu, 46–48.

Raision Yrittäjät 2013. Viitattu 11.11.2013 http://www.yrittajat.fi/fi-FI/varsinais-suomenyrittajat/raisio/.

TiKo 2013 Tietojenkäsittelyn koulutusohjelman markkinointisivusto. Viitattu 11.11.2013 http://www.tiko.turkuamk.fi.

Tilastokeskus 2013 PK-yritys. Viitattu 12.12.2014 http://www.stat.fi/meta/kas/pk_yritys.html.

Tietoturvapäivä 2013a Tietoturvapäivän sivusto. Viitattu 11.11.2013 http://www.tietoturvapäivä.fi.

Tietoturvapäivä 2013b Vuoden 2013 tietoturvapäivän materiaalit. Viitattu 11.11.2013 http://www.tietoturvapaiva.fi/index.php?page=esitysmateriaalit

Tietoturva ry 2013. Viitattu 11.11.2013 http://www.tietoturva.fi/.

VSTKY 2013, Varsinais-Suomen Tietojenkäsittely-yhdistys ry. Viitattu 11.11.2013 http://www.vstky.fi/yhdistys.

VSTKY Roadshow 2013 Road show esitysmateriaalit. Viitattu 11.11.2013 http://www.ttlry.fi/liiketoiminnan-vaatimukset-tietohallinnon-ja-tietoturvan-haasteena-road-show.

X Commerce 2013 Magento Product Overview. Viitattu 11.11.2013 http://www.magentocommerce.com/.

ASIAKKAAN TIETOTURVATIETOISUUDEN VAHVISTAMINEN – CASE KANSALAISEN MIKROTUKI

Virpi Raivonen, FM, KTK
Lehtori, tietojenkäsittelyn koulutusohjelma, Turun ammattikorkeakoulu

Petri Virta, tietojenkäsittelyn koulutusohjelman opiskelija,
Kansalaisen mikrotuen projektipäällikkö

Kansalaisen mikrotuki on opiskelijavetoinen oppimisympäristö, jossa huolletaan Turun alueen asukkaiden tietokoneita. Perushuollon lisäksi toimipisteessä järjestetään neuvontapäiviä ja henkilökohtaista opastusta ajankohtaisista tietoturvaan liittyvistä asioista. Palvelu on asiakkaille maksutonta.

Kansalaisen mikrotuen toiminta käynnistyi Turun kaupungin Ihminen@ Turku-ohjelman ja Turun ammattikorkeakoulun alueellisen vaikuttavuuden kehittämisen yhteistyöprojektina vuonna 2004 (Kunnat.net 2006 ja Tietoyhteiskuntaohjelma 2006). Ihminen@Turku-tietoyhteiskuntaohjelma painottui vuosille 2004–2006. Ohjelmassa oli kirjattuna kolmekymmentä toimenpidesuositusta, joilla pyrittiin tuomaan viestintäteknologia lähelle kaupunkilaisen arkea.

Palvelu koettiin rahoitetun projektin päättyessä tarpeelliseksi, joten toimintaa jatkettiin osana ammattikorkeakoulun yhteiskuntavastuullista vaikuttamista. Toiminta on jatkunut pian kymmenen vuotta. Yhteydenotoista, vuosittain noin 1500, suurin osa tulee alueen seniorikansalaisilta ja opiskelijoilta. Toimipiste on vuoden aikana auki keskimäärin 200 päivää. Lukuvuonna 2012–2013 huollettuja koneita oli noin 500, tiskillä tapahtuvia neuvonta- ja huoltotoimenpiteitä noin 300, vastaanotettuja puheluita 500 ja sähköposteja 36 kappaletta. Keskimääräinen huoltoaika per kone on ollut noin puoli tuntia. Tiskillä tapahtuvien opastusten kesto on vaihdellut puolesta tunnista tuntiin.

Kansalaisen mikrotuessa opiskelijat suorittavat työharjoittelua ja erilaisia opintojaksojen käytännön osuuksia: neuvonta- ja opastustaidon harjoittelua, asiakaspalvelua ja kehittämistehtäviä opinnäytetyön muodossa. Alueen toisen asteen kouluista tulee harjoittelijoita ja työelämään tutustumisjakson suorittajia hakemaan osaamista tietoturvaan liittyvistä tehtävistä. Oppimisympäristö antaa hyvää kokemusta projektipäällikölle henkilöstöhallinnosta, toimipisteen johtamisesta ja kehittämisestä. Toimipisteessä harjoitteluaan suorittavat vaihto-opiskelijat ovat tarjonneet palvelua etenkin englanniksi. Toimipisteessä on ollut tarjolla opastusta ruotsiksi, venäjäksi ja espanjaksi. Harjoittelijoita on ollut myös esimerkiksi Bangladeshista, Vietnamista ja Keniasta.

HENKILÖKOHTAISEN OPASTUKSEN TARVE

Turun alueen asukkaiden tietoturvaosaamista on Kansalaisen mikrotuessa seurattu alusta lähtien. Vuodesta toiseen pysyvien teemojen lisäksi on havaittavissa johonkin tiettyyn ohjelmaan tai laitteeseen liittyviä, vaihtuvia tarpeita. Digibokseihin ja mokkuloihin liittyvät ongelmat ovat pääsääntöisesti vaihtuneet älypuhelinten käyttöön liittyviin kysymyksiin. Käyttöjärjestelmien vaihtuminen on tuonut aallon opastusta tarvitsevia. Windows 8:n lanseeraus aiheutti alkuvuodesta ja vielä syksyllä piikin henkilökohtaisen neuvonnan kysynnässä.

Tutkimusten mukaan osa ihmisistä jää kokonaan tietoyhteiskunnan ulkopuolelle, joko omasta halustaan tai siitä syystä, että osaaminen ja uskallus käyttää internetiä eivät riitä (Berg 2011). Kansalaisen mikrotuessa on havaittu sama asia etenkin seniorikansalaisten suhteen. Epävarmuus omasta osaamisesta ei yhden suoritetun tietokonekurssin jälkeen vielä poistu. Asiakas on vieraillut toimipisteessä ja saanut kertomansa mukaan haluamansa avun. Vaikka hän on saanut asiaan opastusta ja kertoo periaatteessa ymmärtävänsä mistä on kyse, ei uskallus eikä usko omaan osaamiseen ole riittänyt siihen, että hän olisi kokeillut ongelmanratkaisua itse.

Capgeminin Euroopan komissiolle toteuttaman eGovernment-tutkimuksen mukaan 41 % suomalaisista ei käytä julkishallinnon sähköisiä palveluja. Suurin osa näistä 41 %:iin kuuluvista halusi henkilökohtaista palvelua (67 % vastaajista). Osaamattomuus, tiedon puute tai se että ei ole pääsyä palveluihin piti 29 % ulkona (Capgemini 2013). Kansalaisen mikrotuen käyttäjille suunnatuista henkilökohtaisista opastuksista osa on kohdistunut juuri julkis-

ten palveluiden verkkosivustojen käyttöön. Kelan ja pankin sivujen käyttöä ja laskujen maksamista käydään yhdessä lävitse asiakkaan kanssa.

Osa niistä asiakkaista, jotka tulevat toimipisteeseen, haluaa opastusta siihen, millainen tietokone heidän kannattaa hankkia. Asiakas on huomannut, että ei enää tule toimeen ilman tietokonetta. Oma osaaminen ei kuitenkaan riitä ostopäätökseen. Käkäte (Käyttäjille kätevä teknologia) -projektin tekemän tutkimuksen mukaan Suomessa on noin 30 000 yli 75-vuotiasta, joilla ei ole tietokonetta, ja 75–89-vuotiaista vain joka viides on käyttänyt internetiä. 40 000 vanhuksella ei ole edes matkapuhelinta. Tiedonpuute ja epävarmuus vähentävät halukkuutta ottaa teknologiaa arjen tueksi (Intosalmi, Nykänen ja Stenberg 2013).

Toukokuussa 2013 tehdyn kyselyn mukaan 18-vuotiaista ja sitä vanhemmista amerikkalaisista 15 % ei käytä sähköpostia tai internetiä. Heistä 32 % kertoi syyksi sen, että he kokivat, että internetiä ei ole helppo käyttää. Lisäksi he pelkäsivät vakoiluohjelmia, roskapostia ja hakkereita (Zickuhr 2013).

Kansalaisen mikrotuessa järjestetään asiakkaille henkilökohtaista opastusta ja teemapäiviä. Henkilökohtaisessa opastuksessa asiakas voi varata itselleen pääsääntöisesti tunnin ajan, jolloin hänen kanssaan käydään lävitse toivottua asiaa. Usein asiakas ei osaa tarkentaa, mitä hän haluaisi käydä lävitse. Tällöin hänen kanssaan edetään kysymysten ja esimerkkien avulla. Senioriopastuksissa on huomattu, että seniorikansalaisten kanssa kannattaa edetä yleisestä yksityiskohtiin. Käydään rauhassa lävitse käsitteitä, tutustutaan toimintoihin ja vasta sitten edetään ongelmaan. Kun asiakas on ymmärtänyt, mistä on kyse, mihin asiaa tarvitaan ja vielä mistä se löytyy, on asiakastyytyväisyys ollut taattua.

Teemapäivät rakentuvat joihinkin ajankohtaisiin, usein asiakkaiden kohtaamisissa esiin tulleisiin ongelmiin. Facebook-päivänä tehtiin profiileja ja tarkasteltiin sivuston yksityisyysasetuksia. Skype-koulutuksessa otettiin yhteyttä ystäviin ja sukulaisiin Suomessa ja maailmalla. Tiedot talteen -varmuuskopiointipäivän aikana tuli tutuksi pilvipalveluiden käyttö ja etenkin varmuuskopioinnin tärkeys. Marraskuussa 2013 järjestetyssä Älypuhelin-päivässä tarjottiin alkuluennon jälkeen henkilökohtaista neuvontaa asiakasta askarruttaviin ongelmiin. Tärkeimpinä asioina esiin nousivat varmuuskopiointi, puhelinten tietoturva sekä navigointi.

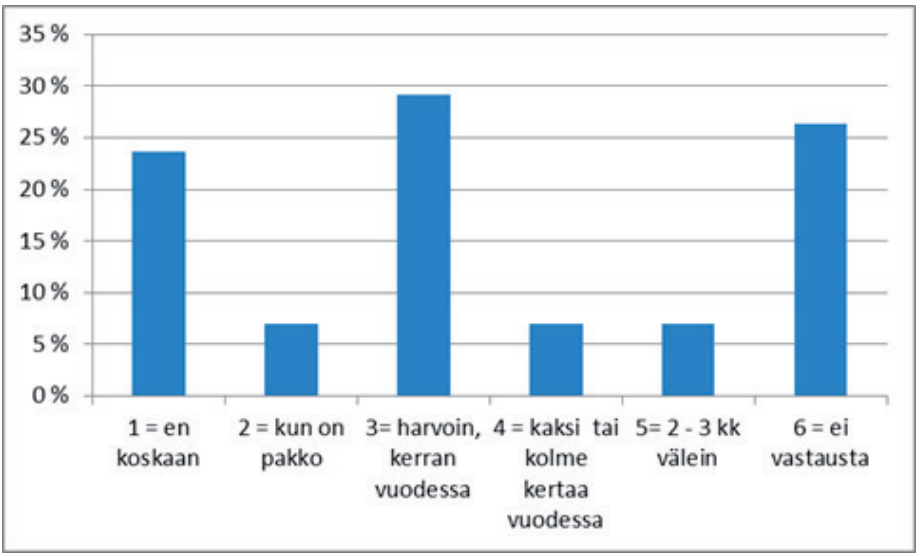
TIETOTURVAOSAAMINEN

Suomen 16–65-vuotiaasta aikuisväestöstä 30 prosentilla eli noin miljoonalla aikuisella on puutteelliset tietotekniikkaan liittyvät ongelmanratkaisutaidot todetaan opetus- ja kulttuuriministeriön tiedotteessa (Opetus ja kulttuuriministeriö 2013).

Kansalaisen mikrotuen toimipisteessä kartoitetaan asiakkaiden tietoturvaosaamista pienimuotoisella kyselyllä (liite 1). Asiakkaalta kysytään koneen vastaanottohetkellä halukkuutta vastata asiakaskyselyyn. Mikäli jokin kysymys ei ole ymmärrettävä asiakkaan mielestä, häntä palveleva henkilö pyrkii selventämään, mitä kysymyksellä tarkoitetaan. Marraskuun loppuun mennessä vastauksia oli tullut 72 kappaletta. Pääsääntöisesti asiakkaiden tietoturvaosaaminen liittyen salasanoihin, liitetiedostoihin ja oman koneen virusohjelman käyttöön oli kyselystä saatujen vastausten perusteella hyvällä tasolla.

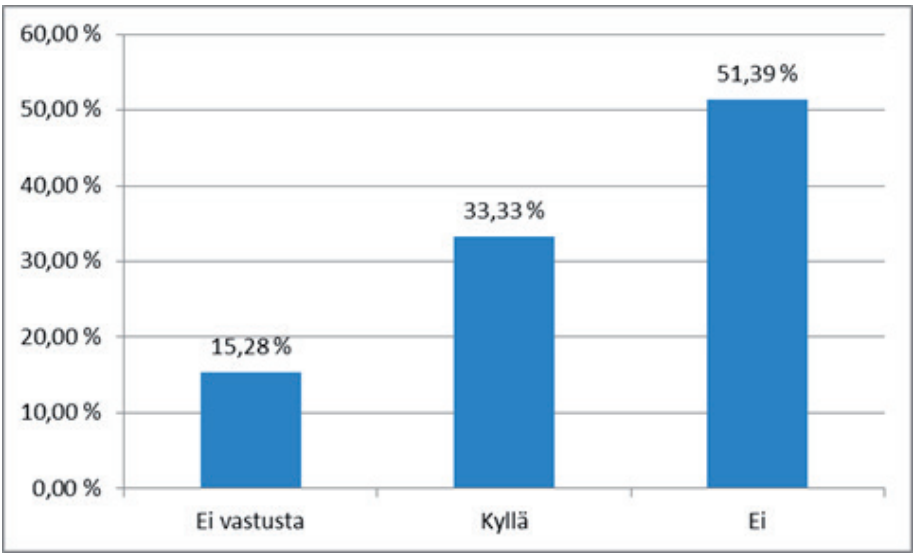
Vastauksista kävi ilmi, että suuri osa asiakkaista tiesi, että hyvä salasan on tarpeeksi pitkä, vähintään kahdeksan merkkiä, ja että se pitää sisällään kirjaimia, numeroita ja mahdollisesti erikoismerkkejä. ArsTechnican artikkelissa Anatomy of a hack: How crackers ransack passwords like “qeadzcwrsfxv1331” (ArsTechnica 2013) todetaan, että nykymenetelmin kahdeksan merkin salasana on jo hyvin haavoittuva. Minimipituudeksi määritettiin 11 merkkiä. Osa vastaajista kertoi hyvän salasanan olevan sellainen, jonka muistaa, esimerkiksi lemmikin tai tutun nimi. Opastusten yhteydessä asiakkaita neuvotaan hyvän salasanan valintaan.

Suomalaisia on opastettu esimerkiksi Yleisradion kotimaan uutisissa siitä, että sama salasana useissa paikoissa vaarantaa tietoturvan (Yle Uutiset 2012). Kansalaisen mikrotuen kyselyyn vastanneista asiakkaista yli puolet, 57 %, ei käytä samaa salasanaa kahdessa tai useammassa palvelussa. Salasanaansa ei vaihda koskaan 24 % vastaajista. Harvoin tai noin maksimissaan kerran vuodessa vaihtavia oli vajaa kolmannes. Osa kertoi vaihtavansa tarvittaessa tai kun on pakko. Syitä siihen, ettei salasanaa vaihdeta, kerrottiin olevan useita: konetta ei käytetä pankkiasioinnissa, salasana on tallennettu pysyvästi koneelle tai vaihdolle ei ole tarvetta. Vastaamatta jätti 26 %. Osa oli laittanut kohtaan kysymysmerkin.



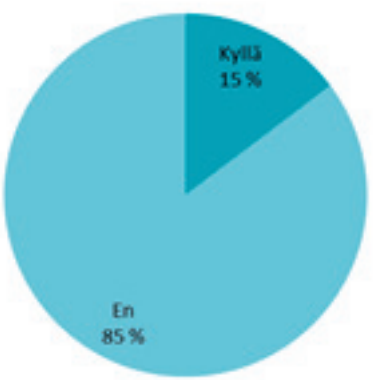
KUVIO 1. *Kuinka usein vaihdat salasanasi?*

Yhtenä teemapäivänä toimipisteessä pidettiin varmuuskopiointipäivä. Päivän aikana käytiin läpi muun muassa se, mitä tarkoitetaan varmuuskopioinnilla, miksi se kannattaa tehdä ja millaisia välineitä siihen on käytettävissä. Päivän aikana koettiin, että asiakkaat kyllä ymmärtävät varmuuskopioinnin tarpeellisuuden, mutta osaamista tai aikaa ei välttämättä ole. Usein myös asia ”unohdetaan” sen hankaluuden takia. Tehdyn kyselyn perusteella asiakkaiden osaaminen tai halu ottaa varmuuskopioita kaipaa vielä tukea. Varmuuskopioita ottaa kolmannes vastaajista, yli puolella ei ole varmuuskopioita, ja vastaajista 15 % jätti vastaamatta tähän kysymykseen.



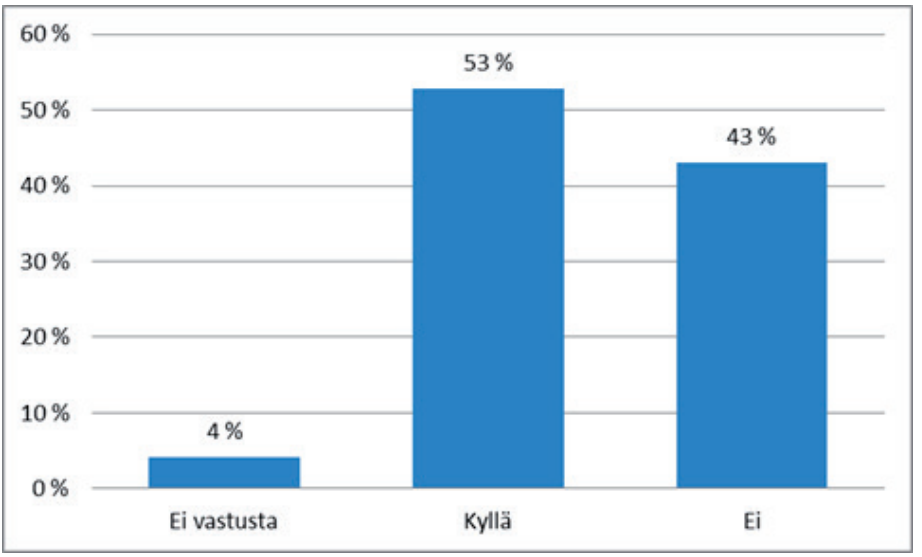
KUVIO 2. *Onko sinulla varmuuskopiot tärkeistä tiedostoistasi?*

Sähköpostien liitetiedostojen avaamisen riskit olivat vastaajilla selvästi tiedossa, sillä 85 % vastaajista ei avaa liitetiedostoa, ellei tiedä, mitä se sisältää.



KUVIO 3. *Avaatko sähköpostien liitetiedostot ilman, että tiedät mitä ne sisältävät?*

Kysymys, joka koski asiakkaan käyttäytymistä virusilmoituksen saatuaan, ei ollut selkeä ja yksiselitteinen. Osa asiakkaista ei selvästikään ymmärtänyt, mitä kysymys tarkoitti. Osa ymmärsi sen tarkoittavan virusta, joka ilmoittelee ja pyytää klikkaamaan ilmoitusta, osa ymmärsi sen tietoturvaohjeistukseksi.



KUVIO 4. *Jos nettisivu ilmoittaa löytäneensä koneeltasi viruksen, seuraatko nettisivulla annettuja toimintaohjeita?*

Selvitettäessä sitä, mistä asiakas on saanut tietoa Kansalaisen mikrotuen toiminnasta, nousi esiin ”viidakkorumpu”. Suurin osa kertoi saaneensa tiedon tuttavalta, naapurilsta, sukulaiselta tai kaverilta. Puskaradio tuntuu toimivan parhaiten tietoisuuden levittämisessä. Muina tiedonlähteinä mainittiin Soneran ja Elisan liikkeet, Auralan kansalaisopisto, Lehmusvalkaman hyvinvointikeskus ja Internet.

TULEVAISUUS

Kansalaisen mikrotuella on saatujen palautteiden perusteella oma roolinsa Turun alueen asukkaiden tietoturvatietoisuuden lisäämisessä. Toimipisteessä pyritään panostamaan markkinointiin, jotta toimintaan liittyvää tietoa saadaan levitettyä vertaistiedon lisäksi muiden kanavien avulla. Henkilökohtaisen opastuksen varaamiseen pyritään kannustamaan vahvemmin. Teemapäiviä järjestetään tukemaan asukkaiden tietoteknistä ja tietoturvaosaamista.

LÄHTEET

ArsTechnica 2013. How-crackers-make-minced-meat-out-of-your-passwords. Viitattu 2.11.2013 http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/.

Berg, Helena 2011. Jopa miljoona digisyrjäytynyttä Suomessa, Tietoasiantuntija 05/2011. Viitattu 26.10.2013 http:/www.tietoasiantuntijat.fi/fi/cfmldocs/index.cfm?ID=1284.

Capgemini 2013. Euroopan komission eGovernment-tutkimus: Lähes puolet suomalaisista ei käytä julkishallinnon sähköisiä palveluita. Viitattu 4.11.2013 http://www.fi.capgemini.com/news/euroopan-komission-egovernment-tutkimus-lahes-puolet-suomalaisista-ei-kayta-julkishallinnon.

Intosalmi, Hennariikka, Nykänen, Jaana ja Stenberg, Lea 2013, Teknologian käyttö ja asenteet 75–89-vuotiailla – Raportti kyselytutkimuksesta. Viitattu 4.11.2013 http://www.ikateknologia.fi/images/stories/Julkaisut/kakate_teknologian_kaytto_asenteet_75_89_netti.pdf.

Kunnat.net 2006. Viitattu 7.11.2013 http://www.kunnat.net/fi/tietopankit/hyvakas/hyvakas-tietopankki/kansalaisen-tietoyhteiskunta/Sivut/default.aspx.

Opetus ja kulttuuriministeriö 2013 Tiedote: Suomalaisten aikuisten perustaidot OECD-maiden parhaimmistoa. Viitattu 7.11.2013 http://www.minedu.fi/OPM/Tiedotteet/2013/10/piaac2013.html.

Tietoyhteiskuntaohjelma 2006. Viitattu 7.11.2013 http://www.tietoyhteiskuntaohjelma.fi/parhaatkaytannot/kansalaisten_valmiudet/fi_FI/1150376237632/index.html.

YLE Uutiset 2012. Sama salasana monessa paikkaa vaarantaa tietoturvasi. Viitattu 7.11.2013 http://yle.fi/uutiset/sama_salasana_monessa_paikassa_vaarantaa_tietoturvasi/5545639.

Zickuhr, Kathryn 2013. Who's Not Online and Why.Viitattu 2.11.2013 http://pewinternet.org/Reports/2013/Non-internet-users.aspx.

LIITE 1: KANSALAISEN MIKROTUKI -KYSELY

Onko tietokoneessasi virustentorjuntaohjelma?

Kyllä:
Ei:
En tiedä:

Käytätkö kahdessa tai useammassa palvelussa samaa salasanaa?

Kyllä:
En:

Kuinka usein vaihdat salasanasi?

Millainen on hyvä salasana? (voit antaa esimerkin)

Jos nettisivu ilmoittaa löytäneensä koneeltasi viruksen, seuraatko nettisivulla annettuja toimintaohjeita?

Kyllä:
En:

Avaatko sähköpostien liitetiedostot ilman, että tiedät mitä ne sisältävät? (esim. mainosviestit)

Kyllä:
En:

Onko sinulla varmuuskopiot tärkeistä tiedostoistasi?

Kyllä:
En:

Mistä kuulit kansalaisen mikrotuesta?

TIETOTURVA KANSALAISEN MIKROTUEN OPPIMISYMPÄRISTÖSSÄ

Tero Mäkelä, Tradenomi
Projektisuunnittelija, tietojenkäsittelyn koulutusohjelma,
Turun ammattikorkeakoulu

Kimmo Virtanen, tietojenkäsittelyn koulutusohjelman opiskelija

Kansalaisen mikrotuki (KMT) on Turun ammattikorkeakoulun oppimis- ja kehittämisympäristö. Sen tarkoituksena on tarjota maksutonta apua, neuvontaa ja koulutusta tietokoneasioissa turkulaisille tietokoneen omistajille. Opastajina toimivat Turun ammattikorkeakoulun opiskelijat. Neuvontaa ongelmatilanteissa saa neuvontapisteestä, puhelimitse ja sähköpostilla. Kansalaisen mikrotuen toiminta keskittyy tietokoneiden laite- ja ohjelmisto-ongelmien ratkaisemiseen. (Kansalaisen mikrotuki 2013.) KMT:n toiminnasta on kerrottu tarkemmin tämän julkaisun artikkelissa *Asiakkaan tietoturvatietoisuuden vahvistaminen – case Kansalaisen mikrotuki*. Tietoturvallisuutta KMT:n toiminnassa on kehitetty vuosien varrella esimerkiksi opinnäytetöiden avulla (Hiltunen & Nummela 2011, Mäkelä 2012).

TIETOTURVATOTEUTUS

Kansalaisen mikrotuen aloituksesta lähtien on kiinnitetty erittäin tarkasti huomiota fyysiseen ja ohjelmistojen tietoturvaan. Kansalaisen mikrotuessa noudatetaan käytäntöjä, joilla varmistetaan asiakkaiden tietoturva. Jokaisen uuden laitteiston ja ohjelmiston asentamisessa on hyödynnetty elinkaarimallia (systems development life cycle - SDLC) ja huomioitu samalla tietoturvanäkökulma kaikissa vaiheissa (Radack 2009, 2–5.).

Asiakkaiden tietokoneet eivät saa jäädä ilman valvontaa. Tällöin tulee keskittyä siihen, miten asiakaskoneita otetaan vastaan ja huolletaan KMT:n vastaanottotiskillä. Työntekijän tulee tehdä päätös, huolletaanko laite heti vai kirjataanko se järjestelmään, jolloin ongelmiin pureudutaan perusteellisemmin.

Palomuuri

Alun perin Kansalaisen mikrotuen käytössä oli vain reititin-tietokone, joka välitti dataliikenteen Kansalaisen mikrotuen verkosta internetiin. Tietoturvasyistä johtuen kyseinen laite korvattiin palomuurilaitteella, jolla pystytään suodattamaan haitallista liikennettä ja jakamaan verkotus järkevästi asiakas- ja henkilökuntaosiin. Palomuurilla on mahdollista suorittaa myös muita toimenpiteitä, kuten tietolikenteen valvontaa ja osoitteenmuunnosta.

Suunnittelussa tavoitteena oli luoda palomuurijärjestelmä, jolla saadaan jaetuksi asiakas- ja työntekijälaitteet omiin verkkoihinsa. Rajatussa asiakasverkossa laitteet voidaan huoltaa turvallisesti vaikuttamatta muiden laitteiden tietoturvallisuuteen haitallisesti (Mäkelä 2012, 2).

Palomuurijärjestelmää asennettaessa tärkeitä toimintoja olivat verkon dataliikenteen lokitus ja lokitiedon riittävän pitkä säilytysaika sekä määriteltyjen yhteyksien sallinta ja esto. Lokitus tarkoittaa järjestelmätiedon keräämistä mahdollisten vikatilanteiden selvittelyä varten. Järjestelmän hallinnan täytyy olla intuitiivista, käyttöliittymän yksinkertainen ja ulkoasultaan selkeä. KMT:n toiminnan luonteesta johtuen järjestelmästä pitää löytyä monipuolisia ominaisuuksia ja sen pitää olla ilmainen käyttää sekä mahdollisimman vakaa. Asiakaslaitteilta estetään kaikki verkkoliikenne internetiin paitsi määriteltyihin sivustoihin ja päivityspalveluihin. Internetiin suuntautuvaa verkkoliikennettä saatiin asennuksen aikana hallittua käyttämällä Squid-ohjelmaa, joka tallentaa verkkosivustoja tai tiedostoja palomuurin välimuistiin. Sieltä ne saadaan nopeasti asiakaskoneiden käyttöön. (Mäkelä 2012, 40–41.)

KMT:n henkilökunnan tietoturvakäytäntöjä

Kansalaisen mikrotuen asiakas- ja huoltotyötietokantaan pääsee käsiksi vain KMT:n henkilökuntaverkosta. Tietokanta itsessään on salasanasuojattu. Fyysisesti tietokanta sijaitsee henkilökunnan tilojen puolella eikä ole helposti nähtävissä. (Hiltunen & Nummela 2011.)

Tiskillä on palvelukello, jolla asiakas ilmoittaa työntekijöille saapumisestaan. Ikkunoissa on verhot, jotka estävät näköyhteyden ulkoa sisälle. Kiinteistö on suojattu asianmukaisilla valvonta- ja hälytinjärjestelmillä. Kaapistoilla ja hyllyillä on saatu laitteet lattialta ja pöydiltä pois, ja samalla on selkeytetty asiakaskoneiden huoltamisjärjestystä. Puhelimessa käytettävä kuulokemikrofoni

ehkäisee asiakkaan mahdollisesti kertomien henkilökohtaisten tietojen kuulumista muille asiakkaille. Monet koneet saattavat vaatia paljon aikaa, kun niitä puhdistetaan esimerkiksi haittaohjelmista. Tavoitteena on kuitenkin välttää tietokoneiden jättämistä päälle yöksi, sillä silloin ne olisivat ilman valvontaa.

KMT:llä tietoturvaohjeita ovat esimerkiksi seuraavat:

- Käsittele vain niitä tiedostoja, jotka ovat työtehtävän kannalta olennaisia
- estä asiakkaita menemästä henkilökunnan työskentelytilaan
- valvo ja ohjaa asiakasta, jos päästät hänet KMT:n asiakaskoneelle
- työtila ei saa jäädä valvomatta työpäivän aikana
- vastuuhenkilön on oltava aina paikalla
- lukitse ovet ja sammuta laitteet tilan jäädessä tyhjäksi
- neuvo asiakasta käyttämään monimutkaisia ja erilaisia salasanoja jokaisessa palvelussa sekä järjestelmässä.

KMT:llä tietoturva-asioista ja säännöistä kerrotaan, kun opiskelija tulee ensimmäisen kerran töihin tai kurssille, minkä jälkeen nämä asiat pitää muistaa. Uutta henkilöstöä tulee kuitenkin usein ja perehdytyksien aikana vanhatkin työntekijät kuulevat asiat uudelleen. KMT:n käytännöt ovat yksinkertaisia ja selkeitä, joten niiden muistaminen ei ole vaikeaa.

Tärkeimmät tietoturva-asiat koskevat asiakkaiden tietokoneita ja niiden sisältämää informaatiota. KMT:llä pystytään pitämään tiedot hyvin salassa. Huollettavien laitteiden vastaanotto ja huoltotila ovat erotettuna toisistaan, joten asiakkaat eivät pääse vastaanottopuolelta työntekijöiden puolelle tai käyttämään valvomatta KMT:n verkkoon kytkettyä konetta. Palvelimen tiedot eivät ole ulkopuolisten tiedossa. (Hiltunen & Nummela 2011.)

KEHITYSSUUNTIA KMT:N TIETOTURVASSA

Jatkuvasta kehityksestä huolimatta KMT:llä jatketaan tietoturvallisuuden parantamista edelleen. Alla on esitelty kohteita, jotka ovat työn alla ja joita käsitellään tarkemmin vuonna 2014 julkaistavassa opinnäytetyössä.

Toimitilaturvallisuus

Kansalaisen mikrotuki sijaitsee vanhassa opetustilassa, mikä tuo toimitilalle paljon etuja. Huoneen verhot ovat pimentävät ja estävät hyvin näköyhteyden ulkoa, mutta keräävät myös paljon pölyä, minkä vuoksi paloturvallisuus tulee ottaa huomioon. Ratkaisu ongelmaan olisi esimerkiksi verhojen vaihto sälekaihtimiin. Koneiden määrän vuoksi myös jatkojohtoja ja verkkokaapeleita on paljon, mutta tämä on marginaalinen ongelma asennetun sähkökourun vuoksi. Siitä löytyy paikat myös verkkokaapeleille.

Nykyinen sisustus estää työntekijöiden näköyhteyden tiskille, jossa saatetaan huoltaa nopeita ja helppoja asiakastapauksia. Työntekijöillä ei ole suoraa näköyhteyttä ovelle, mutta tiskiltä löytyy asiakaspalvelukello, jolla asiakkaat voivat ilmoittaa saapumisensa. Toinen tapa hoitaa näköyhteyden puute olisi määrittää vaihtuva päivystäjä tiskille. Yksi mahdollinen tapa ratkaista ongelma olisi kameravalvonta. Esimerkiksi web-kameran voisi sijoittaa kuvaamaan pääovea, jolloin työntekijät voisivat nähdä näytöltä tiskin koko ajan ja myös potentiaaliset kutsumattomat yövieraat tallentuisivat kameralle.

Tiloissa säilytetään asiakastietolomakkeita, jotka sisältävät tietokantaan laitettavat asiakastiedot. Nämä paperit tulee säilyttää lukitussa kaapissa ja niille tulee määrittää säilytysaika, jonka mentyä umpeen dokumentit hävitetään tietosuojavaatimusten mukaisesti.

Tietoverkkoturvallisuus

Kansalaisen mikrotuen verkko on jaettu eri aliverkkoihin, jolloin asiakaskoneet ja työntekijöiden koneet ovat itsenäisissä verkoissa. Tämä rajoittaa koko verkon saastumisen vaaraa asiakaskoneen vuoksi, koska asiakaskoneet eivät pääse kuin tiettyihin osoitteisiin internetissä. Palomuurissa on asetettuna erilaisia sääntöjä, jotka estävät ja sallivat liikennettä. Kuitenkin ajan kuluessa uudet ohjelmat tulevat tarvitsemaan pääsyn verkkoon, joten KMT:n projektipäällikön tehtäväksi tulee lisätä tarpeen mukaan palomuurin sääntöjä.

Palomuurijärjestelmän vaatimusmäärittelyä tehtäessä todettiin, että asiakaslaitteet olisi saatava eriytettyä toisistaan, jotta mahdolliset haitakkeet eivät leviäisi toisiin asiakaslaitteisiin, henkilökunnan laitteisiin tai ulkoverkkoon. Verkot saatiin eriytettyä liittämällä ne omiin verkkokortteihin ja omiin aliverkkoihin, jolloin asiakasverkon laitteet eivät pääse henkilökuntaverkkoon. (Mäkelä, 2012.)

Ongelmaksi kuitenkin muodostui virtuaalisten verkkojen (VLAN) käyttö, koska Kansalaisen mikrotuen verkon kytkimet eivät tukeneet kyseistä ominaisuutta. Virtuaalisilla verkoilla on mahdollista saada eriytettyä porttikohtaisesti pääsynhallinta eri laitteille. Tästä syystä ei ollut mahdollista estää asiakaslaitteita saastuttamatta toisiaan. Asia ratkaistiin liittämällä vasta esipuhdistetut laitteet verkkoon. (Mäkelä 2012.)

Henkilöstöturvallisuus

Koska kansalaisen mikrotuessa vaihtuvat työntekijät noin puolen vuoden välein, on tärkeää säilyttää ja jatkaa tietotaitoa uusille projektipäälliköille sekä varaprojektipäälliköille. Uuden projektipäällikön perehdytys voi olla hyvin intensiivistä. Tätä varten olisi hyvä olla erityinen ohjenuora projektipäällikölle, joka sisältäisi kaikki pääasiat KMT:n toiminnasta. Ohjenuoraa voisi päivittää projektipäälliköiden toimesta, jos siihen lisättävää asiaa tulisi mieleen esimerkiksi kauden lopussa.

Ohjelmistoturvallisuus ja varmuuskopiointi

Työntekijöiden tietokoneiden viruksentorjuntaohjelmat tulee yhdenmukaistaa, koska epäselvyydet eri ohjelmien lisensoinnista ovat haitanneet toimintaa. Turun ammattikorkeakoululla on lisenssi F-Secure-ohjelmaan. Ohjelmat tarvitsevat hyvin usein päivityksiä, joten sitä varten tulisi valita vastuuhenkilö, joka hoitaa ne päättää kuinka usein päivitykset tarkistetaan.

Asiakaskoneiden selaimiin asennetaan mainossuodatus, koska haitakkeita tulee hyvin usein verkkomainosten välityksellä. Vaikka Java-ohjelmaa käytetään paljon kaikkialla, tietoturvallisuus ei ole aina ajan tasalla ja sitä käytetään yhä vähemmän asiakkaiden käyttötarpeissa. Tällöin kyseinen ohjelma voidaan poistaa ja tarvittaessa asentaa takaisin uudelleen, jos asiakas näin haluaa.

Kansalaisen mikrotuessa on käytössä ulkoisia kiintolevyjä, joihin voi tarvittaessa tallentaa asiakkaiden tärkeitä tiedostoja esimerkiksi tietokoneen vaihdon yhteydessä tai tiedostojen palauttamista varten. Tiedostoja pyritään säilyttämään vain sen ajan kun asiakkaan kone on huollettavana. Kaikki tiedostot hävitetään harjoittelujakson lopussa KMT:n tallenteista.

Asiaskastietokannan tulevaisuuden haasteet

KMT:n järjestelmään on suunniteltu lisättäväksi etäseurantamahdollisuus, jonka avulla asiakkaat pääsisivät katsomaan huollossa olevan koneen tilaa. Tällaista ominaisuutta tarvitaan, sillä asiakkaat tiedustelevat huollossa olevien koneiden tilannetta usein. Olisi toivottavaa, että vaihtoehtoinen tapa selvittää koneen tila pystyttäisiin tarjoamaan. Se vähentäisi soittojen määrää ja antaisi henkilökunnalle mahdollisuuden keskittyä paremmin koneiden huoltamiseen. (Hiltunen & Nummela 2011, 38.)

LÄHTEET

Pakarinen, Hannu 2013. Verkkokauppa opiskelijaprojektina. Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Turku: Turun ammattikorkeakoulu.

Hiltunen, A. & Nummela, T. 2011. Mikrotukipalvelun huoltotietokanta. Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Turku: Turun ammattikorkeakoulu. https://publications.theseus.fi/bitstream/handle/10024/34728/Hiltunen_Atso_Nummela_Toni.pdf

Kansalaisen Mikrotuki 2013. Viitattu 9.10.2013 http://www.kansalaisenmikrotuki.fi/.

Mäkelä, T. 2012. Kansalaisen Mikrotuen palomuurijärjestelmä. Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Turku: Turun ammattikorkeakoulu. https://publications.theseus.fi/bitstream/handle/10024/50500/Makela%20Tero.pdf?sequence=1

Radack, Shirley 2009. The System Development Life Cycle (SDLC). Viitattu 16.10.2013 http://csrc.nist.gov/publications/nistbul/april2009_system-development-life-cycle.pdf.

TIETOTURVAKILPAILU OPPIMISEN VAUHDITTAJANA

Valtteri Holvitie, Ville Mattila ja Rami Sillanpää,
tietojenkäsittelyn opiskelijoita, Turun ammattikorkeakoulu

Jarkko Paavola, TkT
Yliopettaja, tietojenkäsittelyn koulutusohjelma,
Turun ammattikorkeakoulu

Tietoturvakoulutus vaatii laboratoriotyöskentelyä, jotta teoriatunneilla opitut asiat konkretisoituvat. Erityisen tehokkaaksi oppimisen vauhdittajaksi on osoittautunut tietoturvakilpailuun osallistuminen. Kisan luonne ja siihen sisäänrakennettu pelillisyys motivoivat opiskelijoita erityisella tavalla. Kilpailuun kehitetty agenttijuoni ja tilanteen nostattama kilpailuvietti saivat opiskelijat unohtamaan aikaerosta johtuneen myöhäisen kilpailuajankohdan. Tässä artikkelissa tuodaan esiin opiskelijoiden näkökulma niin sanotun Capture the Flag (CTF) -kilpailun tiimoilta, johon Turun ammattikorkeakoulun opiskelijat osallistuivat keväällä 2013.

CAPTURE THE FLAG -KILPAILUN LUONNE

Capture the flag tarkoittaa tietoturvakilpailua, jonka tavoitteena on testata osallistujien tietoturvataitoja, laajentaa kokonaisymmärrystä tietoturvallisuuden alalta, oppia suojautumaan verkkohyökkäyksiltä, oppia tietoturvallisuuden peruskäsitteitä sekä kehittää omia käytännön taitoja eettisestä hakkeroinnista. Kilpailu koostuu erilaisista haasteista eri kategorioissa kaikilla tietoturvan osa-alueilla. CTF -kilpailut on monesti suunniteltu palvelemaan koulutusta, jotta osallistujat saisivat kokemusta muun muassa tietokoneen suojaamisesta sekä johtamisesta ja reagoimisesta niihin hyökkäyksiin, joita reaalimaailmassa tapahtuu. Tapahtuman tarkoituksena on oppia suojautumaan verkkohyökkäyksiltä ja lisätä tietoturvaosaamista.

Tyypillisesti kilpailua varten kerätään ryhmä, jonka päämääränä on yrittää selvittää erilaisia tehtävänannossa määriteltyjä tietoturvatehtäviä eli “lippuja”.

Ryhmät kilpailevat toisiaan vastaan keräämällä lippuja, jotka on pisteytetty vaikeustason mukaan. Ryhmän jäseniltä vaaditaan laajasti erilaisia tietoturvan sekä IT-alan taitoja. Tehtävien jakaminen ryhmän sisällä taitojen mukaan on tärkeää, jotta lippuja löydettäisiin mahdollisimman tehokkaasti. Toisten ryhmien häiritseminen kisan palvelimilla on usein kielletty. Vaikka päämääränä onkin muiden joukkueiden päihittäminen, ei toisten joukkueiden häiritseminen sovi CTF-kilpailun luonteeseen.

HAKKEROINNIN LUOKITTELUA

Hakkerit jaotellaan useaan eri luokkaan hakkeroinnin päämäärän suhteen. Hakkeri-termi esiintyy mediassa usein, ja yleensä sillä viitataan kaikkiin tietoturvamurtoja tekeviin tahoihin. Hakkeri varsinaisesti tarkoittaa kuitenkin innokasta tietokonealan harrastajaa, jollaisiksi luetaan myös eettiset hakkerit. (MOT Kielitoimiston sanakirja 2.0. Kotus) Oikea termi käytettäväksi henkilöistä, jotka tekevät tietomurtoja ilman järjestelmästä vastaavan tahon lupaa, olisi krakkeri tai black hat -hakkeri. (http://www.suomisanakirja.fi/krakkeri)

Yritykset pyrkivät huolehtimaan omasta tietoturvastaan ja suojelemaan liikesalaisuuksiaan. Usein yritykset palkkaavat ulkopuolisen tietoturva-asiantuntijan testaamaan yrityksen verkon turvallisuutta. Tätä kutsutaan eettiseksi hakkeroinniksi ja se tunnetaan myös nimityksellä murtautumistestaus (Certified ethical hacker 2013). Eettisellä hakkeroinnilla pyritään tuottamaan yritykselle tietoa sen verkon haavoittuvuuksista ja parantamaan yrityksen tietoturvaa paikkaamalla löydettyjä haavoittuvuuksia (White hat 2013).

Black hat -hakkerointi eroaa eettisestä hakkeroinnista siten, että krakkeri pyrkii murtamaan yrityksen tietoturvan ja hyötymään hakkeroinnista esimerkiksi myymällä tietoja kilpailijalle tai rikollisjärjestöille, tuhoamalla tiedostoja tai kaappaamalla tietokoneet omaan käyttöönsä (Hacker 2013). Tarkemmin hakkeri-jaottelusta ja murtautumistestauksesta on kerrottu tässä julkaisussa Esko Vainikan artikkelissa *Murtautumistestaus – mitä se tarkoittaa ja miksi sitä tarvitaan*.

Capture the Flag -kisan skenaariossa asetuttiin black hat -hakkerin asemaan. Vastapuolen verkkoon, koneille ja sähköposteihin yritettiin murtautua tar-

koituksena kerätä sieltä mahdollisimman paljon tietoa eli pelin lippuja, joista sai pisteitä. Capture the Flag -kilpailut jaotellaan kahteen pääasialliseen ryhmään: *Jeopardy* sekä *Attack-defence*.

Attack-defence -kilpailussa hyökkäävä joukkue yrittää murtautua verkkoympäristöön tai tietokoneeseen. Puolustava joukkue yrittää estää hyökkäykset. Joukkueita pisteytetään niiden onnistuttua hyökkäämään kohdekoneeseen tai kohdeverkkoon. Vastapuoli saa pisteitä joukkueen onnistuttua puolustautumaan hyökkäyksiä vastaan. Pelkkä tuotannon turvaaminen vaatii tiimiltä hyvää osaamista ja järjestelmien operointia. (CTFtime 2013.)

Hyökkäävä joukkue voi oppia esimerkiksi uusimpia tietoturvatestausmenetelmiä. Tarkoituksena on päästä järjestelmän sisään ja saada laitos haltuun jäämättä kiinni. Puolustavan joukkueen tehtävä on muun muassa havaita hyökkäys, estää vahingot, kerätä riittävästi todisteita hyökkääjän jäljittämiseksi ja tehdä analyysi siitä, mitä puutteita laitoksen tietoturvassa oli ja miten ne voidaan korjata. (Computer security 2013.)

Jeopardy-tyylisessä kisassa osallistujilla on lista suoritettavista tehtävistä erilaisissa kategorioissa, esimerkiksi verkko, salaus tai binääri. Joukkue saa pisteitä jokaisesta suoritetusta tehtävästä. Mitä vaikeampi tehtävä, sitä enemmän pisteitä. Seuraava tehtävä listalta aukeaa suoritettavaksi, kun joku joukkueista on saanut edellisen lipun/tehtävän suoritettua. Kilpailu ratkeaa yhteenlaskettujen pisteiden mukaan (CTFtime 2013.) Kilpailu, johon Turun ammattikorkeakoulu osallistui, oli tätä tyyppiä.

Mixed-tyylinen kilpailu on sekoitus eri CTF-kilpailun lajeja. Jeopardyn sekä Attack-defensen sekoituksessa täytyy hyökätä, puolustaa sekä ratkoa annettuja tehtäviä. Pisteiden jako riippuu kilpailun järjestäjästä. (XLII Security2013.)

TUNNETUIMPIA CTF-TAPAHTUMIA

Useat eri organisaatiot järjestävät vuosittain Capture The Flag -kilpailuja. Summercon on yksi vanhimmista ja pitkäaikaisimmista hakkerointitapahtumista Amerikassa. Tunnetuin ja yksi suurimmista hakkerointitapahtumista on DEF CON (DEF CON 2013), joka pidetään vuosittain Yhdysvalloissa Las Vegasissa. Nykymuodossa ensimmäinen DEF CON pidettiin kesäkuussa 1993. Kolmas tunnettu tapahtuma Yhdysvalloissa on University of Califor-

nia, Santa Barbara Internationalin järjestämä kilpailu UCSB iCTF. Tapahtumaan voivat osallistua vain opiskelijat, jotka opiskelevat yliopistoissa. Aikaisemmin kilpailussa on ollut käytössä vain yksi virallinen verkko. Viime vuosina jokaiselle joukkueelle on tehty erillinen verkko, jossa tarkoituksena on ollut muun muassa hyökätä niin sanottuun "terroristiverkkoon" tavoitteena purkaa pommi. (The UCSB iCTF 2013)

Chaos Communication Congress on Euroopan suurin ja vanhin hakkerikonferenssi, joka sisältää erilaisia luentoja ja työpajoja teknisiä ja poliittisia asioita varten. Tapahtuma on järjestetty vuosittain vuodesta 1984 eteenpäin sekä Hampurissa että Berliinissä. (Chaos Communication Congress 2013.) Toinen Euroopan suurimmista hakkerointitapahtumista on AthCon, joka pidetään vuosittain Ateenassa, Kreikassa. Tapahtumassa on muun muassa istuntoja, jotka sisältävät teknisiä demonstraatioita turvallisuuden uhista sekä hyödyntämisen eri tekniikoista. (AthCon 2013.)

CTF-KILPAILUN TOTEUTUS

Polku, joka vei Turun ammattikorkeakoulun opiskelijat mukaan CTF-kilpailuun, alkoi University of Ontario Institute of Technologyn (UOIT) ja Turun ammattikorkeakoulun yhteisestä tietoturva-aiheisesta Tekes-projektista ReWISE. Lipunryöstössä turkulainen tiimi oli mukana ainoana Kanadan ulkopuolisena joukkueena. Kilpailu järjestettiin 10.2.2013.

Tapahtuma toteutettiin Turun ammattikorkeakoulussa Virtual Private Network -yhteydellä (VPN) Kanadaan, jossa CTF-palvelin oli. Tällä taattiin ohjelmistojen käytön turvallisuus sekä estettiin mahdolliset haittavaikutukset muualle internetiin. Tietoturvatestausohjelmistojen käyttö julkisessa verkossa on lakien mukaan kiellettyä (Finlex 2007).

Lähtökohtaisesti jokaiselle koneelle oli asennettuna Backtrack 5 -Linux, joka on ilmaiseksi kaikkien saatavilla. Backtrack 5:tä käytetään ympäri maailman tietoturvatestaukseen. Nykyisin Backtrack 5:n kehitys on päättynyt ja jakelu kulkee nimellä Kali Linux. Backtrack 5 / Kali Linux sisältää kattavan valikoiman erilaisia ohjelmia, joilla voidaan muun muassa testata tiedostojen kryptausta, tietokoneen haavoittuvuutta sekä salasanojen murtamista.

Kykyjä, joista osallistujille voi olla hyötyä kilpailussa ovat muun muassa reverse-engineering, joka tarkoittaa esimerkiksi ohjelmiston analysointia tutustumalla sen toimintaperiaatteisiin ja binaarikoodiin (Reverse engineering 2013), network sniffing, joka tarkoittaa datapakettien kaappausta verkon yli kulkevasta liikenteestä, protokolla-analysointi (Packet analyzer 2013), järjestelmänhallinta, salausanalysointi ja ohjelmointi (Computer security 2013). Ennen kisaa opiskelijat tutustuivat eettisen hakkeroinnin periaatteisiin. Osallistuvien opiskelijoiden oli tärkeä ymmärtää, milloin ja millä tavalla tietoturvahaavoittuvuuksia saa testata. Pohjatietoina kilpailussa menestyminen edellytti tietoturvatietouden lisäksi osaamista tietoverkoista, tiedostojärjestelmistä ja erityisesti Linux-käyttöjärjestelmästä.

OPPIMISPROSESSI KILPAILUN AIKANA

CTF-kilpailun aikana osallistujat oppivat lähtötasosta riippuen eri asioita, mutta suurimmalla osalla oppimisen pääpaino oli tietoturvatyökalujen tuntemuksen parantamisessa sekä niiden käytäntöön soveltamisen opettelussa. Käytettyjen ohjelmien perusteita on opetettu Turun ammattikorkeakoulussa kaikille osallistuneille, mutta osallistujien ollessa eri vuosikursseilta taitotaso joukkueen sisällä vaihteli huomattavasti.

Ohjelmista joukkue käytti eniten Backtrack 5 -Linuxin työkaluja, ja suurin osa tietoturvatyökaluihin liittyvästä oppimisesta keskittyi kyseisen ohjelmistopaketin eri osiin. Kyseistä ohjelmistopakettia on käytetty myös Turun ammattikorkeakoulussa tietoturva-opetuksessa, joten jokaisella osallistujalla oli valmiina jo vähintään perustiedot ohjelmistopaketin toiminnasta. Ohjelmistopaketin joukkueen eniten käyttämiä ohjelmia kisan aikana olivat *Metasploit, Armitage, Hydra* sekä *Nmap*.

Ohjelmistojen lisäksi kisaan osallistujat oppivat asioita tietotekniikasta ja viestinnästä yleisesti. Kisassa purettiin muun muassa morsetuksesta koostuva viesti sekä korjattiin vääristynyt kuvatiedosto. Yleisesti ajatellen liput osoittivat osallistujille, ettei tietoturva ole aina pelkkää verkon yli tapahtuvaa hyökkäämistä tai suojautumista. Kilpailu herätti ajattelemaan, mitä kaikkea muuta tietoturvaan kuuluu.

Kaikki joukkueen jäsenet oppivat päivän aikana jotain, ja osa osallistujista moninkertaisti tietonsa tietoturvasta kisan aikana. CTF-kisa oppimisympäris-

tönä tarjoaa käytännönläheisyytensä vuoksi huomattavasti enemmän mahdollisuuksia kartoittaa tietoaan kuin pelkkä kurssimuotoinen opiskelu ja opettaa samalla työskentelemään ryhmässä kaikkien osa-alueiden kattamiseksi.

LOPUKSI

Kokonaisuudessaan kilpailuun osallistuminen oli opiskelijaryhmälle positiivinen kokemus. Lippujen löytämiseksi jokaisen täytyi olla hyvin oma-aloitteinen. Oli löydettävä parhaat mahdolliset keinot käyttämällä mahdollisimman vähän resursseja. Erilaisia vaihtoehtoja eri suorituksiin oli useita, joten ryhmän täytyi yhdessä päättää, millä tavalla asiaa kannattaisi lähestyä. Kisassa korostuikin suuresti yhteistyö. Ryhmän sisällä oli osattava jakaa tehtäviä eri kykyjen mukaisesti. Jos itsellä oli vaikeuksia suorittaa jokin tehtävä, joku ryhmän jäsenistä tuli auttamaan ja jopa opettamaan, miten tehtävän voisi mahdollisesti hoitaa. Varsinkin edellisellä mainitulla tavalla tuli opittua paljon uutta.

Opiskelijoilla oli jatkuva yhteys kilpailun ylläpitoon siltä varalta, että eteen tuli esimerkiksi yhteysongelmia tai muita kysymyksiä. Tämän ansiosta pitkäaikaisia keskeytyksiä ei tullut. Organisointi oli kokonaisuudessaan toimiva, ja kommunikaatio toimi koulujen välillä.

Tapahtumaan osallistuneet opiskelijat kokivat kilpailun erittäin motivoivana. Se antoi tietoa omasta osaamisesta sekä myös sen puutteista. Kilpailun jälkeen oli selvää, mitä osaamista tarvitaan lisää. Myös tiimissä toimimisen, osaamisen jakamisen ja yhdistämisen merkitys korostuivat opiskelijoiden keskuudessa. Osa jatkoi heti kilpailun jälkeen tietojen etsimistä kotona. Kilpailu synnytti myös idean oman opiskelijavetoisen tiimin perustamisesta syventämään tunneilla opittuja asioita. Tiimin merkitys korostui kilpailussa, ja kilpailijat kokoivat sen voimavaraksi.

LÄHTEET

The UCSB iCTF 2013. Overview. Viitattu 20.11.2013 http://ictf.cs.ucsb.edu/.

CTFtime 2013. CTF? WTF? Viitattu 20.11.2013 https://ctftime.org/ctf-wtf/.

Computer security 2013. Wikipedia. Viitattu 20.11.2013

http://en.wikipedia.org/wiki/Capture_the_flag#Computer_security.
AthCon 2013. What is AthCon. Viitattu 20.11.2013 http://www.athcon.org/.

Summercon 2013. Wikipedia. Viitattu 20.11.2013 http://en.wikipedia.org/wiki/Summercon.

Chaos Communication Congress 2013. Wikipedia. Viitattu 20.11.2013 http://en.wikipedia.org/wiki/Chaos_Communication_Congress.

Moss, J. 2013. How did DEF CON start?. Viitattu 20.11.2013 http://www.defcon.org/html/links/dc-faq/dc-faq.html.

Moss, J 2013. What is there to do at DEF CON? Viitattu 20.11.2013 http://www.defcon.org/html/links/dc-faq/dc-faq.html.

XLII Security 2013. Capture the Flag in a Nutshell. Viitattu 20.11.2013 http://www.xliisecurity.com/2013/02/what-is-capture-flag.html.

http://www.suomisanakirja.fi/krakkeri. Viitattu 20.11.2013

Packet analyzer 2013. Viitattu 20.11.2013 http://en.wikipedia.org/wiki/Packet_analyzer

Reverse engineering 2013. Viitattu 20.11.2013 http://en.wikipedia.org/wiki/Reverse_engineering

Hacker 2013. Viitattu 20.11.2013 http://en.wikipedia.org/wiki/Hacker_(computer_security)

White hat 2013. Viitattu 20.11.2013 http://en.wikipedia.org/wiki/White_hat_(computer_security)

Certified ethical hacker 2013. Viitattu 20.11.2013 http://en.wikipedia.org/wiki/Certified_Ethical_Hacker

Finlex 2007. Tietoverkkorikosvälineen hallussapito. Viitattu 20.11.2013 http://www.finlex.fi/fi/laki/alkup/2007/20070540#Pid1922055