Ville Kupila

Ohjelmistovuokrauksen tietoturvaongelmat

Tietojärjestelmätieteen
pro gradu –tutkielma
5.10.2010

Jyväskylän yliopisto
Tietojenkäsittelytieteiden laitos
Jyväskylä

TIIVISTELMÄ

Kupila, Ville Eemeli
Ohjelmistovuokrauksen tietoturvaongelmat

Ohjaajat: Eetu Luoma, (Pasi Tyrväinen)
Jyväskylä: Jyväskylän yliopisto, 2010.
105 s.

Ohjelmistojen hankinta ja käyttö on siirtynyt yhä kasvavassa määrin yrityksen omissa tiloissa toimivista asiakaskohtaisista ohjelmistoista kohti verkon yli tapahtuvaan kokonaisvaltaiseen verkkosovelluspalvelujen vuokraamiseen. Tämän rinnalla on noussut huoli tietoturvasta ja yksityisyyden suojasta. Koska dataa varastoidaan ja käsitellään virtuaalisessa ympäristössä oman organisaation ulkopuolella, on tietoturva suunniteltava siten, ettei mikään ulkopuolinen tai sisäinen taho pääse luvatta käsiksi asiakkaiden liiketoimintakriittiseen dataan.

Tämän tutkielman tarkoitus on kirjallisuuteen ja empiiriseen kyselytutkimukseen pohjautuen tunnistaa ohjelmistovuokraukseen liittyviä ongelmakohtia tietoturvan näkökulmasta sekä verrata havaittuja ongelmia ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä. Tutkielman kirjallisuuskatsauksen tuloksena todetaan, että ohjelmistojen ja verkkoselainten, tietoverkon sekä monikäyttäjäarkkitehtuurin tietoturvauhat muodostuvat ohjelmistovuokrauksen keskeisiksi haasteiksi. Kyselytutkimuksesta saatujen vastausten avulla voidaan myös huomata että monikäyttäjäarkkitehtuuriin kohdistuvat tietoturvaongelmat tekevät suurimman eroavaisuuden ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä.

AVAINSANAT: ohjelmistovuokraus, monikäyttäjäarkkitehtuuri, asiakaskohtainen ohjelmisto, tietoturva, yksityisyyden suoja, ohjelmistohankinta.

ABSTRACT

Kupila, Ville Eemeli

Security Issues at Software as a Service

Jyväskylä: University of Jyväskylä, 2010.
103 pages
Master's Thesis

The acquisition and the use of software from the company's own premises towards taking place over the network as a comprehensive web application services is increasingly getting active. Alongside this change rises concern for information security and privacy. Since the data is stored and processed in a virtual environment outside of your organization, information security should be designed so that no external or internal party can have unauthorized access to customers' business critical data.

Based on the literature and survey the purpose of this thesis is to identify software as a service -related problems areas in security point of view. The literature review concludes that software and web browsers, computer network and multi-tenant architecture are the key challenges of software as a service. The survey also shows that the multi-tenant architecture makes the largest difference between software as a service and bespoke software in information security point of view.

Despite the fact that software as a service is not fully ready phenomenon and all the security issues, software as a service is becoming one of the major software development milestones. It seems that in the future, however, companies have a better opportunity to manage their own data, and control software leasing risks.

KEYWORDS: software as a service, multi-tenant architecture, bespoke software, information security, right to privacy, software purchase.

KIITOKSET

Kiitokset ohjaajalleni Eetu Luomalle opastuksesta ja neuvoista.

Lisäksi haluaisin kiittää Nooraa kaikesta.

Just when I thought I was out... they pull me back in.

(Michael Corleone– *The Godfather - Part III)*

SISÄLTÖ

1 JOHDANTO 7
1.1 Tutkimuksen tausta 7
1.2 Tutkimusongelma ja rajaukset 8
1.3 Tutkielman rakenne 9
1.4 Peruskäsitteet 10

2 OHJELMISTOVUOKRAUS 13
2.1 Ohjelmistovuokraus ilmiönä 13
2.2 Ohjelmistovuokrauksen monikäyttäjäarkkitehtuuri 16
2.2.1 Erillinen tietokanta 16
2.2.2 Erillinen kenttä 17
2.2.3 Jaettu kenttä 17
2.3 Ohjelmistovuokrauksen hyödyt ja haitat 19

3 OHJELMISTOVUOKRAUS JA TIETOTURVA 22
3.1 Tietoturvan osa-alueet 22
3.2 Tietoturva verkkoympäristössä ja sen riskit 25
3.3 Ohjelmistovuokraus ja tietoturva 28
3.4 Ohjelmistovuokraus vs. asiakaskohtaiset ohjelmistot 31

4 VIITEKEHYS OHJELMISTOVUOKRAUKSEN TIEOTURVAONGELMIEN TARKASTELUUN 33
4.1 Viitekehyksen muodostaminen ja taustaolettamukset 34
4.1.1 Fyysiset tietoturvauhat 36
4.1.2 Ohjelmistojen tietoturvauhat 37
4.1.3 Verkkoympäristön tietoturvauhat 42
4.1.4 Muut ohjelmistovuokrauksen tietoturvauhat 53
4.2 Viitekehys ohjelmistovuokrauksen tietoturvaongelmista 59

5 KYSELYTUTKIMUS OHJELMISTOVUOKRAUKSEN TIETOTURVAONGELMISTA 65
5.1 Tutkimuksen kulku ja lähtökohdat 65
5.2 Tutkimuksen tulokset 68
5.2.1 Selainten ja ohjelmistojen tietoturva-aukot 69
5.2.2 Selainten ja ohjelmistojen virhetilanteissa vuotavat tiedot 70
5.2.3 Tietoliikenteen paljastuminen epäsuotuisille tahoille 71
5.2.4 Palvelunestohyökkäykset 72
5.2.5 Troijalaiset, virukset ja madot 73
5.2.6 Data käsitellään ja varastoidaan oman organisaation ulkopuolella 74
5.2.7 Dataa ei eristetä riittävän tehokkaasti muiden asiakkaiden datasta 75

5.2.8 Data ei pysy saatavilla virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa 76

6 POHDINTA 80
6.1 Tutkimuksen rajaaminen 80
6.2 Tutkimuksen luotettavuus ja yleistettävyys 81
6.3 Tutkimuksen validiteetti ja reliabiliteetti 82
6.4 Päätelmät 84

7 YHTEENVETO JA JATKOTUTKIMUSKOHTEET 88

LÄHDELUETTELO 91

1 JOHDANTO

1.1 Tutkimuksen tausta

Viimeisten kolmen vuosikymmenen aikana tietojenkäsittely on muuttunut keskitetyistä asiakaspalvelimista kohti hajautettuja järjestelmiä. Tämän muutoksen uutena suuntauksena on muodostunut ohjelmistovuokrauksen ilmiö, jossa tietotekniikkapalveluita ja ohjelmistoja käytetään yhä enenevämmässä määrin verkon yli. (Balachandra, Ramakrishna & Atanu, 2009). Datan varastoinnin ja käsittelyn siirtyessä verkkoon, herää kuitenkin kysymyksiä, jotka tulisi ratkaista. Näistä tietoturva ja yhtiön tietojen vuotamisen riski nousevat yhdeksi keskeisimmiksi ongelmakohdista. (Greschler & Mangan, 2002)

Ohjelmistovuokrausta on sen nuoresta iästä huolimatta käsitelty kirjallisuudessa melko paljon. Esimerkiksi Gold, Mohan, Knight ja Munro (2004) ovat kirjoittaneet palvelukeskeisistä ohjelmistoista. Myös Jacobs (2005) tarkastelee ohjelmistojen toimituksen muuttumista enemmän palvelukeskeisempään suuntaan. Greschler ja Mangan (2002) puolestaan kuvaavat kaksiosaisessa artikkelissa ohjelmistovuokrauksen alkuperää, rakentamista ja käyttöä. Kirjallisuutta läpikäymällä voidaan kuitenkin huomata, kuinka kaupallista ohjelmistovuokrauksen tutkimus ja käyttö tällä hetkellä on. Alan edelläkävijöinä voidaan pitää suurimpia yrityksiä, kuten Microsoftia ja Googlea. Huomattavaa on myös se, että vaikka tietoturva mainitaan monesti suurimmaksi ohjelmistovuokrauksen huolenaiheeksi, on siihen liittyvä tutkimus jäänyt kuitenkin hyvin vähäiseksi (Rittinghouse, 2009, 154). Alan kirjallisuuteen nojautuen voidaankin todeta, kuinka suuri rooli verkkoympäristön turvallisuudella on ohjelmistovuokrauksessa. Ilman toimivia ja turvallisia tietoliikenneyhteyksiä sekä verkkopalveluja ei ohjelmistovuokraus voisi koskaan toimia.

Huolimatta ohjelmistovuokraukseen kohdistuvista ongelmakohdista, tarjoaa ohjelmistovuokraus uusia mahdollisuuksia varsinkin pienille ja keskisuurille yrityksille. Ohjelmistovuokrauksen käyttöönotto onkin viimeisten kolmen vuoden aikana noussut jyrkästi. Ne pienet ja keskisuuret yritykset, jotka olivat aikaisemmin epävarmoja ohjelmistovuokrauksen suhteen, eivät voi enää sivuuttaa sen kykyä luoda yritykselle uusia liiketoimintaa helpottavia työkaluja. Ohjelmistovuokraus luo yrityksille ja organisaatioille mahdollisuuden tiimien, yhteistyökumppanien ja asiakkaiden väliseen yhteistyöhön, mahdollistaen keskittymisen tietojenkäsittelyn sijaan varsinaiseen liiketoiminnan kehittämiseen. (Gold & Mohan & Knight & Munro, 2004)

1.2 Tutkimusongelma ja rajaukset

Tarve aihealueen tutkimiselle heräsi ohjelmistovuokrauksen tietoturva-ongelmien tutkimuksen vähäisyydestä. Vaikka tietoturva mainitaan kirjallisuudessa monesti suurimmaksi ohjelmistovuokrauksen huolenaiheeksi, vain harvassa tapauksessa aihetta käsitellään sen syvällisemmin (Rittinghouse, 2009, 154).

Tämän tutkielman keskeisimpänä tarkoituksena on löytää ne tietoturvaongelmat, jotka ovat oletettavasti suurempia ohjelmisto-vuokrauksessa kuin yrityksen omissa tiloissa toimivissa asiakaskohtaisissa ohjelmistoissa. Lisäksi tutkimuksessa on tarkoitus vertailla havaittuja tietoturvaongelmia näiden kahden mallien välillä sekä selvittää ovatko havaitut tietoturvaongelmat merkittäviä ja todellisuudessa suurempia ohjelmistovuokrauksessa. Edellä mainittujen ohjelmistojen toimituksen ja käytön mallien vertailusta rajataan kuitenkin pakettiohjelmistot ja sovelluspalveluiden tarjoaminen kokonaan pois.

Tämä pro gradu -tutkielma toteutetaan kvalitatiivisin menetelmin, laajana kirjallisuuskatsauksena. Kirjallisuuskatsauksen tuloksena syntynyttä viitekehystä testataan kyselytutkimuksen avulla alan asiantuntijoilla.

Tutkielman luettuaan lukija ymmärtää ohjelmistovuokrauksen roolin tämän päivän tietojenkäsittelyssä sekä on tietoinen sen tyypillisimmistä ongelmakohdista tietoturvan näkökulmasta.

1.3 Tutkielman rakenne

Tutkielma on rakennettu käsittelemään ensin yleisesti ohjelmistovuokrausta ilmiönä sen hyötyjen ja haittojen näkökulmasta, minkä jälkeen esitellään tietoturvan osa-alueita niiden periaatteiden avulla. Tämän jälkeen syvennytään tarkemmin ohjelmistovuokrauksen tietoturvaongelmiin. Ensimmäisessä määritellään tutkielman kannalta keskeinen terminologia ohjelmisto-vuokrauksen, tietoturvan, asiakaskohtaisen ohjelmiston, pakettiohjelmiston ja sovelluspalveluiden tarjoamisen osalta. Luvussa kaksi tutustutaan ohjelmistovuokraukseen ilmiönä ja luodaan katsaus sen monikäyttäjä-arkkitehtuuriin. Monikäyttäjäarkkitehtuurin jälkeen esitellään ohjelmisto-vuokrauksen hyötyjä ja haittoja. Kolmannessa luvussa esitellään tietoturvan ymmärtämisen kannalta sen periaatteita, tutustutaan verkkoympäristön tietoturvaongelmiin, esitellään ohjelmistovuokrauksen tietoturvaongelmat sekä verrataan niitä asiakaskohtaisiin ohjelmistoihin. Luvussa neljä esitellään kirjallisuuden pohjalta muodostettua viitekehystä ohjelmistovuokrauksen tietoturvaongelmista sekä viitekehykseen vaikuttaneita taustaolettamuksia. Luvussa viisi esitellään viitekehyksen pohjalta muostettua haastattelu-tutkimusta. Keskeisiä asiakokonaisuuksia tässä luvussa ovat tutkimuksen kulku ja lähtökohdat, tutkimuksen suunnittelu ja tutkimusaineiston keruu, tutkimuksen kohdejoukko sekä tutkimuksen tulokset. Luvussa kuusi pohditaan tutkimuksen rajaamista, luotettavuutta ja yleistettävyyttä, tarkastellaan tuloksia sekä esitetään päätelmät. Luku seitsemän kokoaa tutkielman yhteen ja esittää jatkotutkimuskohteet.

1.4 Peruskäsitteet

Ohjelmistovuokraus (Software as a Service, SaaS) on käsitteenä avoin erilaisille tulkinnoille. Greschlerin ja Manganin (2002) mukaan ohjelmistovuokrauksella tarkoitetaan ohjelmistojen hankinnan mallia, jossa sovellukset toimitetaan asiakkaille verkon yli palveluna. Jacobsin (2005) mukaan ohjelmisto-vuokrauksella tarkoitetaan puolestaan ohjelmistotoimittajan luomaa sovellusta, jota operoidaan toimittajan palvelimilla ja johon asiakkaat ovat yhteydessä verkon yli standardoiduilla selaimilla ja verkko-ohjelmistoilla. Yleisesti ohjelmistovuokrausta voidaan luonnehtia ohjelmiston toimituksen malliksi, jossa ohjelmiston omistaja toimittaa ja hallinnoi asiakkaan hankkimaa sovellusta (Rovio 2008). Tässä tutkielmassa ohjelmistovuokrauksella tarkoitetaan ainoastaan verkon yli tapahtuvaa ohjelmiston vuokrausta, jossa kahtena pääosapuolena ovat palvelun tarjoaja ja palvelun tilaaja.

Edellä mainitut määritelmät ovat melko pelkistettyjä, eivätkä ne ota kantaa esimerkiksi taustalla oleviin teknologioihin tai protokolliin. Määritelmät eivät myöskään tee eroa kuluttajakeskeisen palvelun ja liiketoimintakeskeisen palvelun välille. Carraron ja Chongin (2006) mukaan ohjelmistovuokraus voidaan jakaa yrityspalveluihin ja kuluttajapalveluihin. Yrityspalvelut ovat usein suuria ja muokattavia liiketoimintaratkaisuja, joiden tarkoituksena on tukea liiketoimintaprosesseja. Näitä ovat esimerkiksi rahoitus sekä toimitusketjun- ja asiakkuudenhallinta. Kuluttajapalvelut ovat puolestaan tarkoitettu tavallisille kuluttajille, joista hyvänä esimerkkinä toimii Googlen maksuton verkkopohjainen sähköpostipalvelu Gmail. Kuluttajapalveluja tuetaan monesti mainonnan avulla ja tarjotaan kuluttajille ilmaiseksi tai hyvin pienillä kustannuksilla.

Monikäyttäjäarkkitehtuurilla (multi-tenant architecture) tarkoitetaan ohjelmistoarkkitehtuuria, jossa yksittäinen palvelimella toimiva ohjelmisto palvelee useita käyttäjiä yhtäaikaisesti. Monikäyttäjäarkkitehtuurimallissa

ohjelmisto ja sen tiedot on suunniteltu siten, että jokainen asiakas pystyy käyttämään niitä mukautetusti verkon yli. (Chong & Carraro & Wolter, 2006)

ISO/EC 17799 (2000) standardin mukaan *tietoturvalla (information security)* tarkoitetaan organisaatioiden informaation suojaamista erilaisilta uhkatekijöiltä, minimoiden organisaatioon kohdistuvia riskejä ja parantaen liiketoiminnan jatkuvuutta. Laajasti ymmärrettynä tietoturvalla tarkoitetaan tiedon ja tietojärjestelmien suojaamista luvattomalta pääsyltä, käytöltä, muokkaukselta ja hävittämiseltä. Dhillonin ja Blackhousen (2001) mukaan tietoturvan rooli onkin muodostunut yhdeksi tärkeimmäksi osatekijäksi ihmisten ja yritysten varastoidessa dataa digitaalissa formaatissa sekä jakaessaan sitä erilaisilla teknologioilla.

Whitmanin ja Mattordin (2009) mukaan tietoturva koostuu neljästä osa-alueesta: tietoturvan johtamisesta, fyysisten laitteiden ja datan turvallisuudesta, verkon turvallisuudesta sekä tietoturvapolitiikasta. Tämän tutkielman painopisteenä on tarkastella ohjelmistovuokrausta verkkoympäristön turvallisuuden näkökulmasta, koska verkkoympäristön toiminnallisuus liittyy keskeisesti ohjelmistovuokraukseen. Verkkoympäristöllä tarkoitetaan tässä tutkielmassa verkkoprotokollien, laitteiden, ohjelmistojen ja verkon käyttäjien kokonaisuutta.

Asiakaskohtaisella ohjelmistolla (bespoke software) tarkoitetaan yrityksen omistamaa ja sen omissa tiloissa toimivaa ohjelmistoa, jonka asentamisesta, päivityksistä ja ylläpidosta yritys huolehtii pääsääntöisesti itse. Asiakaskohtaisia ohjelmistoja ei usein kohdisteta massamarkkinointiin, vaan ne suunnitellaan usein johonkin tiettyyn yrityksen toimintoon tilaajaorganisaation vaatimusten mukaisesti. (Jacobs, 2005)

Pakettiohjelmistot (Commercial off-the-shelf, COTS) ovat usein tavallisille kuluttajille suunnattuja kaupallisia valmisohjelmistoja, joiden hinnoittelu perustuu monesti lisenssiin. Tällaisia ”kaupan hyllyltä” ostettavia

pakettiohjelmistoja ovat esimerkiksi Windows, Photoshop, ja Pinnacle Studio. Myös pakettiohjelmistoja voidaan tarjota ohjelmistovuokrauksen mallia käyttäen. (Mohamed & Ruhe & Eberlein, 2007)

Sovelluspalveluiden tarjoamisella (Application Service Providers, ASP) tarkoitetaan 90-luvulla syntynyttä ilmiötä, jossa yrityksille tarjottiin muutamia liiketoimintaa tukevia sovelluksia verkon yli. Sovelluspalveluohjelmistot olivat rakennettu vain yhdelle vuokraajalle kerrallaan, kun taas ohjelmistovuokrauksessa käyttäjiä voi olla useita. Sovelluspalvelujen tarjoamista pidetään usein ohjelmistovuokrauksen evoluution ensiaskeleena. (Desai & Currie, 2003). Luvussa kaksi esitellään tarkemmin sovelluspalveluiden tarjoamisen ja ohjelmistovuokrauksen yhteneväisyyksiä ja eroavaisuuksia.

2 OHJELMISTOVUOKRAUS

2.1 Ohjelmistovuokraus ilmiönä

Weston ja Kavian (2009) arvioivat, että ohjelmistovuokraus on tulossa enenevässä määrin osaksi nykypäivän ohjelmistokehitystä ja liiketoimintaa. Goldin, Mohanin, Knightin ja Munron (2004) mukaan ohjelmistovuokraus nähdäänkin olevan ohjelmistokehityksen seuraava vallankumous, jossa verkkopalvelujen mahdollisuudet laajenevat yksinkertaisista sovelluksista kohti kokonaisvaltaisia ohjelmistopalveluja.

Ohjelmistovuokraus ei ole kuitenkaan täysin uusi ilmiö. Sen juuret voidaan löytää ajalta, jolloin tietojenkäsittely perustui keskuskoneen *(mainframe computing)* käyttöön. Tälle aikakaudelle oli tyypillistä, että käyttäjät olivat yhteydessä tähän keskuskoneeseen erilaisten ohjelmistojen avulla, jossa kaikki toiminnot suoritettiin keskitetysti. Keskuskoneen ylläpitäjät pystyivät käyttämään näitä ohjelmistoja ja kontrolloimaan eri käyttäjien pääsyä dataan. Keskuskoneitten aikakaudella data oli aina oikeassa paikassa ja mikäli käyttäjillä tuli ongelmia, pystyivät he ottamaan yhteyttä keskuskoneen ylläpitäjiin. Tämän aikakauden suurin ongelma oli kuitenkin siinä, että mikäli useampi käyttäjä oli yhteydessä keskuskoneeseen samanaikaisesti, saattoi se aiheuttaa viiveitä vastauksissa. (Greschler & Mangan, 2002). Vaikka teknologia on kehittynyt tuolta ajalta huomattavasti, ei ongelmaa ole vielä tänäkään päivänä täysin pystytty poistamaan. Tämä aiheuttaa nykyisille palveluntarjoajille haasteita varsinkin tiedon saatavuuden näkökulmasta.

Ohjelmistovuokrausta verrataan monesti jo 1990-luvulla esiin tulleeseen sovelluspalveluiden tarjoamiseen (ASP-malli). Tänäkin päivänä näillä kahdella on monia yhteneviä piirteitä, kuten lisensointiin perustuva käyttö ja taustalla vallitseva, yhtenäisiä piirteitä omaava arkkitehtuuri. (Carraro & Chong, 2006).

ASP-mallia ei alun perin suunniteltu kuitenkaan useamman organisaation käytettäväksi. Yhtenä tämän mallin ongelmana verrattuna ohjelmisto-vuokraukseen onkin siinä, että sovellusta on asiakasyritysten toisistaan erottamiseksi ajettava erillisinä tapahtumina. Vaikka virtuaalisointitekniikalla saavutetaan jonkin verran kustannussäästöjä palvelinympäristön jakamisesta useamman asiakkaan kesken, on palveluntoimittajalla kuitenkin asiakasmäärää vastaava määrä virtuaalisia palvelimia hallittavanaan. Toinen ongelma ilmenee sovelluksen tietosisällön, toiminnallisuuden ja ulkoasun sovittamisessa asiakkaan tarpeiden mukaiseksi. Jos sovittaminen perustuu esimerkiksi ohjelmistotoimittajan palveluna tekemään räätälöintiin tai konfigurointiin, nousevat myös palvelun kustannukset. Korkea hinta saattaa tällöin sulkea monet PK-yritykset palvelun piiristä pois. (Mäkinen, 2006)

Tänä päivänä ohjelmistovuokraus perustuu ASP-mallin tavoin monikäyttäjäarkkitehtuurimalliin, antaen palveluntarjoajille mahdollisuuden keskittää yhden ohjelmistoversion käyttö paremmin useiden asiakkaiden tarpeisiin. Tyypillisesti ohjelmistot vuokrataan suoraan ohjelmiston toimittajalta, mutta on myös tapauksia, joissa käytetään eräänlaisia välikäsiä. Välikäsi kokoaa eri toimittajien ohjelmistopalvelut yhteen ja tarjoaa niitä osana yhtenäistä ohjelmistoalustaa. Puhtaimmillaan ohjelmistovuokraus toteutuu silloin kun palvelun tarjoaja isännöi samaa ohjelmiston versiota keskitetysti, tarjoten eri käyttäjille mahdollisuuden käyttää tätä ohjelmistoa maksua vastaan Internetin yli. (Carraro & Chong, 2006)

Carraron ja Chongin (2006) mukaan ohjelmistovuokrauksesta on kolme näkökulmaa joiden avulla voidaan tehdä ero asiakaskohtaisten ohjelmistojen ja ohjelmistovuokrauksen välille. Näitä ovat lisensiointi, sijainti ja hallinnointi. Nämä kolme tekijää voidaan nähdä eräänlaisena jatkumona, jonka toisessa päässä on asiakaskohtaiset ohjelmistot ja toisessa ohjelmistovuokraus. Asiakaskohtaisten ohjelmistojen ja ohjelmistovuokrauksen eroavaisuutta verrataan Kuviossa 1.

KUVIO 1 Ohjelmistovuokraus vs. pakettiohjelmisto (Carraro & Chong, 2006)

Lisensiointi: Asiakaskohtaisia ohjelmistoja ja pakettiohjelmistoja valmistetaan monesti jokaiselle käyttäjille erikseen kertamaksuun perustuvalla jatkuvalla lisenssillä. Ohjelmistovuokraus eroaa tästä siten, että siinä ohjelmistot on lisensoitu käyttömäärän mukaan. Jokaista asiakasta laskutetaan ainoastaan palvelujen käyttömäärän mukaan. (Carraro & Chong, 2006)

Sijainti: Asiakaskohtaiset ohjelmistot ovat pääsääntöisesti asennettuina tilaajan omaan ympäristöön, kun taas ohjelmistovuokrauksen ollessa kyseessä, ovat ohjelmistot asennettuna palveluntarjoajan palvelimille. (Carraro & Chong, 2006)

Hallinnointi: Perinteisesti IT- osastot ovat vastuussa yrityksen tietojenkäsittelyyn liittyvistä palveluista, kuten asiakaskohtaisten ohjelmistojen hallinnoimisesta. Tämä tarkoittaa monesti runsasta tietämystä verkosta, palvelimista ja ohjelmistoalustoista. Joillekin yrityksille se voi olla kuitenkin liian suuri tehtävä. Ohjelmistovuokrauksessa tämä vastuu on palvelun tarjoajalla. (Carraro & Chong, 2006) Tämän vuoksi asiakkaan tulee pystyä luottamaan palveluntarjoajaan niin tietojen saatavuudessa, kuin turvallisuudessakin. Palveluntasosopimuksella *(Service Level Agreement, SLA)* tarkoitetaan asiakkaan ja palveluntarjoajan välistä laillista sopimusta, jolla varmistetaan, että palvelun laatu, saatavuus ja tuki toteutuu niin kuin on sovittu. Palvelutasosopimus on ainoa laillinen dokumentti, joka määrittelee kahden osapuolen, asiakkaan ja palveluntarjoajan välisen suhteen. (Balachandra ym. 2009)

2.2 Ohjelmistovuokrauksen monikäyttäjäarkkitehtuuri

Luottamus palveluntarjoajaan on ohjelmistovuokrauksen toimivuuden perusedellytys. Jotta luottamus voisi syntyä, on ohjelmistovuokrauksen monikäyttäjäarkkitehtuuri rakennettava niin vahvaksi ja turvalliseksi, että käyttäjät ja asiakkaat voivat rauhassa luottaa tietonsa palveluntarjoajan haltuun. Tähän ajatukseen perustuen Chong & Carraro & Wolter (2006) kuvaavat ohjelmistovuokrauksen monikäyttäjäarkkitehtuuria datan varastoinnin jatkumona, jossa toisena ääripäänä on jaettu data ja toisena on eristetty data. Ohjelmistovuokrauksessa jaetun ja eristetyn datan ero ei ole kuitenkaan kaksijakoinen, vaan eri variaatiot ovat myös mahdollisia. Kuvio 2 esittää eristetyn ja jaetun datan jatkumoa. Seuraavaksi tarkastellaan tätä jatkumoa tarkemmin ja tunnistetaan sen kolme eri vaihetta.

KUVIO 2 Monikäyttäjäarkkitehtuurin eristetyn ja jaetun datan jatkumo

2.2.1 Erillinen tietokanta

Chongin ym. (2006) jatkumon toisena ääripäänä on tilanne, jossa kullakin asiakkaalla on oma tietokanta käytettävänään ja kunkin asiakkaan data on erillään muiden asiakkaiden datasta. Tarjoamalla jokaiselle asiakkaalle oma tietokanta, voidaan sitä helposti laajentaa vastaamaan myös asiakkaiden yksilöllisiä tarpeita. Erillisen tietokannan huonona puolena ovat kuitenkin sen korkeat kunnossapidon ja varmuuskopioinnin kustannukset. Usein tämä malli sopiikin sellaisille asiakkaille, jotka ovat halukkaita maksamaan ylimääräistä tietokannan suojauksesta ja muokattavuudesta. Esimerkiksi pankkitoiminnan ja terveydenhuollon aloilla saattaa olla usein suuriakin vaatimuksia tietojen ja datan eristämiseen. Tämän vuoksi näillä aloilla ei myöskään usein edes harkita

tilannetta, jossa tietokanta jaettaisiin useamman asiakkaan kesken. (Chong & Carraro & Wolter, 2006)

2.2.2 Erillinen kenttä

Toinen lähestymistapa hallita asiakkaiden tietoja, on tarjota asiakkaille yhteinen tietokanta, johon kullekin asiakkaalle on luotu oma tietokenttänsä. Kuten aikaisemmassakin lähestymistavassa, on erillisen kentän malli suhteellisen helppo toteuttaa ja asiakkaat voivat laajentaa tietomalliansa yhtä helposti, kuin erillisen tietokannan tapauksessa. Erillisen kentän hyvänä puolena on sen kyky hallita useita asiakkaita samalla palvelimella. Erillinen kenttä tarjoaa myös tietoturvatietoisille asiakkaille kohtuullisen datan eristämisen tason, mutta ei niin hyvää, kuin erillisen tietokannan mallissa. (Chong & Carraro & Wolter, 2006)

Merkittävä haittapuoli erillisen kentän lähestymistavassa on siinä, että asiakkaan tietoja on vaikeampi palauttaa virhetilanteen sattuessa. Jos jokaisella asiakkaalla on oma tietokanta käytettävänään, voidaan tiedot palauttaa yksinkertaisesti palauttamalla tietokannan viimeisimmän varmuuskopio. Erillisen kentän tapauksessa tietokannan palauttaminen merkitsisi myös muiden asiakkaiden tietojen palauttamista, riippumatta siitä ovatko nämä asiakkaat kokeneet tietojen menetyksiä tai ei. (Chong & Carraro & Wolter, 2006)

2.2.3 Jaettu kenttä

Kolmas tapa hallita useita asiakkaita on käyttää yhteistä tietokantaa ja yhteisiä tietokannan taulukoita. Tässä ns. jaetun kentän mallissa asiakkaat erotetaan toisistaan ainoastaan ID- sarakkeessa olevan tunnistenumeron avulla. Jaetun kentän mallissa on pienimmät laitteisto- ja varmuuskopiokustannukset, koska mallissa pystytään palvelemaan suurinta asiakasjoukkoa kerralla. Koska useat asiakkaat jakavat saman tietokannan taulukon, saattaa tämä lähestymistapa

aiheuttaa lisäkustannuksia varsinkin tietoturvan näkökulmasta. Edes virhetilanteiden sattuessa ei asiakas saa koskaan päästä muiden asiakkaiden tietoihin käsiksi. (Chong & Carraro & Wolter, 2006)

Jaetun kentän malli sopii hyvin sellaisille sovelluksille, jotka pystyvät palvelemaan useita käyttäjiä samanaikaisesti pienellä määrällä palvelimia. Lisäksi tämä lähestymistapa sopii myös sellaisille asiakkaille, jotka ovat valmiita tinkimään datansa eristämisestä vastineeksi pienemmistä kustannuksista. (Chong & Carraro & Wolter, 2006)

Mikä näistä kolmesta edellä mainituista lähestymistavoista on sitten asiakkaan ja varsinkin tietoturvan kannalta paras ratkaisu? Yhteenvetona voisi sanoa, että vastaus kysymykseen on tilannekohtainen, sillä tilanteeseen vaikuttaa aina monta eri muuttujaa. Esimerkkinä ovat asiakkaan likviditeetti, asiakaskohtaiset vaatimukset tietoturvalle sekä luottamus palveluntarjoajaan.

Koska ohjelmistovuokrauksessa asiakkaiden käyttämä ohjelmisto tallentaa palvelimille arkaluontoistakin dataa, ovat asiakkaiden odotukset tietoturvan näkökulmasta monesti kuitenkin korkealla. Palveluntarjoajan ja asiakkaan välisellä palvelutasosopimuksella *(A Service Level Agreement, SLA,)* voidaan ainakin pääpiirteittäin taata tietoturvan taso, käytettiin edellä mainituista malleista mitä tahansa.

Ohjelmistovuokraukseen liittyy myös yleinen harhaluulo, että ainoastaan datan fyysinen eristäminen voi taata sopivan tietoturvan tason. Todellisuudessa myös kaksi jälkimmäistä lähestymistapaa voivat tarjota vahvan turvallisuuden. Usein nämä lähestymistavat tarvitsevat kuitenkin monimutkaisempia salaus-menetelmiä ja suunnittelumalleja. (Chong & Carraro & Wolter, 2006)

2.3 Ohjelmistovuokrauksen hyödyt ja haitat

Vaikka ohjelmistovuokraus on varsin nuori ilmiö, on sen käyttöönotto levinnyt jo varsin laajaan käyttöön varsinkin pienten ja keskisuurten yritysten keskuudessa. Markkinoilta löytyykin jo useita palveluntarjoajia, jotka tarjoavat sovelluksiaan ohjelmistovuokrauksen periaatteita noudattaen. Esimerkiksi Salesforce.com ja NetSuite tarjoavat mm. asiakkuuden, automaation, tuottavuuden ja jopa rahoituksenhallinnan sovelluksia. (Kaplan, 2007)

Kaplan (2007) viittaa vuonna 2006 THINKstrategiesin ja Cutter Consortiumin tekemään tutkimukseen, jonka mukaan yli kahdeksankymmentä prosenttia ohjelmistovuokrausta käyttävistä organisaatioista olivat siihen tyytyväisiä ja suunnittelevatkin laajentavansa ohjelmistovuokrauksen käyttöä tulevaisuudessa. Huolimatta positiivisesta suunnasta yli neljännes tutkimuksen osallistujista osoittivat kuitenkin huolensa luotettavuutta, tietoturvaa ja pitkän aikavälin kannattavuutta kohtaan.

Kirjallisuuteen pohjautuen voidaan havaita, että ohjelmistovuokrauksella on sekä hyviä, että huonoja puolia, niin palvelun tarjoajan, kuin loppukäyttäjän näkökulmasta (Greschler & Mangan, 2002). Seuraavaksi esitellään tarkemmin millaisia hyötyjä ja haittoja asiakkaat ja palveluntarjoajat kokevat ohjelmistovuokrauksessa, jonka jälkeen tutustutaan tarkemmin ohjelmistovuokrauksen ongelmakohtiin.

Ohjelmistovuokrauksen hyödyt:

Greschlerin ja Manganin (2002) mukaan yksi suurimmista ohjelmisto-vuokrauksen hyödyistä asiakkaille on sen kyvyssä vaatia vähemmän resursseja käyttöönotossa ja ylläpidossa. Tämä tarkoittaa käytännössä sitä, että palveluntarjoaja huolehtii kaikesta ohjelmistojen toimivuuteen ja ylläpitoon liittyvistä tehtävistä tarjoten aina päivitetyimmän version ohjelmistosta. Koska ohjelmistovuokrauksen avulla asiakasyritys ei tarvitse asiantuntijatasoista IT-

henkilöstöä, säästää se luonnollisesti resursseja ja antaa mahdollisuuden keskittyä esimerkiksi ydinosaamiseen (Ammerman 2007). Pääsääntöisesti ohjelmistovuokrauksen käyttöönotto nähdäänkin olevan nopeaa ja ohjelmistovuokraus pysyy joustavana myös asiakkaan liiketoiminnan muutoksissa (Greschler & Mangan, 2002).

Ammermanin (2007) mukaan yksi merkittävä hyöty palveluntarjoajille on siinä, että ohjelmistovuokraus operoidaan palveluntarjoajan omissa tiloissa. Tällä tavoin ohjelmistojen hallinta ja ylläpito on huomattavasti helpompaa kuin tilanteessa, jossa ohjelmistot ovat asennettuina kunkin yritysten omille palvelimille ja tietokoneille. Jacobsin (2005) mukaan ohjelmistovuokraus mahdollistaa myös uusien ominaisuuksien levittämistä nopeasti ja usean eri ohjelmiston tarjoamista kustannustehokkaasti. Myös kassavirtojen ennustettavuuden voidaan nähdä paranevan ohjelmistovuokrauksen myötä (Greschler & Mangan, 2002).

Ohjelmistovuokrauksen ongelmakohtia:

Vaikka ohjelmistovuokraukseen liittyvät hyödyt ovat asiakkaille ja palveluntarjoajille melko kiistattomia, liittyy ohjelmistovuokraukseen kuitenkin muutamia huolenaiheita. On hyvin luonnollista olettaa, että toimiva verkkoyhteys on ohjelmistovuokrauksen elinehto. Ilman toimivaa ja suojattua yhteyttä, eivät asiakkaat koskaan pääsisi käsiksi omiin tietoihinsa. Ohjelmistovuokraus aiheuttaakin ongelmia useille asiakkaille kerralla, jos palvelu ei ole saatavilla (Greschler & Mangan, 2002).

Koska ohjelmistovuokraus perustuu täysin palveluntarjoajan kykyyn tarjota, ylläpitää ja suojata asiakkaan tietoja, lisää ohjelmistovuokraus riippuvuutta aina ulkopuoliseen palveluntarjoajaan sekä vähentää asiakkaan kontrollia liiketoimintakriittiseen dataansa. Tietoturvan ja yksityisyydensuojan näkökulmasta ohjelmistovuokraus nähdäänkin olevan varsin ongelmallinen

asia. Keskeisenä teemana ohjelmistovuokrauksessa ja tietoturvassa nousee monesti luottamuksen merkitys palveluntarjoajaan. (Sultan, 2007)

3 OHJELMISTOVUOKRAUS JA TIETOTURVA

Tänä päivänä ohjelmistojen siirtyessä yhä kasvavassa määrin asiakaskohtaisista ohjelmistoista kohti kokonaisvaltaisia verkkosovelluspalveluja, nousee sen rinnalla huoli tietoturvasta ja yksityisyyden suojasta. Varsinkin monien pienten ja keskisuurten yritysten omaksuessa ohjelmistovuokrausta osaksi liiketoimintaa, herää kysymys yrityksen arkaluontoisen datan turvallisuudesta. (Rittinghouse, 2009, 153-154) Tämän luvun tarkoituksena on esitellä tietoturvan osa-alueita sekä niitä tietoturvaan liittyvä huolia, joita yritykset kokevat muuttaessaan toimintaansa asiakaskohtaisista ohjelmistoista kohti ohjelmistovuokrausta.

3.1 Tietoturvan osa-alueet

Tietoturvan tavoitteena on suojata yrityksen arkaluontoinen informaatio ulkoisilta ja sisäisiltä uhkatekijöiltä. Arvioimalla huolellisesti organisaatioon, yhteistyökumppaneihin ja asiakkaihin liittyviä riskejä, voidaan myös parantaa tietoturvaa. Jotta näitä riskejä voitaisiin tunnistaa ja luokitella, on ensin ymmärrettävä tietoturvan osa-alueita. (Stoneburner, 2001). ISO/IEC-17799 (2000) standardin mukaan tietoturva koostuu kolmesta osa-alueesta: luottamuksellisuudesta, eheydestä ja saatavuudesta. Abbas, El Saddik ja Miri (2005) täydentävät näitä osa-alueita vielä kolmella tietoturvan alakäsitteellä, jotka ovat todentaminen, kiistämättömyys ja pääsynvalvonta. Seuraavaksi tarkastellaan kutakin osa-aluetta erikseen.

Luottamuksellisuus (confidentiality)

ISO/IEC-17799 (2000) standardin mukaan luottamuksellisuudella tarkoitetaan sitä, ettei kukaan pääse ilman oikeutta käyttämään sellaista tietoa, jota ei ole tarkoitettu hänen käyttöönsä. Vain sellaiset ihmiset joille tällainen oikeus on myönnetty, voivat lukea ja muokata tietoa. Tiedon luottamuksellisuus on tietoturvan yksi tärkeimmistä kulmakivistä. Stoneburnerin (2001) mukaan

luottamuksellisuuden tulee päteä datan varastoinnin, prosessoinnin ja lähetyksen aikana. Hyvänä esimerkkinä tiedon luottamuksellisuuden pettämisestä voisi toimia tapaus, jossa henkilö saisi sosiaalisella tiedustelulla selvitettyä toisen ihmisen käyttäjätunnuksen ja salasanan. Tällä tavoin henkilö voisi päästä järjestelmään sisään ja pahimmillaa aiheuttaa mittaamattomia vahinkoja muokkaamalla tai poistamalla järjestelmän tiedostoja.

Luottamuksellisuus on varsinkin organisaatiotasolla yksi merkittävimmistä periaatteista. Esimerkiksi työntekijöiden, asiakkaiden tai potilaiden tiedot voivat sisältää hyvin arkaluontoista informaatiota. Tällaista tietoa ei voida päästää sellaisten ihmisten käsiin joille se tieto ei kuulu. (Whitman & Mattord, 2009)

Eheys (integrity)

Tieto on eheä, silloin kun se on kokonainen, valmis ja koskematon. Tiedon eheys toteutuu silloin, kun mikään ulkopuolinen taho ei pysty luvatta muuttamaan tiedon sisältöä tai poistamaan tietoja (Whitman & Mattord, 2009). ISO/IEC-17799 (2000) standardin mukaan tiedon eheydellä siis varmistetaan, että tiedon tarkkuus ja ”täydellisyys” säilyvät tiedon käsittelyn ja säilytyksen aikana.

Eheydellä on kaksi näkökulmaa: datan eheys ja järjestelmän eheys. Datan eheydellä tarkoitetaan sitä, että mikään ulkopuolinen taho ei pääse muuttamaan tietoa datan prosessoinnin, lähetyksen tai varastoinnin aikana. Järjestelmän eheys tarkoittaa puolestaan sitä, että järjestelmän suorittaman toiminnon laatu pysyy muuttumattomana ja vapaana ulkopuolisesta manipuloinnista. Eheys on yleisesti organisaation tärkein tietoturvan periaate saatavuuden jälkeen. (Stoneburner, 2001)

Hyvänä esimerkkinä tiedon eheyteen kohdistuvasta hyökkäyksestä voisi toimia tapaus, jossa hyökkääjä kaappaa viestin sen lähetyksen aikana ja muuttaa

tämän jälkeen viestin sisältöä. Viesti on tällöin korruptoitunut eikä se ole enää tiedon eheyden näkökulmasta luotettava.

Saatavuus (availability)

Saatavuudella tarkoitetaan ISO/IEC-17799 (2000) standardin mukaan tietojen ja palvelujen turvaamista, jossa varmistetaan, että vain luvan saaneilla käyttäjillä on pääsy tietoon. Toisin sanoen informaation saatavuus antaa valtuutetuille käyttäjille ja tietojärjestelmille pääsyn tietoon ilman häiriöitä ja esteitä sekä mahdollisuuden saada tietoa halutussa formaatissa (Whitman & Mattord, 2009).

Todentaminen (authentication)

Todentamisella tarkoitetaan kaikkia niitä keinoja joilla palvelua käyttävän olion aitous voidaan tunnistaa. Oliolla tarkoitetaan tässä yhteydessä käyttäjää, laitetta, tiedon alkuperää, verkkopalvelua tai verkosta www-sivun mukana ladattua ohjelmakoodiriviä. (Stoneburner, 2001)

Jotta olion aitous voitaisiin tunnistaa, on oliolla oltava jokin ominaisuus, mitä muilla samankaltaisilla olioilla ei ole. Näitä ovat yksilölliset ominaisuudet, jokin hallussa oleva esine, tai jokin tieto jolla olio pystyy todentamaan aitoutensa. Yksilöllisiä ominaisuuksia ovat esimerkiksi ulkonäkö, ääni ja käsiala. Hallussa olevalla esineellä, kuten esimerkiksi sähköisellä avaimella voidaan myös todentaa henkilö. Koska avaimia ja esineitä voidaan kuitenkin väärentää ja varastaa, tehostetaan todennusta usein myös tiedon avulla, kuten esimerkiksi salasanalla tai PIN-koodilla. (Järvinen, 2002, 26-27)

Todentaminen on yksi vaikeimmista tietoturvan osa-alueista varmistaa ja monesti siihen kohdistuukin erilaisia hyökkäyksiä. Salasanojen tiedustelu ja arvailu, biometristen tunnisteiden väärentäminen sekä tietojen salaukseen liittyvien julkisten avainten väärentämiset lienevät tunnetuimpia todentamiseen liittyviä uhkatekijöitä. (Abbas, El Saddik ja Miri, 2005)

Pääsynvalvonta (access controll)

Pääsynvalvonnalla varmistetaan, että vain sellaiset henkilöt jotka ovat todennettuja, pääsevät järjestelmän tietoihin. Useasti pääsynvalvonnasta vastaavat ohjelmisto ja käyttöjärjestelmä itse. (Abbas ym. 2005). On myös yleistä, että pääsyä sellaisiin palvelimiin, joista henkilö ei tarvitse tietoa, rajoitetaan (Nikkari, 2007, 15).

Pääsynvalvontaan liittyy oleellisesti myös käytön seuranta. Järjestelmä pitää kirjaa siitä, ketkä ovat avanneet ja muokanneet tiedostoja, käyttäneet ohjelmia sekä kirjautuneet järjestelmään sisään ja sieltä ulos. (Järvinen, 2002, 27). Stoneburnerin (2001) mukaan pääsynvalvonnan turvallisuuden toteutuminen ja seuranta määräävät lopulta koko järjestelmän tietoturvallisuuden tason.

Kiistämättömyys (non-repudiation)

Kiistämättömyys liittyy läheisesti sähköiseen kaupankäyntiin, johon perinteisesti kuuluvat seuraavat ostotapahtumien vaiheet: tilauksen tekeminen, tilauksen vastaanotto ja tuotteen toimittaminen. Kukin näistä vaiheista pitää voida todistaa. (Nikkari, 2007, 15). Organisaation sisäisissä järjestelmissä kiistämättömyys on myös tärkeä tietoturvan osa-alueista. Esimerkiksi toiminnanohjausjärjestelmässä (ERP), johon sisältyy muun muassa palkanlaskenta, kirjanpito, reskontra, varastonhallinta ja tuotannonohjaus, on kussakin osioissa pystyttävä kiistattomasti todentamaan eri tapahtumien vaiheita.

3.2 Tietoturva verkkoympäristössä ja sen riskit

Internet on tänä päivänä yksi nopeimmin kasvaneista globaalin verkoston osista. Internet on kuitenkin hyvin haavoittuvainen hyökkäyksille sen mahdollisten suunnitteluvirheiden ja tietoturvaongelmien takia. Yksikin onnistunut hyökkäys Internetissä olevaan järjestelmään voi aiheuttaa mittaamattomia vahinkoja järjestelmän toiminnalle ja palvelujen käyttäjille.

Internetin rakenne, tietoturvaongelmat, tekniikat, menetelmät ja ohjelmistot kuvastavat yhdessä sitä, miten iso ja vaikea kokonaisuus tietoturvan hallitseminen Internetissä on. (Abbas ym. 2005)

Verkkoympäristön tietoturvauhkia on käsitelty kirjallisuudessa paljon. Esimerkiksi Open Web Application Security Project (OWASP) määrittelee muutaman vuoden välein kymmenen pahinta verkkopalveluihin kohdistuvia uhkakuvaa. Useimmat tämän listan haavoittuvuuksista johtuvat verkkopalveluiden teknisestä toteutuksesta ja altistavat palvelun siten tietoturvauhille. Osa listalla olevista haavoittuvuuksista johtuvat puolestaan käyttäjän osaamattomuudesta tai huolimattomuudesta. (Rantala, 2009). Northcutt ym. (2008) ovat myös luoneet listauksen verkon hyökkäyksistä, jotka todennäköisemmin aiheuttavat suurinta vahinkoa verkkoympäristön käyttäjille. Kummatkin edellä mainitut listaukset ovat varsin kattavia, ja havainnollistavat hyvin verkkoympäristön yksittäisiä uhkatekijöitä. Näiden listausten suurimpana puutteena on kuitenkin se, etteivät ne luokittele uhkia eri kategorioihin. Ymmärtääksemme yksittäisiä verkkoympäristön uhkia, on ensin ymmärrettävä mihin yläkäsitteisiin näitä uhkia voidaan luokitella.

Abbas ym. (2005) ovat luoneet kattavamman luokituksen Internetin tietoturvaongelmille. Heidän mukaan Internetin tietoturvariskien taksonomia koostuu kuudesta verkkoympäristön tietoturvan kategoriasta:

- Manuaalinen hyökkääminen järjestelmään tai henkilön yksityisiin tietoihin
- Datan salakuuntelu tai uudelleenmuokkaus
- Biometriset hyökkäykset
- Tunnistustoimintojen ja menettelytapojen murtaminen

- Haitallinen koodi
- Protokollahyökkäykset

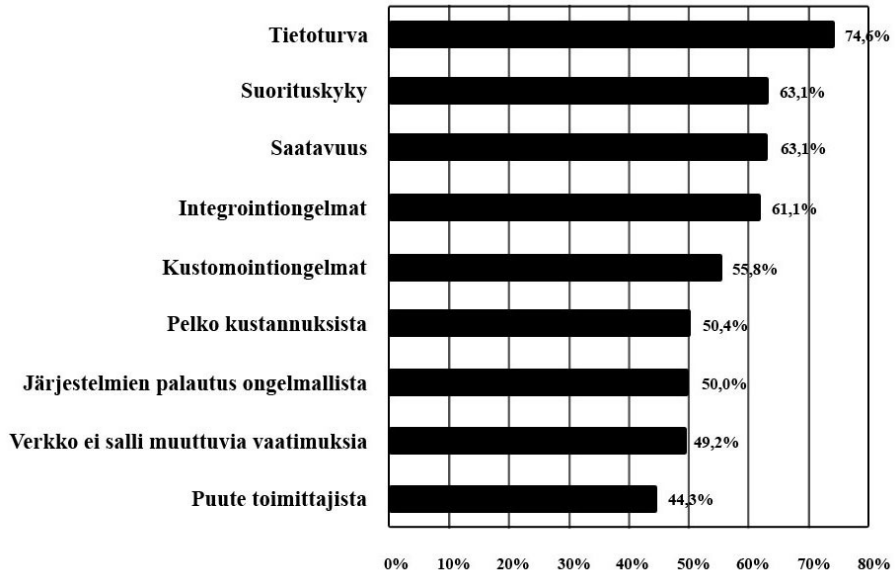
Koska verkkoympäristö on keskeisimmässä roolissa ohjelmistovuokrauksessa, kuvastaa Abbasin ym. (2005) taksonomialuokitus hyvin myös ohjelmisto-vuokraukseen kohdistuvia uhkia, joita verkkoympäristö sille toiminta-alustana luo.

Manuaalisella hyökkäämisellä järjestelmiin tai henkilön yksityisiin tietoihin tarkoitetaan kaikkia niitä manuaalisia menetelmiä ja tekniikoita, joiden avulla hyökkääjä voi päästä järjestelmän tietoihin käsiksi. Tällaisia menetelmiä ovat esimerkiksi salasanan murtaminen ja sosiaalinen tiedustelu. Datan salakuuntelun ja uudelleenmuokkauksen kategoriaan kuuluvat ne uhkatekijät, jotka vaikuttavat dataan sen lähetyksen aikana. Tämän kategorian uhkakuviksi muodostuvat esimerkiksi viestin tahallinen muokkaus lähetyksen aikana tai viestin poistaminen. Biometrisillä hyökkäyksillä tarkoitetaan puolestaan kaikkia niitä järjestelmään kohdistuvia hyökkäyksiä, joissa käytetään hyväksi biometristä tunnistamista. biometrisia hyökkäyksiä ovat esimerkiksi sormenjäljen väärentäminen ja biometrisen allekirjoituksen kopiointi. (Abbas ym. 2005)

Tunnistustoimintojen ja menettelytapojen murtamisen kategoriaan kuuluvat kaikki ne teot, joilla voidaan manipuloida henkilön tunnistamista, valtuuttamista ja pääsynvalvontaa. Haitalliseen koodiin lukeutuvat kaikki haittaohjelmat, virukset, troijalaiset ja virheet koodissa. Protokollahyökkäyksiin sisältyy puolestaan kaikki palvelunestohyökkäykset (DoS) ja verkon protokolliin, kuten TCP/IP perustuvat hyökkäykset. (Abbas ym. 2005)

3.3 Ohjelmistovuokraus ja tietoturva

Rittinghouse (2009, 162) arvioi, että tulevaisuuden tietojenkäsittely tulee enenevämmässä määrin perustumaan ohjelmistovuokrauksen sekä web 2.0:n teknologioihin tyydyttääkseen asiakkaiden ohjelmistotarpeita. Uusien liiketoimintamallien syntyessä ja toiminnan siirtyessä Internetin yli tapahtuvaan tietojenkäsittelyyn, muuttuvat vaatimukset myös tietoturvalle. Rittinghouse (2009, 154) viittaa IDC:n (International Data Corporation) vuonna 2009 tekemään tutkimukseen, jonka mukaan tietoturva onkin ohjelmistovuokrauksen suurin huolenaihe organisaatioille. Kuviossa 3 esitetään keskeiset ohjelmistovuokrauksen huolenaiheet joita tutkimuksessa nousi esille.



KUVIO 3 Ohjelmistovuokrauksen huolenaiheet (Rittinghouse, 2009, 154)

IDC:n tutkimuksessa haastateltiin 244 IT-alan yritysjohtajaa ja heidän alaisiaan siitä, miten he kokevat ohjelmistovuokrauksen nyt ja tulevaisuudessa. Tutkimuksessa henkilöt arvioivat tietoturvauhkia viisiportaisella Likert-asteikolla, jossa numero yksi kuvaa ei lainkaan merkittävää uhkaa ja numero viisi hyvin merkittävää uhkaa. 244 henkilöstä 74,6 % (182 henkilöä) antoi

tietoturvalle numeron neljä tai viisi. Huomattavaa onkin, että aikaisemman vuoden tutkimukselle tietoturva säilytti edelleen paikkansa sijalla yksi. Vastaajat ovatkin edelleen huolissaan, että luottamalla liiketoimintaa ohjaavan informaation ja kriittiset IT -resurssit oman palomuurin ulkopuolelle, voi niihin kohdistua mahdollisia hyökkäyksiä.

Kansainvälisen ICT- alan tutkimus- ja konsultointiyrityksen Gartnerin tutkimuksen mukaan ohjelmistovuokraukseen liittyy paljon riskejä ja uhkia sen takia, koska data varastoidaan ja käsitellään jaetussa virtuaalisessa ympäristössä, oman organisaation ulkopuolella. Tämän vuoksi henkilökohtaisen, luottamuksellisen ja arkaluontoisen datan suojaaminen on ohjelmistovuokrauksessa erittäin tärkeää. Gartnerin tutkimuksen mukaan ohjelmistovuokraukseen liittyy seitsemän tietoturvaan liittyvää tekijää, jotka tulisi ottaa huomioon. Balachandra ym. (2009), Rittinghouse (2009) ja Brodkin (2008) viittaavat teoksissaan Gartnerin tutkimukseen.

Erillisoikeutetut käyttäjät: Arkaluontoisen datan prosessointi yrityksen ulkopuolella tuo mukanaan luontaisen riskin, koska ulkoistetut palvelut sivuuttavat ”fyysisen, loogisen ja henkilökohtaisen kontrollin” ohjelmistoista ja omasta datasta (Balachandra ym. 2009). Yritysten käyttäessä ohjelmistoja sekä varastoidessaan tietoa verkon yli olisi hyvin tärkeä, että palveluntarjoaja pystyy selvittämään kellä kaikilla osapuolilla on pääsy yrityksen dataan. Näitä ovat monesti palveluntilaaja itse sekä palvelun ylläpitoon erikoistuneet henkilöt. Palveluntarjoajan tulisikin pystyä selvittämään, missä määrin nämä erillisoikeuden saaneet ylläpitäjät voivat lukea, muokata sekä poistaa yritysten arkaluontoista dataa. (Rittinghouse, 2009, 64)

Sääntöjen noudattamatta jättäminen: Vaikka yrityksen tiedot olisivatkin ulkopuolisen palveluntarjoajan hallussa, ovat asiakkaat loppujen lopuksi itse vastuussa oman datansa eheydestä ja tietoturvasta (Balachandra ym. 2009). Rittinghousen (2009, 164) mukaan onkin tärkeää varmistaa, että palvelun-

tarjoajat noudattavat tietoturvastandardeja ja ovat valmiita ulkopuolisille auditoinneille.

Datan sijainti: Ihmisten käyttäessä ohjelmistoja sekä varastoidessaan tietoa verkon yli he eivät ole aina tietoisia mihin paikkaan tai edes mihin maahan heidän datansa on varastoitu. Balachandran ym. mukaan (2009) palveluntarjoajien toimivallan datan varastoimiseen ja prosessoimiseen on oltava aina paikallisten tietoturvavaatimusten sekä asiakkaitten yksityisyyden-suojan mukaisia.

Datan huono eristäminen: Dataa varastoidaan verkossa tyypillisesti jaetuissa ympäristöissä yhdessä muiden asiakkaiden kanssa. Tästä saattaakin nousta huoli siitä, millä tavoin yrityksen dataa eristetään muiden palvelua käyttävien yritysten tai henkilöiden datasta. Yksi varsin tehokas ja käytetty keino on tietojen salaaminen. (Brodkin, 2008) Tietojen salaus ei mielestäni kuitenkaan takaa kokonaisvaltaista suojaa, sillä monet salausalgoritmit ovat tänä päivänä melko helppoja purkaa. Rittinghousen (2009, 164) mukaan tietojen salaus tulisi näkyä kaikissa datan käsittelyn vaiheissa ja sen tulisi ennen kaikkea olla testattu alan ammattilaisilla. Tietojen salaukseen liittyy myös paradoksi. Salauksen epäonnistuminen voi tehdä datasta täysin hyödyttömän mutta toisaalta se voi vaikeuttaa myös tiedon saatavuutta.

Elpyminen: Palvelun kaatuessa voivat katastrofin ainekset olla olemassa, mikäli palveluntarjoajalla ei ole kopioita datasta ja sovellusarkkitehtuurista. Palveluun kohdistuukin suuri riski siinä, ettei palveluntarjoajalla ole kykyä tehdä täydellistä järjestelmän palautusta virhetilanteessa. Rittinghousen (2009, 164) mukaan palveluntarjoajalta tulisikin kysyä, miten he voivat hoitaa tällaiset virhetilanteet ja kuinka kauan siinä kestää.

Huono tutkimuksellinen tuki: Laitonta toimintaa verkossa voi olla hyvin vaikeaa havaita ja tutkia. Varsinkin verkkopalveluita on erityisesti hyvin

vaikeita tutkia, sillä palveluun kirjautumisen data ja asiakkaiden tiedot voivat monesti olla hajautettuina useammille datapalvelimille. (Balachandra ym. 2009)

Huono pitkäaikainen toimintakelpoisuus: Pitkäaikainen toimintakelpoisuus viittaa tilaan, jossa palvelun käyttäjän data pysyy saatavissa, vaikka palveluntarjoaja lopettaisi toimintansa tai sulautuisi osaksi toista yritystä. Suurin riski toimintakelpoisuuden ylläpitämisessä onkin se, että palveluntarjoaja ei pysty palauttamaan dataa käyttäjille takaisin. Onkin erityisen tärkeää varmistaa, että tällaisissa tilanteissa palveluntarjoaja pystyy palauttamaan tiedot siinä muodossa että niitä voidaan hyödyntää esimerkiksi vaihtoehtoisilla sovelluksilla. (Balachandra ym. 2009)

Gartnerin tutkimuksen pohjalta voidaan havaita, että ohjelmistovuokraukseen liittyy uhkia, jotka eivät aiheudu pelkästään ohjelmistovuorauksen verkkokeskeisyydestä, vaan yhdessä eri tekijöiden kanssa. Tämän vuoksi ohjelmistovuokraukseen liittyvien tietoturvaongelmien tarkastelussa on verkkoympäristön tietoturvauhkien lisäksi otettava mukaan myös nämä eri tekijät. Ohjelmistovuokraukseen liittyviä uhkakategorioita esitellään kappaleessa 4.1.

3.4 Ohjelmistovuokraus vs. asiakaskohtaiset ohjelmistot

Kaplanin (2007) mukaan ohjelmistovuokrauksessa voidaan paremmin ratkaista haitallisia järjestelmien tietoturva-aukkoja kuin asiakaskohtaisten ohjelmistojen käytössä. Koska ohjelmistovuokraus perustuu monikäyttäjäarkkitehtuuriin, tarvitsee ohjelmisto päivittää vain kerran, mikäli siinä havaitaan tietoturva-aukko. Asiakaskohtaisissa ohjelmistoissa päivitys joudutaan ajamaan jokaiselle käyttäjälle erikseen. Toisin sanoen ohjelmistojen päivittäminen on asiakaskohtaisissa ohjelmistoissa vaikeampaa, koska ohjelmiston toimittajan on huolehdittava ohjelmistojen kaikista eri versioista loppukäyttäjien erilaisissa ohjelmistoympäristöissä. Usein asiakaskohtaiset ohjelmistot on räätälöity erikseen yritysten tarpeiden mukaisesti tehden ohjelmistojen päivityksestä

entistä vaikeampaa. Tämän vuoksi asiakaskohtaisiin ohjelmistoihin jää suuremmalla todennäköisyydellä tietoturva-aukkoja, joita tunkeutujat voivat käyttää hyväkseen. (Kaplan, 2007)

Vaikka ohjelmistovuokraus on varsin tuore aihe ja sen tietoturvaa koskevat huolenaiheet ovat täysin ymmärrettäviä, voidaan kuitenkin havaita, että yritykset ovat luottaneet tietojansa kolmansien osapuolien haltuun jo useita vuosia. Tästä hyvinä esimerkkeinä toimii verkkopankkitoiminta, maksujärjestelmät sekä monet kaupalliset palvelut. Suurimmat yritykset ovat jopa ulkoistaneet kaikki datapalvelimensa kolmansille osapuolille. Siinä missä nämäkin palvelut ovat osoittautuneet turvallisiksi, ei tietoon ole tullut yhtäkään vakavaa tietoturvaan liittyvää tapausta ohjelmistovuokrauksessa. (Kaplan, 2009). Kaplanin mukaan yksi syy tähän on siinä, että mikäli ohjelmistovuokrausta tarjoava yritys haluaa selvitä markkinakilpailussa, on sen pystyttävä takaamaan, että asiakkaiden tiedot ovat turvassa. Tämän vuoksi näissä yrityksissä kiinnitetään tietoturva-asioihin monesti enemmän huomiota. Voidaan kuitenkin olettaa, etteivät yritykset kovin mielellään paljasta esimerkiksi tietovuotoja tai muita ongelmia, vaikka niitä sattuisikin. Uskon, että mikäli jokin palveluntarjoaja jäisi kiinni tämän kaltaisesta tilanteesta, leviäisi tieto nykypäivän kommunikaatiotekniikoilla ja sosiaalisen median avulla ihmisten tietoon hyvinkin nopeasti. Uskon myös, että useissa tapauksissa se myös merkitsisi tällaisen palvelun loppua.

4 VIITEKEHYS OHJELMISTOVUOKRAUKSEN TIEOTURVAONGELMIEN TARKASTELUUN

Tämän tutkielman keskeinen tavoite oli rakentaa mahdollisimman kattava ja yksinkertainen viitekehys ohjelmistovuokraukseen kohdistuvista tietoturvaongelmista. Ohjelmistovuokrauksen tietoturvaongelmien viitekehyksen avulla voidaan tunnistaa ja luokitella keskeisimmät ja oletettavasti merkittävimmät ohjelmistovuokraukseen kohdistuvat tietoturvaongelmat. Viitekehyksen tarkoituksena oli myös toimia kyselytutkimuksen keskeisimpänä työkaluna, jonka avulla vastaajat arvioivat kunkin tietoturvaongelman painoarvoa. Tässä tutkielmassa viitekehykseen kerättiin tarkoituksenmukaisesti tietoturvauhkia, jotka ovat oletettavasti suurempia ohjelmistovuokrauksessa kuin asiakaskohtaisissa ohjelmistoissa.

Ohjelmistovuokrauksen tietoturvaongelmien viitekehys muodostettiin pääasiallisesti ohjelmistovuokrauksen ilmiön ajankohtaisuudesta ja ennen kaikkea tutkimuksen vähäisyydestä johtuen. Suurin osa aihealueen tutkimuksesta onkin vasta pari vuotta vanhoja mutta näiden tutkimusten pääpaino on monesti ollut liiketoiminnallisissa näkökulmissa. Tietoturvakysymyksiä ja ohjelmistovuokrausta ei sen sijaan aikaisemmassa tutkimuksessa ole käsitelty lähes ollenkaan.

Keskeisimpänä ja vertailevana viitekehyksenä tutkimuksessa toimi Gartnerin tutkimus vuodelta 2008, jossa tunnistettiin seitsemän ohjelmistovuokraukseen läheisesti liittyvää tietoturvauhkaa. Näitä uhkia olivat erillisoikeutetut käyttäjät, sääntöjen noudattamatta jättäminen, datan sijainti, datan huono eristäminen, huono elpyminen virhetilanteissa, huono tutkimuksellinen tuki ja huono pitkäaikainen toimintakelpoisuus.

Gartnerin tutkimuksen ehdoton vahvuus on siinä, että tutkimuksessa tunnistetaan monta ohjelmistovuokrauksen ongelmakohtaa ja se edistää asiakkaan ja palveluntarjoajan vuoropuhelua. Tutkimuksesta rajataan sen sijaan

monta ohjelmistovuokraukseen liittyvää ilmiötä, joita laadittu viitekehys pyrkii täydentämään. Näitä ilmiöitä ovat fyysiset tietoturvauhat, ohjelmistojen tietoturvauhat, verkkoympäristön tietoturvauhat ja muut ohjelmistovuokraukseen kohdistuvat tietoturvauhat.

Ohjelmistovuokrauksen tietoturvaongelmien viitekehys sopii hyvin tietoturva-alan tutkijoiden ja työntekijöiden kehittämisen sekä jatkotutkimuksen välineeksi. Lisäksi viitekehys antaa hyvän yleiskuvan ohjelmistovuokrauksen tietoturvan osa-alueista, jota voidaan käyttää myös opetusvälineenä ohjelmistovuokrauksen parissa työskentelevien ihmisten keskuudessa.

Tässä luvussa tarkastellaan ohjelmistovuokrauksen tietoturvaongelmien viitekehyksen luomista ja saatuja tuloksia esittelemällä ensiksi viitekehyksen lähtökohdat sekä taustaolettamukset. Tämän jälkeen esitellään kirjallisuutta ohjelmistovuokraukseen kohdistuvista tietoturvaongelmista. Lopuksi esitellään kerätystä aineistosta tiivistetty ohjelmistovuokrauksen tietoturvaongelmien viitekehys.

4.1 Viitekehyksen muodostaminen ja taustaolettamukset

Ohjelmistovuokrauksen viitekehyksen muodostamisen lähtökohtana oli aihealueesta tehty kirjallisuuskatsaus, jonka tuloksena todettiin, että verkkoympäristöön kohdistuvat tietoturvauhat muodostuvat ohjelmisto-vuokrauksen yhdeksi keskeisimmäksi haasteeksi. Lisäksi lähtökohtana viite-kehykselle oli tutkijan omat ennakko-oletukset ja päätelmät, joiden pohjalta huomattiin, että jako verkkoympäristön tietoturvaongelmiin ei ollut riittävä. Keskeisinä ennakko-oletuksina ohjelmistovuokrauksen tietoturvaongelmista nousivat verkkoympäristön tietoturvan lisäksi fyysinen tietoturva. Lisäksi huomioitiin ohjelmistoissa itsessään mahdollisesti ilmenevät tietoturva-ongelmat. Näiden ennakko-oletusten taustalla ovat ohjelmistovuokrauksen piirteet, joiden mukaan ohjelmiston täytyy:

1) sijaita fyysisesti jollakin datapalvelimella

2) olla käytettävissä verkon yli palveluna

Lisäksi huomioitiin ohjelmistoissa itsessään mahdollisesti ilmenevät tietoturvaongelmat.

Viitekehyksen laatimisessa keskityttiin aluksi mahdollisimman monien uhkatekijöiden löytämiseen. Uhkiin viittaavaa kirjallisuutta etsittiin pääasiallisesti sähköisistä tietokannoista, kuten Googlen Scholar -palvelusta. Hakusanoina käytettiin monia ohjelmistovuokraukseen ja tietoturvaan liittyviä yhdistelmiä. Luokitteluperustana käytettiin kirjallisuuden avulla havaittuja fyysisiä, ohjelmistojen ja verkkoympäristön uhkia. Lisäksi havaittiin, että on olemassa uhkia, jotka eivät sijoitu mihinkään näistä kolmesta kategoriasta. Sen vuoksi luokitteluun otettiin neljäs uhkakategoria, muut ohjelmistovuokrauksen tietoturvauhat. Lopulta eri uhkia yhdistelemällä ja luokittelemalla saatiin muodostettua lista neljästä tärkeimmästä ohjelmistovuokraukseen vaikuttavasta uhkakategoriasta. Näitä olivat:

1) fyysiset tietoturvauhat

2) ohjelmistojen tietoturvauhat

3) verkkoympäristön tietoturvauhat

4) muut ohjelmistovuokrauksen tietoturvauhat

4.1.1 Fyysiset tietoturvauhat

Fyysisillä tietoturvauhkilla tarkoitetaan Järvisen (2002), Laaksosen ym. (2006) ja Nikkarin (2007) mukaan niitä tekijöitä, jotka voivat vahingoittaa organisaatioon tietoja ja järjestelmiä fyysisellä tasolla. Näitä ovat mm. varkaus, tulipalo, vesivahinko, sähköhäiriöt, työntekijöiden inhimilliset virheet sekä kulunvalvontaan liittyvät riskit. Kallhoffin (2007) mukaan fyysiset tietoturvauhat ovat aina yhteydessä luontoon, ympäristöön, jakelujärjestelmiin, ihmisten käyttäytymiseen tai poliittiseen ympäristöön.

Fyysiset uhat ovat viitekehyksen kannalta perusteltuja, sillä myös ohjelmisto-vuokrauksessa käytettävät ohjelmistot ja palvelimet sijaitsevat fyysisesti jossakin. Näihin palvelimiin ja fyysisiin paikkoihin voidaan siis katsoa vaikuttavan samat fyysiset uhkatekijät kuin asiakaskohtaisten ohjelmistojen kanssa. Tämän pohjalta voidaankin tehdä johtopäätös, ettei ohjelmisto-vuokrauksessa ja asiakaskohtaisissa ohjelmistoissa ole fyysisten tietoturva-uhkien osalta suuria poikkeavuuksia. Fyysiseen tietoturvaan vaikuttaa kuitenkin aina kunkin kohdeorganisaation tietoturvapoliittiset päätökset sekä yrityksen sisäiset tietoturvapäätökset.

Taulukossa 1 kuvataan ohjelmistovuokraukseen vaikuttavia fyysisiä uhkia. Vasemmassa sarakkeessa esitellään kirjallisuudesta löydettyjä fyysisiä tietoturvauhkia. Keskimmäisessä sarakkeessa esitellään fyysisten tietoturva-ongelmien tunnistamisessa käytettyjä lähteitä. Oikeanpuolisessa sarakkeessa otetaan kantaa siihen, eroavatko fyysiset tietoturvauhat ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä. Fyysisten tietoturvauhkien kohdalla mallien välillä ei nähty suuria eroavaisuuksia.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
FYYSISIÄ TIETOTURVAUHKIA		
Varkaus	(Järvinen 2002), (Laaksonen & Nevasalo & Tomula 2006), (Nikkari 2007)	Ei poikkea mallien välillä
Tulipalo	(Järvinen 2002), (Laaksonen & Nevasalo & Tomula 2006), (Nikkari 2007)	Ei poikkea mallien välillä
Vesivahinko	(Järvinen 2002), (Laaksonen & Nevasalo & Tomula 2006), (Nikkari 2007)	Ei poikkea mallien välillä
Sähköhäiriö	(Järvinen 2002), (Laaksonen & Nevasalo & Tomula 2006), (Nikkari 2007)	Ei poikkea mallien välillä
Työntekijöiden inhimilliset virheet	(Järvinen 2002), (Laaksonen & Nevasalo & Tomula 2006), (Nikkari 2007)	Ei poikkea mallien välillä
Kulunvalvontaan liittyvät riskit	(Järvinen 2002), (Laaksonen & Nevasalo & Tomula 2006), (Nikkari 2007)	Ei poikkea mallien välillä

TAULUKKO 1 Fyysisiä tietoturvauhkia

4.1.2 Ohjelmistojen tietoturvauhat

Ohjelmistojen tietoturvauhat muodostuivat luonnollisesti yhdeksi ohjelmistovuokraukseen kohdistuvista uhkatekijöistä. Jos ohjelmistovuokrausta tarkastellaan pelkästään sovelluksen kehittämisen näkökulmasta, voidaan havaita, etteivät asiakaskohtaiset ohjelmistot ja ohjelmistovuokrauksen sovellukset eroa paljon toisistaan. Kummassakin tapauksessa voidaan

varsinaiseen sovellukseen katsoa vaikuttavan samat ohjelmistokehityksen periaatteet ja menetelmät. Tähän päätelmään perustuen voidaan myös väittää, että samat ohjelmistoihin vaikuttavat uhkat pätevät niin asiakaskohtaisissa ohjelmistoissa kuin ohjelmistovuokrauksen sovelluksissa. Huomattavaa kuitenkin on, että mikäli ohjelmiston käyttö tai kehittäminen tapahtuu verkossa, kohdistuu siihen lisääntyvästi myös verkkoympäristön uhkatekijöitä.

Landwehrin, Bullin, McDermottin ja Choin (1994) mukaan ohjelmistoja koskevat tietoturvauhat voidaan jakaa kahteen kategoriaan: tahallisiin ja ei tahallisiin uhkiin. Tahallisiin ohjelmistojen uhkiin lukeutuvat esimerkiksi troijalaiset, virukset, madot ja ansat koodissa. Myös ohjelmiston suunnittelussa syntyvät huonot päätökset voivat johtaa tietoturva-aukkoihin ohjelmistotasolla. Tahallisia ohjelmistoihin vaikuttavia tietoturvauhkia esitellään taulukossa 2. Taulukossa esitellään myös käytettyjä kirjallisuuslähteitä sekä vertaillaan ohjelmistoihin vaikuttavia tahallisia tietoturvauhkia ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
OHJELMISTOJEN TIETOTURVAUHKIA		
Tahalliset		
Troijalaiset, virukset, madot	(Landwehr & Bull & McDermott & Choi 1994), (Weber & Karger & Paradkar 2005), (Savolainen & Niemelä & Savola 2007), (Abbas ym. 2005), (Van der Stock & Williams & Wichers 2007), (Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Ei poikkea mallien välillä
Ansat koodissa (trapdoor)	(Landwehr & Bull & McDermott & Choi 1994), (Weber & Karger & Paradkar 2005), (Savolainen & Niemelä & Savola 2007)	Ei poikkea mallien välillä
Huono päätöksenteko ohjelmiston suunnittelussa	(Savolainen & Niemelä & Savola 2007)	Ei poikkea mallien välillä

TAULUKKO 2 Ohjelmistojen tahallisia tietoturvauhkia

Ohjelmistoihin kohdistuvia tietoturvauhkia voidaan luokitella myös tahattomiin uhkiin. Näitä ovat Landwehrin ym. (1994), Weberin ym. (2005) ja Savolaisen ym. (2007) mukaan piilevät reitit koodissa, ohjelmistobugit sekä muut vahingot ja inhimilliset erehdykset. Piilevät reitit ilmenevät esimerkiksi ohjelmistoihin jääneinä takaovina, joiden kautta hyökkääjä voi manipuloida ohjelmiston toimivuutta. Bugit ovat taas ohjelmiston kehitysvaiheessa jääneitä virheitä koodissa, joita pystytään hallitsemaan ainoastaan iteratiivisella ohjelmistokehittämisellä. Muut vahingot ja inhimilliset virheet viittaavat puolestaan niihin uhkatekijöihin joita esimerkiksi ohjelmistosuunnittelija voi omalla toimintatavalla saada aikaan. Näitä voivat olla esimerkiksi väsyneenä tehdyt huonot ohjelmointiratkaisut tai vaikkapa työaseman jättäminen päälle

päivän päätteeksi. Taulukko 3 kuvastaa ohjelmistoihin kohdistuvia tahattomia tietoturvauhkia. Vasemmassa sarakkeessa esitellään kirjallisuudesta poimittuja uhkia. Keskimmäisessä sarakkeessa esitellään kirjallisuuslähteet. Oikeanpuoleisessa sarakkeessa vertaillaan ohjelmistoihin vaikuttavia tahattomia tietoturvauhkia ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä. Huomattavaa näiden kahden mallin vertailussa on se, että kummassakin ohjelmistojen hankinnan ja käytön mallissa voidaan havaita vaikuttavan samoja tahattomia ohjelmistojen tietoturvauhkia. Tämän vuoksi voidaan olettaa, ettei näiden kahden mallin välillä ole ohjelmistojen tahattomien tietoturvauhkien välillä poikkeavuuksia.

UHAT	**LÄHDE**	**OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT**
OHJELMISTOJEN TIETOTURVAUHKIA		
Tahattomat		
Piilevät reitit koodissa	(Landwehr & Bull & McDermott & Choi 1994), (Weber & Karger & Paradkar 2005), (Savolainen & Niemelä & Savola 2007)	Ei poikkea mallien välillä
Bugit	(Landwehr & Bull & McDermott & Choi 1994), (Weber & Karger & Paradkar 2005), (Savolainen & Niemelä & Savola 2007)	Ei poikkea mallien välillä
Muut vahingot ja inhimilliset erehdykset	(Savolainen & Niemelä & Savola 2007)	Ei poikkea mallien välillä

TAULUKKO 3 Ohjelmistojen tahattomia tietoturvauhkia

Ohjelmistoihin kohdistuvia tietoturvauhkia voidaan myös lajitella Wangin ym. (2003) mukaan myös ohjelmistotason uhkakategoriaan. Tähän tasoon kuuluu

Wangin ym. (2003), Savolaisen ym. (2007) ja Abbasin ym. (2005) mukaan ohjelmistojen luvaton toiminnallisuuden manipulointi, ohjelmistojen datan luvaton manipulointi sekä luvattomien käyttöoikeuksien hankkiminen.

Ohjelmistojen luvaton toiminnallisuuden manipulointi ilmenee siinä, että hyökkääjä/järjestelmän luvaton käyttäjä muokkaa ohjelmiston lähdekoodia tavalla, joka muuttaa oleellisesti ohjelmiston pääasiallista toimintaa (Wang & Wang, 2003), (Savolainen ym. 2007). Tämän uhkan osalta eri mallien välillä ei nähdä olevan suuria eroavuuksia, sillä sekä ohjelmistovuokrauksessa että asiakaskohtaisten ohjelmistojen käytössä voi epäsuotuisat käyttäjät muokata ohjelmiston toiminnallisuutta. Ohjelmistojen datan luvaton manipulointi liittyy myös läheisesti edelliseen uhkaan. Tässä uhkassa epäsuotuisa käyttäjä pääsee muokkaamaan puolestaan ohjelmiston tuottamaa dataa vääristämällä ohjelmistotulosteita (Wang & Wang, 2003). Myöskään ohjelmistojen datan luvattomassa manipuloinnissa ei mallien välillä katsota olevan suuria eroavaisuuksia, vaan kummassakin tapauksessa uhka on lähes samansuuruinen. Luvattomien käyttöoikeuksien hankkimisella tarkoitetaan epäsuotuisaa toimintaa, jossa käyttäjä pääsee saamiensa käyttäjätunnuksien avulla muokkaamaan ja käyttämään ohjelmistoja sekä järjestelmiä. Ohjelmistovuokrauksessa ja asiakaskohtaisissa ohjelmistoissa tämä uhka katsotaan olevan samansuuruinen. Ohjelmistotason tietoturvauhkia, käytettyjä kirjallisuuslähteitä sekä ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen tietoturvauhkien vertailua esitellään taulukossa 4.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
OHJELMISTOJEN TIETOTURVAUHKIA		
Ohjelmistotason uhat		
Ohjelmiston luvaton toiminnallisuuden manipulointi	(Wang & Wang 2003), (Savolainen & Niemelä & Savola 2007)	Ei poikkea mallien välillä
Ohjelmiston datan luvaton manipulointi	(Wang & Wang 2003)	Ei poikkea mallien välillä
Luvattomien käyttöoikeuksien hankkiminen	(Wang & Wang 2003)	Ei poikkea mallien välillä

TAULUKKO 4 Ohjelmistotason tietoturvauhkia

4.1.3 Verkkoympäristön tietoturvauhat

Verkkoympäristön tietoturvaongelmien selvittämisessä keskeisintä oli löytää mahdollisimman kattava jako yksittäisten verkkoympäristön uhkien luokitteluun. Pohjan luokittelulle muodosti Abbasin ym. (2005) Internetin tietoturvauhkataksonomia, joka esiteltiin kappaleessa 3.2. Northcutt ym. (2008) täydensivät tätä luokitusta yksittäisillä verkkoympäristön uhkatekijöillä, jotka todennäköisemmin aiheuttavat suurinta vahinkoa verkon käyttäjille. Kansainvälisen vapaaehtoisjärjestön OWASP:n *(Open Web Application Security Project)* luokittelu oli myös perusteltua ottaa tarkasteluun mukaan. OWASP Top Ten 2007 -listan tarkoituksena on perehdyttää ohjelmistokehittäjät, suunnittelijat, arkkitehdit ja organisaatiot ymmärtämään sovellus-haavoittuvuuksien seurauksia verkkoympäristössä.

Taulukko 5 kuvaa kirjallisuudesta havaittuja verkkoympäristön tietoturvauhkia manuaalisen tunkeutumisen näkökulmasta. Vasemmassa sarakkeessa esitellään kirjallisuudesta poimittuja manuaalisen tunkeutumisen tietoturvamenetelmiä, joista keskeisimmiksi ohjelmistovuokrauksen näkökulmasta nousee verkkourkinta eli tietojen kalastelu ja tietoliikennehyökkäykset.

Vajjhalan, Rossin, Shahn, Gadkarin ja Gonsalvesin (2007) sekä Northcuttin ym. (2008) mukaan verkkourkinnassa eli tietojen kalastelussa on kyse rikollisesta toiminnasta, jossa epäsuotuisa käyttäjä pyrkii saamaan haltuun luottamuksellisia tietoja, kuten henkilö- tai tilitietoja, esiintymällä tiedon saantiin oikeutettuna henkilönä. Esimerkiksi Digitoday otsikoi joulukuussa 2005 tietojenkalastelutapauksesta, jossa suomalaisiin sähköpostiosoitteisiin oli lähetty satojatuhansia huijausviestejä Nordean nimissä. Huijarit olivat tätä kautta saaneet käsiinsä asiakkaiden pankkitunnuksia, joiden avulla huijarit saivat käsiinsä lähes 60 000 euroa asiakkaiden pankkitileiltä. (Kuivalainen, 2005). Ohjelmistovuokrauksessa verkkourkinnan uhka voidaan katsoa olevan lisääntynyt riski sen vuoksi, että keskitetyllä palveluntarjoajalla on hallussaan useamman asiakkaan luottamuksellisia tietoja. Tämä saattaa houkutella tunkeilijoita kalastelemaan näitä luottamuksellisia tietoja.

Tietoliikennehyökkäyksillä puolestaan tarkoitetaan kaikkia niitä keinoja, joilla hyökkääjät pyrkivät estämään, salakuuntelemaan ja manipuloimaan tietoliikennettä (Van der Stock & Williams & Wichers, 2007). Ohjelmisto-vuokrauksen näkökulmasta uhka on varsin merkittävä, sillä toimivat ja turvalliset tietoliikenneyhteydet ovat näiden palveluiden elinehto. Tieto-liikenneverkko on ohjelmistovuokrauksessa myös asiakkaiden ainoa väylä päästä käsiksi omiin tietoihinsa, joten mikäli jokin kolmas osapuoli pääsee tämän liikenteen väliin tai pahimmillaan estämään koko liikenteen, voi se aiheuttaa yrityksille mittaamattomia vahinkoja.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
VERKKOYMPÄRISTÖN TIETOTURVAUHKIA		
Manuaalinen tunkeutuminen systeemiin tai henkilön tietoihin		
Sosiaalinen tiedustelu	(Abbas ym. 2005), (Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Ei poikkea mallien välillä
Salasanatiedostojen arvaaminen/varastaminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Käyttöjärjestelmään hakkeroituminen	(Abbas ym. 2005), (Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Ei poikkea mallien välillä
Käyttäjätilien varastaminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Verkkourkinta, tietojen kalastelu	(Vajjhala & Ross & Shah & Gadkari & Gonsalves 2007), (Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Mahdollinen lisääntynyt riski
Roskaposti (Spam)	(Lichtenstein 1997)	Ei poikkea mallien välillä
Hyökkäykset yrityksen sisältäpäin (työntekijät)	(Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Ei poikkea mallien välillä
Tietoliikennehyökkäykset	(Van der Stock & Williams & Wichers 2007)	Mahdollinen lisääntynyt riski

TAULUKKO 5 Manuaaliset hyökkäykset osana verkkoympäristön tietoturvauhkia

Taulukossa 6 kuvataan myös verkkoympäristön tietoturvauhkia datan salakuuntelun ja uudelleenmuokkauksen näkökulmasta, esitellään käytettyjä kirjallisuuslähteitä sekä arvioidaan esiteltyjä uhkia ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen näkökulmista. Keskeisimmiksi tämän taulukon uhkiksi ohjelmistovuokrauksen näkökulmasta voidaan nostaa salakuuntelu, kaapatun viestin uudelleen muokkaus, vakoiluohjelmat, henkilökohtaisia tietoja keräävät botit sekä ohjelmiston virhetilanteissa vuotavat tiedot. Salakuuntelu ja kaapatun viestin muokkaus voidaan nähdä olevan lisääntyneitä riskejä sen vuoksi, koska ohjelmistovuokrauksessa käyttäjät käyttävät ohjelmiaan verkon välityksellä. Verkkovälitteisyys luo luontaisen mahdollisuuden hyökkääjillä päästä tietoliikenteen väliin ja pahimmillaan muuttamaan tietoliikenteen sisältöä. Toisaalta tämän päivän tietoliikenneyhteyksiä salataan jo niin tehokkaasti erilaisilla salausalgoritmeilla, ettei niiden murtaminen ole kovin helppoa. Edellä mainituista syistä verkkoympäristö tarjoaa myös asiakaskohtaisia ohjelmistoja paremman ympäristön erilaisten vakoiluohjelmien ja henkilökohtaisia tietoja keräävien bottien käytölle.

Ehkä merkittävimpänä uhkana voidaan kuitenkin nostaa ohjelmistojen virhetilanteissa vuotavat tiedot. Monikäyttäjäympäristössä virhetilanteissa vuotavat tiedot voisivat pahimmillaan näkyä muille käyttäjille, paljastaen esimerkiksi liiketoiminnan kannalta salaista tietoa. Asiakaskohtaisissa ohjelmistoissa tätä uhkaa ei luonnollisesti ole olemassa.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
VERKKOYMPÄRISTÖN TIETOTURVAUHKIA		
Datan salakuuntelu tai uudelleenmuokkaus		
Salakuuntelu	(Abbas ym. 2005)	Mahdollinen lisääntynyt riski
Kaapatun viestin muokkaus	(Abbas ym. 2005)	Mahdollinen lisääntynyt riski
Luvaton datan poistaminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Salaisten avainten selvittäminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Vakoiluohjelmat	(Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Mahdollinen lisääntynyt riski
Henkilökohtaisia tietoja keräävät botit	(Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Mahdollinen lisääntynyt riski
Ohjelman virhetilanteissa vuotavat tiedot	(Van der Stock & Williams & Wichers 2007)	Mahdollinen lisääntynyt riski

TAULUKKO 6 Datan salakuuntelu tai uudelleenmuokkaus osana verkkoympäristön tietoturvauhkia

Abbasin ym. (2005) mukaan biometrisillä hyökkäyksillä tarkoitetaan niitä hyökkäyksiä, joissa käytetään hyväksi biometristä tunnistamista, kuten esimerkiksi sormenjäljen väärentämistä. Biometristen hyökkäysten ei voida kuitenkaan sanoa lisääntyneen ohjelmistovuokrauksen myötä tai olevan

vakavampi uhka kuin asiakaskohtaisissa ohjelmistoissa, sillä useimmissa tapauksissa nämä hyökkäykset tapahtuvat yritysten sisältä käsin. Yritysten kulunvalvonta nouseekin yhdeksi merkittävimmäksi tekijäksi estää järjestelmään kohdistuvia biometrisiä hyökkäyksiä. Taulukko 7 esittää verkkoympäristön biometrisia hyökkäyksiä.

UHAT	**LÄHDE**	**OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT**
VERKKOYMPÄRISTÖN TIETOTURVAUHKIA		
Biometriset hyökkäykset		
Sormenjäljen väärentäminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Digitaalisen allekirjoituksen väärentäminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Biometristen valtuuksien varastaminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Biometristen sensorien sekoittaminen	(Abbas ym. 2005)	Ei poikkea mallien välillä

TAULUKKO 7 Biometriset hyökkäykset osana verkkoympäristön tietoturvauhkia

Verkkoympäristön tietoturvauhkista tunnistustoimintojen ja menettelytapojen voittaminen oli myös syytä ottaa tarkasteluun mukana. Näistä uhkista ohjelmistovuokrauksen näkökulmasta merkittävimmäksi Abbas ym. (2005), Van der Stock ym. (2007) ja Savolainen ym. (2007) mainitsevat hyökkäykset

käyttäjä- ja istuntotunnisteiden salausmenetelmiä vastaan sekä palvelun tulvimisen eli floodauksen. Verkkoympäristön tietoturvauhkia tunnistus-toimintojen ja menettelytapojen voittamisen näkökulmasta esitellään taulukossa 8.

Hyökkäyksellä käyttäjä- ja istuntotunnisteiden salausmenetelmiä vastaan voidaan mahdollistaa hyökkääjille salasanojen sekä käyttäjä- tai istuntotunnisteiden keruun järjestelmästä. Tätä kautta sovelluksen käyttäminen toisten valtuuksilla mahdollistuu. Valitettavasti verkkosovelluksissa käytetään vielä tänäkin päivänä harvoin asianmukaisia salausmenetelmiä käyttäjä- tai istuntotunnisteiden salaamiseen. Ohjelmistovuokrauksen näkökulmasta tämä on vakava asia sillä ohjelmistovuokrauksessa käyttäjät kommunikoivat järjestelmien välillä pääsääntöisesi verkko-ohjelmistojen välityksellä. (Van der Stock ym. 2007)

Palvelun floodauksella eli tulvimisella tarkoitetaan sitä, että käyttäjä tai botti lähettää palvelimelle useita viestejä peräkkäin pienellä aikavälillä, jolloin järjestelmä ylikuormittuu. Ohjelmistovuokrauksessa tämän voidaan katsoa olevan lisääntynyt riski sen vuoksi, että käyttäjät käyttävät usein samaa ohjelmistoversiota jaetulla palvelimella. Mikäli hyökkääjä pääsee floodaamaan tätä palvelinta, saattaa se estää useiden käyttäjien ohjelmiston käytön kerralla.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
VERKKOYMPÄRISTÖN TIETOTURVAUHKIA		
Tunnistustoimintojen ja menettelytapojen voittaminen		
PIN-koodien selvittäminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Hyökkäys käyttäjä- ja istuntotunnisteiden salausmenetelmiä vastaan	(Abbas ym. 2005), (Van der Stock & Williams & Wichers 2007)	Mahdollinen lisääntynyt riski
Samanaikainen palvelun "floodaus"	(Abbas ym. 2005), (Savolainen & Niemelä & Savola 2007)	Mahdollinen lisääntynyt riski
Julkisten avainten väärentäminen	(Abbas ym. 2005)	Ei poikkea mallien välillä
Valtuuksien ja käyttöoikeuksien väärentäminen	(Abbas ym. 2005)	Ei poikkea mallien välillä

TAULUKKO 8 Tunnistustoimintojen ja menettelytapojen voittaminen osana verkkoympäristön tietoturvauhkia

Taulukossa 9 kootaan yhteen uhkia ja hyökkäyksiä verkkosivujen haavoittuviin osiin. Näistä ohjelmistovuokrauksen näkökulmasta merkittävimmiksi nousevat troijalaiset, virukset ja madot, SQL injektio, sekä verkkosivun rakenteen muuttaminen cross-site scripting ja XSS hyökkäyksillä.

Troijalaiset, virukset ja madot voidaan nähdä olevan uhka niin kauan kun työasemat ovat yhteydessä verkkoon. Luonnollisesti ohjelmistovuokrauksessa

asiakkaiden työasemat ovat yhteydessä verkkoon, mahdollistaen erilaisten haittaohjelmien tunkeutumisen käyttäjän tietokoneelle. Asiakaskohtaisiin ohjelmistoihin ja niitä käyttäviin työasemiin verrattuna uhka voidaan siis katsoa olevan hieman suurempi ohjelmistovuokrauksen osalta. Toisaalta monet asiakaskohtaisia ohjelmistoja käyttävä työasemat ovat tänä päivänä myös yhteydessä julkiseen Internetiin, mahdollistaen haittaohjelmien tunkeutumisen yrityksen järjestelmiin. (Van der Stock ym. 2007). Usein troijalaiset, virukset ja madot ovat kuitenkin seurausta heikosta viruksentorjunnasta, järjestelmissä olevista tietoturva-aukoista tai muista tekijöistä. Tämän vuoksi näiden uhkien voidaan katsoa olevan enemmänkin ongelman seuraus kuin syy.

Taustajärjestelmäkyselyn rakenteen muutoshyökkäykset, erityisesti SQL-tietokantakyselyn rakenteen muutoshyökkäys (SQL-injektio), ovat tyypillisiä verkkosovelluksiin kohdistuvia hyökkäysmenetelmiä, mahdollistaen hyökkääjälle komentojen ajamisen tai tiedon muuttamisen taustajärjestelmässä. Verkkosivun rakenteenmuutoshyökkäykset (XSS, Cross-site scripting) voivat myös haavoittaa verkkosovelluksia. Näissä hyökkäyksissä voidaan muuttaa esimerkiksi selaimessa sivuston ulkoasua tai kaapata sivuston istunto-tunnisteita. (Van der Stock ym. 2007). Ohjelmistovuokrauksen verkkosovelluskeskeisyydestä johtuen kaikkien edellä mainittujen hyökkäysmenetelmien voidaan katsoa aiheuttavan ohjelmistovuokrauksessa ylimääräisen tietoturvauhkan.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
VERKKOYMPÄRISTÖN TIETOTURVAUHKIA		
Haitallinen koodi/tiedosto/hyökkäykset verkkosivujen haavoittuviin osiin		
Takaovet järjestelmissä	(Abbas ym. 2005), (Van der Stock & Williams & Wichers 2007)	Ei poikkea mallien välillä
Troijalaiset	(Landwehr & Bull & McDermott & Choi 1994), (Weber & Karger & Paradkar 2005), (Savolainen & Niemelä & Savola 2007) (Abbas ym. 2005), (Van der Stock & Williams & Wichers 2007), (Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Mahdollinen lisääntynyt riski
Virukset, Madot	(Landwehr & Bull & McDermott & Choi 1994), (Weber & Karger & Paradkar 2005), (Savolainen & Niemelä & Savola 2007), (Abbas ym. 2005), (Van der Stock & Williams & Wichers 2007), (Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Mahdollinen lisääntynyt riski
SQL-injektio	(Abbas ym. 2005), (Van der Stock & Williams & Wichers 2007), (Vajjhala & Ross & Shah & Gadkari & Gonsalves 2007), (Huang & Huang & Lin & Tsai 2003), (Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Mahdollinen lisääntynyt riski

Cross-site scripting ja selaimen ohjelmointi XSS hyökkäyksillä	(Abbas ym. 2005), (Van der Stock & Williams & Wichers 2007), (Shanmugam & Ponnavaikko 2007), (Huang & Huang & Lin & Tsai 2003), (Northcutt & Skoudis & Sachs & Ullrich & Liston & Cole & Schultz & Dhamankar & Yoran & Schmidt & Pelgrin & Paller 2008)	Mahdollinen lisääntynyt riski
Haitallisen tiedoston suoritus (Esimerkiksi sähköpostin kautta avattu saastunut linkki.)	(Van der Stock & Williams & Wichers 2007)	Ei poikkea mallien välillä

TAULUKKO 9 Tunnistustoimintojen ja menettelytapojen voittaminen osana verkkoympäristön tietoturvauhkia

Protokollahyökkäykset voidaan nostaa verkkoympäristön tietoturvauhkista yhdeksi haasteellisimmista uhkatekijäksi. Protokollahyökkäyksistä tunnetuin lienee DdoS hyökkäys eli palvelunestohyökkäys. Myös IP-osoitteiden varastamisen ja kaappauksen voidaan katsoa kuuluvan protokollahyökkäysten piiriin. Protokollahyökkäyksistä varsinkin palvelunestohyökkäys voidaan katsoa ohjelmistovuokrauksen kannalta hyvin vakavaksi uhkatekijäksi. Palvelunestohyökkäyksessä verkkopalvelu lamautetaan niin, ettei palvelu ole enää käytettävissä. Palvelunestohyökkäys eroaa muista hyökkäyksistä siten, että siinä tavoitteena ei ole järjestelmään tunkeutuminen, vaan järjestelmän toiminnan häiritseminen tai estäminen. (Abbas ym. 2005), (Savolainen ym. 2007), (Wang & Wang, 2003). Ohjelmistovuokrauksen näkökulmasta yksikin onnistunut palvelunestohyökkäys lamauttaisi mahdollisesti lukuisten käyttäjien sovellusten käytön yhtäaikaisesti ja aiheuttaisi mittavia liiketoiminnallisia vahinkoja. Taulukossa 10 esitellään protokollahyökkäyksiä, kirjallisuuslähteitä sekä verrataan protokollahyökkäysten painoarvoa ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
VERKKOYMPÄRISTÖN TIETOTURVAUHKIA		
Protokollahyökkäyset		
DDoS-hyökkäykset	(Abbas ym. 2005), (Savolainen & Niemelä & Savola 2007), (Wang & Wang 2003)	Mahdollinen lisääntynyt riski
IP-osoitteiden varastaminen	(Abbas ym. 2005)	Mahdollinen lisääntynyt riski
IP-osoitteiden kaappaus	(Abbas ym. 2005)	Mahdollinen lisääntynyt riski

TAULUKKO 10 Protokollahyökkäykset osana verkkoympäristön tietoturvauhkia

4.1.4 Muut ohjelmistovuokrauksen tietoturvauhat

Viitekehystä varten oli tärkeää löytää myös ne olemassa olevat ohjelmistovuokrauksen uhkatekijät, joita kirjallisuudessa on mainittu. Keskeisimmiksi tämän osa-alueen lähteiksi muodostui Balachandra ym. (2009), Rittinghouse (2009) ja Brodkin (2008). Kussakin lähteessä käsiteltiin kansainvälisen ICT- alan tutkimus- ja konsultointiyrityksen, Gartnerin muodostamaa listausta ohjelmistovuokraukseen kohdistuvista muista tietoturvauhista. Näitä uhkatekijöitä käsiteltiin tarkemmin kappaleessa 3.3..

Taulukossa 11 kuvataan ohjelmistovuokraukseen kohdistuvia muita tietoturvauhkia erillisoikeutettujen käyttäjien näkökulmasta. Erillisoikeutetut käyttäjät ovat ohjelmistovuokrauksen näkökulmasta monesti varsin hankala uhkatekijä, sillä asiakkailla ei käytännössä ole mahdollisuutta tietää ketkä pääsevät lukemaan, muokkaamaan ja poistamaan heidän tietojansa. Hankalaksi

tämän uhkan tekee lisäksi se, ettei asiakkailla ole mitään takeita siitä, mitä nämä erillisoikeutetut käyttäjät tekevät saamillaan tiedoilla vaihtaessaan esimerkiksi työpaikkaa. Lisäksi asiakkaat eivät voi muuta kuin luottaa palveluntarjoajaan ja siihen ettei kellään ulkopuolisella ole mahdollisuutta päästä käsittelemään asiakkaan tiedostoja.

Asiakaskohtaisiin ohjelmistoihin verratessa erillisoikeutettujen käyttäjien uhan voidaan siis katsoa olevan lievästi suurempi ohjelmistovuokrauksen tapauksessa. Asiakaskohtaisissa ohjelmistoissahan yritys on aina tietoinen siitä, keillä kaikilla on valtuutus lukea, muokata tai poistaa tietoja. Toisaalta asiakaskohtaisten ohjelmistojenkaan tapauksessa ei yritys voi olla tietoinen siitä miten nämä valtuutetut henkilöt säilyttävät vaitiolovelvollisuutensa vaihtaessaan työpaikkaa tai siirtyessään toisiin työtehtäviin.

UHAT	**LÄHDE**	**OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT**
MUITA OHJELMISTOVUOKRAUKSEN TIETOTURVAUHKIA		
Erillisoikeutetut käyttäjät		
Yrityksen dataan pääsee erillisoikeutettujen käyttäjien lisäksi muita käyttäjiä	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski
Palvelun ylläpitäjien oikeudet lukea, muokata ja poistaa dataa	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski

TAULUKKO 11 Erillisoikeutetut käyttäjät osana ohjelmistovuokrauksen muita tietoturvaongelmia

Myös sääntöjen noudattamatta jättämisen voidaan katsoa olevan mahdollinen lisääntyvä riski ohjelmistovuokrauksessa, mikäli kommunikaatio ei toimi asiakkaan ja palveluntarjoajan välillä. Ulkoistaessaan tietojenkäsittelyään yritysten tulisikin keskustella palveluntarjoajan kanssa siitä, mitä tietoturvastandardeja he käyttävät, kuinka usein niitä auditoidaan sekä sopia yksityiskohtaisesti palveluntasosopimuksesta. Asiakaskohtaisissa ohjelmistoissa yritys joutuu hoitamaan kaiken tämän itse ja vastaamaan siitä, että tietoturva on ajan tasalla. Taulukko 12 kuvaa sääntöjen noudattamatta jättämisen riskejä sekä vertailee uhkia suhteessa asiakaskohtaisiin ohjelmistoihin.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
MUITA OHJELMISTOVUOKRAUKSEN TIETOTURVAUHKIA		
Sääntöjen noudattamatta jättäminen		
Palveluntarjoaja ei noudata tietoturvastandardeja	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski
Palveluntarjoaja ei noudata SLA-sopimusta	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009)	Mahdollinen lisääntynyt riski

TAULUKKO 12 Sääntöjen noudattamatta jättäminen osana ohjelmistovuokrauksen muita tietoturvaongelmia

Muista ohjelmistovuokrauksen tietoturvaongelmista datan sijainnin ja eristämisen voidaan katsoa olevan ohjelmistovuokrauksen yksistä haasteellisimmista uhkatekijöistä. Datan sijainti ja eristäminen tekevät myös

suurimman eroavaisuuden ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä, sillä ohjelmistovuokrauksessa asiakkailla ei ole täyttä kontrollia omaan dataansa. Monesti datan varastointi tapahtuu ohjelmistovuokrauksessa oman organisaation ulkopuolisilla palvelimilla ja joskus jopa maiden rajojen ulkopuolella. Lisäksi nämä palvelimet sisältävät usein monien asiakkaiden tietoja kerralla. Tämä aiheuttaa asiakkaille luontaisen tietoturvariskin. Taulukossa 13 kootaan yhteen datan sijaintiin ja eristämiseen liittyviä ohjelmistovuokrauksen muita tietoturvauhkia, esitellään käytettyjä kirjallisuuslähteitä sekä vertaillaan havaittuja uhkia asiakaskohtaisten ohjelmistojen kanssa.

UHAT	**LÄHDE**	**OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT**
MUITA OHJELMISTOVUOKRAUKSEN TIETOTURVAUHKIA		
Datan sijainti ja eristäminen		
Data käsitellään ja varastoidaan oman organisaation ulkopuolella	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski
Dataa ei eristetä muiden asiakkaiden datasta	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski
Datan eristämisessä ei käytetä päivitettyjä salausalgoritmejä	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski

TAULUKKO 13 Datan eristäminen osana ohjelmistovuokrauksen muita tietoturvaongelmia

Huonosti elpyminen virhetilanteista nousee ohjelmistovuokrauksessa tietoturvauhkaksi, mikäli palveluntarjoajalla ei ole kopioita asiakkaiden datasta tai sovellusarkkitehtuurista ja näin ollen ei kykene tekemään täydellistä järjestelmän palautusta. Palveluntasosopimus on ainoa laillinen dokumentti jolla tämän tason uhkia voidaan ainakin teoriassa välttää. Tämän tason uhkia esitellään lähteineen ja asiakaskohtaisiin ohjelmistoihin verraten taulukossa 14.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
MUITA OHJELMISTOVUOKRAUKSEN TIETOTURVAUHKIA		
Huono elpyminen virhetilanteista		
Palveluntarjoajalla ei ole kopioita datasta ja sovellusarkkitehtuurista	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski
Palveluntarjoaja ei kykene tekemään täydellistä järjestelmän palautusta virhetilanteessa	(Balachandra & Ramakrishna & Atanu 2009), (Rittinghouse 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski

TAULUKKO 14 Elpyminen virhetilanteissa osana ohjelmistovuokrauksen muita tietoturvaongelmia

Muista ohjelmistovuokrauksen tietoturvauhkista Balachandra ym. (2009) ja Brodkin (2008) esittelevät huonon tutkimuksellisen tuen. Tällä tarkoitetaan sitä, että palveluntarjoaja ei kykene tutkimaan palvelun laitonta käyttöä, mikäli hyökkääjä pääsee järjestelmiin joillakin hyökkäysmenetelmillä käsiksi. Sekä ohjelmistovuokrauksessa, että asiakasohjelmistoissa tämän havaitseminen

vaatii asiantuntijatasoisia palvelunylläpitäjiä sekä yrityksen kykyä reagoida näihin hyökkäyksiin. Varsinkin suuremmilla ohjelmistovuokrausta tarjoavista palveluntarjoajista on kuitenkin usein huomattavasti paremmat resurssit estää näitä hyökkäyksiä kuin esimerkiksi joillakin pienillä tai keskisuurilla ohjelmistovuokrausta käyttävillä yrityksillä. Tämän vuoksi tämän uhkan voidaan katsoa olevan jopa isompi asiakaskohtaisten ohjelmistojen piirissä. Taulukko 15 esittää huonon tutkimuksellisen tuen uhkaa.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
MUITA OHJELMISTOVUOKRAUKSEN TIETOTURVAUHKIA		
Huono tutkimuksellinen tuki		
Palveluntarjoaja ei kykene tutkimaan laitonta palvelun käyttöä	(Balachandra & Ramakrishna & Atanu 2009), (Brodkin 2008)	Suurempi asiakaskohtaisissa ohjelmistoissa

TAULUKKO 15 Tutkimukselliseen tukeen liittyviä muita ohjelmisto-vuokrauksen tietoturvaongelmia

Viimeisenä ohjelmistovuokraukseen kohdistuvana muuna uhkana Balachandra ym. (2009) ja Brodkin (2008) esittelevät huonon pitkäaikaisen toiminta-kelpoisuuden. Tällä tarkoitetaan sitä, että data ei pysy saatavilla palvelun-tarjoajan lopettaessa toimintansa, palveluntarjoaja ei pysty lähettämään dataa takaisin asiakkaille tai palveluntarjoajalla ei ole varasuunnitelmia. Asiakas-kohtaisiin ohjelmistoihin verratessa nämä aiheuttavat asiakkaille ylimääräisen uhkan, sillä asiakkaat eivät voi koskaan olla varmoja siitä, kuinka kauan kyseinen palveluntarjoaja on olemassa. Tämän vuoksi yritysten tulisikin tarkoin

punnita, onko heillä resursseja hoitaa tietojenkäsittelyään itse. Taulukossa 16 kootaan yhteen huonoon pitkäaikaiseen toimintakelpoisuuteen liittyviä tietoturvaongelmia, vertaillaan uhkia asiakaskohtaisten ohjelmistojen kanssa sekä esitellään kirjallisuuslähteitä.

UHAT	LÄHDE	OHJELMISTOVUOKRAUS VS. ASIAKASKOHTAISET OHJELMISTOT
MUITA OHJELMISTOVUOKRAUKSEN TIETOTURVAUHKIA		
Huono pitkäaikainen toimintakelpoisuus		
Data ei pysy saatavilla, palveluntarjoajan lopettaessa toimintansa	(Balachandra & Ramakrishna & Atanu 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski
Palveluntarjoaja ei pysty lähettämään dataa takaisin asiakkaille	(Balachandra & Ramakrishna & Atanu 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski
Palveluntarjoajalla ei ole varasuunnitelmia	(Balachandra & Ramakrishna & Atanu 2009), (Brodkin 2008)	Mahdollinen lisääntynyt riski

TAULUKKO 16 Pitkäaikaiseen toimintakelpoisuuteen liittyviä muita ohjelmistovuokrauksen tietoturvaongelmia

4.2 Viitekehys ohjelmistovuokrauksen tietoturvaongelmista

Kerätyn lähdeaineiston osalta voidaan havaita, että ohjelmistovuokraukseen liittyviä uhkia on olemassa paljon. Koska tutkielman kannalta ei kuitenkaan ollut olennaista muodostaa viitekehystä, jossa lueteltaisiin kaikki ohjelmisto-

vuokraukseen löyhästikin liittyvät tietoturvaongelmat, oli järkevämpää muodostaa lista, joka olisi huomattavasti lyhyempi mutta kattaisi kuitenkin suurimman osan kirjallisuudesta havaituista ongelmista. Lisäksi viitekehyksen tuli olla myös mahdollisimman selkeä, jotta sitä voitaisiin testata empiirisessä kyselytutkimuksessa.

Viitekehyksen luomisessa keskeisessä roolissa toimivat aiemmin tehdyt havainnot, joiden mukaan fyysiset uhat, ohjelmistojen uhat, verkkoympäristön uhat sekä muut ohjelmistovuokrauksen uhat vaikuttavat keskeisimmin ohjelmistovuokraukseen. Näissä kategorioissa havaittiin kuitenkin paljon päällekkäisyyttä eri uhkien osalta. Tämän vuoksi uhkille oli tarpeen muodostaa uusi luokitus, jotta ohjelmistovuokrauksen tietoturvaongelmat voitaisiin kattaa paljon tiiviimmin. Uhkakategorioita ja eri uhkia yhdistelemällä voitiin havaita, että kolme keskeisintä ohjelmistovuokraukseen vaikuttavaa tekijää tietoturvan näkökulmasta olivat:

1) ohjelmistojen ja verkkoselainten tietoturva
2) tietoverkon tietoturva
3) monikäyttäjäarkkitehtuurin tietoturva

Ohjelmistojen ja verkkoselainten tietoturva on yksi merkittävin ohjelmisto-vuokraukseen vaikuttavasta tekijästä, koska ohjelmistovuokrauksen periaatteella valmistetut ohjelmistot toimivat pääsääntöisesti eri verkko-selainten välityksellä. Tästä johtuen näihin ohjelmistoihin ja selaimiin kohdistuvat ongelmat näkyvät erityisesti juuri ohjelmistovuokrauksessa. Tietoverkon tietoturva on perusteltua ottaa lopulliseen viitekehykseen siitä syystä, että ohjelmistovuokrauksen toiminta perustuu verkon yli tapahtuvaan

tietojenkäsittelyyn. Ilman toimivia ja turvallisia tietoliikenneyhteyksiä, ei ohjelmistovuokrauskaan voisi koskaan toimia. Monikäyttäjäarkkitehtuurin tietoturva viittaa puolestaan kaikkiin muihin uhkatekijöihin, jotka muodostuvat asiakkaiden luovuttaessa tietoresurssinsa toisen osapuolen haltuun ja säilyttäessään niitä datapalvelimilla yhdessä muitten asiakkaiden kanssa. Yhdessä nämä kolme kategoriaa kattavat ison osan ohjelmistovuokraukseen vaikuttavista tietoturvaongelmista. Taulukossa 17 esitellään ohjelmistovuokrauksen tietoturvaongelmien viitekehys.

OHJELMISTOJEN JA VERKKOSELAINTEN TIETOTURVAONGELMAT
Selainten ja ohjelmistojen tietoturva-aukot
Selainten ja ohjelmistojen virhetilanteissa vuotavat tiedot
TIETOVERKON TIETOTURVAONGELMAT
Tietoliikenteen paljastuminen sellaisille tahoille, joille ko. tieto ei kuulu
Palvelunestohyökkäykset
troijalaiset, virukset, madot
MONIKÄYTTÄJÄARKKITEHTUURIN TIETOTURVAONGELMAT
Data käsitellään ja varastoidaan oman organisaation ulkopuolella
Dataa ei eristetä riittävän tehokkaasti muiden asiakkaiden datasta
Data ei pysy saatavilla virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa

TAULUKKO 17, Ohjelmistovuokrauksen tietoturvaongelmien viitekehys

Ohjelmistoihin ja verkkoselaimiin kohdistuvista tietoturvaongelmista voidaan havaita, että kaikki näihin liittyvistä ongelmista ja hyökkäyksistä juontavat juurensa ohjelmassa tai selaimessa oleviin tietoturva-aukkoihin. Olipa tällaisiin sovelluksiin kohdistuva hyökkäys toteutettu millä menetelmällä tahansa, käytetään hyökkäyksessä aina hyväksi hyökkäyksen kohteeksi joutuneen sovelluksen haavoittuvia osia. Voidaankin huomata, ettei varsinaisena

tietoturvaongelmana ole siis hyökkäys itse, vaan ohjelmistoon tai verkkoselaimeen jääneet tietoturva-aukot kooditasolla.

Toinen keskeinen ohjelmistoihin ja verkkoselaimiin kohdistuva ongelma on ohjelmiston tai selaimen virhetilanteissa vuotavat tiedot. Ei ole kovinkaan epätavallista, että virhetilanteen sattuessa, saattaa näytölle ilmaantua virhetilanteeseen johtanut syy. Tällainen ilmoitus voi pahimmillaan kuitenkin paljastaa järjestelmän heikkouksia, joita hakkerit tai muut epäsuotuisat käyttäjät voivat käyttää hyväksi.

Tietoverkon tietoturvaongelmien tarkastelussa ja uhkatekijöiden yhdistelyssä keskeisintä oli löytää jokin yhdistävä linkki tietoverkon ongelmatekijöiden muodostumiselle. Kerätyn datan pohjalta tällainen linkki on tietoliikenteen paljastuminen epäsuotuisille tahoille. Toinen keskeinen uhkatekijä tietoverkon näkökulmasta on palvelunestohyökkäykset järjestelmää tai ohjelmistoa vastaan. Palvelunestohyökkäykset ovat ohjelmistovuokrauksen tietoturvan näkökulmasta yksi vakavimmista uhkatekijöistä, sillä asiakkaat eivät voi käyttää ohjelmistoja mikäli palvelu ei ole saatavilla. Palvelunestohyökkäysten onnistuminen näkyy myös heti eikä sitä voi peitellä. Palvelunestohyökkäykset aiheuttavat suurinta tuhoa niin asiakkaille, kuin palveluntarjoajillekin.

Monikäyttäjäarkkitehtuurin keskeisin tietoturvaongelma on siinä, että data käsitellään ja varastoidaan oman organisaation ulkopuolella. Tämä muodostaa luontaisen uhan koska tällöin yritysten ”oma kontrolli” dataan pienenee. Toinen ongelma kohdistuu tietojen tallennukseen ja eristämiseen usein maantieteellisestikin erillään olevissa datapalvelimissa. Keskeisenä huolenaiheena tässä on tietojen eristäminen muiden asiakkaiden datasta. Kolmas tietoturvaongelma liittyy puolestaan palvelun saatavuuteen virhetilanteissa tai palveluntarjoajan lopettaessaan toimintansa. Mikäli palveluntarjoaja ei pysty palauttamaan asiakkaan tietoja halutussa muodossa ja formaatissa, herää usein

huoli siitä, minne tiedot päätyvät. Tämänkaltaiset ongelmat vaikuttavat suoranaisesti palvelujen saatavuuteen ja tietojen eheyteen.

5 KYSELYTUTKIMUS OHJELMISTOVUOKRAUKSEN TIETOTURVAONGELMISTA

Tässä luvussa tarkastellaan kyselytutkimusta ohjelmistovuokrauksen tietoturvaongelmista. Kyselytutkimuksessa testattiin kuinka merkittävinä uhkina vastaajat pitävät kirjallisuuskatsauksen pohjalta rakennetun viitekehyksen tietoturvaongelmia. Kyselytutkimukseen vastasi useita ICT- alan tietoturva-asiantuntijoita. Ensimmäiseksi esitellään kyselytutkimuksen kulkua ja lähtökohtia. Tämän jälkeen käydään läpi kyselytutkimuksesta saatuja tuloksia.

5.1 Tutkimuksen kulku ja lähtökohdat

Tämän tutkielman keskeisimpänä tarkoituksena oli löytää ne tietoturvaongelmat, jotka ovat oletettavasti suurempia ohjelmistovuokrauksessa kuin asiakaskohtaisissa ohjelmistoissa. Lisäksi tutkimuksessa oli tarkoitus vertailla havaittuja tietoturvaongelmia ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä sekä selvittää ovatko havaitut tietoturvaongelmat merkittäviä ja todellisuudessa suurempia ohjelmistovuokrauksessa. Jälkimmäistä ongelmaa varten muodostettiin kyselytutkimus, jonka lähtökohtana työssä oli aihealueen laajan kirjallisuuskatsauksen tuotoksena syntynyt viitekehys ohjelmistovuokrauksen oletettavasti merkittävimmistä tietoturvaongelmista. (Liite 1). Kyselytutkimus suoritettiin harkintaotantaa käyttäen, joka Robsonin (1994) mukaan perustuu tutkijan näkemykseen vastaajien kiinnostavuudesta. Tutkittavina kohteina olivat suomalaiset ICT-alan yrityksissä työskentelevät tietoturva-alan asiantuntijat, joilla on tietämystä ohjelmistovuokrauksesta ja niihin kohdistuvista ongelmakohdista.

Tutkimusaineisto kerättiin huhti- ja toukokuun 2010 aikana. Tutkimusta varten luotiin kyselylomake, jossa kysyttiin viitekehykseen kerättyjen tietoturva-ongelmien merkitystä ohjelmistovuokrauksessa. Kyselylomakkeessa vastaajia

pyydettiin myös arvioimaan ja vertailemaan kutakin ongelmaa ohjelmisto-vuokrauksen ja asiakaskohtaisten ohjelmistojen välillä. Saatujen vastausten pohjalta voitiin karkeasti arvioida tietoturvaongelmien merkitystä kahdessa toimitusmallissa.

Lomaketta muodostettaessa pääpaino oli sen käytettävyydessä ja selkeydessä. Tällä pyrittiin varmistamaan se, ettei vastaajan tarvitsisi käyttää aikaa lomakkeen opetteluun ja että vastaaminen olisi mahdollisimman helppoa. Lomakkeessa kysyttiin aluksi taustakysymyksiä, joissa vastaajaa pyydettiin kertomaan yrityksensä nimi ja toimiala, kuinka isosta organisaatiosta on kyse ja millainen on vastaajan asema tässä organisaatiossa. Tämän jälkeen vastaajaa pyydettiin arvioimaan viitekehyksen tietoturvaongelmia sekä perustelemaan vastaukset kysymysten alla olevaan tyhjään tilaan. Ohjelmistovuokrauksen tietoturvaongelmien viitekehys esiteltiin kappaleessa 4.2.

Ennen kyselylomakkeen lähettämistä vastaajille lomaketta testattiin neljällä aihealuetta tuntemattomilla henkilöillä ja yhdellä aihealuetta tietävällä henkilöllä. Tällä tavoin pyrittiin varmistamaan, että lomake olisi mahdollisimman selkeä ja siten maksimoisi vastausten määrän. Testauksesta saatujen muutosehdotusten pohjalta lomaketta muokattiin vielä käyttäjä-ystävällisemmäksi. Testaus suoritettiin iteroiden, useassa vaiheessa.

Kyselylomake lähetettiin vastaajille aluksi sähköpostin liitetiedostona Excel-taulukkona. Tämä kyselytapa ei kuitenkaan saanut aikaan haluttua vastausmäärää, tuottaen ainoastaan yhden vastauksen avoimine perus-teluineen. Alhaisen vastausmäärän ja lomakkeen huonon käytettävyyden johdosta kyselylomakkeesta päädyttiin muodostamaan sähköinen lomake Internetiin. Lomakkeessa oli asteikollisia ja avoimia kysymyksiä ohjelmisto-vuokraukseen kohdistuvista tietoturvaongelmista.

Paranneltu kyselylomake lähetettiin OWASP:n *(Open Web Application Security Project)* suomenkieliselle sähköpostilistalle, jolle kuuluu arviolta 150 henkilöä.

OWASP on verkkosovelluksien tietoturvaan keskittynyt kansainvälinen vapaaehtoisjärjestö, jonka tarkoituksena on perehdyttää ohjelmistokehittäjät, suunnittelijat, arkkitehdit ja organisaatiot ymmärtämään sovellushaavoittuvuuksien seurauksia. Kokemusteni pohjalta ja eräältä Suomen johtavassa ohjelmistoyrityksessä työskentelevältä tietoturva-asiantuntijalta saamani lausunnon mukaan OWASP:n sähköpostilista olikin lähes ainut väylä tavoittaa kerralla Suomen ohjelmistovuokrauksen asiantuntijat.

Tutkimusaineiston keruussa kyselytutkimus laitettiin 27.4.2010 owasp-helsinki@lists.owasp.org sähköpostilistalle saatekirjeen kanssa. Saatekirjeessä motivoitiin vastaajaa osallistumaan kyselytutkimukseen sekä esiteltiin tutkimuksen aihepiiri. Palautusaika vastauksilla oli 7.5.2010 mennessä. Vastauksia saatiin ensimmäisellä kerralla yhteensä neljä kappaletta. Kyselytutkimuksen muistutusviesti lähetettiin 10.5.2010, jonka jälkeen vastauksia saatiin neljä kappaletta lisää.

Yhteensä tässä tutkimuksessa suoritetut kyselyt tuottivat yhdeksän vastausta avoimine vastauksineen. Havaittiin, että sähköinen lomake paransi huomattavasti vastausmäärää ja suurin osa vastauksista oli myös perusteltuja. Myös ensimmäisellä kierroksella Excel taulukon avulla saatu vastaus päädyttiin säilyttämään lopullisten vastausten joukossa ja osana tutkimusta, sillä vastaukset olivat pääasiallisesti perusteltuja.

Tutkimuksen kannalta merkittävimmiksi vastaajien ominaisuuksiksi nousi heidän asemansa kotiorganisaatioissaan. Vastaajien keskuudesta löytyi niin toimitusjohtajia, asiantuntijoita kuin konsultteja, joista jokainen oli tietoturva-alan ammattilainen. Kullakin vastaajalla katsottiin olevan hyvä tietämys ohjelmistovuokrauksesta ja siihen kohdistuvista tietoturvaongelmista. Yritysten koko vaihteli aina yhdestä työntekijästä kuuteensataan työntekijään. Taulukko 18 kokoaa vastaajat ja vastaajien keskeiset ominaisuudet yhteen.

YRITYS JA TOIMIALA	YRITYKSEN KOKO	VASTAAJAN ASEMA ORGANISAATIOSSA
Ohjelmistojen suunnittelun ja valmistuksen pienyritys	1 henkilö	Toimitusjohtaja
ICT-alan konsultointi-, projekti- ja ulkoistamispalvelujen pienyritys	5 henkilöä	Toimitusjohtaja
Tietoturvakonsultoimiseen keskittynyt yritys	Ei tietoa	Tietoturvakonsultti
Ei tietoa (anonyymi)	123 henkilöä	Tietoturva-asiantuntija
Tietoturvakonsultoimisen pienyritys	1 henkilö	Toimitusjohtaja/ tietoturvakonsultti
Tietoturvaan keskittynyt PK-yritys	85 henkilöä	Tietoturvakonsultti
Yritysneuvonta	600 henkilöä	Tietoturva-asiantuntija
ICT-alan konsultointiyritys	400 henkilöä	Riskienhallintakonsultti
Telekommunikaatioalan PK-yritys	35 M€	Toimitusjohtaja

TAULUKKO 18 Kyselytutkimuksen vastaajat ja vastaajien keskeiset ominaisuudet

5.2 Tutkimuksen tulokset

Kyselytutkimuksen ensimmäisessä osassa vastaajaa pyydettiin arvioimaan kutakin tietoturvaongelmaa asteikolla: merkittävä, ei merkittävä. Kahtiajaon tarkoituksena oli saada karkea kuva siitä mitkä tietoturvaongelmat nousevat eniten esiin sekä helpottaa tulosten käsittelyä. Toisessa osassa vastaajaa

pyydettiin arvioimaan uhkien painoarvoa suhteessa asiakaskohtaisiin ohjelmistoihin. Seuraavaksi esitellään saatuja tuloksia.

5.2.1 Selainten ja ohjelmistojen tietoturva-aukot

Kysymyksessä yksi kysyttiin kuinka merkittävänä ongelmana vastaajat kokevat selainten ja ohjelmistojen tietoturva-aukot ohjelmistovuokrauksessa. Valtaosa vastaajista (78%) piti näitä ongelmia merkittävinä uhkina. Yleinen selitys näiden uhkien merkittävyydelle oli, että selaimiin ja verkko-ohjelmistoihin jää usein niiden kehitysvaiheessa suhteellisen paljon tietoturva-aukkoja ja näiden kautta hyökkääjät pystyvät rikkomaan tiedon luottamuksellisuuden, eheyden ja saatavuuden. Suurin osa vastaajista pitikin selainten roolia yhtenä merkittävimpänä osana ohjelmistovuokrauksen ilmiötä ja palvelun käyttöä.

Osa vastaajista oli kuitenkin sitä mieltä, että vaikka verkkoselaimet ovat iso osa ohjelmistovuokrausta, ovat hyökkäykset tänä päivänä siirtymässä yhä enenevässä määrin verkkosovelluksiin ja asiakaspuolelle. Tämä perusteltiin siten, että selainkäyttöisten sovellusten haavoittuvuudet eivät kohdistu selaimiin vaan pikemminkin ohjelmistoon itseensä. Sovellusvikojen kautta voidaan aiheuttaa myös merkittäviä riskejä liiketoiminnalle.

Ensimmäisessä kysymyksessä noin viidesosa vastaajista (22%) vastaajista ei pitänyt selainten ja ohjelmistojen tietoturva-aukkoja merkittävinä. Yhtenevä selitys tähän oli siinä, että keskitetyssä palveluntarjonnassa uhka on paremmin hallittavissa ja tietoturva-aukkoihin pystytään reagoimaan nopeammin. Tämän vuoksi uhka on aina olemassa, mutta se ei ole niin suuri, että se haittaisi ohjelmistovuokrauksen turvallisuutta ja toimivuutta.

Kaksi kolmasosaa vastaajista (67%) arvioi myös selainten ja ohjelmistojen tietoturva-aukkojen olevan suurempi ongelma kuin asiakaskohtaisissa ohjelmistoissa. Huomattavin yhteinen selitys vastauksissa oli se, että ohjelmistovuokrattuihin sovelluksiin pääsee julkisen Internetin kautta. Mikäli

jaetussa ympäristössä, verkkosovelluksissa tai järjestelmissä on heikkouksia, on suurempi riski joutua hyökkäyksen kohteeksi. Ohjelmistovuokratussa palvelussa on monesti myös isompi käyttäjäkunta, mikä luo mahdollisesti hyökkääjille mielenkiintoisemman hyökkäyskohteen.

Noin viidesosa vastaajista (22%) piti selainten ja ohjelmistojen tietoturva-aukkoja puolestaan yhtä suurena ongelmana asiakaskohtaisten ohjelmistojen kanssa. Tämä selitettiin siten, että kaikki käyttävät selaimia tänä päivänä surffatessaan myös vähemmän turvallisilla sivustoilla. Se, että selaimia käytetään myös ohjelmistovuokrauksessa, ei vaikuta ohjelmistovuokrauksen turvallisuuteen sen enempää, kuin asiakaskohtaisissa ohjelmistoissakaan.

5.2.2 Selainten ja ohjelmistojen virhetilanteissa vuotavat tiedot

Kysymyksessä kaksi kysyttiin kuinka merkittävänä ongelmana vastaajat kokevat selainten ja ohjelmistojen virhetilanteissa vuotavia tietoja. Noin puolet vastaajista (55%) piti tätä ongelmaa merkittävänä uhkana. Selainten ja ohjelmistojen virhetilanteessa vuotavien tietojen uhkan merkittävyyttä perusteltiin siten, että selainten vuotama virhetieto ei ole tyypillisesti merkityksellistä, mutta sovellusten virhetilanteissa vuotamat tiedot puolestaan ovat. Pahimmillaan sovellukset voivatkin vuotaa salasanoja tai muuta henkilökohtaista ja liiketoimintakriittistä informaatiota.

Lähes puolet vastaajista (45%) ei pitänyt selainten ja ohjelmistojen virhetilanteissa vuotavia tietoja kuitenkaan merkittävänä uhkana ohjelmisto-vuokrauksessa. Havaittava selitys tälle oli se, että virhetilanteissa saadaan usein tietoa vain ohjelmiston tai palvelun tekotavasta. Harvemmin virhetilanteet paljastavat mitään sellaista tietoa, joka olisi liiketoiminnan kannalta merkittävää. Havaittavaa vastauksissa oli myös se, että vaikka tätä uhkaa ei pidetä kovin merkittävänä, ei uhkan mahdollisuutta voi myöskään sulkea täysin pois.

Yli puolet vastaajista (55%) piti ohjelmistojen virhetilanteissa vuotavia tietoja myös suurempana uhkana kuin asiakaskohtaisissa ohjelmistoissa. Vastaukset perusteltiin siten, että koska asiakaskohtaisissa ohjelmistoissa järjestelmiä käyttää vain yksi asiakas ja ohjelmistovuokrauksessa useat eri asiakkaat, voivat virheilmoitukset paljastaa enemmän informaatiota ja vaarantaa usean asiakkaan tiedot kerralla. Noin kolmasosa vastaajista (33%) arvioi tämän uhkan olevan yhtä suuri asiakaskohtaisten ohjelmistojen kanssa. Ainoastaan yksi vastaaja piti uhkaa pienempänä. Perusteluja näille vastauksille ei saatu.

5.2.3 Tietoliikenteen paljastuminen epäsuotuisille tahoille

Kysymyksessä kolme vastaajilta kysyttiin tietoliikenteen paljastumisen merkitystä ohjelmistovuokrauksen tietoturvan kannalta. Kysymyksen kolme osalta noin kolmasosa vastaajista (33%) piti tätä merkittävänä uhkana. Tämän uhkan merkittävyyttä perusteltiin siten, että tietoliikenteen paljastuessa voidaan saada käyttäjätunnuksia, salasanoja, istuntotunnisteita ja muuta tärkeää informaatiota. Toisaalta suurin osa ohjelmistoista käyttää sovellusliikenteen salausta (SSL/TLS), joten vastaajien kesken tämänkin riskin nähtiin olevan hallinnassa.

Suurin osa vastaajista (67%) pitikin tietoliikenteen paljastumista pienenä uhkana ohjelmistovuokrauksessa. Havaittava yhteneväisyys vastauksissa oli se, että operaattoriverkkoja ei ole kovin helppo päästä salakuuntelemaan, johtuen tämän päivän tehokkaista tietoliikenteen salausmenetelmistä. Kriittistä tietoa on siirretty verkossa muutenkin jo pitkään, joten sen vuoksi uhkan ei koettu vaikuttavan ohjelmistovuokraukseen yhtään suuremmalla painoarvolla kuin muuhunkaan verkon välityksellä tapahtuvaan tiedonsiirtoon.

Suurin osa vastaajista (67%) piti myös tietoliikenteen paljastumista sellaisille tahoille joille ko. tieto ei kuulu suurempana uhkana kuin asiakaskohtaisissa ohjelmistoissa. Yhteinen havaittava selitys oli se, että mikäli tietoliikenne kulkee

julkisessa verkossa, eikä asiakkaan omassa verkossa, on tietoliikenteeseen käsiksi pääseminen ulkopuolisille huomattavasti helpompaa. Lisäksi palveluntarjoajan verkkoon pääsevät työntekijät aiheuttavat ylimääräisen uhan.

Noin viidesosa vastaajista (22%) piti tätä uhkaa puolestaan pienempänä uhkatekijänä, kuin asiakaskohtaisissa ohjelmistoissa. Vastaukset perusteltiin sillä, että asiakaskohtaisissa ohjelmistoissa yhteydet ovat paremmin tiedostettuja ja salattuja. Tämän vuoksi näiden yhteyksien kontrollin aste on huomattavasti parempi kuin ohjelmistovuokrauksessa.

5.2.4 Palvelunestohyökkäykset

Kysymyksessä neljä palvelunestohyökkäykset olivat valtaosan vastaajien (67%) mielestä merkittävä uhka ohjelmistovuokrauksessa. Noin kolmasosa vastaajista (33%) ei puolestaan pitänyt tätä uhkaa kovin merkittävänä.

Yhteinen tämän uhkan merkittävyyttä puoltava selitys oli se, että palvelunestohyökkäyksistä voi koitua suoria taloudellisiakin vaikutuksia, jos palvelu ei ole saatavilla. Varsinkin kuuluisat tai tunnetut palvelut ja asiakkuudet voivat myös houkutella toimijoita iskemään. Huomattavaa vastauksissa oli kuitenkin se, että palvelunestohyökkäysten uhka riippuu monesti liiketoiminnan laadusta. Varsinkin isolla palveluntarjoajalla on monesti paremmat resurssit reagoida palvelunestohyökkäyksiin, sillä isompi asiakasmassa on jakamassa liiketoiminnan kustannuksia.

Liiketoiminnan ja ohjelmistovuokrauspalvelun luonne vaikuttavat myös siihen kuinka merkittävänä palvelunestohyökkäykset vastaajien keskuudessa koettiin. Erään vastaajan mielestä muun muassa pokeripalveluille palvelunesto-hyökkäykset voisivat olla oikeasti suuri uhka, mutta esimerkiksi joillekin kyytienvälityspalveluille uhka ei olisi puolestaan niin merkittävä.

Suurin osa vastaajista (67%) piti myös palvelunestohyökkäyksiä suurempana uhkana kuin asiakaskohtaisissa ohjelmistoissa. Havaittava selitys liittyi siihen, että julkisessa verkossa palvelunestohyökkäykset on huomattavasti helpommin toteutettavissa, kuin asiakkaan omassa verkossa. Usein julkiseen verkkoon palvelunestohyökkäysmielessä käsiksi pääsevän porukan katsotaankin olevan suurempi kuin yritysten sisäisessä verkossa.

Noin viidesosa vastaajista (22%) arvioi kuitenkin palvelunestohyökkäysten olevan pienempi kuin asiakaskohtaisissa ohjelmistoissa. Vastaukset perusteltiin siten, että varsinkin asiakkaan näkökulmasta katsottuna palveluntarjoajilla on huomattavasti paremmat resurssit reagoida palvelunestohyökkäyksiin kuin tilanteessa, jossa yritys yrittäisi selviytyä näistä hyökkäyksistä itse. Keskitetyn ongelmanhallinnan katsotaan olevan myös hyvä asia, jossa palveluntarjoajalle on mahdollisuus saada kunnon tietoliikennekaista ja kuormantasausjärjestelyt.

Ainoastaan yksi vastaaja oli sitä mieltä, että palvelunestohyökkäykset ovat yhtä vakava uhka ohjelmistovuokrauksessa ja asiakaskohtaisten ohjelmistojen käytössä. Vastaaja perusteli väitettään siten, että uhkan vakavuus riippuu aina hyökkäyksen todellisesta kohteesta. Tämän vuoksi ei voida sanoa kumpi edellä mainituista ohjelmistojen hankinnan ja käytön malleista on palvelunestohyökkäysten osalta turvallisempi.

5.2.5 Troijalaiset, virukset ja madot

Kysymyksessä viisi alle puolet vastaajista (44%) piti troijalaisia, viruksia ja matoja, merkittävänä uhkana. Yli puolet vastaajista (56%) piti näitä tietoturvaongelmia puolestaan merkityksettöminä.

Suoraa yhteyttä ohjelmistovuokrauksen avulla toteutetuiden palvelujen sekä troijalaisten, virusten ja matojen välillä ei vastauksista ilmennyt. Sen sijaan työasemilla, joilla näitä palveluita käytetään, uhka koettiin merkittäviksi.

Suurin osa haittaohjelmista asettaakin jonkinlaisen tietojenkeräysohjelman, jonka avulla voidaan kerätä erilaisia tunnisteita ja salasanoja.

Valtaosa vastaajista (67%) piti troijalaisia, viruksia ja matoja yhtä suurena uhkana ohjelmistovuokrauksessa ja asiakaskohtaisten ohjelmistojen käytössä. Vastaajat olivatkin sitä mieltä, että todennäköisesti sillä ei ole merkitystä troijalaisten, virusten ja matojen kannalta, onko palvelu sisä- vai ulkoverkossa. Eräs vastaaja perusteli vastaustaan myös siten, että mikäli haittaohjelma on päässyt ohjelmistoa käyttävän henkilön työasemalle lähettämään tunnisteita ulkopuolisille, on haittaohjelmistossa todennäköisesti myös komentokanava, jolla haittaohjelman saastuttamalla koneella voidaan komentaa tekemään toimenpiteitä yrityksen verkossa. Tämän vuoksi yrityksen sisäverkon suojaukset eivät välttämättä suojaa palvelua yhtään enempää, kuin ohjelmistovuokrauksessa.

Yksi vastaaja oli kuitenkin sitä mieltä, että ohjelmistovuokrausta harjoittavan palveluntarjoajan tunnettavuudella on myös merkitystä siihen, kuinka todennäköisesti tämä palvelu kohtaa ongelmia virusten, matojen ja troijalaisten kanssa. Tunnetulla palveluntarjoajalla saattaakin olla suurempi todennäköisyys joutua haittaohjelman uhriksi kuin räätälöityä ohjelmistoa käyttävällä yrityksellä.

5.2.6 Data käsitellään ja varastoidaan oman organisaation ulkopuolella

Kysymyksessä kuusi kysyttiin kuinka merkittävänä uhkana vastaajat kokevat datan varastoinnin oman organisaation ulkopuolella. Suurin osa vastaajista (78%) piti tätä merkittävänä uhkana.

Suurin huolenaihe vastauksissa oli juuri se, että ohjelmistovuokrauksessa asiakas luovuttaa tietonsa toisen osapuolen haltuun, eikä tieto ole tällöin enää omassa suojatussa ympäristössä. Tämä luonnollisesti aiheuttaa riippuvuuden palveluntarjoajaan ja sen tietoturvatasosta. Ohjelmistovuokraus koettiin

vastauksissa myös hyvin epäkypsäksi muuttuvine käytäntöineen, jossa erilaiset regulaatiot voivat esimerkiksi aiheuttaa ongelmia luottamuksellisen ja salaisen materiaalin osalta.

Vain muutama vastaajista (22%) ei kuitenkaan pitänyt datan käsittelyä organisaation ulkopuolella suurena uhkana. Vastaajat perustelivat vastauksiaan sillä, että tänä päivänä dataa käsitellään joka tapauksessa oman organisaation ulkopuolella. Harva yritys pystyykin todellisuudessa operoimaan kaikkia järjestelmiä omilla laitteilla ja omissa tiloissaan. Erään vastaajan mukaan ongelmia voi kuitenkin syntyä, mikäli palveluntarjoajat eivät vastaa sopimuksellisesti tai toteutuksen puolesta yhtä korkeaa tietoturvatasoa kuin mitä organisaation tekemät sopimukset tai liiketoiminnan tarpeet mahdollisesti edellyttävät.

Valtaosa vastaajista (78%) arvioi datan varastointia oman organisaation ulkopuolella myös suuremmaksi ongelmaksi kuin asiakaskohtaisten ohjelmistojen käytössä. Havaittava yhteneväisyys vastauksissa liittyi siihen, että ohjelmistovuokrauksessa asiakkaalla ei ole näkyvyyttä siihen, miten hänen tietoaan varastoidaan, käsitellään, kuka tietoon pääsee käsiksi ja missä tieto edes fyysisesti sijaitsee. Noin viidesosa vastaajista (22%) arvioi tämän uhkan olevan yhtä suuri asiakaskohtaisten ohjelmistojen kanssa. Perusteluja vastauksille ei kuitenkaan saatu.

5.2.7 Dataa ei eristetä riittävän tehokkaasti muiden asiakkaiden datasta

Melkein kaikki vastaajat (89%) olivat sitä mieltä, että datan heikko eristäminen muiden asiakkaiden datasta kysymyksessä seitsemän oli merkittävä uhkatekijä. Vain yksi vastaaja oli eri mieltä.

Yhtenevä huolenaihe vastauksista oli se, että data usein sisältää liikesalaisuuksia ja sellaista tietoa, jota ei missään olosuhteissa saisi näkyä muille. Esimerkiksi jonkin ohjelmistovirheen vuoksi toisen käyttäjän data voisi

paljastua toiselle käyttäjälle. Liiketoiminnan ja varsinkin kilpailun kannalta tällainen virhe voisi olla hyvin merkittävää. Siksi palveluntarjoajan tulisikin sopimuksin varmistaa, että tällaista ei missään olosuhteissa pääse käymään.

Valtaosa vastaajista (78%) piti myös datan heikkoa eristämistä muiden asiakkaiden datasta suurempana uhkana kuin asiakaskohtaisten ohjelmistojen käytössä. Vastaukset perusteltiin sillä, että asiakaskohtaisissa ohjelmistoissa tallennetaan vain organisaation omaa tietoa, jolloin tietojen sekoittuminen muiden asiakkaiden dataan ei käytönnössä ole edes mahdollista. Toisaalta tietojen vuotaminen ja sekoittuminen firman sisällä käyttäjätasolla voi jossain tapauksissa olla tuhoisaa.

5.2.8 Data ei pysy saatavilla virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa

Viimeisen kysymyksen osalta kaikki vastaajat (100%) vastasivat datan huonon saatavuuden virhetilanteissa tai palveluntarjoajan lopettaessa toimintansa merkittäväksi uhkatekijäksi.

Kysymys nähtiin olevan vastauksissa liiketoiminnan uskottavuuteen ja laatuun liittyvä. Ohjelmistovuokrauksessa palveluntarjoaja hallitsee palvelua ja siellä varastoitua dataa. Mikäli virhetilanteita pääsee käymään tai pahimmillaan palveluntarjoaja menee esimerkiksi konkurssiin, on asiakkaalla vain palvelun-tasosopimuksen mukaiset oikeudet. Vastaajat olivatkin sitä mieltä, että tämän vuoksi datan saatavuus tulisi ottaa huomioon jo järjestelmää rakentaessa ja sopimuksen sanktio- ja takuujärjestelyissä. Myös sopimusteknisillä mekanismeilla voidaan varmistaa, että data on saatavilla, mikäli palveluntarjoaja menee konkurssiin.

Viimeisessä kysymyksessä myös suurin osa vastaajista (89%) piti datan huonoa saatavuutta virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa suurempana uhkana ohjelmistovuokrauksessa kuin asiakaskohtaisissa

ohjelmistoissa. Vastaukset perusteltiin siten, että räätälöidyissä ohjelmistoissa lähdekoodit ja tallennettu data on asiakkaan suorassa hallinnassa. Tällöin asiakkaalla on myös täysi kontrolli siihen, mitä resursseja ongelman korjaamiseen käytetään. Ohjelmistovuokrauksessa asia ei usein ole kuitenkaan näin. Tämä saattaakin olla monille yrityksille suurin este hankkia palvelu ohjelmistovuokrauksen avulla.

Taulukossa 19 esitellään vastaajien mielipiteiden jakautuminen ohjelmistovuokraukseen kohdistuvien ongelmakohtien välillä. Taulukon vasemmassa sarakkeessa näkyy ohjelmistovuokrauksen viitekehys ja ohjelmistovuokrauksen tietoturvaongelmat. Kahdessa oikean puolimmaisessa sarakkeessa esitellään puolestaan saatua vastausmäärää näiden ongelmien merkittävyyden osalta. Taulukko 20 kuvaa saatuja tuloksia ohjelmistovuokrauksen tietoturvaongelmista suhteessa asiakaskohtaisiin ohjelmistoihin. Taulukon vasemmassa sarakkeessa näkyy ohjelmistovuokrauksen tietoturvaongelmat. Muissa sarakkeissa esitellään vastaushajonta sen suhteen, onko kysytty tietoturvaongelma suurempi, pienempi, yhtä suuri tai ei ongelma asiakaskohtaisissa (ak.) ohjelmistoissa.

OHJELMISTOVUOKRAUKSEN TIETOTURVAONGELMAT	Merkittävä uhka	Ei merkittävä uhka
OHJELMISTOJEN JA VERKKOSELAINTEN TIETOTURVAONGELMAT		
Selainten ja ohjelmistojen tietoturva-aukot	7	2
Selainten ja ohjelmistojen virhetilanteissa vuotavat tiedot	5	4
TIETOVERKON TIETOTURVAONGELMAT		
Tietoliikenteen paljastuminen sellaisille tahoille, joille ko. tieto ei kuulu	3	6
Palvelunestohyökkäykset	6	3
troijalaiset, virukset, madot	4	5
MONIKÄYTTÄJÄARKKITEHTUURIN TIETOTURVAONGELMAT		
Data käsitellään ja varastoidaan oman organisaation ulkopuolella	7	2
Dataa ei eristetä riittävän tehokkaasti muiden asiakkaiden datasta	8	1
Data ei pysy saatavilla virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa	9	0

TAULUKKO 19 Ohjelmistovuokrauksen tietoturvaongelmien painoarvo kyselytutkimuksessa

OHJELMISTOVUOKRAUKSEN TIETOTURVAONGELMAT	suurempi kuin ak. ohjelmis-toissa	pienempi kuin ak. ohjelmis-toissa	Yhtä suuri kuin ak. ohjelmis-toissa	ei ongelma ak. ohjelmis-toissa
OHJELMISTOJEN JA VERKKOSELAINTEN TIETOTURVAONGELMAT				
Selainten ja ohjelmistojen tietoturva-aukot	6	1	2	
Selainten ja ohjelmistojen virhetilanteissa vuotavat tiedot	5	1	3	
TIETOVERKON TIETOTURVAONGELMAT				
Tietoliikenteen paljastuminen sellaisille tahoille, joille ko. tieto ei kuulu	6	2	1	
Palvelunestohyökkäykset	6	2	1	
troijalaiset, virukset, madot	1	2	6	
MONIKÄYTTÄJÄ-ARKKITEHTUURIN TIETOTURVAONGELMAT				
Data käsitellään ja varastoidaan oman organisaation ulkopuolella	7	0	2	
Dataa ei eristetä riittävän tehokkaasti muiden asiakkaiden datasta	7	1		1
Data ei pysy saatavilla virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa	8	0	1	

TAULUKKO 20 Ohjelmistovuokrauksen tietoturvaongelmat suhteessa asiakaskohtaisiin (ak.) ohjelmistoihin.

6 POHDINTA

Tämän tutkielman tarkoituksena oli tunnistaa ohjelmistovuokraukseen kohdistuvia tietoturvauhkia, luoda viitekehys ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen tietoturvauhkien vertailulle sekä testata viitekehystä kyselytutkimuksella. Tässä luvussa tarkastellaan tutkimuksessa saatuja tuloksia, pohditaan tutkimuksen rajauksia, luotettavuutta, yleistettävyyttä, validiteettia ja reliabiliteettia sekä tehdään päätelmät ohjelmistovuokraukseen kohdistuvista tietoturvaongelmista.

6.1 Tutkimuksen rajaaminen

Tässä pro gradu- tutkielmassa viitekehykseen kerättiin tietoturvauhkia, jotka ovat oletettavasti suurempia ohjelmisto-vuokrauksessa kuin asiakaskohtaisissa ohjelmistoissa. Tällä keinolla pyrittiin nostamaan esille juuri ne tietoturvaongelmat, jotka ovat ohjelmistovuokrauksen kannalta merkittävimpiä ja ongelmallisimpia. Tästä syystä viitekehyksestä jouduttiinkin karsimaan pois joitain uhkia, jotka ovat ongelmallisia ohjelmistovuokrauksessa, mutta eivät oletettavasti ole niin suuria, että asiakaskohtaisten ohjelmistojen vertailussa nousisivat kovin merkittäviksi esiin. Esimerkiksi tulipalon uhka voidaan katsoa olevan ohjelmistovuokrauksessa tällainen ongelma. Jos kuitenkin vertaamme tulipalon uhkan suuruutta asiakaskohtaisten ohjelmistojen kanssa, voidaan huomata, ettei tämä uhka ole ohjelmistovuokrauksessa kuitenkaan suurempi. Tämän vuoksi viitekehykseen kerättiinkin ne tietoturvaongelmat jotka ovat jo lähtökohtaisesti ongelmallisempia ohjelmistovuokrauksen osalta.

Toinen tutkimuksen rajaus liittyi ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen vertailuun, josta jätettiin tarkoituksenmukaisesti pakettiohjelmistot ja sovelluspalveluiden tarjoaminen kokonaan pois. Tämä rajaus tehtiin sen vuoksi, että tutkimuksessa haluttiin säilyttää yhteys liiketoimintanäkökulmaan. Tänä päivänä iso osa yritysten käyttämistä

sovelluksista onkin räätälöity heidän tarpeitaan vastaaviksi, kun taas pakettiohjelmistot ovat suunnattu enemmän kuluttajille. Sovelluspalveluiden tarjoamiseen liittyy puolestaan ongelmia, jotka ohjelmistovuokraus on pystynyt paremmin ratkaisemaan. Näistä esimerkkeinä sovelluksen tietosisällön, toiminnallisuuden ja ulkoasun sovittaminen asiakkaan tarpeiden mukaiseksi. Ohjelmistovuokraus nähdäänkin tässä tutkimuksessa kilpailevana ohjelmistojen hankkimisen ja käytön mallina, joka mitä ilmeisimmin tulee olemaan suurin kilpailu-uhka juuri räätälöidyille ohjelmistoille. Tämän vuoksi tässä tutkimuksessa olikin kiinnostavampaa vertailla vain ohjelmistovuokrausta ja asiakaskohtaisia ohjelmistoja tietoturvan näkökulmasta.

6.2 Tutkimuksen luotettavuus ja yleistettävyys

Tutkimuksen luotettavuudella tarkoitetaan sitä, että tutkimustulokset ja tutkittava todellisuus vastaavat mahdollisimman hyvin toisiaan. Tutkimuksen yleistäminen puolestaan tarkoittaa uusien näkökulmien tuomista esiin sekä niiden perustelua teoreettisen viitekehyksen avulla. (Alasuutari, 1993, 207-235)

Ohjelmistovuokraus on tänä päivänä ilmiö, joka ei näy ainoastaan IT-sektorilla, vaan on myös hyvin sirpaleinen ja sovellettavissa toimialasta riippumatta. Hyvänä esimerkkinä ilmiön sirpaleisuudesta on se, että ohjelmisto-vuokrauksen periaatteella tehtyjä sovelluksia käytetään tänä päivänä muun muassa monissa asiakkuuden, automaation ja tuottavuuden hallintaan keskittyvissä palveluissa. Myös Google ja Microsoft tarjoaa puolestaan omia palvelujaan ohjelmistovuokrauksen periaatteita noudattaen. Huolimatta kentän sirpaleisuudesta ja sovelluskohteiden moninaisuudesta säilyy ohjelmisto-vuokrauksen perusajatus; tarjota ohjelmistoa verkon yli palveluna. Tästä johtuen tämän tutkimuksen tutkimustulokset ovat hyödynnettävissä myös toimialasta riippumatta.

Yhtenä tutkimuksen suurimmista ongelmista ja haasteista oli se, ettei aikaisempaa tutkimusta ohjelmistovuokraukseen kohdistuvista tietoturva-ongelmista oltu tehty. Suurin osa ohjelmistovuokraukseen kohdistuvista lähdemateriaaleista keskittyikin kuvaamaan ohjelmistovuokrausta ainoastaan liiketoiminnan näkökulmasta, jättäen tietoturvakysymykset lähes käsittelemättä. Tämä asetti suuria haasteita varsinkin soveltuvan lähdekirjallisuuden löytymisessä ja viitekehyksen luomisessa. Lähdekirjallisuuden vähäisyys osaltaan voidaan katsoa vaikuttavan heikentävästi tutkimuksen luotettavuuteen ja yleistettävyyteen.

Myös vastausmäärän jääminen suhteellisen pieneksi nähtiin kysely-tutkimuksessa yhtenä suurimpana puutteena tutkimuksen luotettavuutta ja yleistettävyyttä arvioidessa. Kyselytutkimusta suunniteltaessa vastauksia arvioitiin tulevan yli kaksikymmentä. Tutkimuksen lopuksi vastauksia saatiin kerättyä yhdeksän kappaletta. Vastausmäärän suhteellista pienuutta kompensoivat kuitenkin vastaajien asemat organisaatioissaan. Jokaisella vastaajalla katsottiinkin olevan asiantuntijatasoinen tietämys ohjelmisto-vuokrauksesta ja sen eri ulottuvuuksista, kuten tietoturvasta. Vaikka tutkielman kannalta vastausmäärän katsottiin olevan riittävä, mahdollistaa se ainoastaan varovaisten arvioiden ja johtopäätösten tekemisen ohjelmisto-vuokrauksen tietoturvaongelmista.

6.3 Tutkimuksen validiteetti ja reliabiliteetti

Tilastokeskuksen (2006) mukaan reliabiliteetti ja validiteetti ovat kvantitatiivisessa tutkimuksessa mittarin tärkeimmät ominaisuudet. Reliabiliteetti osoittaa sen, missä määrin mittari mittaa tutkittavaa ominaisuutta, kuinka luotettava ja pysyvä mittari on sekä mittaustulosten pysyvyyttä ja johdonmukaisuutta. Tässä tutkimuksessa reliabiliteettia pyrittiin nostamaan valikoimalla potentiaaliset vastaajat alanasiantuntijoista ja kontaktoimalla heitä spesifin sähköpostilistan kautta.

Ohjelmistovuokraukseen kohdistuvien tietoturvaongelmien painoarvon asteikko oli kyselytutkimuksessa luokiteltu asteikolla 1-2 (merkittävä uhka – ei merkittävä uhka). Tällaisella luokittelulla ei kuitenkaan saada selville riittävän luotettavasti mahdollisia eroja eri uhkien välillä. Osa vastaajista saattoikin pitää jotain uhkaa merkittävänä, muttei niin merkittävänä kuin jotain toista. Asteikko ei myöskään ottanut huomioon syitä eri uhkien taustalla. Tämän tutkielman tarkoituksena ei kuitenkaan ollut vertailla eri uhkien merkittävyyttä ja kokoa, vaan tunnistaa onko uhka olemassa vai ei. Tämän vuoksi kaksiportaisen asteikon katsottiin olevan tämän asian mittaamiseen riittävä.

Ohjelmistovuokraukseen ja asiakaskohtaisiin ohjelmistoihin kohdistuvien uhkien vertailussa käytettiin puolestaan neliportaista Likert-asteikkoa (suurempi uhka kuin asiakaskohtaisissa ohjelmistoissa – pienempi uhka kuin asiakaskohtaisissa ohjelmistoissa – yhtä suuri uhka asiakaskohtaisissa ohjelmistoissa – ei ongelma asiakaskohtaisissa ohjelmistoissa). Tällä luokittelulla saatiin kattavasti vastaajien arviot eri ohjelmistovuokraukseen kohdistuvien tietoturvaongelmien painoarvosta suhteessa asiakaskohtaisiin ohjelmistoihin. Lisäksi vastaajia pyydettiin perustelemaan jokaisessa kysymyksessä antamaansa vastausta avoimessa kentässä. Näin saatiin muodostettua luotettavampi ja kattavampi vastaus kustakin tietoturva-ongelmasta.

Validiteetilla tarkoitetaan mittarin pätevyyttä eli sitä, mittaako se tarkoitettua asiaa. Yleisimmin arvioitavia validiteetin lajeja ovat sisältö-, kriteeri- ja rakennevaliditeetti. (Tilastokeskus, 2006) Tässä työssä tarkastelu rajoitettiin rakenne- ja sisältövaliditeettiin. Rakenne- ja sisältövaliditeettia varmistettiin testaamalla kyselylomake alasta tietävillä, mutta myös tietämättömillä koehenkilöillä.

Kyselytutkimuksessa vastaajat olivat vastanneet lähes kaikkiin lomakkeen kysymyksiin, vaikka vastauksissa oli kuitenkin jonkin verran puutteita

avointen kysymysten osalta. Tämä voi olla merkki siitä, ettei kysymyksiä oltu täysin ymmärretty, vastausvaihtoehdot olivat suppeita tai vastaajilla ei ollut aikaa perustella vastauksiaan kaikkiin avoimiin kohtiin.

6.4 Päätelmät

Kyselytutkimuksen tuloksissa ei ilmennyt suuria yllätyksiä, vaan vastaukset noudattivat linjaa, jota tutkija osasi odottaakin. Lähes jokainen uhka koettiin vastausmääriltään merkittäväksi uhkatekijäksi. Ainoastaan tietoliikenteen paljastuminen sellaisille tahoille, joille ko. tieto ei kuulu sekä troijalaiset, virukset ja madot olivat uhkia joita ei pidetty kovin merkittävinä. Selkeästi yhtenevimmät vastaukset uhkien merkittävyydestä saatiin monikäyttäjä-arkkitehtuurin tietoturvaongelmien osalta. Datan huono saatavuus virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa olikin vastauksien osalta selkeästi merkittävin uhkatekijä ja sai eniten kannatusta. Datan huono eristäminen muiden asiakkaiden datasta ja datan varastointi oman organisaation ulkopuolella nousivat seuraavaksi merkittävimpinä uhka-tekijöinä esiin. Selainten ja ohjelmistojen tietoturva-aukot saivat myös huomattavan paljon kannatusta vastaajien keskuudessa.

Tähän jakaumaan johtaneista syistä merkittävämmäksi ongelmaksi ja ohjelmistovuokrausta jarruttavasta tekijöistä vaikuttaisikin liittyvän asiakkaan ja palveluntarjoajan väliseen riippuvuussuhteen syntymiseen. Asiakkaalla ei ole käytännössä muuta mahdollisuutta kuin luottaa palveluntarjoajan tietoturvatasoon ja siihen, etteivät liikesalaisuudet pääse muiden tietoon. Sopimusteknisillä mekanismeilla voitaisiin kuitenkin osaltaan pienentää asiakkaan kokemaa epävarmuutta. Ohjelmistovuokrauksen ei voida katsoa olevan vielä täysin kypsä ilmiö, jossa vakiintuneiden käytäntöjen puute aiheuttaa ongelmia varsinkin salaisen materiaalin osalta. Näyttäisikin siltä, ettei valtaosa yrityksiä ole vielä valmiita käyttämään ohjelmistovuokrattuja sovelluksia.

Huomattavaa vastauksissa on myös se, että tietoverkkoon kohdistuvat tietoturvaongelmat jakoivat eniten mielipiteitä. Vastauksissa voidaankin nähdä palvelun luonteen ja uhkien vakavuuden välinen vastakkaisasettelu. Toisille palveluille tietoverkkoon kohdistuvat ongelmat voivat olla vakavampia kuin toisille. Lisäksi tietoverkkoon kohdistuvat ongelmakohdat nähtiin vastauksissa enemmän ongelman seurauksina kuin syynä. Tietoliikenteen paljastuminen, palvelunestohyökkäykset, virukset, troijalaiset ja madot ovatkin usein seurausta jostakin vakavammasta tekijästä heikentää tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Tästä hyvänä esimerkkinä edellä mainitut selaimiin ja ohjelmistoihin jäävät tietoturva-aukot.

Ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen uhkien vertailussa ei myöskään ilmennyt suurempia yllätyksiä. Lähes kaikkien kysymysten kohdalla jokainen uhka koettiin olevan suurempi ohjelmistovuokrauksessa kuin asiakaskohtaisissa ohjelmistoissa. Vain troijalaiset, virukset ja madot olivat uhka, joka koettiin valtaosan vastaajien mielestä yhtä suureksi ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen kanssa. Huomattavaa vastauksissa on se, että ohjelmistovuokrausta ja asiakaskohtaisia ohjelmistoja verrattaessa pientä vastausten hajontaa oli havaittavissa. Vaikka osiossa yksi jokin tietty uhka oli koettu merkittäväksi, osoittaa ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen vertailu, etteivät vastaukset ole näin mustavalkoisia. Se, että jokin uhka koettiin merkittäväksi, ei vielä kerro sitä kuinka merkittävä uhka todellisuusessa on. Tämä näkyi myös avoimissa vastauksissa, joissa korostettiin sitä, ettei uhka merkittävyydestään huolimatta ole välttämättä kovin suuri uhka todellisuudessa. Myös ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen vertailussa tämä sama ilmiö oli havaittavissa. Vaikka suurin osa uhkista koettiin vastausmäärältään suuremmaksi kuin asiakaskohtaisissa ohjelmistoissa, kertoo se ainoastaan mielipiteiden jakautumisesta. Avointen vastausten osalta voidaankin huomata, että kyse on jälleen kerran uhkien vivahde-eroista. Kärjistetysti uhkien voidaan kuitenkin

katsoa olevan suurempi ohjelmistovuokrauksessa sekä vaikuttavan siihen isommalla painoarvolla.

Tutkielman kannalta merkittävää on, että vaikka tietoturva koetaankin suurimmaksi ohjelmistovuokrauksen ongelmakohdaksi, ei tämä tutkimus todista ohjelmistovuokrauksen olevan turvattomampi kuin esimerkiksi asiakaskohtaiset ohjelmistot. Kirjallisuudesta ja kyselytutkimuksesta saatujen havaintojen mukaan tilanne onkin usein päinvastainen. Asiakaskohtaiset ohjelmistot koetaan monesti turvallisemmiksi vaihtoehdoiksi muun muassa sen takia, että kontrolli omaan dataan säilyy. Se että tiedot on säilytetty oman palomuurin takana, ei kuitenkaan vielä takaa, että tiedot ovat turvassa.

Ohjelmistovuokraukseen liittyy myös paljon eri tekijöitä, jonka vuoksi asiakaskohtainen ohjelmisto saattaa olla joillekin yrityksille parempi vaihtoehto. Luottamalla sensitiivisen datan toisen osapuolen haltuun, luotetaan myös siihen, että niitä käsitellään tietoturvan periaatteita noudattamalla. Koskaan ei voi kuitenkaan olla varma siitä ketkä pääsevät käsiksi tietoihin ja millä tavoin nämä henkilöt käyttävät tietoja esimerkiksi vaihtaessaan työpaikkaa. Jatkotutkimusten kannalta olisikin tärkeää tutkia, millainen merkitys luottamuksella on, kun pohdimme ohjelmistovuokrausta tietoturvan näkökulmasta.

Tietoturvakysymyksistä huolimatta voidaan havaita, että ohjelmistovuokrauksesta on tulossa yksi merkittävistä ohjelmistokehityksen virstanpylväistä. Vaikka suurempia onnettomuuksia tällä alalla ei vielä ole tapahtunut tai ainakaan tietooni tullut, ei tietoturvakysymyksiä voi kuitenkaan unohtaa. Näyttäisi siltä, että tulevaisuudessa yrityksillä on kuitenkin parempi mahdollisuus hallita omaa dataansa sekä kontrolloida ohjelmistovuokrauksen riskejä. Avoin keskustelu palveluntarjoajan ja asiakkaan välillä on myös tärkeää pelisääntöjen ymmärtämisen kannalta. Tulevaisuudessa erilaisten tietoturvastandardien ja turvallisten ohjelmistokehittämisen menetelmien kehittyminen nousee todennäköisesti myös avainasemaan.

Tietoturva on asioiden toteuttamista. Jokainen sovellus ja järjestelmä vaativat aina ihmisiltä tietoturvan toimeenpanoa, riippumatta siitä, onko kyseessä asiakaskohtainen ohjelmisto tai vuokrattu ohjelmisto. Tietoturvaan liittyy myös subjektiivisia uskomuksia siitä kuinka turvalliseksi jokin järjestelmä koetaan. Tällöin kyse ei ole enää tietoturvasta itsestään vaan kyse on jostakin henkilökohtaisesta koetusta tunnetilasta. Tähän tunnetilaan vaikuttaa esimerkiksi tietämys, aikaisemmat kokemukset sekä luottamus näitä järjestelmiä kohtaan. Näin ollen emme voi siis sanoa kumpi edellä mainituista ohjelmistojen käytön malleista on turvallisempi. Tieteellisen tutkimuksen ja koulutuksen avulla voimme kuitenkin ymmärtää paremmin tämän päivän riskejä ja tietoturvaa sekä luoda parempia vaatimuksia myös tämän päivän palveluntarjoajille. Tieteellisellä tutkimuksella voimme herättää keskustelua ja puuttua niihin ongelmakohtiin, joita tutkimuksessa ja näissä järjestelmissä voidaan havaita. Tämä keskustelu on elintärkeää, mikäli haluamme ohjelmistovuokrattujen järjestelmien olevan turvallista myös tulevaisuudessa.

7 YHTEENVETO JA JATKOTUTKIMUSKOHTEET

Ohjelmistovuokraus on tänä päivänä yksi keskustelluimmista yritysten tietojenkäsittelyyn liittyvistä ilmiöistä ja se on leviämässä yhä laajempaan käyttöön varsinkin pienten- ja keskisuurten yritysten keskuudessa. Ohjelmistovuokraus nähdäänkin tänä päivänä hyvin joustavana ohjelmistojen hankinnan ja käytön mallina korvaten monia puutteellisuuksia ja haasteellisuuksia, joita yritysten omiin tiloihin hankitut asiakaskohtaiset ohjelmistot voivat aiheuttaa. Ohjelmistovuokraus siirtää ohjelmistojen kehittämisen, ylläpidon ja hallinnoimisen asiakkaalta palveluntarjoajalle, luoden tällä tavalla asiakkaalle mahdollisuuden keskittyä esimerkiksi ydinosaamiseen. Vaikka ohjelmistovuokraus tarjoaa monia etuja niin loppukäyttäjälle kuin palveluntarjoajille, liittyy siihen kuitenkin huolenaiheita, joista tietoturva ja yksityisyydensuoja ovat yksi merkittävimmistä.

Tässä tutkielmassa esiteltiin ohjelmistovuokraukseen liittyviä tietoturvaongelmia sekä vertailtiin havaittuja tietoturvaongelmia ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä. Jälkimmäistä ongelmaa varten suoritettiin kyselytutkimus. Kirjallisuuden pohjalta havaittiin, että keskeisimmiksi ohjelmistovuokrauksen tietoturvaongelmiksi muodostuvat: selainten ja ohjelmistojen tietoturva-aukot, selainten ja ohjelmistojen virhetilanteissa vuotavat tiedot, tietoliikenteen paljastuminen sellaisille tahoille, joille ko. tieto ei kuulu, palvelunestohyökkäykset, troijalaiset, virukset, madot, datan käsittely ja varastoiminen oman organisaation ulkopuolella, datan huono eristäminen muiden asiakkaiden datasta ja datan huono saatavuus virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa.

Kyselytutkimuksen tuloksena todettiin, että lähes jokainen viitekehyksen uhka nähtiin olevan suhteellisen suuri ongelma ohjelmistovuokrauksessa. Ainoastaan virukset, troijalaiset ja madot koettiin uhkina, jotka ovat enemmän seurausta muista tietoturvaongelmista. Monikäyttäjäarkkitehtuuriin

kohdistuvat tietoturvaongelmat saivat tutkimuksessa yksimielisimmin kannatusta uhkien merkittävyyden näkökulmasta. Ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen vertailu osoitti, että lähes kaikki viitekehykseen kerätyt uhkat voidaan katsoa olevan lievästi suurempia ongelmia ohjelmistovuokrauksessa kuin asiakaskohtaisissa ohjelmistoissa. Vain troijalaiset, virukset ja madot koettiin valtaosan vastaajien mielestä samansuuruiseksi näiden kahden toimintamallin välillä.

Tutkimuksen perusteella todettiin, että tietoturvaan liittyvien ongelmien ja haasteiden vuoksi ohjelmistovuokraus ei ole vielä täysin kypsä ilmiö. Tämän vuoksi ohjelmistovuokrauksen palveluntarjoajan kanssa tulisikin keskustella siitä:

1) kuka pääsee käyttämään organisaation tietoja
2) millaisia tietoturvastandardeja palveluntarjoajat noudattavat
3) missä data fyysisesti säilytetään
4) millä tavoin se eristetään muiden asiakkaiden datasta
5) kuinka elvytään virhetilanteissa
6) kuinka palveluntarjoaja estää ja tutkii luvattoman järjestelmiin tunkeutumisen
7) miten voidaan varmistaa pitkäaikainen toimintakelpoisuus jos palveluntarjoaja lakkaa olemasta tai sulautuu esimerkiksi osaksi toista yritystä.

Lisäksi ohjelmistovuorauksen palveluntarjoajien tulisi keskittyä myös yrityksen fyysiseen tietoturvaan sekä varmistaa, että ohjelmistojen kehittämisessä noudatetaan tietoturvastandardeja ja turvallisia ohjelmistokehittämisen menetelmiä.

Tietoturvaongelmista huolimatta tämä tutkimus ei kuitenkaan osoita ohjelmistovuokrauksen olevan turvattomampi ohjelmistojen hankkimisen ja käytön malli. Tämä tutkielma pyrki kuitenkin nostamamaan muutamia keskeisimpiä ohjelmistovuokraukseen kohdistuvia ongelmakohtia esiin tietoturvallisuuden näkökulmasta, jotta voisimme myös varautua niihin paremmin.

Jatkotutkimuksen kannalta luottamuksen rooli osana tietoturvaa ja ohjelmistovuokrausta olisikin yksi mahdollinen tutkimuskohde. Keskeistä tämän alueen käsittelyssä olisikin selvittää, onko tietoturva pelkkä tunnepitoinen tila ja millä tavoin luottamus vaikuttaa tämän tunnetilan muodostumisessa uusien ilmiöiden, kuten tässä tapauksessa ohjelmistovuokrauksen käyttöönotossa. Jatkotutkimuksen kannalta olisi mielenkiintoista myös selvittää millä tavoin esimerkiksi riskienhallintaa voitaisiin soveltaa ohjelmistovuokrauksessa tai millainen vaikutus sopimusteknisillä mekanismeilla on ohjelmistovuokrauksen turvallisuuteen.

LÄHDELUETTELO

Alasuutari P. 1993 Laadullinen tutkimus. Gummerus. Helsinki

Abbas A., El Saddik A. & Miri A. 2005. A State of the Art Security Taxonomy of Internet Security: Threats and Countermeasures. Computer Science and Engineering 19(1), 27-36.

Ammerman M. 2007. SaaS 101: The Benefits [online]. SaaSBlogs, Understanding The Software as a Service Revolution [viitattu 13.10.2009]. Saatavilla www-osoitteessa <http://www.saasblogs.com/2007/05/02/>.

Balachandra R.K., Ramakrishna P.V. & Atanu. 2009. Cloud Security Issues. IEEE International Conference on Services Computing Bangalore, India, September 21-25. IEEE Computer Society, 517-520.

Brodkin J. Gartner: Seven cloud-computing security risks: Data integrity, recovery, privacy and regulatory compliance are key issues to consider [online]. Networkworld [viitattu 17.12.2009]. Saatavilla www-osoitteessa <http://www.networkworld.com/news/2008/070208-cloud.html?page=1>.

Carraro G., Chong F. & Wolter R. 2006. Building Distributed Applications, Multi-Tenant Data Architecture. The Microsoft Corporation, 1-20.

Carraro G. & Chong F. 2006. Building Distributed Applications, Software as a Service (SaaS): An Enterprise Perspective. The Microsoft Corporation, 1-17.

Desai B. & Currie W. (2003): Application Service Providers: A model in Evolution. Proceedings of the 5th international conference on

Electronic commerce Pittsburgh, Pennsylvania, September 30-October 03. 174-180.

Dhillon G., & Blackhouse J. 2001. Current directions in IS security research: towards socio-organizational perspectives. Information Systems Journal 11(2), 127-53.

Gold N., Mohan A., Knight C. & Munro M. 2004. Understanding Service Oriented Software. IEEE Software 21(2), 71–77.

Greschler D. & Mangan T. 2002. Networking lessons in delivering ‚Software as a Service' Part I. International Journal of Network Management 12(5), 317-321.

Huang Y.W., Huang S.K., Lin T.P., & Tsai C.H. 2003. Web application security assessment by fault injection and behavior monitoring. Proceedings of the 12th international conference on World Wide Web Budapest, Hungary, ACM, 148 – 159.

ISO/IEC 2000, ISO/IEC 17799 Information technology — Code of practice for information security management, ISO/IEC International Standard.

Jacobs D. 2005. Enterprise Software As Service, Online Services are Changing the Nature of Software. ACM Queue 3(6), 36-42.

Järvinen P. 2002. Tietoturva & Yksityisyys. Docendo Finland Oy, Jyväskylä.

Kallhoff J. 2007. GIAC Research in the Common Body of Knowledge [online] Giac [viitattu 21.7.2010] Saatavilla www-osoitteessa <http://www.giac.org/resources/whitepaper/physical/287.php>.

Kaplan J. 2009. Should Security Concerns Stall SaaS Adoption? [online]. Datamation. [viitattu 14.10.2009] Saatavilla www-osoitteessa

<http://itmanagement.earthweb.com/secu/article.php/3825461/Should-Security-Concerns-Stall-SaaS-Adoption.htm>.

Kaplan J.M. 2007. SaaS: Friend Or Foe? Software-as-a-service offerings are expanding, and gaining more acceptance. Business Communications Review, 50-53.

Kuivalainen J. 2005. KRP: Kalastelijoiden Nordea-potti kohoaa 60 000 euroon [online]. Digitoday [viitattu 6.9.2010] Saatavilla www-osoitteessa < http://www.digitoday.fi/page.php?page_id=66&news_id=200518646>

Laaksonen M., Nevasalo T., & Tomula K. 2006. Yrityksen tietoturvakäsikirja - Ohjeistus, toteutus ja lainsäädäntö. Oy Nordprint Ab, Helsinki.

Landwehr C., Bull A., McDermott J. & Choi W. 1994. A taxonomy of computer program security flaws. ACM Computing Surveys 26(3), 211 – 254.

Lichtenstein S. 1997. Developing Internet security policy for organizations. Proceedings of the Thirtieth Hawaii International Conference on Wailea, HI January 1997. System Sciences, 350 – 357.

Mohamed A., Ruhe G., Eberlein A. 2007. Decision Support for Handling Mismatches between COTS Products and System Requirements. Proceedings of the 6th international IEEE conference on Commercial off the Shelf (COTS) Based Software Systems Banff, Alta, February 26–March 2. 63-72.

Mäkinen T. 2006. Thoughts on the role of Architect and use of Architecture as a tool for both Business and IT [online]. Architects Plot. [viitattu 12.1.2010] Saatavilla www-osoitteessa <http://blogs.msdn.com/pasim/archive/2006/05/10/saas-n-hd.aspx >

Nikkari T. 2007. Sisäinen tietoturva – tietovuodon vaikutukset pk-yrityksen toimintaan ja toimintatapojen muutosten vaikutus sisäiseen tietoturvallisuuteen. Case: BK-Automation Oy. Tampereen yliopisto. Tietojenkäsittelyopin pro gradu -tutkielma.

Northcutt S., Skoudis E., Sachs M., Ullrich J., Liston T., Cole E., Schultz E., Dhamankar R., Yoran A., Schmidt H., Pelgrin W. Paller A. 2008. Top Ten Cyber Security Menaces for 2008 [online]. Sans. [viitattu 12.1.2010] Saatavilla www-osoitteessa <http://www.sans.org/2008menaces/ >

Rantala A. 2009. Tietoturva - eFront [online]. Tieto- ja viestintätekniikka [viitattu 15.01.2010]. Saatavilla www-osoitteessa <https://webapps.jyu.fi/wiki/display/opentvt/Tietoturva+-+eFront>

Rittinghouse J. 2009. Cloud Computing: Implementation, Management, and Security [online]. Boca Raton: CRC Press [viitattu 14.10.2009]. Saatavilla www-osoitteessa < http://books.google.fi/books?id=NJluq7mLXL0C&dq=rittinghouse+cloud+computing&printsec=frontcover&source=bl&ots=jHIXPNn2n3&sig=jYTLkrgBwVUFuUwGKd4N85DA9ak&hl=fi&ei=_bpBS4GMAZTu-AaRz-muCg&sa=X&oi=book_result&ct=result&resnum=1&ved=0CAoQ6AEwAA#v=onepage&q=&f=false>.

Robson C. 1994. Real World Research – A resource for social scientists and practioner researchers. Oxford. Blackwell.

Rovio E-E. 2008. SaaS lyhyesti [online]. Basware [viitattu 13.10.2009]. Saatavilla www-osoitteessa

http://www.tieke.fi/mp/db/file_library/x/IMG/36531/file/Rovio_SaaS_20081125.pdf>.

Savolainen P., Niemelä E. & Savola R. 2007. A Taxonomy of Information Security for Service-Centric Systems. Proceedings of the 33rd EUROMICRO Conference on Lubeck, August 2007. Software Engineering and Advanced Applications (28)31, 5-12.

Shanmugam J. & Ponnavaikko M. 2007. A solution to block Cross Site Scripting Vulnerabilities based on Service Oriented Architecture. Proceeding of the 6th IEEE/ACIS International Conference on Melbourne, July 11-13. Computer and Information Science, 861 – 866.

Stoneburner G. 2001. Underlying Technical Models for Information, Technology Security [online] National Institute of Standards and Technology (NIST). [viitattu 13.10.2009]. Saatavilla www-osoitteessa <http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf>.

Sultan A. 2007. SaaS 101: The Drawbacks [online]. SaaSBlogs [viitattu 21.10.2009]. Saatavilla www-osoitteessa <http://www.saasblogs.com/2007/10/16/>.

Tilastokeskus 2006. [online]. Käsitteet [viitattu 2.9.2010] Saatavilla www-osoitteessa < http://www.stat.fi/meta/kas/reliabiliteetti.html>

Tilastokeskus 2006. [online]. Käsitteet [viitattu 2.9.2010] Saatavilla www-osoitteessa <http://www.stat.fi/meta/kas/validiteetti.html>

Vajjhala S., Ross S., Shah U., Gadkari N. & Gonsalves R. 2007. Internet Security Threats [online]. [viitattu 12.1.2010] Saatavilla www-osoitteessa <http://www.swetav.com/Internet_Security_Project_CS4235.pdf>

Van der Stock A., Williams J. & Wichers D. 2007. The Ten Most Critical Web Application Security Vulnerabilities - 2007 Update [online]. The Open Web Application Security Project [viitattu 12.1.2010] Saatavilla www-osoitteessa <http://www.owasp.org/images/e/e8/OWASP_Top_10_2007.pdf >.

Wang H. & Wang C. 2003. Taxonomy of security considerations and software quality. Communications of the ACM (46)6, 75-78.

Weber S., Karger P. & Paradkar A. 2005. A software flaw taxonomy: aiming tools at security. International Conference on Software Engineering archive Proceedings of the 2005 workshop on Software engineering for secure systems—building trustworthy applications St. Louis, Missouri, July 2005. Software Engineering for Secure Systems (SESS) --- Building Trustworthy Applications. ACM SIGSOFT Software Engineering, 1 – 7.

Weston, R. & Kaviani S. 2009. SaaS Vendor Selection, A Systematic Approach to Selecting a Software-as-a-service Vendor [online]. Hyperoffice [viitattu 13.10.2009]. Saatavilla www-osoitteessa <http://www.hyperoffice.com/files/pdf/saas_vendor_selection.pdf>.

Whitman, M.E. & Mattord H.J. 2009. Principles of Information Security, Third Edition [online]. Canada: Thomson Course Technology [viitattu 14.10.2009]. Saatavilla www-osoitteessa < http://www.google.com/books?hl=fi&lr=&id=gPonBssSm0kC&oi=fnd&pg=PR15&dq=Principles+of+Information+Security&ots=cZ97RNswoX&sig=MMT0q-hlVnvDJNJRm_xKmnA0HuM#v=onepage&q=&f=false>.

LIITE 1

KYSELYLOMAKE OHJELMISTOVUOKRAUKSEN TIETOTURVAONGELMISTA

Tämä kyselylomake liittyy Jyväskylän yliopistolla informaatioteknologian tiedekunnassa tietojärjestelmätiedettä opiskelevan Ville Kupilan pro gradu -tutkielmaan ohjelmistovuokrauksen (SaaS) tietoturvaongelmista.

Kyselylomakkeen tarkoituksena on selvittää kuinka merkittäviä ohjelmistovuokraukseen kohdistuvat tietoturvaongelmat ovat sekä vertailla ongelmakohtia ohjelmistovuokrauksen ja asiakaskohtaisten ohjelmistojen välillä.

Ohjelmistovuokrauksella tarkoitetaan tässä yhteydessä ohjelmistotoimittajan luomaa sovellusta, jota operoidaan toimittajan palvelimilla ja johon asiakkaat ovat yhteydessä verkon yli standardoiduilla selaimilla ja verkko-ohjelmistoilla. Asiakaskohtaisella ohjelmistolla tarkoitetaan puolestaan yrityksen omistamaa ja sen omissa tiloissa toimivaa ohjelmistoa, jonka asentamisesta, päivityksistä ja ylläpidosta yritys huolehtii pääsääntöisesti itse.

TAUSTAKYSYMYKSET

Yritys ja toimiala: _____ _

Yrityksen koko: _____ _

Vastaajan asema organisaatiossa: _____

OHJELMISTOJEN JA VERKKOSELAINTEN TIETOTURVAONGELMAT

1) Selainten ja ohjelmistojen tietoturva-aukot

Merkittävä uhka ☐

Ei merkittävä uhka ☐

_____

_____

_____

_____

Onko tämä tietoturvaongelma ohjelmistovuokrauksessa:

Suurempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Pienempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Yhtä suuri kuin asiakaskohtaisissa ohjelmistoissa ☐

Ei ongelma asiakaskohtaisissa ohjelmistoissa ☐

_____

_____

_____

_____

2) Selainten ja ohjelmistojen virhetilanteissa vuotavat tiedot

Merkittävä uhka ☐

Ei merkittävä uhka ☐

_____

_____

_____

_____

Onko tämä tietoturvaongelma ohjelmistovuokrauksessa:

Suurempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Pienempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Yhtä suuri kuin asiakaskohtaisissa ohjelmistoissa ☐

Ei ongelma asiakaskohtaisissa ohjelmistoissa ☐

_____

_____

_____

_____

TIETOVERKON TIETOTURVAONGELMAT

3) Tietoliikenteen paljastuminen sellaisille tahoille, joille ko. tieto ei kuulu

Merkittävä uhka ☐

Ei merkittävä uhka ☐

_____

_____

_____

_____

Onko tämä tietoturvaongelma ohjelmistovuokrauksessa:

Suurempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Pienempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Yhtä suuri kuin asiakaskohtaisissa ohjelmistoissa ☐

Ei ongelma asiakaskohtaisissa ohjelmistoissa ☐

_____

_____

_____

_____

4) Palvelunestohyökkäykset

Merkittävä uhka ☐

Ei merkittävä uhka ☐

_____

_____

_____

_____

Onko tämä tietoturvaongelma ohjelmistovuokrauksessa:

Suurempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Pienempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Yhtä suuri kuin asiakaskohtaisissa ohjelmistoissa ☐

Ei ongelma asiakaskohtaisissa ohjelmistoissa ☐

_____

_____

_____

_____

5) troijalaiset, virukset, madot

Merkittävä uhka ☐

Ei merkittävä uhka ☐

_____

_____

_____

_____

Onko tämä tietoturvaongelma ohjelmistovuokrauksessa:

Suurempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Pienempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Yhtä suuri kuin asiakaskohtaisissa ohjelmistoissa ☐

Ei ongelma asiakaskohtaisissa ohjelmistoissa ☐

_____

_____

_____

_____

MONIKÄYTTÄJÄARKKITEHTUURIN TIETOTURVAONGELMAT

6) Data käsitellään ja varastoidaan oman organisaation ulkopuolella

Merkittävä uhka ☐

Ei merkittävä uhka ☐

_____

_____

_____

_____

Onko tämä tietoturvaongelma ohjelmistovuokrauksessa:

Suurempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Pienempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Yhtä suuri kuin asiakaskohtaisissa ohjelmistoissa ☐

Ei ongelma asiakaskohtaisissa ohjelmistoissa ☐

_____

_____

_____

_____

7) Dataa ei eristetä riittävän tehokkaasti muiden asiakkaiden datasta

Merkittävä uhka ☐

Ei merkittävä uhka ☐

_____

_____

_____

_____

Onko tämä tietoturvaongelma ohjelmistovuokrauksessa:

Suurempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Pienempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Yhtä suuri kuin asiakaskohtaisissa ohjelmistoissa ☐

Ei ongelma asiakaskohtaisissa ohjelmistoissa ☐

_____

_____

_____

_____

8) Data ei pysy saatavilla virhetilanteessa tai palveluntarjoajan lopettaessa toimintansa

Merkittävä uhka ☐

Ei merkittävä uhka ☐

_____

_____

_____

_____

Onko tämä tietoturvaongelma ohjelmistovuokrauksessa:

Suurempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Pienempi kuin asiakaskohtaisissa ohjelmistoissa ☐

Yhtä suuri kuin asiakaskohtaisissa ohjelmistoissa ☐

Ei ongelma asiakaskohtaisissa ohjelmistoissa ☐

_____

_____

_____

_____