VAASAN YLIOPISTO

TEKNILLINEN TIEDEKUNTA

TIETOTEKNIIKKA

Johannes Töyli

Pilvipalveluiden tietoturva PK- yrityksissä

Tietotekniikan

pro gradu- tutkielma

VAASA 2016

Sisällysluettelo sivu

KUVALUETTELO **SIVU**

LYHENTEET

API	Application Programming Interface – ohjelmointirajapinta, Määritelmä jonka mukaan ohjelmat voivat keskustella keskenään
DNS	Domain Name System – Internetin nimipalvelu, joka muuttaa verkkotunnuksia IP-osoitteiksi.
DoS	Denial of Service – palvelunestohyökkäys, verkkosivulle kohdistetaan niin paljon liikennettä, että sivuston käyttö estyy
DDoS	Distributed Denial of Service – hajautettu palvelunestohyökkäys, verkkosivulle kohdistetaan niin paljon liikennettä, että sivuston käyttö estyy
FAT	File Allocation Table – Microsoftin kehittämä tietokoneen tiedostojärjestelmä arkkitehtuuri
IaaS	Infrastructure as a Service – pilvipalveluiden yksi kolmesta pääluokasta. Palvelimien ja palvelinsalien ulkoistaminen
PaaS	Platform as a Service – pilvipalveluiden yksi kolmesta pääluokasta. Pilvipalvelun palvelualustan ulkoistaminen
Phishing	Verkkourkinta eli tietojenkalastelu
PK- yritys	Pieni tai keskisuuri yritys – Vähemmän kuin 250 työntekijää ja liikevaihto alle 50 miljoonaa euroa
PRIME	Privacy And Identity Management for Europe – Järjestelmä yksityisten tunnistetietojen hallintaan Euroopassa
SaaS	Software as a Service – pilvipalveluiden yksi kolmesta pääluokasta. Ohjelmiston hankkiminen pilvipalveluna
SSL	Secure Socket Layer – Salausprotokolla, jolla voidaan suojata tietoliikenne IP- verkkojen yli

SSO	Single Sign-On – kertakirjautuminen, mahdollistaa käyttäjän kirjautumisen useaan palveluun yhdellä tunnuksella
SQL	Structured Query Language – IBMn kehittämä standardoidu kyselykieli relaatiotietokannoille
TCP	Transmission Control Protocol – Tietoliikenneprotokolla jolla luodaan tietokoneiden välille yhteyksiä, jotta voidaan lähettää turvallisesti tavujonoja
TLS	Transport Layer Security – Salausprotokolla, jolla voidaan suojata tietoliikenne IP- verkkojen yli. Tunnettu aiemmin nimellä SSL.
UDP	User Datagram Protocol – Vaihtoehtoinen protokolla TCP:lle jolla voidaan lähettää tiedostoja
XSS	Cross-Site Scripting – Hyökkäys, jolla voidaan ujuttaa haitallista koodia normaalisti luotettavalle verkkosivulle

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Johannes Töyli
Tutkielman nimi: Pilvipalveluiden tietoturva PK-yrityksissä
Ohjaajan nimi: Tero Vartiainen
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Tietotekniikka
Opintojen aloitusvuosi: 2009
Tutkielman valmistumisvuosi: 2016 **Sivumäärä:** 136

TIIVISTELMÄ:

Tämän tutkielman tarkoituksena on tutkia PK-yrityksien asenteita ja mielipiteitä pilvipalveluita ja niiden tietoturvaa kohtaan. Tutkielman empiirinen osio sisältää kyselytutkimuksen, jonka vastaajina toimivat suomalaiset PK-yritykset. Tutkielman teoria koostuu pilvipalveluiden tietoturvaa käsittelevistä tutkimuksista sekä yrityksien ja erityisesti PK-yrityksien pilvipalveluiden käyttöön liittyvistä tutkimuksista. Siinä käsitellään myös yhdeksän Cloud Security Alliancen listaamaa tietoturvauhkaa pilvipalveluita kohtaan.

Nykyään pilvipalvelut ovat todella suosittuja ja niiden käyttö myös yrityksissä lisääntyy vuosi vuodelta. PK-yrityksen saama hyöty pilvipalvelusta voi olla todella suuri ja erityisesti kustannustehokas. Pilvipalveluiden tuomat edut antavat PK-yrityksille mahdollisuuden laajentaa ja ennen kaikkea tehostaa toimintaansa. Pilvipalvelut tuovat kuitenkin myös haasteita käyttäjilleen. Pilvipalveluiden tietoturva ei kuitenkaan ole ainoastaan pilvipalveluntarjoajan vastuulla vaan myös asiakkaan on huolehdittava oma osuutensa. Tästä syystä tutkielmassa kartoitetaan PK-yrityksien asenteita ja mielipiteitä pilvipalveluiden tietoturvaan.

Kyselytutkimuksen perusteella monissa PK-yrityksissä käytetään pilvipalveluita. Pilvipalveluita käyttävissä yrityksissä oltiin yleisesti positiivisemmin asennoituneita pilvipalveluita kohtaan kuin PK-yrityksissä, joissa pilvipalveluita ei ole käytössä. Pilvipalvelua käyttävät PK-yritykset näkivät enemmän etuja pilvipalveluissa, mutta suhtautuivat myös tietoturvauhkiin vähemmän vakavasti kuin yritykset, jotka eivät käyttäneet pilvipalveluita. PK-yrityksien suhtautuminen eri tietoturvauhkiin vaikutti kyselyn perusteella kuitenkin järkevältä ja ylireagointeja tai vähättelyjä ei esiintynyt. Pilvipalveluiden lukumäärällä ei ole vaikutusta asenteisiin ja mielipiteisiin ennen kuin niiden määrä on vähemmän kuin seitsemän.

Tutkielmaan saatujen vastauksien perusteella, Suomessa PK-yritykset ovat siirtyneet pilvipalveluiden käyttäjäksi muuta Eurooppaa nopeammin. Myös Yhdysvallat ovat Suomen perässä. Syyt, miksi PK-yritykset ovat siirtyneet pilvipalveluihin, olivat kuitenkin hyvin samankaltaisia eri maissa. Myös tietoturvauhkiin suhtautuminen oli eri maiden välillä samankaltaista.

AVAINSANAT: Tietoturva, Pilvipalvelut, PK-yritys, Uhat, Pilven tietoturva

UNIVERSITY OF VAASA
Faculty of technology
Author: Johannes Töyli
Topic of the Master's Thesis Cloud security in SME's
Instructor: Tero Vartiainen
Degree: Master of Science in Economics and Business Administration
Major: Computer Science
Year of Entering the University 2009
Year of Completing the Master's Thesis: 2016 **Pages:** 136

ABSTRACT:

The purpose of my research was to study small and medium-sized enterprises attitudes and opinions on cloud services and cloud security. Empirical section includes survey and the participants are small and medium-sized enterprises. Thesis's theory is about cloud security and other researches that has been made of the topic. Theory also covers researches of small and medium-sized enterprises and their use of cloud services. It includes nine security threats that Cloud Security Alliance has listed.

Nowadays cloud services are really popular and also small and medium-sized enterprises have adopted them. Small and medium-sized enterprises can get a lot of benefits from cloud services since cloud services are cost-effective. Because of cloud services, small and medium-sized enterprises can have an opportunity to grow and to have an opportunity to intensify their business. Cloud services also add new security threats. Security of the cloud services does not belong only to the service providers but the customers need to do their part. Because of this, in this research attitudes and opinions are surveyed.

According to this study, over half of Finnish small and medium-sized enterprises use cloud services. Small and medium-sized enterprises that use cloud services tended have more positive attitude to cloud services than those that did not. Cloud service users saw more benefits in cloud services but also reacted milder to security threats. According to this research, small and medium-sized enterprises generally had a good attitude to security threats and they did not overreacted or downplayed the security threats. The amount of cloud services has no effect on attitudes or opinions when the amount is lower than seven.

According to answers in this research, small and medium-sized enterprises in Finland have adopted cloud services more than small and medium-sized enterprises in rest of the Europe or in the USA. Reason for cloud adaptation was very similar in all the countries and concerns about security threats were also very similar in all the countries.

KEYWORDS: Cloud, Security, SME, Cloud Security

1. JOHDANTO

Pilvipalveluiden käyttö on yleistynyt viime vuosina todella nopeasti. Myös yritykset ovat olleet erittäin kiinnostuneita pilvipalveluiden käyttöönotosta. Pilvipalveluiden kustannukset ovat laskeneet sille tasolle, että myös pienet ja keskisuuret yritykset ovat voineet ottaa tarvitsemiaan palveluita käyttöön. Hyöty voi PK-yritykselle olla todella suuri, kun he saavat käyttöönsä pilvipalveluiden laskentatehon, etäkäytön, tallennustilan ja tietoturvan, vaikka yrityksessä ei olisi vahvaa IT-osaamista itsessään. Nämä puolestaan auttavat PK-yrityksiä jokapäiväisessä liiketoiminnassa sekä kasvussa.

Pilvipalvelut muodostuvat kolmesta eri kategoriasta. SaaS (Software as a service), PaaS (Platform as a service) sekä IaaS (Infrastructure as a service). SaaS-mallilla tarkoitetaan, että ohjelmisto (software) hankitaan palveluna sen sijaan, että ostettaisiin ohjelmistolle lisenssi. SaaS-mallissa ohjelmistoa käytetään verkon yli ja käyttöliittymä on kaikille asiakkaille sama. Saas-malliin on myös tullut oma alamallinsa SECaaS (Security as a Service). SECaaS-mallissa asiakkaalle toimitetaan esimerkiksi tietoturvaan liittyvät ohjelmistot pilvipalvelun kautta, joten ne ovat aina ajan tasalla ja yrityksen käytettävissä. Myös niiden hallinnointi voidaan ulkoistaa palveluntarjoajalle. PaaS-malli tarkoittaa palvelualustan ulkoistamista. Siinä palveluntarjoaja vuokraa asiakkaalle esimerkiksi käyttöjärjestelmää, laitteistoa tai tallennustilaa internetin yli. IaaS-mallissa organisaatio ulkoistaa palvelimen tai palvelinsalin. Laitteet omistaa niitä tarjoava organisaatio ja he ovat myös vastuussa niiden ylläpidosta.

Omien laitteiden, kuten palvelimien, ja ohjelmistojen ostaminen PK- yritykselle on niin iso kustannus, että se ei välttämättä ole heille kannattavaa. Hyöty olisi suuri, mutta suhteutettuna kustannuksiin liian vähäinen. Pilvipalvelut kuitenkin mahdollistavat näiden laitteiden käyttämisen kustannustehokkaasti eikä yrityksen tarvitse sijoittaa omiin laitteisiin. Pilvipalvelut ottavat huomioon myös eri tarpeet eri mallien avulla, joten yritys pystyy sijoittamaan tarpeelliseksi kokemansa summan palveluihin.

Pilvipalveluiden käyttäminen PK-yrityksissä tuo mukanaan myös haasteita. Yksi näistä haasteista on tietoturva. Pilvipalvelut voivat parantaa PK- yrityksen tietoturvaa kokonais-

valtaisesti, mutta samaan aikaan pilvipalvelut luovat uusia tietoturvaongelmia, jotka yrityksen tulisi ottaa huomioon. Uudet uhat eivät ole aina niin itsestään selviä ja PK-yrityksen voi olla vaikea hahmottaa näitä uhkia. Osa pilvipalveluiden tietoturvauhkista ovat samoja kuin niin sanotun perinteisen tietotekniikan uhat eli esimerkiksi tietomurrot, mutta pilvipalveluiden mukana on syntynyt myös aivan uusia. Pilvipalveluiden myötä myös PK-yritykset säilyttävät arvokasta tietoaan palvelimilla, jotka omistavat jokin ulkopuolinen taho ja palvelimet voivat sijaita myös toisella puolella maapalloa.

1.1. Tutkielman rajaus ja tavoitteet

Tutkielma aihe on jatkoa kandidaatin tutkielmalleni ”Pilven tietoturva”.

Tutkielman tavoitteena on selvittää suomalaisten PK-yritysten pilvipalveluiden tietoturvaan liittyviä asenteita sekä mielipiteitä. Asenteita ja mielipiteitä selvitetään myös yleisesti pilvipalveluista. Tutkielman tavoitteena on saada selville ovatko PK-yritykset huolestuneita pilvipalveluiden tietoturvasta ja mitkä asiat heitä erityisesti pilvipalveluissa huolestuttavat. Tavoitteeseen sisältyy selvittää edellä mainitut asiat yrityksiltä, jotka käyttävät pilvipalveluita, mutta myös yrityksiltä, jotka eivät käytä pilvipalveluita. Saatuja tuloksia verrataan toisiinsa ja tutkitaan eroavatko ne toisistaan sekä tutkitaan kokonaiskuvaa tuloksista. Tutkimuksessa verrataan kyselyn tuloksia myös ulkomailla tehtyihin vastaaviin tutkimuksiin. Tämän avulla nähdään ovatko haasteet ja vaikeudet samanlaisia ulkomailla kuin Suomessa PK- yritysten keskuudessa.

Tutkimuksen hypoteesina on ensinnäkin todistaa eroaako PK-yrityksien mielipiteet ja asenteet pilvipalveluita ja niiden tietoturvaa kohtaan sen perusteella onko heillä käytössään pilvipalvelu vai ei. Toisena hypoteesina tutkimuksella on selvittää onko pilvipalveluiden käytössä olemisella merkitystä asenteiden ja mielipiteiden muokkaamisessa.

Tutkimuksessa ei oteta kantaa siihen, miten tietoturva on toteutettu PK-yrityksissä eikä siihen miten se on toteutettu pilvipalveluidentarjoajien toimesta.

1.2. Tutkimusmenetelmät

Tutkimus on kvantitatiivinen tutkimus, joka toteutetaan kyselytutkimuksena. Kyselyn tuloksena saadaan tietoa PK-yrityksien asenteista ja mielipiteistä koskien pilvipalveluiden tietoturvaa. Kysely toteutetaan Google Forms-palvelulla ja sen levityksessä apua saadaan Vaasan Yrittäjiltä.

1.3. Tutkielman rakenne

Tutkielman ensimmäinen kappale sisältää johdannon, jossa käydään läpi tutkielman rajaus ja tavoitteet. Tutkielman toisessa kappaleessa käydään läpi tutkielman kannalta oleelliset teoriat sekä taustatiedot. Kappaleessa käsitellään pilvipalveluita sekä niiden tietoturvaa ja tietoturvauhkia perustuen aikaisemmin tehtyihin tutkimuksiin. Kappaleessa myös käydään läpi PK-yrityksien saamat hyödyt ja haasteet pilvipalveluista aikaisempien tutkimuksien perusteella.

Kolmannesta kappaleesta alkaa tutkimuksen kysely. Kappaleen alussa käydään läpi kyselyä yleisellä tasolla ja avataan kyselyn rakennetta sekä vastaajia. Tämän jälkeen esitetään kyselyn tulokset ja analysoidaan niitä. Kolmannessa kappaleessa kyselyn tuloksia verrataan myös ulkomailla tehtyihin tutkimuksiin. Näitä tutkimuksia on niin Euroopan osalta kuin myös Yhdysvaltojen osalta. Viides kappale sisältää kyselyn johtopäätökset ja kuudes kappale yhteenvedon sekä mahdolliset aiheet ja tarpeet jatkotutkimuksiin.

2. PILVIPALVELUT

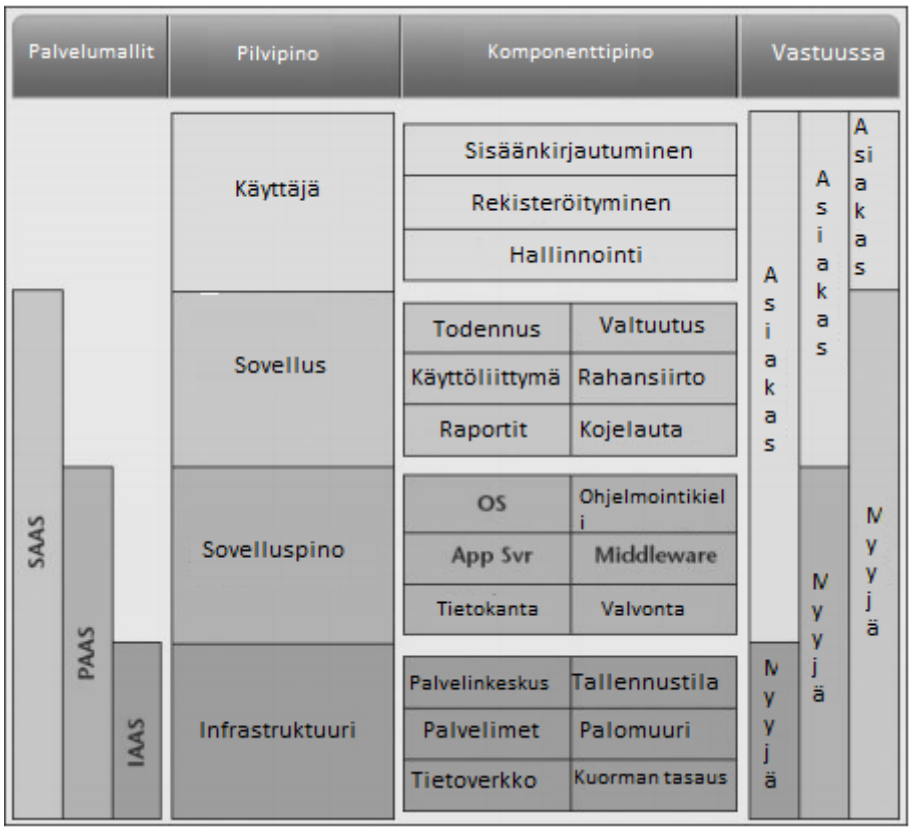
Yrityksen toimiminen internetissä ei ole uusi asia. Pankit ja suuret valmistajat olivat ensimmäisiä, jotka hyödynsivät elektronista tietoverkkoa yrityksen B2B (Business-to-business) toiminnassa esimerkiksi EDI-sanoman avulla. Internetin yleistyessä 1990-luvulla Amazon ja Ebay olivat puolestaan ensimmäisiä yrityksiä, jotka toivat sähköisen kaupankäynnin myös B2C-puolelle (Business-to-Consumer) eli kuluttajille. Nykypäivänä internet on nopea ja luotettava ja siihen on helppo pääsy miljoonilla ihmisillä ympäri maailmaa, joten harvalla yrityksellä nykypäivänä ei ole omia verkkosivuja. Moni PK-yritys myös toimii ainoastaan internetissä eikä heillä ole ollenkaan perinteistä kivijalkaliikettä. (Motahari-Nezhad, Stephenson, Singhal 2009).

B2B- sekä B2C-mallit ovat molemmat hyötyneet lukuisista uusista innovaatioista internetissä, kuten esimerkiksi siirtyminen staattisista sivustoista dynaamisiin ja XML:n (Extensible Markup Language) esittelystä. Tätä Web 1.0 aikakautta kuvaa se, että melkein kaikki backend IT-järjestelmät luotiin, ylläpidettiin ja käytettiin yritysten omistajien toimesta. Moni yritys kuitenkin siirtyi ulkoistamaan liiketoimintaprosessejaan niiden tuomien etujen takia. Näitä etuja olivat muun muassa yrityksen ketteryys, toimintojen tehokkuus, kustannusten lasku sekä parantunut kilpailukyky. Ulkoistetut liiketoimintaprosessit eivät välttämättä olleet aina internetissä. Web 2.0 sekä palveluihin suuntautuneen tietojenkäsittelyn tulemisen jälkeen myös PK-yritykset kiinnostuivat tästä enemmän. (Motahari-Nezhad ym. 2009).

Seuraava vaihe oli pilvipalveluiden synty. Pilvipalvelut vievät internetiä yhä pidemmälle yritysten käytettäväksi. Pilvipalveluiden laskentatehoa voidaan käyttää hyväksi ilman suuria investointeja vaativien laitteiden hankintaa ja niiden avulla saadaan lisää tallennustilaa. Koska pilvipalvelut perustuvat internetiin, ne ovat myös aina saatavilla välittömästi ja monella eri laitteella.

2.1. Pilvipalveluiden palvelumallit

Pilvipalveluiden palvelumalleilla tarkoitetaan sitä mitä asiakkaan ostamaan pilvipalveluun kuuluu eli millä tasolla se toteutetaan, ohjelmistosta fyysisiin palvelimiin. Pilvipalveluiden palvelumallit voidaan jakaa kolmeen pääluokkaan. Nämä luokat ovat Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) sekä Infrastructure-as-a-Service (IaaS). Jokainen taso IaaS-tasolta ylöspäin siirryttäessä vähentää asiakkaalta vaadittua osaamista sekä tuotteiden ja infrastruktuurin tarvetta.



Kuva 1. Pilvipalveluiden palvelumallien jaottelu. (Kavis J Michael 2014: 46).

2.1.1. Software as a Service

The National Institute of Standards and Technology (NIST) määrittelee SaaS- mallin, että asiakkaalla on mahdollisuus käyttää palveluntarjoajan sovelluksia, jotka toimivat palveluntarjoajan pilvi-infrastruktuurissa. Sovellukset ovat käytettävissä usealla asiakasohjelmalla, kuten esimerkiksi verkkoselaimella tai jonkun pienen ohjelman käyttöliittymällä. Asiakkaalla ei ole mahdollisuutta tai tarvetta hallita tai ohjata pilvipalvelun infrastruktuuria, kuten tietoverkkoa, palvelimia, käyttöjärjestelmiä, tallennustilaa tai yksittäisten sovellusten ominaisuuksia, pois lukien jotain sovelluksen henkilökohtaisia asetuksia. (NIST 2011).

Cloud Security Alliance (CSA) on määritellyt SaaS-mallin olevan ohjelmiston toimitusmalli, jossa ohjelmisto ja siihen liittyvä tieto ovat ylläpidettynä keskitetysti tyypillisesti pilvessä. Käyttäjällä niihin on normaalisti pääsy yksinkertaisen asiakasohjelman avulla kuten verkkoselaimella internetin yli. (CSA 2011).

SaaS-malli on siis pinon ylimmäisenä palvelumalleissa. Siinä asiakkaalle toimitetaan täysin toimiva ohjelmisto palveluna. Asiakkaan eli palvelun käyttäjän tarvitsee siis ainoastaan muuttaa halutessaan joitain ohjelmistokohtaisia asetuksia sekä hallita käyttäjiä ja niiden oikeuksia. Pilvipalveluntarjoaja hoitaa kaiken muun infrastruktuuriin liittyvän, käyttöönottoon liittyvän, kuten testauksen, ja myös kaiken joka liittyy itse ohjelmiston tai palvelun toimittamiseen asiakkaalle. SaaS-mallia käytetään yrityksissä usein asioissa, jotka eivät liity suoraan yrityksen ydinliiketoimintaan ja ei ole näin kriittistä yrityksen tai sen toiminnan kannalta. Tämän ansioista heidän ei tarvitse tukea sovelluksen infrastruktuuria, toimittaa tukea tai palkata henkilökuntaa ylläpitämään sitä vaan sen sijaan voivat käyttää ohjelmistoa internetin yli maksamalla palvelun käytöstä. (Kavis 2014: 51–52).

2.1.2. Platform as a Service

Platform as a Service-mallin CSA määrittelee olevan tietojenkäsittely alusta, joka toimitetaan asiakkaalle palveluna. PaaS-malli laajentaa SaaS-mallia tuomalla mukaan myös

rauta-pohjaista palvelua. Tämä tuo helpotusta sovelluksien käyttöönotossa, sillä asiakkaan ei tarvitse huolehtia kustannuksista. Tarvittavan osien ostaminen ja hallitseminen on monimutkikasta puhumattakaan hostingin provisioinnista, joten PaaS- malli mahdollistaa helpon ja edullisen vaihtoehdon. PaaS-mallin mahdollistaa laitteiston tuen internetissä koko ohjelmiston elinkaaren osalta eli sen kehityksestä käyttöönottoon.

NISTin määrittelyn mukaan PaaS-malli mahdollistaa asiakkaan käyttää hyväkseen pilvipalvelun infrastruktuuria luodessaan sovelluksia. Näiden sovellusten luomiseen pilvipalveluntarjoajalla on tuki määriteltyihin ohjelmointikieliin, kirjastoihin, palveluihin ja työkaluihin, joita asiakas voi käyttää. Asiakas ei hallitse tai ylläpidä PaaS-mallin alapuolella sijaitsevaa infrastruktuuria eli tietoverkkoa, palvelimia, käyttöjärjestelmiä, tallennustilaa. Asiakkaalla on kuitenkin oikeudet hallita käyttöönotettuja sovelluksia ja mahdollisesti sovelluksien ylläpito- ympäristön asetuksiin.

Platform as a Service-malli sijaitsee siis SaaS-mallin alapuolella ja IaaS-mallin yläpuolella. PaaS-malli tiivistää monia sovellus pino-tason (application stack) toimintoja ja tarjoaa nämä toiminnot asiakkaalle palveluna. PaaS-malli mahdollistaa sen, että ohjelmistokehittäjän, joka suunnittelee skaalautuvia järjestelmiä, ei tarvitse luoda uudestaan asioita, jotka ovat jo olemassa. Esimerkiksi he voivat keskittyä täysin omaan ansaintalogiikkaan, kun heidän ei tarvitse ohjelmoida uudestaan välimuistin hallintaa, asynkronista viestintää tai tietokannan skaalautuvuutta vaan nämä löytyvät PaaS-mallista sisäänrakennettuna.

PaaS-pilvipalveluntarjoajat hallitsevat kaikkea PaaS-mallin alapuolella olevaa infrastruktuuria eli esimerkiksi muistin jakamista ja voivat jopa vähentää asiakkaan saamaa laskentatehoa, jotta kaikki asiakkaat saavat laskentatehoa tasaväkisesti. Ensimmäiset PaaS-palveluntarjoajat kuten Force.com tai Google Apps Engine hallitsivat yksin PaaS-tasoa kuin myös alapuolella olevaa tasoa. Google Apps Engine vaati alun perin, että kehittäjät käyttävät Python-ohjelmointikieltä ja infrastruktuurin on oltava Googlen palvelinsaleissa. Uusia PaaS-palveluntarjoajia on kuitenkin tullut markkinoille ja he ovat olleet avoimempia ratkaisuissaan. Heidän PaaS-malleissa asiakas on saanut itse päättää missä infrastruktuurissa PaaS-mallia käyttävät ja kehittäjille on monia mahdollisuuksia kehittää ohjelmistojaan kuten Python, Ruby, PHP ja Node.js. Yrityksille tämä on erittäin tärkeää, sillä he monesti suosivat tai jopa vaativat, että ainakin osa ohjelmistosta on yksityisessä pilvessä

yrityksen omissa tiloissa. Erityisesti isommat yritykset käyttävät hybridi pilveä eli pitävät tärkeät tiedot omassa yksityisessä pilvessä ja vähemmän tärkeät julkisessa pilvessä. Myös Google on siirtynyt tarjoamaan useampia ohjelmointikieliä asiakkailleen. (Kavis 2014: 48–50).

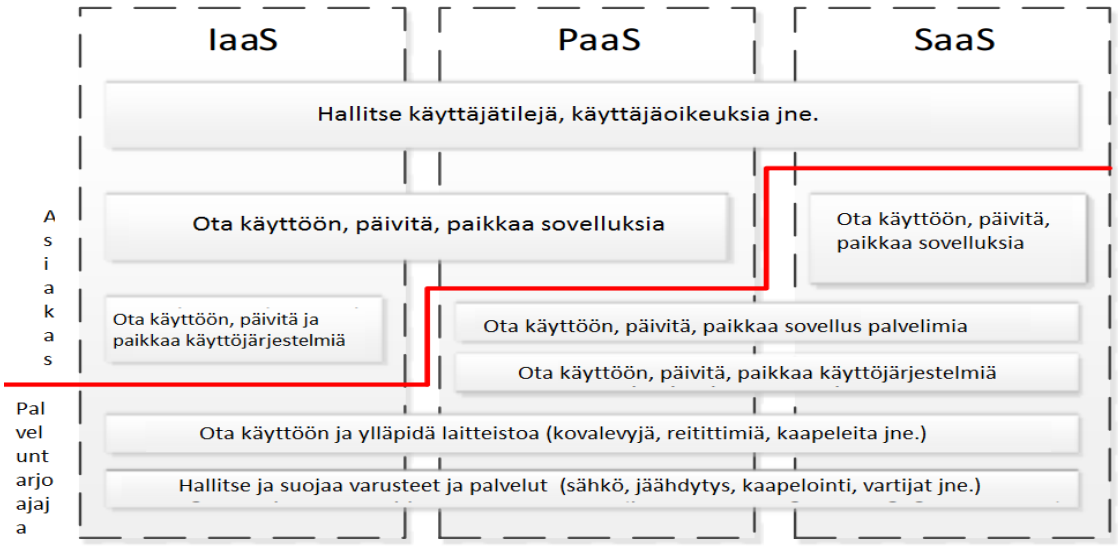
PaaS-mallin yksi erittäin iso hyöty on siinä, että ne monesti tukevat kolmannen osapuolen lisäosia. Näitä lisäosia voi olla esimerkiksi tietokantoihin, valvontaan, tietoturvaan, sähköposteihin tai maksuihin liittyen. Näiden avulla kehittäjät pystyvät tarjoamaan korkean palveluntasositoumuksen ja pystyvät saavuttamaan suuren hyödyn nopeudessa ja kustannustehokkuudessa. Heidän ei siis tarvitse ylläpitää ohjelmointirajapinnan (APIn) alapuolella olevaa teknologiaa. PaaS-malli mahdollistaa yrityksien panostaa omaan ydinosaamiseensa. Vaikka Platform as a Service-malli on pilvipalveluiden palvelumalleista vähiten kehittynyt, niin analyysit odottavat sen kasvavan suuresti seuraavien vuosien aikana. (Kavis 2014: 50–51).

2.1.3. Infrastructure as a Service

NISTin määrittelyn mukaan Infrastructure as a Service-mallissa asiakkaalle tarjotaan pääsy pilvipalvelun laskentatehoon, tallennustilaan, tietoverkkoon sekä muihin tietotekniikan peruslaatuisiin resursseihin. Näiden resurssien avulla asiakas voi suorittaa haluamiaan ohjelmistoja, esimerkiksi käyttöjärjestelmää ja sen ohjelmia. Asiakkaalla ei kuitenkaan ole oikeuksia hallita IaaS-mallin alapuolella olevaa pilvipalvelun infrastruktuuria, mutta asiakkaalla on oikeudet hallita käyttöjärjestelmiä, tallennustilaa, sekä ottaa käyttöön sovelluksia. Asiakkaalla voi myös olla oikeudet hallita tietoverkkojen komponentteja esimerkiksi palomuureja.

Cloud Security Alliance puolestaan määrittelee IaaS-mallin olevan malli, jossa asiakkaalle toimitetaan tietokoneen infrastruktuuri palveluna, tyypillisesti alustan virtualisointi ympäristönä. Infrastruktuurin mukana tulevat myös puhdas tallennustila sekä tietoverkosto. Sen sijaan, että asiakas ostaisi palvelimet, ohjelmiston, tilan palvelinkeskukselle ja muut tarvittavat komponentit, ostavat he nämä resurssit täysin ulkoistettuna palveluna.

IaaS-mallissa iso osa tehtävistä, jotka liittyvät fyysisen palvelinsalin ja fyysisen infrastruktuurin ylläpitoon, ovat tiivistetty ja saatavilla palveluiden kokoelmana. Näihin palveluihin päästään käsiksi joko koodi-pohjaisella tai internet-pohjaisella käyttöliittymällä. IaaS-mallin avulla asiakkaat pääsevät kokonaan eroon fyysisen infrastruktuurin hoitamisesta, mutta kehittäjien tulee esimerkiksi edelleen ohjelmoida sovellukset kokonaan ja ylläpitäjien tulee edelleen asentaa, hallita ja paikata kolmannen osapuolen ratkaisut. Infrastructure as a Servicen-mallin ansiosta asiakkaan ei enää tarvitse tilata fyysisiä komponentteja toimittajilta ja odottaa toimitusta, että pääsevät asentamaan niitä, vaan samat resurssit ovat asiakkaan käytettävissä virtuaalisena, silloin kuin niitä tarvitaan. Tämä onnistuu kutsumalla ohjelmointirajapintaa (API) tai käynnistämällä internet-pohjainen hallinnointikonsoli. IaaS-mallissa kustannukset kertyvät, kun palvelu on käynnissä, eli palvelun ollessa sammutettuna ei asiakkaalle synny myöskään kuluja. Mallin avulla asiakas pystyy keskittämään resurssinsa ydintoimintaan eli sovelluksien kehittämiseen ja hallinnointiin eikä aikaa mene hukkaan palvelinkeskuksien ja infrastruktuurin hoitamiseen. (Kavis 2014: 47).



Kuva 2. Pilvipalveluiden palvelumallien tehtävät jaoteltuina. (ENISA 2015).

2.2. Pilvipalveluiden toimitusmallit

Palvelumallien lisäksi pilvi voidaan jakaa neljään eri ryhmään niiden toimitusmallien perusteella (Deployment model). Nämä mallit ovat julkinen, yksityinen, hybridi sekä yhteisö. Nämä neljä mallia voivat myös yhdistyä eri tavoilla, riippuen markkinoista ja asiakkaiden vaatimuksista. Esimerkiksi virtuaalinen yksityinen pilvi, joka on tapa hyödyntää julkisen pilven infrastruktuuria yksityisenä tai osittain yksityisenä ja yhdistää nämä resurssit asiakkaan palvelinkeskuksen sisäisiin resursseihin. Yhdistäminen tapahtuu tyypillisesti VPN:llä eli virtuaalisella erillisverkolla (Virtual Private Network). (CSA 2014).

2.2.1. Julkinen pilvi

NISTin määritelmän mukaan julkinen pilvi on pilvi-infrastruktuuri, joka on yleinen, avoin sekä kaikkien käytettävissä. Sitä hallitsee ja ylläpitää yritys, akateeminen taho, julkinen taho tai jokin niiden risteytys. Se sijaitsee fyysisesti pilvipalveluntarjoajan tiloissa.

Julkinen pilvi on multitenant-ympäristö, missä loppukäyttäjä maksaa käytetyistä resursseista yhdessä muiden asiakkaiden kanssa. Loppukäyttäjällä ei ole mitään tietoa missä heidän ohjelmisto fyysisesti sijaitsee, muuten kuin palvelinkeskuksen sijainti. Fyysisen laitteiston yläpuolelle lisätään tiivistelmä taso (abstraction layer) ja tämä näytetään loppukäyttäjälle ohjelmistorajapintoina. Loppukäyttäjä pystyy hyödyntämään näitä rajapintoja luomalla virtuaalisia laskentaresursseja, jotka pyörivät isoissa resurssien ryppäissä, ja ovat monien käytössä (Kavis 2014: 53).

Julkisten pilvien etuja ovat muun muassa käyttö-pohjainen hinnoittelu missä asiakas maksaa ainoastaan resursseista joita hän on käyttänyt. Tämä mahdollistaa sen, että asiakas voi ottaa käyttöönsä enemmän laskentatehoa kuin hän tarvitsee sekä vähentää sen määrää, kun tarvetta ei enää ole. Asiakkaan ei enää tarvitse hankkia fyysistä laitteistoa, joten he voivat eliminoida turhia laskenta syklejä. Laskenta syklit laskevat kuinka kauan prosessointiaikaa sovelluksella kestää suorittaa. Julkisen pilven etuna on myös joustavuus. Loppukäyttäjällä on näennäisesti rajattomasti resursseja käytettävissä ja loppukäyttäjä voi

määritellä ohjelmistollisia ratkaisuja, jotka dynaamisesti nostavat tai laskevat resurssien käyttöjä, jolloin ne kestävät myös mahdolliset piikit kuormituksessa. Tämän avulla loppukäyttäjä voi reagoida kuormituksen piikkeihin reaaliajassa, kun taas yksityisessä, asiakkaan tiloissa sijaitsevalla palvelimella, asiakkaan tulee jo entuudestaan omistaa tai vuokrata resurssit piikkien hallintaan. Kun loppukäyttäjä päätyy ottamaan julkisen pilvipalvelun käyttöönsä, hän käytännössä ulkoistaa palvelinkeskusten ja infrastruktuurin hallinnan yritykselle, jonka ydintoiminta ja osaaminen ovat näiden hallinta. Näin loppukäyttäjä joutuu vähemmän huolehtimaan infrastruktuurista ja voi keskittyä enemmän omaan ydinosaamiseensa. (Kavis 2014: 54).

Julkisilla pilvipalveluilla on myös heikkouksia. Yksi näistä heikkouksista on hallinnan puute. Kun asiakas ottaa käyttöönsä julkisen pilvipalvelun, hän joutuu käytännössä luottamaan siihen, että pilvipalveluntarjoaja pitää kiinni SLA:ssa (Service-level agreement) eli palveluntasosopimuksessa tekemistään lupauksista suorituskyvyn ja saatavuuden suhteen. Jos pilvipalveluntarjoajalla on palveluskatkos, eikä asiakas ole suunnitellut tilannetta asianmukaisesti, on asiakas täysin pilvipalveluntarjoajan armoilla palauttaakseen palvelun toimintaan. Myös sääntely tuo omia haasteita julkisen pilvipalvelun käyttöönottoon. Sääntelyt kuten PCI DSS (Payment Card Industry Data Security Standard), Yhdysvalloissa HIPAA (Health Information Portability and Accountability Act) ja tietosuojakysymykset pakottavatkin yrityksiä usein hybridi pilven käyttöön julkisen pilven sijaan. Rajalliset kokoonpanot saattavat myös olla esteenä julkisen pilvipalvelun käyttöön. Julkisten pilvipalveluiden kokoonpanot eli muun muassa laitteisto on määritelty niin, että ne sopivat suurimpaan osaan tilanteista, mutta jos asiakkaalla on tarvetta erityiselle laitteistolle, ei pilvipalveluntarjoajalla todennäköisesti ole sitä tarjota. (Kavis 2014: 55).

2.2.2. Yksityinen pilvi

Yksityinen pilvi on tarkoitettu olevan käytössä ainoastaan yhdellä organisaatiolla, joka käsittää useampia käyttäjiä, esimerkiksi liiketoimintayksikköjä. Sitä hallitsee ja ylläpitää organisaatio itse, kolmas taho tai näiden yhdistelmä. Yksityinen pilvi voi sijaita fyysisesti joko paikan päällä tai jossakin muualla. (NIST 2014).

Yksityisen pilvipalvelun yksi isoista hyödyistä on siinä, että se poistaa monia julkisen pilvipalvelun heikkouksia kuten hallinnan puutteen, sääntelyn ongelmat sekä rajalliset kokoonpanot. Toisin kuin julkiset pilvet, jotka sijaitsevat aina pilvipalvelun palvelinkeskuksissa, yksityiset pilvet voivat sijaita joko yrityksen omissa tiloissa tai pilvipalveluntarjoajan palvelinkeskuksissa. Jos yksityinen pilvi sijaitsee paikan päällä yrityksen omissa tiloissa, käyttäjillä on täysi hallinta infrastruktuurista, sillä he ylläpitävät itse palvelinkeskusta ja voivat lisätä tai poistaa siitä mitä laitteistoa haluavat. Jos pilvi sijaitsee pilvipalveluntarjoajan tiloissa, on käyttäjä pilvipalveluntarjoajasta riippuvainen laitteiston osalta, mutta heidän resurssejaan ei jaeta muiden käyttäjien kesken. Tämä tarjoaa käyttäjälle enemmän vaikutusmahdollisuuksia ja parantaa tietoturvaa, mutta myös kustannukset ovat korkeammat kuin julkisessa pilvessä. Yksityiset pilvet laskevat joitain sääntelyn riskejä tiedon omistamisen, yksityisyyden ja tietoturvan osalta, koska saatuja resursseja ei jaeta kenenkään kanssa vaan niihin on pääsy ainoastaan palvelun tilaajalla. (Kavis 2014: 55–56).

Yksityinen pilvi kuitenkin heikentää joitain pilven parhaita puolia kuten joustavuutta, resurssien yhdistämistä ja mahdollisuutta maksaa ainoastaan käyttämistään resursseista. Yksityisen pilven käyttäjät voivat määritellä resurssien käyttöä vastaavalla tavalla kuin julkisessa pilvessä, mutta tämä mahdollisuus on rajattu siihen infrastruktuuriin, joka on jo ostettu ja jota hallitaan sisäisesti. Tämä puolestaan nostaa kustannuksia sekä vähentää ketteryyttä, koska sisäisten resurssien on hallittava fyysistä infrastruktuuria sekä ylimääräinen kapasiteetti tulee ensin hankkia ja sen jälkeen vielä hallita. Ylimääräisen kapasiteetin hankkiminen puolestaan poistaa resursseista maksamisen tarpeiden mukaan, sillä tämä kapasiteetti on asiakkaan käytössä vaikka sille ei olisi tarvetta. (Kavis 2014: 56).

2.2.3. Hybridi pilvi

Hybridi pilvi määritellään NISTin ja CSAn toimesta olevan yhdistelmä kahdesta tai useammasta eri pilven toimitusmalleista (julkisesti, yksityisestä, yhteisöstä). Nämä kaksi tai useampaa toimitusmallia toimivat itsenäisinä kokonaisuutena, mutta ovat sidottu yhteen

standardeilla tai teknologialla, joka mahdollistaa tiedon ja sovelluksen siirrettävyyden näiden välillä. (Kavis 2014: 57).

Hybridi pilven avulla on siis mahdollista saada eri pilvipalveluiden toimitusmallien parhaita puolia käyttöön yhtä aikaa. Hybridi-pilvipalvelun julkista pilveä tulisi käyttää mahdollisimman paljon, jotta käyttäjä saisi kaikki pilvipalvelun mahdollistamat hyödyt käyttöönsä eli joustavuuden ja suuret resurssien yhdistämisen. Käyttämällä kuitenkin yksityistä pilveä julkisen pilven rinnalla, käyttäjä pystyy ratkaisemaan julkisen pilven ongelmia eli tiedon omistajuuden ja yksityisyyden ongelmat. (Kavis 2014: 57).

Hybridi pilven etuja ovat yksityisen pilven turvallisuus ja hallinnointi ja pääomakustannusten pieneminen johtuen organisaation infrastruktuurin uusimisesta, jossa tarpeet ulkoistetaan julkisen pilvipalvelun pilvipalveluntarjoajalle. Hybridi pilvi tehostaa resurssien jakamista sekä kustannusten vähentämistä väliaikaisissa projekteissa, koska hybridi pilvessä voidaan käyttää julkisen pilven etuja. Julkisen pilven käytön myötä myös infrastruktuurin kustannusten optimointi helpottuu sovelluksien kehityksen eri vaiheissa. Julkinen pilvi voidaan valjastaa kehitykseen ja testaukseen, samalla kun yksityistä pilveä voidaan käyttää sovelluksen tuotantoon. SaaS-malli julkisessa pilvessä myös vähentää kustannuksia sovelluksen poistamisessa käytöstä. Hybridi pilvi myös tukee cloud-burstingia, jonka avulla äkillistä kuormaa voidaan tasata julkisen pilven laskentateholla ja sovelluksien käyttö ei häiriinny. Hybridi pilvi myös parantaa organisaation ketteryyttä kokonaisvaltaisesti julkisen pilven avulla. (Goyal Sumit 2014).

Koska hybridi pilvi ulottuu myös organisaation ulkopuolelle, avaa se mahdollisuuden useammalle hyökkäykselle. Organisaatioiden, jotka käyttävät hybridi pilveä, tulisi myös ottaa huomioon, että kun he käyttävät ja hallitsevat monimutkaista ympäristöä hallintatyökaluilla, tulee heidän myös pohtia sen vaikutusta tietoturvaan. Hallintatyökalu voi olla osa pilvipalvelua tai kolmannen osapuolen tuottama, mutta sen tulisi hallita identiteetti ja sen tulisi pakottaa tietoturva koko hybridi pilven ympäristöön. Helpompi tapa hallita identiteettiä on ulottaa yrityksen nykyinen identiteetti ja pääsynvalvonta julkiseen pilveen. Tällä lähestymistavalla saattaa olla kuitenkin yrityksen kannalta huonoja vaikutuksia tietoturvaan. Hybridi pilvi helpottaa tiedonsiirtoa yksityisestä ympäristöstä julkiseen ympäristöön, mutta tämä saattaa vaikuttaa yksityisyyteen sekä tiedon eheyteen, koska

julkisen pilven yksityisyyden hallinta eroaa merkittävästi yksityisen pilven vastaavasta. Myös yleiset tietoturvaan liittyvät riskit ovat hybridi pilven huolena, kuten esimerkiksi kuinka salausavaimia hallitaan julkisessa pilvessä verrattuna täysin yksityiseen pilveen. (Goyal Sumit 2014).

2.2.4. Yhteisöpilvi

Yhteisöpilvi eli Community cloud on pilvipalveluiden toimitusmalli, jonka käyttäjinä on jokin tietty yhteisö samasta organisaatiosta ja heillä on jokin yhteinen tehtävä tai määränpää. Yhteisöpilven voi omistaa ja hallita yksi tai useampi organisaatio yhteisön sisältä, kolmas taho tai näiden yhdistelmä. Yhteisöpilvi voi sijaita paikan päällä yrityksen tiloissa tai pilvipalveluntarjoajan palvelinkeskuksessa. (NIST 2014).

Yhteisöpilvi on edelleen nuori, mutta on saavuttamassa suosiota erityisesti startup-yritysten ja PK-yritysten keskuudessa. Yhteisöpilvi on yksityisen ja julkisen pilven välimaastossa. Sen tarkoituksena on olla sopiva omalle kohderyhmälleen. Yhteisöpilvi on samantyylinen kuin yksityinen pilvi, mutta sen infrastruktuuri ja laskennalliset resurssit ovat eksklusiivisia kahdelle tai useammalle organisaatiolle yhden sijaan. Näillä organisaatioilla on yhteinen näkökohta joko tietoturvassa, yksityisyydessä tai säännöksissä. Yhteisöpilvi pyrkii yhdistämään klusteri verkon hajautetut resurssit, digitaalisen ekosysteemin hajautetun hallinnan sekä vihreän tietojenkäsittelyn kestävyyden. Samaan aikaan yhteisöpilvi pyrkii hyödyntämään itsehallinnan hyötyjä autonomisesta tietojenkäsittelystä. (Goyal Sumit 2014).

Yhteisöpilven rakentaminen ja käyttöönotto on todennäköisemmin halvempaa kuin täysin yksityisen pilven, sillä kustannukset jaetaan kaikkien yhteisöpilveen tulevien kesken. Tästä huolimatta yhteisöpilven hallinnointi voidaan ulkoistaa pilvipalveluntarjoajalle, jolloin pilvipalveluntarjoaja olisi puolueeton kolmas osapuoli, jolla ei ole mitään sitoumuksia yhteenkään muuhun osapuoleen, pois lukien mitä sopimuksessa on mainittu. Yhteisöpilvessä sijaitsevien työkalujen avulla pilveen tallennettua tietoa voidaan käyttää hyväksi koko toimitusketjun osalta, kuten esimerkiksi palautuksien seurantaa. (Goyal Sumit 2014).

Yhteisöpilven heikkona puolena ovat, että sen kustannukset ovat julkista pilveä suuremmat sekä yhteisöpilvessä on kiinteä määrä kaistanleveyttä ja tallennustila on jaettu kaikkien pilven käyttäjien kesken. (Goyal Sumit 2014).

2.3. PK- yritykset ja pilvipalvelut

Pilvipalveluista on tulossa todella merkittävä asia PK-yritysten toiminnassa ja kilpailukyvyssä. Pilvipalvelut tarjoavat PK-yrityksille skaalautuvia infrastruktuureja ja mahdollisuuksia palveluina, joten yritykset voivat käyttää niitä, kun tarvitsevat ja sen verran kuin tarvitsevat. Pilvipalveluiden ja niiden eri mallit auttavat yrityksiä toimimaan älykkäämmin tarjoamalla joustavan ja ennen kaikkea kustannustehokkaan pääsyn teknologiaan ja tietoon. Pilvipalvelut mahdollistavat yrityksissä ajattelun omien seinien ulkopuolelle, sillä nyt yritykset voivat ottaa käyttöönsä markkinoiden parhaat ratkaisut ja valita tehokkaimmat tietotekniset palvelut useammasta lähteestä yhtä aikaa. Näin työntekijöiden ja asiakkaiden vaatimuksiin voidaan vastata nopeammin ja pienemmillä kustannuksilla. Yrityksiltä, riippumatta yrityksen koosta, puuttuu usein tarpeellinen ymmärrys tietotekniikasta ja tästä syystä projektien tietotekninen toteutus jää huonommaksi, jolloin myös sen hyöty yritykselle ja liiketoiminnalle jää heikoksi tai olemattomaksi. Tämä on ongelma erityisesti pienemmissä yrityksissä, joilla ei ole osaavaa IT-henkilökuntaa tai johdon tietotekninen osaaminen on heikkoa. Pilvipalvelut eivät tuo tähän ratkaisua, mutta pilvipalvelut helpottavat varsinkin PK-yritysten toimintaa yksinkertaistamalla tietotekniikan käyttöä. (Open Group 2012).

Tyypillisesti yrityksen IT-organisaatio on odottanut, että heille tulee pyyntö toteuttaa jokin tietotekninen projekti, jonka tarkoituksena on tukea yritystä. Pyynnön jälkeen he ovat kartoittaneet vaatimukset, rakentaneet palvelun sovittujen tekniset tietojen mukaisesti ja sen jälkeen ylläpitäneet sitä. Koko prosessi on siis ollut tyypillisesti reagoiva eli muualta tullut pyyntö on se, joka on laukaissut toiminnot. IT-organisaation toiminta voi olla myös ennakoivaa. Tällöin IT-organisaatio ei odota muualta tulevaa pyyntöä vaan IT-organisaa-

tio voi tarjota etukäteen määriteltyä ja sovittua palvelukatalogia. Palvelukatalogista voidaan tehdä tilauksia. Palvelukatalogi vaatii kuitenkin etukäteissuunnittelua ja erityisesti IT-puolen huomioon ottamista. Palvelukatalogissa olevat palvelut eivät vaadi tilauksen jälkeen rakentamista vaan ne ovat valmiina käytettäväksi heti tai viimeistään parin päivän sisällä. PK-yritysten IT-organisaatiot ovat todella pieniä tai olemattomia, joten heillä ei ole varaa raskaaseen sisäiseen palvelukatalogiin. Pilvipalvelut kuitenkin mahdollistavat PK-yrityksille täyden palvelukatalogin, josta yritys voi tilata haluamansa palvelun, kun sille on tarvetta. Pilvipalveluntarjoajat voivat toimia niin suurella volyymilla, että saavuttavat mittakaavaedun, mihin yksittäisellä PK-yrityksellä ei ole mahdollisuutta, ja pystyvät palvelemaan satoja PK-yrityksiä. (Open Group 2012).

PK-yritykset hyötyvät pilvipalveluista esimerkiksi laajentuessaan uusille markkinoille tai tuottaessaan uusia liiketoimintalinjoja tai jopa kokonaan uusia liiketoimintoja. Kun yritys käyttää pilvipalvelua, voidaan tarvittavat uudet ohjelmistot ja muut tarpeelliset tietotekniset puolet ottaa käyttöön välittömästi pilvipalvelussa sen sijaan, että ne jouduttaisiin rakentamaan kokonaan itse. Pilvipalveluiden ansiosta yritys voi mahdollisesti saada tuotteensa nopeammin markkinoille ja sen seurauksena saada uusia asiakkaita sen sijaan, että asiakkaat olisivat siirtyneet kilpailijalle. Pilvipalvelut auttavat yritystä pysymään ketteränä, kun IT-palveluita voidaan ottaa käyttöön tai poistaa käytöstä nopeasti ja periaatteessa rajattomalla kapasiteetillä. PK-yritysten ei myöskään tarvitse sitoa suuria määriä pääomaa IT-palveluihin, kun he voivat vuokrata nämä palvelut pilvipalveluntarjoajalta ja vuokra voidaan päättää heti, kun sitä ei enää tarvita. (Open Group 2012).

2.3.1. Pilvipalveluiden hyödyt PK-yrityksille

Tietotekniikka on erittäin tärkeä osa-alue nykypäivänä melkein jokaisella toimialalla. PK-yrityksiä pidetään maailmalla elintärkeänä maailmanlaajuiselle taloudelle, mutta johtuen PK-yrityksille ominaisista rajoitteista, kuten työntekijöiden määrästä ja pääoman suuruudesta, PK-yritykset ovat usein asenteeltaan konservatiivisia uusia teknologioita kohtaan. PK-yritysten resurssien puute verrattuna suuriin yrityksiin johtuu monesta asiasta, kuten esimerkiksi siitä, että PK-yritykset toimivat usein erittäin pirstaloituneilla toimialoilla,

kuten vähittäiskaupan alalla ja palveluissa. Näillä aloilla esiintyy todella runsasta kilpailua ja moni kilpailija käyttää todella aggressiivista hinnoittelustrategiaa. PK-yritykset ovat myös usein omistajavetoisia, jolloin osa yrityksen tuottamasta voitosta maksetaan suoraan omistajalle palkkana. Tämän takia pääomaa on vähemmän uusiin investointeihin. Verolain muutoksella tai korkojen muutoksella on myös suurempi vaikutus PK-yrityksiin kuin isompiin yrityksiin, jolloin PK-yritysten päämäärä on helposti lyhyen ajan tähtäimellä suuremmassa likviditeetissä ja uusien teknologioiden adoptointiin suhtaudutaan konservatiivisemmin. Vaikka PK-yritykset ovat konservatiivisempia uusia teknologioita kohtaan, osittain johtuen heidän tarpeestaan yksinkertaisempiin IT-ratkaisuihin, ovat he kuitenkin monesti innokkaita ulkoistamaan tietotekniset vaatimuksensa. PK-yrityksien innostus ulkoistamiseen johtuu siitä, että näin ollen he voivat keskittyä enemmän ydinosaamiseensa. Tästä johtuen myös pilvipalvelut voivat olla houkutteleva vaihtoehto PK-yrityksille. (Mojtaba 2012).

Monesti pilvipalveluihin siirtymisen aloite yrityksessä tapahtuu päälliköiden, hallituksen jäsenien tai yrityksen johtajien tasolta, ei IT-asiantuntijoiden. Usein siirtymisen pilvipalveluun myös johtaa teknologia-painotteinen kolmas osapuoli. Yritysten siirtymisestä pilvipalveluun, jopa 61 % johtuu yrityksen toimitusjohtajan tai muun johtotason työntekijän toimesta. (Rackspace 2015).

Yksi pilvipalveluiden suurimmista hyödyistä PK-yrityksille on kustannuksien aleneminen ja se onkin yksi suurimmista syistä miksi PK-yritykset siirtyvät pilvipalveluiden käyttäjäksi. Riippuen pilvipalvelun mallista, kustannuksissa voidaan säästää niin laitteiston kuin ohjelmistonkin osalta. Myös hallinnointi- ja ylläpitokustannuksissa voidaan säästää. Normaalisti pilvipalvelut nähdään yrityksen tapana muuntaa pääomamenot juokseviksi kuluiksi, mutta onnistuneella siirtymisellä myös juoksevat kulut voivat laskea. Suurimmat arvon lähteet pilvipalveluista ovat olleet investoinnin maksimoinnin mahdollisuus sekä se, että yritys on voinut keskittyä täysin omaan ydinosaamiseensa teknologian sijaan. Siirtyminen talonsisäisestä infrastruktuurista pilvipalveluun voi tuoda yritykselle jopa 37 % säästön kuluihin. (Mojtaba 2012).

Pilvipalvelut parantavat yritysten hallintaa tuloistaan ja menoistaan niin rahoitushenkilökunnan kuin asiakkaiden osalta ja heidän hallinnollinen taakka vähenee. Myös yrityksen

kassavirran hallinta helpottuu, kun pilvipalveluiden etukäteismaksu on pieni ja pilvipalvelut toimivat kuukausittaisella laskutuksella eikä isoja laitehankintoja tarvitse tehdä sekä erilaisten muuttujien määrä pienenee, kuten sähkön hinnanvaihtelu. PK-yritysten lisäksi myös kehitysmaat hyötyvät pilvipalveluiden matalista kustannuksista, sillä kummallakaan ei ole aina mahdollisuutta tehdä isoja sijoituksia, mutta kuitenkin he tarvitsevat pilvipalveluiden tuomia palveluita kehittyäkseen. (Azarnik, Shayan, Alizadeh & Karamizadeh 2012).

Vuonna 2013 94 % PK-yrityksistä olivat sitä mieltä, että ohjelmistojen oleminen ajan tasalla on tärkeää. Tästä huolimatta ainoastaan 59 % yrityksistä ilmoitti, että heidän kaikki ohjelmistonsa ovat päivitettyinä, vaikka heillä olisi käytössään päivityksiin tarvittavat resurssit. Yksi syy tähän on se, että PK-yrityksillä menee viikossa noin 11 tuntia pelkästään ohjelmistopäivityksiin ja suuremmilla yrityksillä jopa 15 tuntia viikossa. F-Securen havaitsemasta TOP10 haittaohjelmasta 70 – 80 % olisi ollut estettävissä, jos ohjelmistot olisivat olleet päivitettyinä. (Gold 2014). Pilvipalveluihin siirtyminen helpottaisi yrityksien ohjelmistopäivityksiä huomattavasti kuin myös uusien ohjelmistojen käyttöönottoa. Pilvipalveluntarjoajat ylläpitävät pilvipalveluiden ohjelmistoja, joten PK-yrityksien ei enää tarvitse itse päivittää kaikkia käyttämiään ohjelmistoja ja he säästävät aikaa. Pilvipalveluiden myötä myös järjestelmien hallinnointi ja ylläpito helpottuu ja yksinkertaistuu, sillä yritys pääsee ohjelmistoihin käsiksi verkkoselaimella tai vastaavalla yksinkertaisella pääteohjelmalla. Vastaavasti ylläpito helpottuu ja tulee varmemmaksi, kun ylläpitäjä voi olla varma, että kaikilla käyttäjillä on käytössään oikea ja viimeisin versio ohjelmistosta. Yritykselle tärkeä tieto voidaan myös varmuuskopioida todella nopeasti, jolloin tiedon häviämisen riski pienenee. (Mojtaba 2012).

Nykyajan taloudellisessa ympäristössä yrityksen yksi tärkeimmistä ominaisuuksista on vastata asiakkaiden nopeasti muuttuviin tarpeisiin. PK-yrityksille se voi olla jopa ehto selviämiselle ja myös tässä pilvipalvelusta voi olla apua PK-yrityksille. Pilvipalvelut mahdollistavat yrityksille nopeamman reagoinnin prosesseihinsa, tuotteisiinsa ja palveluihinsa markkinoiden vaihtelusta johtuen. Yritykset voivat jättää pois järjestelmien infrastruktuurin eli laitteiston huollon, varaosat, uusien koneiden lisäämisen ja infrastruktuurin ohjelmistot, sillä niistä vastaavat pilvipalveluntarjoajat. Tämän lisäksi pilvipalveluntarjoajat ovat vastuussa varmuuskopioinnista, kunhan yritys itse on määritellyt sen, ja

jokainen ohjelmisto on kaikkien käyttäjien saatavilla välittömästi. (Azarnik ym. 2012). Pilvipalveluiden ansiosta yrityksen omistama tieto ja ohjelmistot on saatavilla työntekijöille, yhteistyökumppaneille ja asiakkaille riippumatta heidän fyysisestä sijainnista (Mojtaba 2012).

Pilvipalvelut mahdollistavat myös palvelumallit, jotka eivät aikaisemmin olleet mahdollisia. Tällaisia palvelumalleja ovat muun muassa interaktiiviset ohjelmistot, jotka ovat tietoisia sijainnistaan, ympäristöstään ja kontekstista. Nämä ohjelmistot saavat tietonsa joko ihmiseltä tai sensoreilta, kuten kosteus- ja liikesensorit. Myös tiedon käsittely yrityksissä on nopeutunut, kun yritykset voivat käsitellä pilvipalveluiden laskentatehon avulla todella suuria määriä tietoa suhteellisen lyhyessä ajassa. Analyytikot voivat käyttää pilvipalvelun laskentatehoa hyväkseen, jotta ymmärtävät paremmin asiakkaita, asiakkaiden ostokäyttäytymistä tai tuotantoketjua. Yritykset ovat nykyään yhä enemmän tietoisia ympäristövaikutuksista ja siirtyminen pilvipalvelun käyttäjäksi voi auttaa yritystä pienentämään omaa ekologista jalanjälkeään. Pilvipalveluntarjoajilla on usein suuret palvelinkeskukset ja heillä on suuremmat resurssit valita ympäristöystävällisiä energiamuotoja ja heillä on myös paremmat mahdollisuudet valita palvelinkeskuksien sijainnit viilennyksen kannalta edullisista kohteista. (Azarnik ym. 2012).

Pilvipalveluista on myös tietoturvan kannalta hyötyä PK-yrityksille. Koska pilvipalveluita käyttävät useat asiakkaat, myös niiden tietoturvaan on panostettu aivan eri tavalla kuin yksittäisellä PK-yrityksellä olisi mahdollista panostaa. Jos PK-yritys panostaisi yksistään pilvipalveluihinsa käyttämän summan pelkästään tietoturvaan, ei se välttämättä saisi yhtä turvallista alustaa käyttöönsä. Pilvipalveluissa tietoturvaa parantavat muun muassa suodatus, virtuaalikoneiden ja hypervisorin tuoma suoja ja jatkuva päivittämien. Pilvipalveluiden palvelimia sijaitsee myös useassa maantieteellisessä sijainnissa ja yrityksen tieto tai ohjelmisto voidaan prosessoida fyysisesti lähellä tai toimittaa lähemmästä sijainnista, jolloin tietoverkon latenssi on pienempi ja parantaa saatavuutta sekä tehokkuutta. Usea maantieteellinen sijainti auttaa myös ehkäisemään paikallisia ongelmia, kuten luonnonkatastrofeja ja voi auttaa palvelunestohyökkäyksissä. Pilvipalveluissa on myös hyvä vastausaika mahdollisiin tapahtumiin ja uhkien hallinointiin. Pilvipalveluntarjoajat myös joutuvat kilpailemaan keskenään ja tietoturva on yksi todella suuri kilpailuvaltti. Asiakkaat, kuten PK-yritykset, tekevät ostopäätöksensä monen asian summana ja tietoturva on

yksi niistä. Pilvipalveluntarjoajalla tulee olla siis hyvä maine luottamuksellisuudessa, eheydessä, joustavuudessa ja tietoturvassa, jotta asiakas voi luottaa heihin. (ENISA 2009 & ENISA 2015).

Tietoturva on todella tärkeää niin pilvipalveluntarjoajalle kuin asiakkaille. Tietoturva tulee myös ottaa huomioon aina, kun tehdään jotain uutta, esimerkiksi verkkosivusto yritykselle. Sivuston luominen on yksinkertaista, mutta tietoturvan huomioiminen ei aina ole niin helppoa, varsinkaan PK-yritykselle. Pilvipalveluntarjoajien koosta johtuen heillä on kuitenkin resurssit kehittää ja ottaa käyttöön erilaisia tietoturvaa parantavia ohjelmistoja ja voivat tarjota näitä asiakkailleen käytettäväksi. Asiakkaat voivat menettää jonkin verran muokattavuutta, mutta saavat vastineeksi huomattavasti paremman tietoturvan. Kolmansien osapuolten, lähinnä tietoturvayrityksien, mukaan tuleminen on myös mahdollista ja heidän tehtävänään on tarkistaa jatkuvasti mahdollisia tietoturva-aukkoja, tätä palvelua kutsutaan myös nimellä Security-as-a-Service ja myös pilvipalveluntarjoaja voi tehdä heidän kanssaan yhteistyötä. Pilvipalvelut mahdollistavat myös tarkemman ja tehokkaamman lokien pitämisen, joten asioiden tarkistaminen jälkikäteen on helpompaa ja virtualisoinnin takia mahdollista ilman, että palvelua tarvitsee ajaa alas. Pilvipalveluiden palvelinkeskukset ovat myös fyysisesti vartioituja ja suojattu erilaisilta katastrofeilta. (ENISA 2009 & ENISA 2015).

2.3.2. Pilvipalveluiden haasteet PK-yrityksille

Vaikka pilvipalvelut ovat todella hyödyllisiä PK-yrityksille ja tuovat muiden etujen lisäksi parannusta myös tietoturvaan, on pilvipalveluissa itsessään myös asioita, jotka ovat haasteellisia. PK-yrityksiä ovat hidastaneet pilvipalveluiden suhteen muun muassa osaavan henkilökunnan puute. PK-yrityksellä ei välttämättä ole talon sisällä työntekijää, jolla olisi kattava tieto pilvipalveluista ja niiden tuomista hyödyistä tai haasteista. Pilvipalvelut saattavat vaikuttaa liian monimutkaisilta eikä täysin tiedetä mitä pilvipalveluntarjoaja oikeasti tarjoaa palveluillaan. Osittain syynä tähän on koulutuksen puute yrityksissä, yrityksissä ei ole pilvipalveluita ymmärtävää johtoa eikä asiakasrajapinnan tukea. PK-yri-

tyksien suurimpia huolenaiheita ovat myös tiedon turvallisuus ja yritykset eivät ole halukkaita antamaan pilvipalveluntarjoajille täyttä hallintaa tietoihin. PK-yrityksien huolenaiheina on myös tiedon fyysinen sijainti sekä sitä suojaavat lainkäyttöalueet. Myös yhteensopivuus voi olla ongelma pilvipalvelun käyttäjäksi siirtyessä, sillä asiakasyrityksen ohjelmointirajapinta ei välttämättä ole yhteensopiva pilvipalveluntarjoajan vastaavan kanssa. Yhteensopivuus on kuitenkin PK-yrityksille vaikea asia, sillä heillä ei välttämättä ole mitään tietoa aiheesta eivätkä he myöskään osaa varautua siihen etukäteen. Pilvipalveluntarjoajat pitävät yhtenä suurimpana haasteena pilvipalveluita koskevia sopimuksia, kun taas PK-yritykset ovat usein hämmentyneitä vaikeista termeistä, joita sopimuksissa käytetään. PK-yrityksien mahdollinen tiedon puute näkyy haasteena myös sopimuksissa PK-yrityksien ja pilvipalveluntarjoajien välillä. Pilvipalveluntarjoajat voivat sanella sopimuksen kohdat johtuen PK-yrityksien vajavaisesta ymmärryksestä asiaa kohtaan ja tämä voi olla haitaksi asiakasyritykselle. (Khan & Al-Yasiri 2015).

Ohjelmistojen haavoittuvuudet ovat iso haaste pilvipalveluissa. Esimerkiksi PK-yrityksen käyttämässä SaaS-pohjaisessa sähköpostipalvelussa voi olla haavoittuvuus SQL-injektiolle ja asiakasyrityksen arkaluontoiset sähköpostit voivat joutua hyökkääjän käsiin. Tämän vaikutuksena PK-yrityksen maine voi vaurioitua pysyvästi tai he voivat menettää kilpailullisen edun. Eri pilvipalveluiden malleissa on vastuu jaettu eri lailla ja PK-yrityksien olisi hyvä tiedostaa erot näissä malleissa ja ymmärtää oma vastuunsa. PK-yrityksen tietoja voi joutua vääriin käsiin myös esimerkiksi konfiguraatiovirheen takia, jonka mahdollistaa pilvipalveluiden jaettu infrastruktuuri. Pilvipalveluita käytetään internetin välityksellä, joten PK-yrityksien on myös tiedostettava internetin käytöstä johtuvat haasteet. Pilvipalvelut muun muassa voidaan kaataa käyttämällä hajautettua palvelunestohyökkäystä, liikennettä voidaan kuunnella pilvipalvelun ja asiakkaan välillä ja tietoja voidaan kalastella. Nämä hyökkäykset voivat myös kohdistua mihin vaiheeseen tiedonsiirtoa tahansa, pilvipalvelimeen tai yrityksen omiin laitteisiin. PK-yrityksen työntekijät ja omistajat ovat myös henkilökohtaisesti alttiita hyökkäyksille. Tietoa jaetaan sähköpostien välityksellä tai muulla vastaavalla tavalla ja hyökkääjä voi lähettää väärennetyn sähköpostin yrityksen työntekijälle ja esiintyä pilvipalveluntarjoajan asialla. (ENISA 2009 & ENISA 2015).

Pilvipalveluntarjoajat antavat asiakkailleen rajapinnan, jonka avulla asiakas voi hallita eri asioita, kuten SaaS-mallissa työntekijöiden käyttöoikeuksia ja PaaS- ja IaaS-malleissa virtuaalikoneita ja ohjelmistoja. Näihin rajapintoihin on kuitenkin mahdollista hyökkääjän päästä käsiksi eri keinoin ja vaikutukset PK-yritykseen voivat olla todella ikävät. PK-yrityksien tulisi varmistaa, että pilvipalveluntarjoaja on suojannut rajapinnat hyvin ja erityisesti, että yrityksen omien järjestelmänvalvojien tietokoneen ja ohjelmistot ovat turvattuna. Pilvipalveluiden yksi isoista eduista on, että tietoon pääsee käsiksi melkein mistä vain esimerkiksi matkapuhelimella ja kannettavalla tietokoneella. Kannettavien laitteiden katoaminen tai varkaus on kuitenkin suhteellisen yleistä, joten laitteen kadotessa voi yritys menettää arkaluontoista tietoa tai mahdollisia käyttöoikeuksia pilvipalveluihin, joissa arkaluontoista tietoa säilytetään. Yritykset myös sallivat usein työntekijöiden käyttää työssään omia laitteitaan, joten erityisesti PK-yrityksissä niiden turvallisuuden takaaminen on erittäin hankalaa. Kaikki laitteet, joilla tietoon pääsee käsiksi, tulisi salata ja varmistaa, että niiden katoaminen tai varkaus ei aiheuta isoa vahinkoa yritykselle. Maailmalla kadotetaan tai varastetaan joka minuutti 113 puhelinta, joten niiden suojaaminen on tärkeää. (ENISA 2015 & World Backup Day).

Erilaiset luonnonkatastrofit, kuten maanjäristykset ja tulvat, voivat vahingoittaa fyysisiä palvelinkeskuksia, jolloin pilvipalvelu saattaa olla tavoittamattomissa. Tällöin yritys ei pääse käsiksi omaan tietoonsa, joten yrityksen tulisi varmuuskopioida tietonsa mahdollisimman usein ja formaatissa, jonka he voivat siirtää uuteen palvelinkeskukseen tai uudelle pilvipalveluntarjoajalle tarvittaessa. (ENISA 2015). Yritykset usein käyttävät paljon aikaa ja rahaa varmuuskopiontiin, mutta unohtavat varmistaa yhden tärkeimmistä asioista eli varmuuskopion toimivuuden. Jopa 48 % katastrofista palautumisen testaukset ovat yrityksissä epäonnistuneet eikä yksinkertaisemmat varmuuskopioinnin palautukset ole onnistuneet juurikaan paremmalla prosentilla. (Cook 2008). Koska pilvipalveluita käyttävät yritykset ja muut niiden asiakkaat käyttävät samojen fyysisten laitteiden resursseja, voivat resurssit loppua ruuhka-aikoina tai ongelmatilanteissa, kuten hyökkäyksien aikana. Ennen pilvipalveluntarjoajan valintaa, yrityksen tulisi varmistua, että pilvipalveluntarjoaja on kykenevä selviämään, jos liikenteen määrä palvelimilla kasvaa todella suureksi ja mitä mahdollisia korvauksia yritys voi hakea, jos palvelun käyttö tästä huolimatta

estyy. Liikenteen määrä voi myös nostaa yrityksen kustannuksia, koska pilvipalvelut monesti laskuttavat asiakkaitaan liikenteen määrän mukaan. Pilvipalvelut myös toimivat internetissä, joten yrityksellä on oltava toimiva internet-liittymä, jotta voivat käyttää pilvipalveluaan ja päästä käsiksi tietoonsa. Internetin toimiminen ei kuitenkaan ole täysin varmaa ja yritys ei aina pysty siihen itse vaikuttamaan, joten myös yrityksen käyttämällä internetpalveluntarjoajalla on merkitystä pilvipalveluiden toimimisen suhteen.(ENISA 2015 & Shagin 2012).

PK-yrityksille on todella tärkeää, että heillä on suunniteltuna liiketoiminnan jatkuvuus ja siinä on huomioitu pilvipalveluiden käyttö. Pilvipalveluita käytettäessä on mahdollista, että yritys joutuu tilanteeseen, missä pilvipalveluntarjoajan vaihto ei onnistu tai nykyiseltä pilvipalveluntarjoajalta poistuminen kokonaan on todella hankalaa ja aikaa vievää. Tämä tilanne voi syntyä esimerkiksi taloudellisista syistä tai oikeudellisista syistä. Pilvipalveluntarjoaja voi esimerkiksi menettää palvelimensa oikeuden määräyksellä tai voi joutua hakeutumaan konkurssiin. Tällöin asiakkaana olevan yrityksen on todella vaikeaa tai jopa mahdotonta saada omia tietojaan ja asiakirjojaan ulos pilvipalvelimilta. Tärkeää olisi käyttää tiedon muotoina standardoituja muotoja sekä standardoituja rajapintoja ja tehdä usein varmuuskopioita, jotta pilvipalveluntarjoajalta poistuminen on mahdollisimman helppoa ja nopeaa. Pilvipalveluiden yksi eduista on se, että niillä on useita palvelimia ja useissa maissa. Tämä voi olla kuitenkin yritykselle myös haaste, sillä palvelimia koskee tällöin pilvipalvelimen sijaintimaan lainsäädäntö. Lainsäädäntö voi muun muassa määrätä, että jos yksi pilvipalvelun asiakas on tehnyt rikoksen, voidaan kaikki pilvipalvelun palvelimet määrätä tutkittavaksi. Tällöin muita asiakkaita ei välttämättä huomioida ollenkaan vaikka he menettävät pääsyn tietoonsa ja tiedon luottamuksellisuus ja eheys vaarantuu. (ENISA 2015).

2.4. Pilvipalveluiden tietoturva

Pilvipalvelun tärkeimpiä periaatteita on, että sen on oltava luotettava. Jotta pilvipalvelu olisi luotettava, on sen oltava luottamuksellinen, eheä ja aina saatavilla. Luottamuksellisuus tarkoittaa, että asiakkaan tietoihin ei ole pääsyä kenelläkään muulla kuin asiakkaalla itsellään ja tiedon eheys tarkoittaa, että asiakkaan tietoa ei pysty kukaan ulkopuolinen muuttamaan ja tietoon tehdyistä muutoksista jää aina jälki. Pilvipalvelun saatavuus tarkoittaa, että asiakkaalla on aina oltava pääsy omiin tietoihinsa, kunhan hänellä on siihen soveltuva asiakaslaite esimerkiksi verkkoselain.

Pilvipalveluiden lisääntyminen ja suosion kasvu ovat tuoneet uusia ongelmia sekä uhkia tietoturvaan. Yksi suuri muutos entisiin malleihin on se, että kuluttajat ja yritykset käyttävät pilvipalveluita oman tietonsa säilömiseen, jolloin tieto on kolmannen osapuolen omistamilla palvelimilla, asiakkaan oman tallennustilan sijaan. Asiakkaat käyttävät pilvipalveluissa myös muiden omistamaa laskentatehoa. SaaS- ja PaaS-mallien tietoturva on asiakkaan näkökulmasta samankaltaisia, sillä näissä kummassakaan palvelumallissa asiakkaalla ei ole pääsyä pilvipalvelun infrastruktuurin alimpiin osiin. SaaS- ja PaaS-malleissa vastuu itse pilvipalvelun alustan tietoturvasta on pilvipalveluntarjoajalla ja asiakkaan vastuulle jää valita pilvipalveluntarjoaja huolella ja perehtyä heidän tietoturvaansa mahdollisimman hyvin, ennen pilvipalveluntarjoajan valinnan tekemistä. Pilvipalveluntarjoajat eivät kuitenkaan kerro julkisesti yksityiskohtia millä ja miten pilvipalvelut toimivat, jotta hyökkääjillä ei olisi tarkkaa tietoa siitä. Tällä voidaan hankaloittaa hyökkääjien toimintaa, jotta he eivät pääse helposti hyödyntämään esimerkiksi käyttöjärjestelmän heikkouksia.

Software as a Service-palvelumallissa alustan tietoturvan lisäksi pilvipalveluntarjoajalla on myös vastuu käytetyistä ohjelmistoista ja niiden tietoturvassa. Asiakkaan vastuulle jää operatiivinen turvatoiminta. Operatiiviset turvatoimet sisältävät muun muassa pääsyoikeuksien hallinnan ja käyttäjienhallinnan pilvipalveluntarjoajan toimittamilla työkaluilla. Platform as a Service-palvelumallissa asiakkaan vastuu tietoturvasta on kuitenkin suurempi kuin SaaS-mallissa. Asiakkaan tulee muun muassa olla perillä pilvipalvelun alustan

käyttämistä rajapinnoista, jotta asiakas voi määritellä autentikointi- ja käyttöoikeuskontrollit omaan ohjelmistoonsa. Pilvipalveluntarjoajan tulisi tarjota nämä työkalut asiakkailleen ja työkalujen tulisi sisältää ainakin käyttäjien autentikoinnin, pääsyoikeuksien hallinnan ja SSL sekä TLS tuet.

Infrastructure as a Service-palvelumallissa asiakkaan vastuu tietoturvasta on suurin kolmesta palvelumallista. Suurempi vastuu tietoturvasta johtuu siitä, että asiakkaalla on pääsy koko infrastruktuuriin pois lukien raudan ja virtuaalisten palvelimien välissä olevaan virtualisointi osioon. Tässä mallissa asiakkaalla on vastuu myös ohjelmistojen tietoturvasta sillä ohjelmistot pyörivät asiakkaan virtuaalisilla palvelimilla. Asiakkaan vastuulla on ohjelmistoja kehittäessä ottaa huomioon yleisimpien haavoittuvuuksien paikkaaminen sekä ohjelmistojen päivittäminen. IaaS-palvelumallissa pilvipalveluntarjoaja ei myöskään tarjoa valmiita työkaluja autentikointiin tai käyttöoikeuksien hallintaan.

IaaS-palvelumallin virtualisointiosio on pilvipalveluiden kannalta todella tärkeä ja on siksi ruvennut kiinnostamaan myös mahdollisia hyökkääjiä. Hyökkääjän päästessä käsiksi tähän virtuaaliosioon on koko pilvipalvelu vaarassa. Pilvipalveluntarjoajan tulisikin estää kaikki pääsy tähän osioon.

2.4.1. Tietomurto

Cloud Security Alliancen listauksen mukaan pahin uhka pilvipalveluille on tietomurrot. Tietomurto tarkoittaa tapahtumaa missä tahallisesti tai tahattomasti julkaistaan järjestelmästä tietoa ilman tiedon omistajan tietämystä tai lupaa. Murron kohteena oleva tieto on yleensä luottamuksellista tai sillä on tiedon omistajalle taloudellista hyötyä. Luottamuksellisia tietoja ovat muun muassa asiakkaan henkilötiedot ja muut yksilöitävissä olevat tunnistetiedot. Nämä tunnistetiedot asiakkaan on myös pakko antaa ottaessaan käyttöön pilvipalvelua.

Vuonna 2014 tehtiin 783 tietomurtoa, joka oli ennätysmäärä tietomurtoja yhdessä vuodessa. Määrällisesti suurin osa tietomurroista kohdistui terveydenhuollonsektoriin, joihin

tehtiin 333 tietomurtoa eli 42,5 % kaikista vuoden 2014 tietomurroista. Toiseksi suurimpana sektorina olivat yritykset joihin kohdistui 33 % tietomurroista. Yrityksistä kuitenkin saatiin varastettua huomattavasti enemmän asiakirjoja kuin terveydenhuollon puolelta, sillä jopa 79,7 % kaikista varastetuista asiakirjoista olivat peräisin yrityksistä. Terveydenhuollonsektorilta asiakirjoja oli ainoastaan 9,7 % mikä oli kuitenkin toiseksi eniten. Muita sektoreita olivat finanssi, opetus sekä hallitus/puolustusvoimat. (Identity Theft Resource Center 2014).

Hakkerointi oli vuonna 2014 suurin syy tietomurroille. Tietomurtoja tehtiin 227 kappaletta mikä oli 29 % kaikista tietomurroista. Hakkerointi oli myös jo viidettä vuotta peräkkäin suurin syy tietomurroille. Toiseksi suurimpana syynä olivat alihankkijat, jotka tahallaan tai tahattomasti paljastavat tietoa, joka oli salaista. Alihankkijoiden osuus oli 15,1 % ja 118 kappaletta. Muita syitä tietomurtoihin oli sisäpiiriläisen varkaus, tieto liikkeessä, tahaton tiedon paljastaminen, työntekijän huolimattomuus ja fyysinen varkaus. (Identity Theft Resource Center 2105).

Monet yksityisyyslait säätelevät kuinka yksityisyystietoja tulee kerätä, säilyttää, käyttää sekä paljastaa. Nämä yksityisyyslait pakottavat myös pilvipalveluntarjoajat huolehtimaan asiakkaiden tiedoista, mutta pilvipalveluntarjoajat kuitenkin antavat hyvin vähän tai eivät ollenkaan tietoa kuinka he säilyttävät asiakkaiden tiedot, kenellä niihin on pääsy sekä kuinka turvallisesti niitä säilytetään. Jos pilvipalveluntarjoaja ei ole luotettava, ei asiakkaalla ole mitään mahdollisuutta tietää kuinka turvassa hänen tunnistetietonsa ja muut arkaluontoiset tiedot ovat väärinkäytöksiltä sekä identiteettivarkauksilta. Kun tiedetään kenellä asiakkaan tietoja on, kenellä niihin on pääsy ja on kyky ylläpitää niiden valvontaa, voidaan myös estää niiden tietojen varastamista tietomurtojen yhteyksissä.

Pilvipalveluissa tunnistetietojen hallinnointi, joka on yksi keino estää niiden varastamista, on monimutkaisempaa kuin normaaleissa verkkopohjaisissa järjestelmissä. Tämä johtuu siitä, että asiakkaalla voi olla tili usealla eri palveluntarjoajalla tai useita tilejä yhdellä palveluntarjoajalla. Normaalisti sovellukset pitävät kirjaa ja hallitsevat käyttäjiä itse, pilvipalveluissa tämä ei kuitenkaan toimi, koska asiakkaalla voi olla tili usealla pilvipalveluntarjoajalla tai useita tilejä yhdellä. Näiden tilien välinen tunnistetietojen jakaminen

voisi johtaa tunnistetietojen kartoitukseen eli yksityisyyden menetykseen. Tunnistetietojen hallinnointiin on useita eri järjestelmiä. Nämä järjestelmät kuitenkin nojaavat usein kolmanteen osapuoleen ja tämä osapuoli voi olla myös itse pilvipalveluntarjoaja, jolloin kolmas osapuoli ei ole enää itsenäinen. Kolmannen osapuolen mukana oleminen on myös tietoturvariski. Turvallisempi järjestelmä olisi sellainen, missä ei kolmatta osapuolta ole mukana ollenkaan. Järjestelmää voitaisiin käyttää tuntemattomilla isännillä ja sen tieto olisi aina salattu, kun järjestelmä keskustelee pilvipalveluiden kanssa. Se käyttäisi aktiivista nippumallia, jossa tiedot kuljetetaan salattuina ja monien koneiden välillä. Koska tietoa voitaisiin vaihtaa nipun ja isännän välillä paikallisesti, estäisi se muun muassa man-in-the-middle–hyökkäykset.

Tietomurtojen estämiseksi käytetään monesti tiedon salausta. Tieto joka halutaan suojata eli salata on usein arkaluontoista organisaatiolle tai käyttäjälle. Salaus pyrkii minimoimaan tietomurtojen haittoja, koska jos hyökkääjä saa käsiinsä asiakirjoja, jotka ovat salattuja, ei niillä voi vielä tehdä mitään. Salaus saattaa myös estää tiedon oikean omistajan käyttämästä tietoja, sillä salauksen purkamiseen käytettävä avain voi kadota, korruptoitua tai hyökkääjä voi saada sen käsiinsä, jolloin salaus on hyödytön.

Yksi keino suorittaa tietomurto on Brute Force-hyökkäys. Brute Force-hyökkäyksessä käytetään hyväksi sanakirjoja sekä ohjelmia arvaamaan käyttäjän salasana. Brute Force mahdollistaa satojen tuhansien salasanayhdistelmien arvaamisen sekunnissa. Brute Forcea käytetään pilvipalveluihin murtautumisessa, mutta pilvipalvelut ovat myös mahdollistaneet Brute Forcen käytön tehostumisen. Brute Force-hyökkäyksessä tarvitaan laskentatehoa ja sitä pilvipalvelut tarjoavat käyttäjilleen halvalla, pilvipalvelut myös mahdollistavat anonyyminä olemisen, joten hyökkääjän kiinnijääminen on vaikeutunut.

Brute Force-hyökkäys voidaan estää tai sitä voidaan hankaloittaa muun muassa rajoittamalla salasanan syöttämiskertoja. Kun salasana on syötetty tarpeeksi useasti väärin, pitää käyttäjän ratkaista CAPTCHA-arvoitus. CAPTCHA sisältää yleensä helppoja yhteenlaskuja tai kirjainyhdistelmiä, mutta ne esitetään kuvana, joten tietokoneen vaikea niitä ratkaista. Google on myös kehittänyt uuden reCAPTCHA-ohjelmointirajapinnan, jossa käyttäjän tarvitsee vain klikata ruutua, todistaakseen ettei ole tietokone. reCAPTCHA

tarkkailee käyttäjän toimia sivulla ennen CAPTCHAa, sen aikana ja sen jälkeen, määritelläkseen onko käyttäjä ihminen vai tietokone. (Shet Vinya 2014).

Salasanojen salaus on myös keino estää tietomurtoja ja parantaa käyttäjien yksityisyyttä ja tietoturvaa. Kun käyttäjä todennetaan, palvelimet eivät yleensä tallenna salasanoja selkokielisenä vaan ne salataan eli tiivistetään. Käyttäjän syöttäessä selkokielisen salasanansa, se tiivistetään ja tätä tiivistettä verrataan tietokantaan tallennettuun tiivisteeseen. Hyökkääjä voi kuitenkin saada käsiinsä tämän tiivisteen esimerkiksi tietomurron yhteydessä. Tiivisteen avulla ei kuitenkaan voida suoraan kirjautua käyttäjän tileihin vaan tiiviste on ensin avattava. Tiiviste voidaan avata muodostamalla useita salasanavaihtoehtoja. Jotta tämä olisi vaikeampaa, käyttäjän salasanaan lisätään satunnainen kirjain tai numero ja se otetaan mukaan tiivisteeseen. Moni sivusto myös rohkaisee käyttäjää valitsemaan salasanan, joka ei ole sanakirjassa ja on mahdollisimman hankala. Käyttäjä voi joutua sisällyttämään salasanaansa isoja ja pieniä kirjaimia sekä erikoismerkkejä ennen kuin palvelu hyväksyy salasanan. Käyttäjä voi kuitenkin tästä johtuen valita salasanan joka on häneen itseensä viittaava ja motivoituneelle hyökkääjälle tällaisen salasanan arvaaminen voi olla helpompaa kuin sanakirja-pohjainen, sillä hyökkääjä voi saada salasanan tietoonsa käyttäjää manipuloimalla.

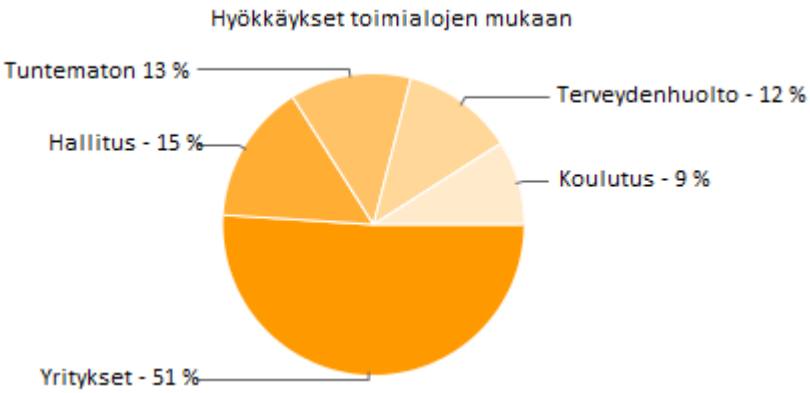
2.4.2. Tiedon häviäminen

Tiedon häviäminen voi tapahtua tiedolle joka on levossa tai tiedolle joka on liikkeessä. Tiedon liikkeessä olemisella tarkoitetaan, että tietoa siirretään esimerkiksi tietoverkon yli. Tiedon häviäminen voi tapahtua monella eri tavalla. Tieto voi korruptoitua, tieto voidaan joko vahingossa tai tahallisesti poistaa tai ylikirjoittaa käyttäjän tai hyökkääjän toimesta. Tieto voi hävitä myös, jos tiedon tallennukseen käytetty fyysinen laite hajoaa tai se varastetaan tai virus tuhoaa tiedon. (Techopedia).

Tyypillinen nykyajan yritys lähettää ja vastaanottaa miljoonia sähköposteja sekä ladata, tallentaa tai siirtää tuhansia tiedostoja eri kanavia pitkin päivittäin. Yritysten vastuulla on myös todella paljon tietoa, joka on arkaluontoista ja heidän odotetaan pitävän se turvassa

asiakkaiden, yhteistyökumppaneiden, sääntelyviranomaisten tai osakkeenomistajien toimesta. Siitä huolimatta yritykset joutuvat jatkuvasti tiedon häviämisien tai tietovuotojen uhreiksi. Tiedon häviämisen seurauksena yrityksen kilpailukyky ja maine voivat huomattavasti heikentyä, mutta voivat aiheuttaa myös muita ongelmia yritykselle, kuten oikeusjuttuja tai sääntelyseuraamuksia löyhän tietoturvan takia. (Liu & Kuhn 2010).

Vuonna 2015 tapahtui noin 1472 kappaletta julkisesti ilmoitettua tietojen häviämistä, mikä oli kasvua edeltävään vuoteen noin 200 kappaletta. Näistä tietojen häviämisistä jopa 51 % tapahtui yrityksille, joka oli selkeästi suurin yksittäinen sektori. Yritykset ovat suurin sektori myös aikavälillä 2006–2015, kun 50 % tietojen häviämisistä on tapahtunut yrityksille. Toiseksi suurin sektori osuudeltaan oli hallitukset (15 %) joka on myös toiseksi suurin vuodesta 2006 eteenpäin tarkasteltuna (17 %). (DataLossdb 2015).



Kuva 3. Tietojen häviämisten jakautuminen vuonna 2015. (DataLossdb 2015).

Selkeästi suurin syy tietojen häviämiselle vuonna 2015 oli hakkeroinnit 34 % osuudella, hakkerointi on ollut myös vuodesta toiseen suurin syy ja vuodesta 2006 alkaen sen osuus on 31 %. Vuonna 2014 petosten ja huijausten seurauksena tapahtuneet tietojen häviämiset olivat toiseksi suurin yksittäinen syy 11 % osuudella, vuonna 2015 tuo osuus kuitenkin putosi kolme prosenttiyksikkö ollen enää 8 %. Vuodesta 2014 vuoteen 2015 suurin yksittäinen nousija on skimmaus. Skimmauksessa uhrin luotto- tai pankkikortin tiedot kopioidaan pienellä elektronisella laitteella esimerkiksi pankkiautomaatilla käynnin yhteydessä. Vuonna 2014 skimmauksen osuus oli ainoastaan 3 % kun vuonna 2015 se oli 15 %. (DataLossdb 2015).

Tiedon häviäminen voidaan jaotella kahteen eri pääkategoriaan sen tyypin mukaisesti. Ensimmäinen kategoria on vuoto. Tietovuodossa tieto ei ole enää organisaation hallinnassa. Vuoto tapahtuu yleisimmin tietokantojen hakkeroinneissa ja se on myös yleisin identiteettivarkauden muoto. Toinen kategoria on tiedon häviäminen tai tuhoutuminen. Tässä kategoriassa toimiva tai oikea kopio tiedosta ei ole enää organisaation hallinnassa. (Liu ym. 2010).

Organisaatioita velvoittavat hallituksien määräämät säännökset kuten myös toimialojen omat ja immateriaalioikeuksien säännökset. Nämä säännökset määräävät muun muassa sen kuinka organisaation tulee käsitellä yleisesti tietoa ja erityisesti henkilö- ja muita tunnistetietoja. Säännökset ovat yksi suurimmista syistä miksi organisaatioiden tulee huolehtia siitä, että arkaluontoista tietoa ei häviä tai vuoda. Euroopan Unioni ja Yhdysvallat ovat myös säätäneet määräykset joiden mukaan organisaatioiden on ilmoitettava kuluttajille jos heidän tietojen edes epäillään vuotaneen. Immateriaalioikeuksien piiriin kuuluvat tiedot saattavat olla organisaatiolle suurempi arvoltaan kuin muu organisaation omaisuus ja siksi niiden suojaamiseksi on kehitetty menettelytapoja ja mekanismeja varkauksien ja häviämisten ehkäisemiseksi.

Tieto voi olla kolmessa eri vaiheessa: levossa, päätepisteessä tai liikkeessä. Levossa tieto sijaitsee esimerkiksi tietokannoissa, päätepisteissä muun muassa kannettavissa tietokoneissa ja liikkeessä tieto liikkuu tietoverkosta ulkopuoliseen maailmaan esimerkiksi sähköpostilla. Koska tieto voi olla eri vaiheissa, myös tiedon suojaamiseen eri vaiheessa tarvitaan eri keinoja. Tiedon ollessa liikkeessä, sitä voidaan syvätarkistaa, mutta se ei ole hyvä keino tiedon ollessa levossa. Tiedon häviämisen estämiseksi tulee organisaation ottaa huomioon myös hallinnolliset toimet. Tiedon käytön menettelytapojen tulee ottaa huomioon pääsyoikeuksista päättäminen ja tapojen valvonta. Myös tietojen häviämisestä toipuminen ja siitä raportointi on otettava huomioon.

Tiedon arkaluonteisuus tulee määritellä, siitä pitää luoda luettelo ja se tulee paikallistaa sen ollessa tallennettuna. Myös esimerkiksi työntekijöiden kannettavilla tietokoneilla sijaitseva tieto tulee sisällyttää tähän, jotta se voidaan paikantaa ja pitää turvassa. Organisaatioiden tulee valvoa arkaluonteisen tiedon käyttöä ja ymmärtää sen käytön malli, jotta voidaan havaita tiedon mahdolliset väärinkäytöt. Valvonnan tulee sisältää niin liikkeessä

oleva tieto kuin myös päätepisteissä oleva tieto. Arkaluonteisen tiedon suojaamisen tavoitteena on estää tiedon poistuminen organisaation ulkopuolelle. Arkaluontoinen tieto tulee suojata tiedon jokaisessa vaiheessa ja se tulee salata ja sen siirtämistä tulee rajoittaa kuin myös pääsyoikeuksia.

Organisaation ei ole järkevää suojella kaikkea tietoaan yhtä tarkasti ja huolellisesti vaan määritellä arkaluontoisin tieto ja suojata se kunnolla. Arkaluontoisen tiedon suojaamiseen ei kuitenkaan ole yhtä ainoaa menetelmää vaan organisaation tulee etsiä heidän tarpeisiinsa parhaiten soveltuva menettelytapa. Tiedon suojaaminen ei saa kuitenkaan hankaloittaa tai estää työntekijän työskentelyä tai vähentää järjestelmien toimintakykyä.

2.4.3. Tilin tai palvelun kaappaaminen

Tilin tai palvelun kaappaaminen ei ole uusi tietoturvauhka vaan ne ovat olleet käytössä jo kauan ohjelmistojen haavoittuvuuksien paljastamisen, petosten sekä phishingin eli käyttäjän tietojenkalastelun muodossa. Pilvipalvelut ovat tuoneet uusia ulottuvuuksia tähän. Varastetuilla tunnuksilla hyökkääjä pystyy kirjautumaan käyttäjän, esimerkiksi yrityksen, pilvipalveluihin ja voivat seurata yrityksen liiketoimintaan liittyviä tapahtumia, manipuloida yrityksen tietoja kuten asiakirjoja tai uudelleenohjaamaan yrityksen asiakkaita yrityksen verkkosivuilta haitallisille sivuille. Varastetuilla tunnuksilla hyökkääjät voivat myös altistaa koko pilvipalvelun vaaralle, jos heillä on pääsy pilvipalvelun kriittisille alueille.

Yrityksen asiakkaat voivat suojata itsensä tarpeeksi vahvalla salasanalla, mutta vahvinkaan salasana ei auta, jos hyökkäyksen kohteena on palveluntarjoaja eli yritys. Myös yrityksen käyttämän pilvipalveluntarjoaja voi joutua hyökkäyksen kohteeksi jolloin asiakasyritys joutuu epäsuoraksi kohteeksi. Esimerkiksi vuonna 2010 verkkokauppa Amazon.com joutui hyökkäyksen kohteeksi, kun heidän verkkosivuillaan oli cross-site script (XSS) bugi, jota hyväksikäyttämällä oli mahdollista varastaa asiakkaan istunnon ID. Asiakkaan ID:n avulla oli mahdollista päästä käsiksi asiakkaan tileihin ja käyttäjätietoihin.

Tilin tai palvelun kaappaamiseen voidaan käyttää ainakin kahdeksaa eri menetelmää. Nämä menetelmät ovat istunnon kaappaaminen, SQL-injektio, Cross-site scripting, man-in-the-middle-hyökkäys, wrapping-hyökkäys, käyttäjän manipulointi ja phishing.

Käyttäjä ei välttämättä itse huomaa, että hänen istuntonsa on kaapattu. Istunnon kaappausta yritetään estää salaamalla käyttäjän ja palvelun palvelimen välillä ja minimoidaan tunnisteen arvauksen mahdollisuus, mutta tämä ei kuitenkaan täysin poista kaappauksen mahdollisuutta. Hyökkääjä voi edelleen saada istunnon tunnisteen kaapattua liikenteen joukosta haitallisen koodin avulla tai haitallisen verkkoselaimen lisäosalla. Istunnon kaappaamiselta voidaan suojautua pitämällä istunnon evästeet eri alidomainilla, jolloin ne ovat esimerkiksi haitallisen JavaScript-koodin ulottumattomissa tai luomalla kyseinen eväste käyttäjän omalla koneella. Nämä jättävät käyttäjän silti haavoittuvaiseksi XSS:lle ja selaimen kaappaukselle.

Jokainen internetissä oleva sivusto tai internetiin pohjautuva ohjelma tarvitsee tietokantaa. Tietokannan käyttö altistaa nämä kuitenkin SQL-injektiolle haavoittuvaiseksi. SQL-injektiossa tietokannalle syötetään haitallisia käskyjä, jotka saavat tietokannan käyttäytymään odottamattomalla tavalla. Tietokannat eivät osaa eritellä haitallista ja normaalia käskyä, joten hyökkääjä pääsee SQL-injektion avulla tietokannan tietoihin käsiksi. Tästä syystä käyttäjän syötteeseen ei tule luottaa vaan se on vahvistettava ennen tietokantaan tallennusta. Tietokantaan ei tule myöskään yhdistää järjestelmänvalvojan tunnuksilla vaan on käytettävä rajoitetumpia tunnuksia. Tietokannan palauttamia virheiden tietoja tulee myös rajoittaa, jotta hyökkääjä ei voi käyttää niitä hyväkseen. Tietokannassa olevat ja sinne tallennettavat salasanat ja muu arkaluontoinen tieto on aina suojattava.

XSS eli Cross-Site Scriptingissä pilvipalvelu lähettää selaimelle verkkosivun, jota ei ole validoitu ja se sisältää käyttäjän tietoja. Validoimattomuus mahdollistaa hyökkääjä ujuttamaan verkkosivulle haitallista koodiaan ja saa näin käyttäjän tiedot. Jotta XSS ei olisi mahdollista, tulee hyväksyä ainoastaan tieto joka tunnetaan. Tämä tarkoittaa sitä, että tieto itsessään ei sisällä mitään haitallista. Tiedosta tulee myös poistaa kaikki haitallinen, esimerkiksi käyttäjän syöttämät erikoismerkit ja, ellei ole pakko, niin rajataan ISO 8859-1- merkistöön kuulumattomat merkit ulkopuolelle.

Epärehellinen välittäjä (man-in-the-middle) hyökkäyksessä hyökkääjä asettuu käyttäjän ja palvelimen väliin, jolloin kaikki liikenne kulkee hyökkääjän kautta. Hyökkääjää voidaan yrittää estää pääsemästä palvelimen väliin salaamalla liikenne, mutta myös HTTPS-yhteydessä hyökkäys on mahdollinen. Jos liikenne on salattu HTTPS-yhteydellä, hyökkääjä voi käyttää hyväkseen HTTPS-palvelimen lähettämää sertifikaattia, joka sisältää palvelimen julkisen avaimen. Hyökkääjä muokkaa tätä sertifikaattia itselleen sopivaksi ja korvaa sillä alkuperäisen sertifikaatin, koska käyttäjät eivät yleensä tarkista selaimen käyttämää sertifikaattia, on hyökkäys mahdollinen.

Wrapping-hyökkäyksessä hyökkääjä käyttää hyväkseen käyttäjän virtuaalipalvelimen ja palvelimen kommunikoinnissa käytettävän TLS (Transport Layer Security) kerrosta ja SOAP-viestejä. SOAP-viesti pitää sisällään rakenteellista informaation joka vaihdetaan palvelimen ja verkkoselaimen välillä keskustelun aikana. Hyökkääjä tekee tästä SOAP-viestistä kopion ja lähettää sen palvelimelle oikeutettuna käyttäjänä jolloin palvelin hyväksyy sen ja antaa hyökkääjälle pääsyn pilveen. Saatuaan pääsyn pilvipalveluun, hyökkääjä voi käyttää sitä hyväkseen ja ajaa haitallista koodiaan. Tämä voidaan kuitenkin estää SOAP-viestin headeriin lisättävällä STAMP-bitillä, joka muuttuu jos havaitaan kolmas osapuoli. Kun vastaanottaja saa SOAP-viestin ja tarkistaa STAMP-bitin sekä huomaa sen muuttuneen, luodaan uusi allekirjoitus ja se lähetetään palvelimelle. Koska allekirjoitus on nyt eri kuin se oli alkuperäisessä SOAP-viestissä, ei hyökkääjällä ole enää pääsyä palvelimelle.

Haittaohjelma injektiossa (Malware injection) hyökkääjä pyrkii lisäämään haitallisen koodin tai ohjelman pilvipalveluun. Koodi tai ohjelma näyttää sallitulta, mutta se pystyy salakuuntelemaan pilvipalvelun liikennettä. Tämä onnistuu hyökkääjän tiedon muokkaamisella joka aiheuttaa deadlockin tai toiminallisuuden muuttumisen joka pakottaa käyttäjän odottamaan pyytämättömän työn loppumista. Tämän jälkeen hyökkääjä voi lisätä pilvipalveluun oman haitallisen koodinsa tai ohjelmansa ja se toimii IaaS- tai SaaS-palvelimissa. Palvelimissa tarkistetaan ainoastaan vastaako palvelu olemassa olevaa palvelua ja sen eheyttä ei tarkisteta, joten hyökkääjän tarvitsee vain kopioida olemassa oleva palvelu ja muokata sitä. Pilvipalvelun IaaS-tasolle voidaan lisätä eheyttä FAT-järjestelmäarkkitehtuurilla. Tämän avulla saadaan tietoon mitä koodia tai ohjelmia käyttäjä aikoo

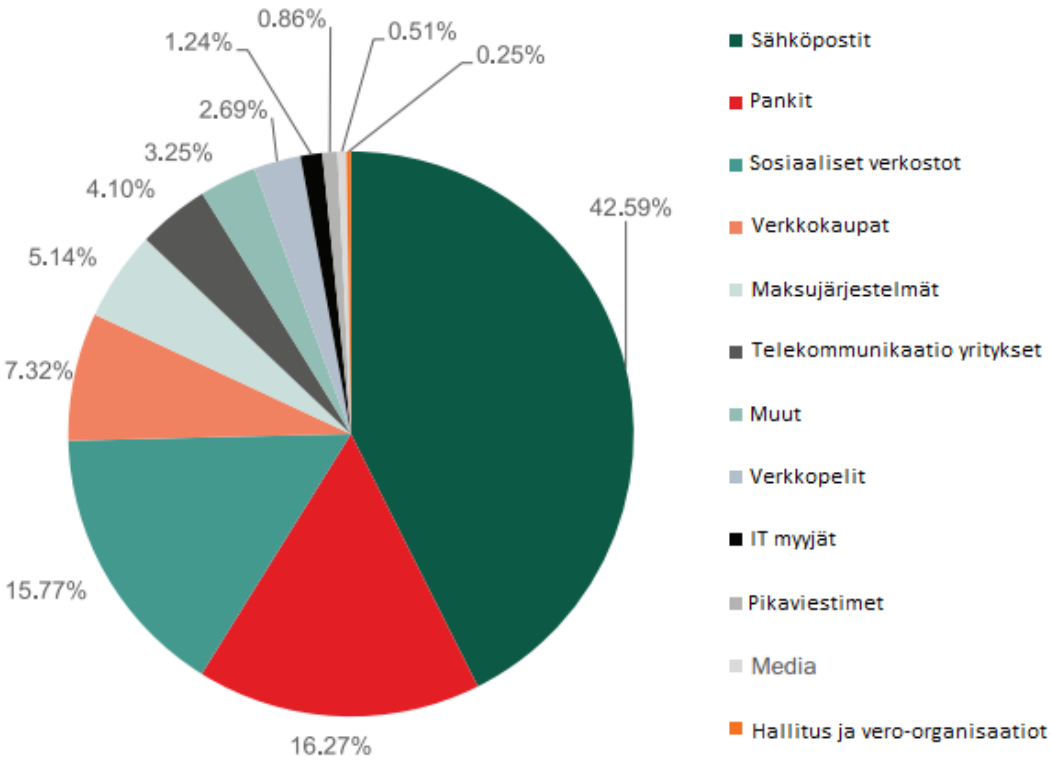
suorittaa ja sitä voidaan verrata jo aiemmin tapahtuneeseen ja päätellä tämän pohjalta eheys.

Käyttäjän manipulointi (Social Engineering) on hyökkäys, jossa käytetään hyväksi ihmisen psykologisia heikkouksia tavoitteena saada haltuun esimerkiksi yrityksen salasanoja. Iso osa ihmisistä ei usko, että he voisivat olla tällaisen hyökkäyksen kohteena, joten he ovat helpommin niille alttiina. Ihmiset eivät myös välttämättä huomaa tuleensa hyökkäyksen kohteeksi ja heillä voi olla tiedossaan tietoa, jonka tärkeyttä tai arkaluontoisuutta he eivät ymmärrä. Hyökkäyksen kohteelta saatu tieto ei välttämättä yksinään ole merkittävä, mutta kun se yhdistetään muista lähteisiin saatuihin tietoihin, sen arvo voi olla hyvinkin merkittävä.

Käyttäjän manipuloimisen estämiseksi tulee olla hyvä puolustus joka sisältää useita tasoja. Ensimmäinen eli alin taso on koko puolustuksen perusta. Siihen sisältyy se, että käyttäjä, kuten työntekijä, ei saa koskaan joutua tilanteeseen jossa hän ei ole varma onko tiedon jakaminen sallittua. Työntekijän tulee siis tietää hänen hallussaan olevan tiedon arvo. Seuraavalla tasolla määritellään työntekijän koulutuksen ja motivoinnin suositukset. Koulutuksen tulee opettaa työntekijälle miten tunnistaa luottamuksellinen tieto ja koulutuksen jälkeen työntekijän on ymmärrettävä oma vastuunsa asiassa. Kolmannella tasolla tulee huomioida se, että ainakin avaintyöntekijät tulee kouluttaa vastustamaan käyttäjän manipulointi-hyökkäystä. Neljännellä tasolla tulee varmistaa työntekijöiden koulutuksen jatkuvuus, jotta työntekijän tietotaito asiasta ei unohdu. Viides taso sisältää hyökkäyksen tunnistamisen eli yrityksessä tulisi olla ainakin yksi työntekijä jonka vastuulla on tunnistaa kaikki joilla on oikeus olla kyseisissä tiloissa. Viimeisellä tasolla tulee määritellä kuinka yritys ja sen työntekijät reagoivat hyökkäykseen.

Tietojenkalastelussa eli phishingissä hyökkääjä yrittää saada tietoa käyttäjältä esimerkiksi lähettämällä hänelle sähköpostin käyttäjän pankin nimissä. Sähköpostissa esitetään jokin ongelma, esimerkiksi luottokortin väärinkäyttö, ja pyydetään asiakasta syöttämään kortin tiedot verkkosivulle ongelman ratkaisemiseksi. Verkkosivusto on identtinen pankin omien kanssa ja jopa URL-osoite voi olla todella paljon samankaltainen kuin pankin käyttämät, mutta verkkosivuston omistaa hyökkääjä. Kun käyttäjä syöttää kortin tiedot, menevät ne suoraan hyökkääjälle.

Vuonna 2013 jopa 37,3 miljoonaa ihmistä ympäri maailmaa joutui tietojenkalastelun uhriksi internetissä. Määrä kasvoi 12 kuukaudessa 19,9 miljoonasta 37,3 miljoonaan. Palveluista Yahoo, Google, Facebook sekä verkkokauppa Amazon olivat hyökkäysten kohteena eniten, yhteensä 30 % kaikista hyökkäyksistä. Jopa 20 % tietojenkalasteluyrityksistä tehtiin pankkien ja muiden finanssialan laitosten nimissä. Tietojenkalasteluyritykset usein myös kohdistuivat samoihin maihin kuten Venäjälle, Yhdysvaltoihin, Brasiliaan ja Iso-Britanniaan ja yli puolet kaikista hyökkäyksistä kohdistui vain 10 maahan. Tietojenkalastelu ei ole vain yksi uhka muiden joukossa vaan on jo yksinään erittäin merkittävä ja näkyvä uhka. (Kaspersky Lab 2014). Vuonna 2013 50 % yrityksiin kohdistuneista tietojenkalasteluhyökkäyksistä kohdistui isoihin, yli 2051 työntekijää työllistäviin, yrityksiin. Toiseksi eniten hyökkäyksiä tehtiin PK-yrityksiin joiden osuus oli 31 %. 251–2500 yritystä työllistäviin yrityksiin kohdistui 19 % hyökkäyksistä. (Symantec 2014).



Kuva 4. Tietojenkalasteluyritysten jakautuminen vuonna 2014. (Kaspersky Lab 2015).

Vuonna 2014 finanssialaan, mihin lukeutuvat muun muassa pankit, maksujärjestelmät ja verkkokaupat, kohdistui 28,73 % kaikista tietojenkalasteluyrityksistä. Tämä oli laskua

vuodesta 2013 2,72 %. Näistä suurin yksittäinen sektori oli pankit, joihin kohdistui finanssialan iskuista 16,27 %. Kokonaisuudessa hyökkäykset ja niiden kohteeksi joutuneet ihmiset laskivat jopa 20 % ja tähän on muutamia yksittäisiä syitä. Yksi syistä on se, että lainvalvojat aktiivisesti ympäri maailmaa haastoivat oikeuteen rikollisia, jotka levittivät tietojenkalasteluhyökkäyksiä. Hyökkääjät myös ovat vaihtaneet taktiikkaansa, sillä sen sijaan, että he hyökkäisivät loppukäyttäjää kohtaan, on heidän fokuksensa siirtynyt enemmän organisaatioihin, jotka työskentelevät finanssi-informaation ja maksujärjestelmien parissa. Hyökkäysten ja uhrien lasku johtuu myös siitä, että hyökkääjät keskittyivät enemmän yksittäisiin ja tarkkaan valittuihin kohteisiin massahyökkäysten sijaan. (Kaspersky Lab 2015).

Hyökkäyksiä voidaan myös torjua. Yksi keino on kouluttaa käyttäjät tietojenkalasteluyritysten varalta. Myös lain keinot hyökkääjien rankaisemiseen ja tekniset tavat voivat estää hyökkäyksiä. Teknisiin tapoihin kuuluu muun muassa hyökkäyksen havaitseminen ajoissa. Verkkosivut voidaan helposti havaita tietojenkalasteluyritykseksi, mutta niiden havaitseminen tarpeeksi ajoissa on vaikeaa. Keinoja havaita sivustoja haitalliseksi on esimerkiksi että sivuston omistaja tutkii juuri-DNS:n haitallisten sivujen varalta tai varustaa sivuston havaitsemaan, jos se kopioidaan työkalujen avulla. Myös sivuston turvallisuuden parantaminen auttaa ehkäisemään tietojenkalastelua. Osa pankeista käyttää muun muassa erillistä laitetta, joka kytketään tietokoneeseen ja asiakas käyttää sitä ostaessaan internetistä luottokortillaan. Sähköpostien roskaposti-filtterit torjuvat myös hyökkäyksiä, kun ne eivät koskaan pääse asiakkaalle asti. Käyttäjän koneelle voidaan myös asentaa tietojenkalastelun tunnistavan ohjelman. Moni nykyajan anti-virus ohjelma sisältää myös tietojenkalasteluyritykset ja ilmoittaa siitä käyttäjälle (AV Comparatives 2015).

2.4.4. Epäluotettava rajapinta tai ohjelmointirajapinta

Pilvipalveluntarjoajat tarjoavat asiakkailleen rajapintoja, joilla voidaan toteuttaa autentikointia, kulunvalvontaa, salausta sekä aktiivisuuden valvontaa. Rajapintoja suunnitellessa tulee ottaa huomioon näiden asioiden tuomat vaatimukset, jotta niiden tahallinen tai

tahaton kiertäminen voitaisiin estää. Jos rajapinnoissa on tietoturva-aukkoja ja organisaatiot luottavat niihin sokeasti, ovat organisaatiot myös itse alttiina tietoturvauhille.

Pilvipalveluissa sekä yleisesti internetissä käytetään ohjelmistorajapintojen (API) avaimia ja niillä voidaan tunnistaa kolmannen osapuolen ohjelmistoja, jotka käyttävät palvelua. Näiden digitaalisten avaimien tarkoitus on suojata palvelua hyökkäyksiltä, mutta niitä on käytetty jo usean vuoden ajan itse hyökkäyksissä. Seuraavaksi voi olla vuorossa uniikit koodit, joilla pilvipalvelut tunnistavat toisensa. Näiden uniikkien koodien avulla hyökkääjä voisi käyttää hyväkseen koko pilvipalvelun laskentatehoa aiheuttaakseen palvelunestohyökkäyksen tai nostaa asiakkaan kustannuksia käyttämällä pilvipalvelun resursseja, jolloin asiakas joutuu maksamaan käytetyistä resursseista. Stuxnet tietokonemadon kehittäjät onnistuivat varastamaan digitaalisia avaimia, joten Stuxnet pystyi kiertämään suojaukset helposti. Stuxnetin kehittäjien uskotaan olleen Yhdysvaltain ja Israelin hallitukset ja sen kohteena ydinvoimalat, erityisesti Iranin ydinohjelma (Kushner 2013).

Ohjelmistorajapintojen avaimet luotiin alun perin tunnistamaan ohjelmistot ja niiden ohjelmistorajapintojen käyttö, mutta kehittäjät ovat käyttäneet niitä myös suoraan turvallisuuteen. Avaimia ei kuitenkaan ole suunniteltu tähän käyttöön ja kehittäjät eivät pidä avaimia kriittisenä osa-alueena turvallisuuden suhteen. Organisaatiot monesti lähettävät avaimia eteenpäin esimerkiksi salaamattomalla sähköpostilla tai säilyttävät niitä omilla kovalevyillään sekä sisällyttävät ne suoraan ohjelmistoihinsa. Pilvipalvelutarjoajien tulisikin avata ohjelmistorajapintojen avaimet mahdollisimman selkeästi kolmansille osapuolille ja kaikkien osapuolien käsitellä niitä turvallisesti. Tällä hetkellä ainakaan SaaS-pilvipalvelutarjoajat eivät kerro asiakkailleen kuinka suojata avaimet ja miksi se on tärkeää.

Arkaluontoisen tiedon suojaamiseen tulisi käyttää vahvempia menetelmiä kuin ohjelmistorajapintojen avaimia. Koska avaimia kuitenkin käytetään turvallisuuteen ja kehittäjät jakavat niitä toisilleen, olisi niiden jakamiseen käytettävä turvallista ja salattua SSL-menetelmää tukevaa kommunikaatiota. Pilvipalveluiden ohjelmistorajapinnoilla ei ole yhteistä standardia, joten käyttäjän tulisi aina olla tietoinen palveluntarjoajan käyttämästä

ohjelmistorajapinnasta. Standardien puute voi heikentää tietoturvaa, mutta on hyvä keino sitouttaa asiakas.

Kertakirjautuminen (Single Sign-On SSO), joka mahdollistaa kirjautumisen useaan palveluun yhdellä käyttäjän autentikoinnilla, on yleistynyt viime vuosina nopeasti. Kertakirjautuminen parantaa käyttäjäystävällisyyttä, mutta tuo mukanaan myös tietoturvauhkia. Suurin tietoturvauhka kertakirjautumisessa on palveluiden käyttämässä kommunikaatioyhteydessä. Tutkijat onnistuivat muun muassa pääsemään käsiksi palveluiden väliseen kommunikaatioon ja saivat itselleen toisen palvelun tekemän tietojen pyynnön. Tätä pyyntöä muokkaamalla he onnistuivat kirjautumaan palveluihin ja tekemään muun muassa ostoksia uhrin tunnuksilla. Myös Facebook-tunnuksen kaappaaminen onnistui vastaavalla menetelmällä. Tämän estämiseksi on kehitelty uusia palveluita. Google on tuonut kaksivaiheisen kirjautumisen, jossa käyttäjän kirjautuu normaalisti palveluun, mutta saa tämän jälkeen puhelimeensa kertakäyttöisen koodin, joka hänen on myös syötettävä palveluun ennen kuin sen käyttö on mahdollista. Palvelu aktivoituu kuitenkin ainoastaan, jos käyttäjä kirjautuu ennestään tuntemattomasta laitteesta tai sijainnista palveluun.

2.4.5. Palvelunestohyökkäys

Palvelunestohyökkäyksellä tarkoitetaan hyökkäystä jonka päämääränä on estää palvelun käyttö, esimerkiksi jonkin organisaation verkkosivu. Hyökkäyksessä palveluun ohjataan niin paljon liikennettä, että palvelimet eivät pysty käsittelemään sitä, josta seuraa palvelun kaatuminen. Palvelunestohyökkäys voidaan jakaa kahteen eri kategoriaan. Ensimmäinen on tavallinen palvelunestohyökkäys (Denial of Service, DoS) ja toinen on hajautettu palvelunestohyökkäys (Distributed Denial of Service, DDoS). Tavallinen palvelunestohyökkäys suoritetaan yleisimmin Smurf, SYN Flood tai UDP Flood muodossa ja siinä käytetään yhtä tietokonetta. Smurf DoS-hyökkäyksessä lähetetään suuri määrä ICMP (Internet Control Message Protocol) kaikuliikennettä eri IP-osoitteisiin, joita kutsutaan vahvistimiksi (Amplifier). Näissä paketeissa on määritelty uhrin osoite ja kun vahvistimet vastaavat näihin paketteihin, vastaavat he paketeissa määriteltyyn osoitteeseen, joka on uhrin. Vastaavia vahvistimia voi olla satoja, joten liikenteen määrä nousee todella isoksi.

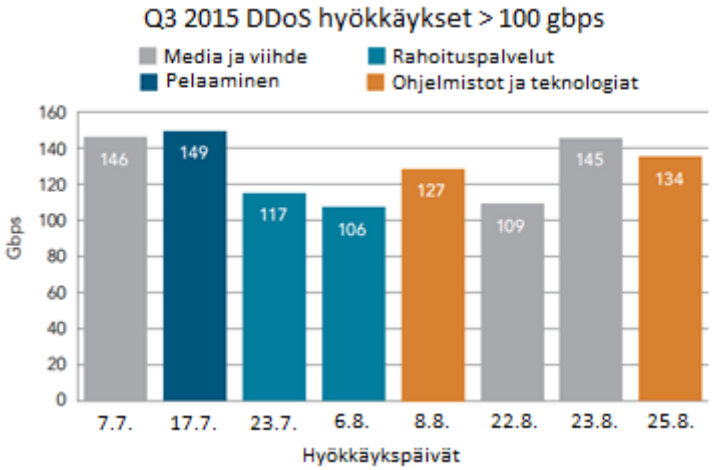
Smurf DoS hyökkäyksestä kärsivät sekä hyökkäyksen uhri kuin myös vahvistimena toimivat koneet.

SYN Flood, joka tunnetaan myös TCP SYN-hyökkäyksenä, käyttää hyväkseen TCP:n (Transmission Control Protocol) kolmitiekättelyä. Kolmitiekättelyssä palvelu vaatii kolmen TCP paketin vaihtoa ennen kuin asiakas saa käyttöluvan. Ensimmäiseksi palvelin vastaanottaa asiakkaan lähettämän SYN (synchronize/start) pyynnön ja vastaa siihen SYN/ACK (synchronize/acknowledge) paketilla. Viimein asiakas vastaa tähän lähettämällä ACK (acknowledge) paketin. Palvelunestohyökkäyksessä asiakas ei koskaan vastaa viimeisellä ACK paketilla, joten palvelin jää odottamaan niitä turhaan. Kun SYN paketteja on lähetettä suuri määrä, ei palvelin pysty niitä käsittelemään ja ylikuormittuu. UDP Flood-hyökkäyksessä käytetään hyväksi UDP-kaikupalvelua (User Datagram Protocol) sekä merkkigeneraattoria. Hyökkäyksessä yhdistetään UDP kaikupalvelu sekä toisella koneella olevaa merkkigeneraattoripalvelu ja nämä vaihtavat keskenään merkkejä niin kauan että palvelin ylikuormittuu. Hyökkäyksessä voidaan käyttää myös ICMP-paketteja.

Distributed Denial of Service hyökkäyksessä hyökkäykseen osallistuu useampi tietokone yhtä aikaa ja usein koneet sijaitsevat ympäri maailmaa. Vaikka DDoS-hyökkäyksien määrä nousi viimeisen vuoden aikana, niiden kesto laski kuten myös keksimääräinen internet-kaistan käyttö. Syitä tähän on monia, mutta yksi suuri syy on erilaisten stressitestityökalujen, joilla voidaan testata sivustojen liikenteen sietokykyä, käytön kasvu. Näitä työkaluja käytetään myös itse hyökkäysten tekemiseen. Työkalut ovat tilaus-pohjaisia ja yleisesti niiden tarjoamien hyökkäyksien kesto on vain 20–60 minuuttia, joten niiden käytön lisääntymisen vuoksi myös hyökkäyksien kesto on lyhentynyt. Perinteisesti DDoS-hyökkäys on tehty bottiverkon avulla ja hyökkäys kesti kunnes se saatiin nujerrettua, hyökkääjä antoi periksi tai bottiverkko saatiin ajettua alas. Bottiverkon rakentaminen ja ylläpito on kuitenkin työlästä, joten hyökkääjien on helpompi käyttää stressitestityökalua. (Akamai 2015).

Vuoden 2015 kolmannella neljänneksellä Iso-Britannia oli hyökkäysten suurin lähtömaa, kun sen osuus oli 26 % kaikista DDoS-hyökkäyksistä. Seuraavana tuli Kiina (21 %) ja kolmantena Yhdysvallat (17 %). Hyökkäyksen keskimääräinen kesto oli 18,86 tuntia joka

oli laskua vuoden takaisesta 22,36 tunnista. Todella suurten DDoS-hyökkäyksien, liikennettä yli 100 gigabittiä sekunnissa, määrä laski vuoden 2015 toiselta neljännekseltä 12 kappaleesta kahdeksaan ja verrattuna vuoden 2014 kolmanteen neljännekseen niiden määrä laski 53 %. Suurin yksittäinen hyökkäys oli 149 Gigabittiä sekunnissa liikennettä ja hyökkäys oli kohdennettu mediaa ja viihdettä tarjoavaa palvelua kohtaan, kuten voimme alla olevasta kuvasta huomata. (Akamai 2015).



Kuva 5. Isojen DDoS-hyökkäysten liikenne sekunnissa. (Akamai 2015).

Kuten DoS, myös DDoS voidaan jakaa useampaan tapaan. Yleisimmät tavat ovat Trinoo/Wintrinoo, Tribe flood network (TFN), TFN2K, Stacheldraht, Shaft, Mstream, Knight sekä Trinity. DDoS-hyökkäykset voidaan jakaa neljään eri tyyppiin. Deeply-Nested XML hyökkäyksessä käytetään hyväksi SOAP-viestien ominaisuutta joka sallii viestin rakenteisiin sisäkkäisten XML viestien upottamisen. Viesti lähetetään verkkopalvelun ylläpitäjälle ja tavoitteena on, että palvelimen XML jäsennin purkaa viestiä ja se täyttää palvelimen muistin.

WSDL-hyökkäyksessä (Web Service Description Language) pyritään palvelin kuormittamaan WSDL:n avulla. WSDL on verkkopalveluissa tärkeä, mutta sillä on monimutkainen rakenne. WSDL:llä ei ole selkeää standardointia, joten WSDL:ää ei ole saatu turvattua tarpeeksi hyvin. Tekniset tiedot ovat myös yleensä julkisesti saatavilla, joten hyökkääjän on helppo saada ne käsiinsä ja pystyy hyödyntämään niitä hajautetussa palvelunestohyökkäyksessä. Web Services Securityn (WSS) on tarkoitus tuoda verkkopalveluihin luottamuksellisuutta, eheyttä sekä luotettavuutta, mutta voi mahdollistaa semanttisen

hyökkäyksen. SOAP-viestiin voidaan sisällyttää yksi <wsse:Security>-kohdan HEADER-tagiin per toimija/rooli, mutta usean <wsse:Signature>-allekirjoituksen. Palvelimet eivät kuitenkaan aina osaa odottaa useaa WWS-allekirjoitusta SOAP-viestissä ja lukevat jokaisen allekirjoituksen erikseen. Allekirjoituksen lukeminen ja niiden julkisten avaimien purkaminen on raskasta, joten tämä voi ylikuormittaa palvelimen. Viimeisenä muotona on haitallinen ulkoisen mallin-viite. XML-mallin syntaksi sallii dokumentin viitata ulkoisesti määriteltyyn XML-nimiavaruuteen ja XML-jäsennin yrittää muodostaa yhteyden viitattuun sijaintiin saadakseen sen käyttöönsä. Hyökkääjä voi käyttää tätä hyväkseen viittaamalla haitalliseen malliin tai sijaintiin, jolloin XML-jäsennin noutaa haitallisen tai määrältään suuren mallin, joka kuormittaa palvelimen.

Pilvipalvelun yleistyminen on myös tuonut täysin uuden puolen palvelunestohyökkäyksiin, jota kutsutaan taloudellinen hajautettu palvelunestohyökkäys (Economic Distributed Denial of Service, EDDoS). EDDoSin tarkoituksena ei ole ainoastaan estää pääsyä palveluun vaan saada myös palveluntarjoajan pilvipalvelun käytöstä aiheutuneet kustannukset nousemaan niin korkeaksi, että pilvipalvelun laskentatehon ostaminen ei ole enää taloudellisesti kannattavaa. Pahimmillaan EDDoS voi jopa johtaa kestävän kehityksen taloudelliseen estämiseen (Economic Denial of Sustainability, EDoS).

Johtuen pilvipalveluiden yleistymisestä, myös hajautettujen palvelunestohyökkäyksien muoto on osittain muuttunut. Pilvipalveluihin voidaan hyökätä joko suoralla tai epäsuoralla palvelunestohyökkäyksellä. Suorassa palvelunestohyökkäyksessä lähetään pilvipalvelulle suuret määrät turhia pyyntöjä, johon pilvipalvelu vastaa ottamalla käyttöönsä enemmän laskentatehoa selvitäkseen liikenteen lisäyksestä. Tämän ansiosta hyökkäys voidaan kohdistaa yhteen ainoaan palveluun ja kun liikenne kasvaa liian suureksi ottaa siitä vastuulla oleva palvelin käyttöönsä enemmän laskentatehoa jolloin muiden palvelimien resurssit joutuvat käyttöön myös. Tämän seurauksena koko pilvipalvelu voi kaatua. Epäsuorassa hyökkäyksessä periaate on sama kuin suorassa, mutta itse hyökkäys tehdään toiseen palveluun ja palvelu, joka halutaan alun perin kaataa, kaatuu pilvipalvelun resurssien jakamisen johdosta. Pahimmillaan voidaan hyökkäykseen käyttää toista pilvipalvelua, jolloin kaksi pilvipalvelua käyttäisivät isot määrät resursseistaan turhaan ja molemmat kärsisivät hyökkäyksestä.

Puolustusmekanismia DDoS-hyökkäyksiä vastaan rakennettaessa tulisi ottaa huomioon viisi periaatetta. Ensimmäiseksi DDoS-hyökkäyksien hajautetun luonteen vuoksi, myös puolustuksen tulisi olla hajautettua. Toiseksi palvelulla tulisi olla korkea NPSR (Normal Packet Survival Ratio), jotta ei tulisi niin paljoa sivullisia uhreja ja puolustuksen solmukohtien tulisi olla turvallisia luotettavuuden, lähteiden todentamisen, eheyden sekä viestien tuoreuden takaamiseksi. Puolustuksen ei tulisi tarvita keskitettyä ohjausta ja sen tulisi ottaa huomioon myös mahdolliset tulevaisuudessa lisättävät järjestelmät ja niiden yhteensopivuus.

2.4.6. Vaarallinen sisäpiiriläinen

Sisäpiiriläiseksi luetaan yrityksen nykyinen tai entinen työntekijä, urakoitsija tai muu liikekumppani, jolla on tai on ollut pääsy yrityksen tietoverkkoon, järjestelmään tai datana. Kun sisäpiiriläinen väärinkäyttää tätä pääsyä ja vaikuttaa negatiivisesti yrityksen datan tai järjestelmän luotettavuuteen, eheyteen tai saatavuuteen, kutsutaan häntä vaaralliseksi sisäpiiriläiseksi. Pilvipalveluiden yhteydessä vaarallinen sisäpiiriläinen voi tarkoittaa vaarallista ylläpitäjää, pilvipalvelun heikkouden paljastamista, pilvipalvelun hyväksikäyttämisen pahassa tarkoituksessa tai läpinäkyvyyden puutetta ylläpitoprosesseissa.

Vaarallinen ylläpitäjä on useimmiten pilvipalveluntarjoajan työntekijä, joka varastaa arkaluontoista materiaalia. Tekijän tavoitteena on monesti taloudellinen hyöty, mutta myös työnantajan infrastruktuurin sabotointi toimii motiivina. Vaarallinen ylläpitäjä voi kantaa kaunaa työnantajaansa kohtaan, mutta hyökkäyksen uhrina on pilvipalveluntarjoajan asiakas, jonka tietoja on varastettu tai tuhottu. Koska ylläpitäjällä on helppo pääsy asiakkaan tietoihin, arkaluontoisen tiedon saaminen ei ole vaikeaa. Vaarallinen ylläpitäjä voi myös poistaa pilvipalvelusta kriittisiä ohjelmistoja, jolloin pilvipalveluiden käyttäminen ei asiakkailta onnistu. Ylläpitäjät voidaan jakaa neljään kategoriaan: hosting-yrityksen ylläpitäjät, virtuaali-tason ylläpitäjä, järjestelmän ylläpitäjät sekä ohjelmistojen ylläpitäjät. Hosting-yrityksen ylläpitäjät voivat muun muassa tehdä man-in-the-middle-hyökkäyksen näkymättömänä kaikkiin pilvipalvelun järjestelmiin kun taas virtuaali-tason ylläpitäjät voivat tehdä kopioita virtuaalikoneista ja käyttää niitä hyväkseen tai muokata

yksittäisiä virtuaalikoneita, jolloin osa pilvestä käyttäytyy vaarallisen ylläpitäjän tahtomalla haitallisella tavalla. Järjestelmien ylläpitäjät voivat suorittaa perinteisiä käyttöjärjestelmiin kohdistuvia hyökkäyksiä kuten troijalaiset ja ohjelmistojen ylläpitäjät voivat muun muassa muuttaa ohjelmistojen asetukset turvattomiksi tai kopioida kaiken ohjelmistojen tiedon, jolloin asiakkaiden tieto on vaarassa.

Pilvipalvelun heikkouden paljastamisessa vaarallinen sisäpiiriläinen käyttää hyväkseen haavoittuvuuksia, jotka ovat seurausta pilvipalvelun käyttämisestä ja tämän avulla saa pääsyn arkaluontoiseen tietoon. Pilvipalvelun käyttö helpottaa vaarallisen sisäpiiriläisen työtä, koska pilvipalveluun on pääsy myös etänä ja tarjoaa parempaa anonymiteettiä. Pilvipalvelun heikkouden paljastaminen voi olla tahallista, mutta myös tahatonta. Tahattomuus on yleensä seurausta pilvipalvelun ja paikallisen järjestelmän eroista turvallisuuspolitiikoissa tai kulunvalvonnassa. Tahattomassa heikkouden paljastamisessa hyökkääjä voi lähettää sähköpostin yrityksen työntekijälle, joka sisältää haittaohjelman. Haittaohjelman avulla hyökkääjä voi päästä käsiksi työntekijän ja yrityksen sähköpostipalveluun, joka toimii pilvipalvelussa. Pilvipalvelun käytöstä johtuva latenssi antaa hyökkääjälle aikaa varastaa tietoa, vaikka hyökkäys havaittaisiin nopeasti. Latenssi johtuu muun muassa siitä, että pilvipalvelimet eivät ole yrityksen omassa kontrollissa, joten niiden sulkeminen on hitaampaa hyökkäyksen havaitsemisen jälkeen.

Pilvipalveluiden hyväksikäyttäminen pahassa tarkoituksessa hyökkääjä käyttää pilvipalvelua hyökätäkseen työnantajaansa kohtaan. Hyökkäyksen kohteena oleva järjestelmä ei välttämättä ole missään tekemisessä pilvipalvelun kanssa, mutta sisäpiiriläinen käyttää pilvipalvelun tehoa hyväkseen. Vaarallinen sisäpiiriläinen voi siis hyökätä pilvipalveluiden avulla yritystä kohtaan hajautetulla palvelunestohyökkäyksellä tai kun työntekijä irtisanotaan yritysestä, hän varastoi arkaluontoista materiaalia pilvipalveluihin, jotta voi hyväksikäyttää näitä tietoja myöhemmin.

Läpinäkyvyyden puutetta ylläpitoprosesseissa voi parantaa nostamalla toimitusketjun valvontaa, laajalla toimittajien arvioinnilla, henkilöstöresursseja koskevien vaatimusten lisäämisellä osaksi sopimuksia, läpinäkyvyyden vaatimisella tietoturvaan, raportoinnin noudattamisella sekä tietoturvaloukkausten ilmoittamisprosessien määrittelyllä. Moni

näistä on mahdollista saavuttaa pilvipalveluntarjoajan kanssa tehdyn sopimuksen valvonnalla, mutta läpinäkyvyydestä johtuen se voi olla hankalaa. Pilvipalveluiden asiakasyritykset eivät voi olla varmoja, että pilvipalveluntarjoajien ylläpitäjät ovat luotettavia ja että heidän rekrytoinnissa käytetään tarpeeksi tiukkoja prosesseja. Nykypäivänä kuitenkin isot pilvipalveluntarjoajat ottavat tämän turvallisuusriskin tosissaan rekrytoidessaan henkilökuntaa. Ylläpitäjien pääsyä myös rajoitetaan asiakkaiden tietoihin.

Vaarallisten sisäpiiriläisten estäminen on vaikeaa. Riskiä voidaan kuitenkin pienentää kun pilvipalvelun käyttöönotto, pilvipalveluun siirtyminen ja ylläpitäminen suunnitellaan tarkasti. Yrityksen tulee myös ottaa huomioon, että koko tietoturva ei ole pilvipalveluntarjoajan vastuulla vaan yrityksen tulee itse muun muassa rajoittaa tarvittaessa työntekijöiden oikeuksia ja suunnitella tiedon katoamisen estämisen eri prosessit. Yrityksen tulee sopia pilvipalveluntarjoajan kanssa myös pilvipalveluihin liittyvien uhkien hoitamisesta sekä koulutettava erityisesti omat ylläpitäjät, jotta tahattomia tietoturvauhkia ei synny. Paikallisten järjestelmien tiedon suojaamiseksi yritys voi tarvittaessa rajoittaa työntekijöiden pääsyä ulkopuolisiin palveluihin, kuten Facebookiin, ja ohjelmistojen avulla havaita, jos arkaluontoista tietoa lähetetään sähköpostilla.

Yksi keino estää haitallisen sisäpiiriläisen hyökkäykset on käyttää kertakäyttöisiä salasanoja. Kun vaarallinen sisäpiiriläinen, tai jokin muu taho kuin tiedon omistaja, yrittää katsoa asiakkaan arkaluontoisia tietoja, saisi tiedon omistaja sähköpostiinsa siitä tiedon ja kertakäyttöisen salasanan. Jos asiakas on itse katsomassa tietoja, hän saa tiedon näkyviin salasanan avulla, mutta jos tietoa yrittää katsoa esimerkiksi vaarallinen sisäpiiriläinen, asiakas saa itselleen siitä tiedon ja hyökkääjä ei pääse käsiksi tietoon. Pilvipalveluiden ja paikallisten järjestelmien välinen liikenne ja tieto tulisi salata ja salaukseen tarvittavia avaimia säilöä paikallisesti. Tällöin pilvipalveluntarjoajan ylläpitäjällä olisi pääsy tietoon, mutta tieto olisi salattu jolloin sillä ei tekisi mitään ja vastaavasti paikallisella ylläpitäjällä olisi salauksen purkuun vaadittavat avaimet, mutta ei tietoa jota purkaa. (Mahajan & Sharma 2015). Suomalainen TeamDrive-pilvipalveluntarjoaja on ottanut käyttöön asiakkaan tiedon salauksen ja pilvipalveluntarjoajalla ei ole pääsyä asiakkaan tietoihin. Asiakkaan tieto salataan jo asiakkaan omalla laitteella ja salausavaimet säilytetään myös asiakkaan omalla laitteella. Normaalisti salausavaimet säilötään pilvipalvelussa, jolloin tietoturva on heikompi. (TeamDrive & Protacon 2015).

2.4.7. Pilvipalvelun väärinkäyttö

Pilvipalveluiden väärinkäyttö voi olla joko pilvipalvelun käyttämistä rikolliseen toimintaan tai pilvipalveluntarjoajan laiton toiminta. Pilvipalveluiden yksi suurimmista hyödyistä on sen tarjoama suuri laskentateho helposti ja edullisesti esimerkiksi PK-yrityksille, mutta se on hyödyllistä myös rikollisille. Pilvipalveluun rekisteröityminen on mahdollista varastetuilla henkilötiedoilla ja varastetulla luottokortilla, mikä hankaloittaa rikollisten kiinnijäämistä, kun heidän henkilöllisyytensä ei ole tiedossa. Tämän jälkeen hyökkääjällä on anonyymisti käytössään pilvipalvelun tuoma laskentateho, jonka avulla hän voi nopeuttaa toimintaansa jopa vuosilla kuin ilman pilvipalvelua. Laskentatehoa tarvitaan muun muassa salausavaimien purkamiseen, joka on hidasta. Pilvipalvelu voidaan myös liittää osaksi hyökkääjän bottiverkkoa. Vuonna 2011 Sonyn maksuympäristö joutui ilmeisesti Brute Force-hyökkäyksen kohteeksi, jossa käytettiin hyväksi pilvipalveluiden laskentatehoa. Hyökkääjät saivat käsiinsä arviolta 77 miljoonan ihmisen henkilötiedot ja 11 miljoonan ihmisen luottokorttitiedot. Pilvipalveluihin voidaan myös säilöä varastettua tai lainvastaista materiaalia kuten varastettuja henkilötietoja tai lasten hyväksikäyttö materiaalia. Pilvipalveluntarjoaja voi myös syyllistyä pilvipalvelun väärinkäyttöön. Näissä tapauksissa sivullisena uhrina on usein pilvipalveluntarjoajan asiakas, kun esimerkiksi pilvipalvelun palvelimet takavarikoidaan ja asiakas ei enää pääse käsiksi omiin tiedostoihinsa.

Väärinkäytösten estämiseksi pilvipalveluntarjoajien tulisi tiukentaa asiakkaiden rekisteröintiä palveluun. Rekisteröinnin yhteydessä tulisi varmistaa, että asiakkaan antamat sähköpostiosoite ja puhelinnumero ovat oikeat ja tiliä ei tulisi aktivoida ennen kuin asiakas tämän voi todistaa. Pilvipalveluiden väärinkäyttäjistä tulisi myös pitää listaa, josta selviäisi ainakin sähköpostiosoite, IP-osoite ja esimerkiksi PayPal maksutiedot. Haitallinen käyttäjä saattaa yrittää rekisteröitymistä uudelleen samalla IP-osoitteella tai maksaa palvelu samasta PayPalista, joten haitallisen käyttäjän toimia saataisiin estettyä tai ainakin hidastettua. Haitallinen käyttäjä voi päästä näistä toimista huolimatta rekisteröitymään, joten pilvipalveluntarjoajan pitäisi valvoa liikennettä, jotta voitaisiin havaita mahdolliset väärinkäytöt sekä tehostaa varastettujen luottokorttien valvontaa.

Kaikki pilvipalveluntarjoajat eivät kuitenkaan onnistu tunnistamaan tai estämään haitallista liikennettä heidän omista pilvipalveluistaan. Tutkimuksessa testattiin pilvipalveluita neljällä eri tavalla ja kuudella eri hyökkäyksellä. Ensimmäisessä tavassa uhrina oli tietokone, joka sijaitsi tyypillisessä tietoverkossa ja kaikki haitallinen liikenne ohjattiin tätä tietokonetta vastaan pilvipalvelusta. Toisessa tavassa uhri sijaitsi samassa pilvipalvelussa kuin mistä hyökkäykset tehtiin ja kolmannessa tilanne oli muuten sama, mutta hyökkäys eli haitallinen liikenne tuli toiselta pilvipalveluntarjoajalta. Viimeisessä tavassa hyökkäystä jatkettiin eri tyyleillä jopa 48 tunnin ajan. Näillä tutkimuksilla saatiin tutkittua pilvipalveluntarjoajien tehokkuutta tunnistaa haitallista liikennettä ulospäin menevän liikenteen joukosta, sisäänpäin tulevasta sekä pilvipalvelun sisällä tapahtuvasta liikenteestä. Yksikään pilvipalveluntarjoaja ei sulkenut tai käynnistänyt uudestaan ulospäin menevän tai sisäänpäin tulevan haitallisen liikenteen yhteyttä kuten ei myöskään pilvipalvelun sisällä tapahtuvan haitallisen liikenteen. Tiedon liikkumista ei rajoitettu millään tavalla eikä pilvipalveluntarjoajilta vastaanotettu minkäänlaista yhteydenottoa. Yksi palveluntarjoaja esti sisäänpäin tulevan ja ulospäin menevän liikenteen SSH-, FTP- ja SMTP-yhteyksillä, mutta niiden kierto onnistui vaihtamalla oletusarvoista porttia. (Pedram Hayati 2012).

Pilvipalveluiden väärinkäytön estämiseksi pilvipalveluntarjoajat voisivat ottaa käyttöön pantti-tyylisen Bitcoin-mikromaksun, jonka asiakkaat maksavat rekisteröityessään pilvipalvelun käyttäjäksi ja saisivat sen takaisin, kun lopettavat käytön. Maksun suuruus olisi pilvipalveluntarjoajan päätettävissä ja suuruus voisi vaihdella asiakastyypin mukaan, palaava asiakas maksaa vähemmän kuin uusi. Maksu olisi sidottu asiakkaan julkiseen salausavaimeen ja maksun suoritettuaan asiakas ilmoittaisi avaimen pilvipalveluntarjoajalle, joka käyttäisi sitä varmistaakseen maksusuorituksen. Tämän jälkeen asiakas saisi palvelun käyttöönsä. Pilvipalveluntarjoajan tulee tämän jälkeen seurata aktiivisesti liikennettä esimerkiksi roskapostintunnistimella tai IaaS-mallissa Hypervisorilla, joka mahdollistaa usean käyttöjärjestelmän jakaa yhden palvelimen resurssit, jotta väärinkäyttö voidaan havaita. Jos pilvipalveluntarjoaja havaitsee väärinkäyttöä, voi se sulkea asiakkaan tilin ja tämä johtaisi mikromaksun jäämiseen pilvipalveluntarjoajalle. Suurin hyöty tästä mallista olisi siinä, että pilvipalveluntarjoajat saisivat maksun asiakkaalta jo ennen pilvipalvelun käyttöä. Moni väärinkäyttö havaitaan vasta kun se on jo aiheuttanut vahinkoa,

esimerkiksi sähkölaskun nousun, joten tämän mallin ansiosta pilvipalveluntarjoaja voisi korvata nuo kustannukset näistä talletuksista.

Maksun suuruus on kuitenkin ongelmallinen pilvipalveluntarjoajalle, sillä sen ollessa liian suuri eivät asiakkaat tule palvelun käyttäjiksi ja sen ollessa liian pieni ei sillä ole haluttua vaikutusta. Maksun suuruuden ratkaisemiseksi voitaisiin seurata pimeitä markkinoida ja palveluiden, jotka ovat suosittuja hyökkäysten tekemisessä, hintaa nostettaisiin. Myös asiakkaan takaisin saama summa tulisi olemaan pienempi kuin asiakkaan tekemä tallennus, johtuen toimituskuluista. Jos jostain kohteista tulisi usein rahasiirtoja, voitaisiin niissä myös pitää pienempiä toimituskuluja, kuten Visalla kauppiaiden koodijärjestelmässä. Pilvipalveluntarjoaja voisi myös käyttää hyväkseen Bitcoinin hinnanvaihtelua. Pilvipalveluntarjoaja voisi pitää Bitcoineja itsellään ja odottaa hinnan nousua ennen kuin myyvät ne, joten hinnan tulisi olla oikeassa valuutassa kiinteä ja vaihdella Bitcoineissa. Pilvipalveluntarjoajien tulee myös lisätä hintoihin Bitcoinin valuuttavaihdoksesta perittävien kulujen summa.

Bitcoinien pseudonyymi toisi myös ongelmia asiakkaan ja pilvipalveluntarjoajan välille, sillä jos asiakas esimerkiksi lähettää sähköpostia pilvipalveluntarjoajalle, voi se rikkoa Bitcoinin julkisen salausavaimen pseudonyymin. Jos asiakas tämän jälkeen haluaisi uuden julkisen salausavaimen säilyttääkseen pseudonyyminsä, ei pilvipalveluntarjoaja voisi enää yhdistää asiakkaan maksua aikaisempiin ostoihin ja asiakkaan hinta nousisi. Asiakkaalla ei ole mitään takeita siitä, että hän saa talletuksensa takaisin, varsinkaan pienemmiltä pilvipalveluntarjoajilta, vaikka pilvipalvelun väärinkäyttöä ei ole tapahtunut.

2.4.8. Puutteellinen huolellisuus

Moni yritys siirtyy pilvipalveluiden käyttäjäksi ja odottavat alenevia kustannuksia, enemmän tehokkuutta ja parempaa turvallisuutta. Yrityksellä ei välttämättä ole täysin oikeaa kuvaa siitä, mitä uhkia pilvipalvelut tuovat. Ennen pilvipalveluihin siirtymistä yrityksen olisi tehtävä tarkka analyysi, jotta pilvipalvelun uhat saadaan minimoitua ja hyödyt maksimoitua. Ensimmäiseksi yrityksen on ymmärrettävä pilven rakenne ja toimintaperiaatteet

sekä miten sen käyttö vaikuttaa tiedon turvallisuuteen. Yrityksen tulee vaativa pilvipalveluntarjoajalta läpinäkyvyyttä ja pyytää toimittamaan yksityiskohtainen selvitys turvallisuusarkkitehtuurista ja hyväksyä säännöllinen tarkistus. Yrityksen tulee olla varma pilvipalveluntarjoajan sisäisestä turvallisuudesta ja sen vahvuudesta sekä tuntea lait ja säännökset jotka koskevat pilvipalveluiden käyttöä ja niihin tallennettuja tietoja. Viimeiseksi yrityksen tulee jatkuvasti seurata pilvipalveluiden kehitystä ja sen vaikutusta niiden turvallisuuteen.

Yrityksen tulisi lisäksi yhdessä pilvipalveluntarjoajan kanssa selvittää käyttäjien kulunvalvontaan, sääntelyn noudattamiseen, tiedon sijaintiin, tiedon erotteluun, katastrofista toipumisen vahvistukseen, katastrofista toipumiseen ja pitkänaikavälin kannattavuuteen liittyvät asiat ennen kuin siirtävät toimintojaan pilvipalveluun. Käyttäjien kulunvalvonnan osalta yrityksen tulisi saada pilvipalveluntarjoajalta informaatiota pilvipalveluntarjoajan rekrytoinnista sekä tieto kenellä on pääsy yrityksen tietoihin. Erityisesti isojen yritysten tulisi myös määrätä omat rajoitteensa siihen, että ketkä pääsevät näkemään heidän tietojaan. Yrityksen on myös varmistuttava, että pilvipalveluntarjoaja on sitoutunut sääntelyn noudattamiseen ja sallii ulkopuolisten tekemät tarkistukset. Myös tiedon säilyttämisestä sovitulla lainkäyttöalueella on sovittava etukäteen ja pilvipalveluntarjoajan tulisi esittää todisteet siitä, että heillä on käytössä tehokkaat salausmallit tiedolle ja että asiakasyrityksen tiedot pidetään turvallisesti erossa muiden asiakkaiden tiedoista ja näihin ei ole muilla pääsyä.

Yrityksen tulee tietää etukäteen miten pilvipalveluntarjoaja toimii katastrofin tapahtuessa ja yrityksen tiedon joutuessa sen saavuttamattomiin. Pilvipalveluntarjoajan tulee etukäteen kertoa heidän suunnitelmansa katastrofin varalle johon kuuluu todistus tietojen palauttamista kuin myös itse palvelun palauttamisesta toimintaan. Tieto siitä, kuinka yritys saa omat tiedostonsa ja tietonsa takaisin pilvipalvelusta, jos pilvipalveluntarjoaja hakeutuu konkurssiin tai myydään, ja että se on käytettävässä muodossa, tulee myös vaatia.

Selkeä strategia auttaa yritystä siirtymään turvallisesti pilvipalveluiden käyttäjäksi ja sen kattavuus tulee määritellä pilvipalveluun tallennettavan tiedon arkaluontoisuuden mukaan. Yrityksen on tehtävä riski/hyötyanalyysi, jotta ymmärretään pilvipalvelun tuomat hyödyt ja riskit sekä myös se, että pilvipalveluntarjoajan tietoturvauhat saattavat heijastua

yritykseen. Yrityksen tulee myös realistisesti arvioida sisäisten ja ulkoisten palveluiden kustannukset, jotka aiheutuvat pilvipalveluntarjoajan suhteiden hoitamisesta sekä kustannukset jotka tulevat kun jo olemassa olevat järjestelmät integroidaan pilvipalveluun. Kaikki yrityksen elimet tulee myös konsultoida tässä vaiheessa pilvipalveluun siirtymisen johdosta.

Strategian tulee sisältää myös määritelmä yrityksen palveluista jotka ovat ei-kriittisiä, sisältävät julkista tietoa tai vaatisivat suurta infrastruktuuria ja sijoituksia, jotta niiden toimittaminen olisi mahdollista sisäisesti. Näiden palveluiden siirtäminen pilvipalveluun on yritykselle eduksi ja maksimoisi pilvipalvelun hyödyt. Kriittiset yrityksen ydinosaamista sisältävät ja kriittistä informaatiota sisältävät palvelut aiheuttaisivat pilvipalvelussa suuremman riskin. Kaikkea tietoa yrityksen ei kannata laittaa pilvipalveluun tai ainakaan julkiseen pilvipalveluun. Yrityksen tulee selvittää olisiko heille edullisempaa ja turvallisempaa siirtää joitain palveluita yksityiseen tai hybridi pilvipalveluun. Jos pilvipalveluun tallennetaan arkaluontoista tietoa, on pilvipalveluntarjoajan kanssa tehtävä tarkka sopimus sen suojelemisesta ja saatavuudesta. Pilvipalveluntarjoajan tietoturvan tulee olla paremmalla tasolla kuin se on yrityksen sisäisissä palveluissa tai ainakin samalla tasolla. Pitkänaikavälin määritelmässä yrityksen tulee ottaa huomioon muun muassa pilvipalveluntarjoajan talous, kolmannen osapuolen arviot sekä maine. Yrityksellä tulee olla selkeä poistumisstrategia pilvipalvelusta, jotta toimintaa voidaan jatkaa keskeytyksettä ja tiedon vaarantumatta, jos pilvipalveluntarjoaja esimerkiksi hakeutuu konkurssiin.

2.4.9. Jaetun teknologian haavoittuvuudet

Infrastructure as a Service- mallin pilvipalveluntarjoajat käyttävät jaettua infrastruktuuria taatakseen asiakkailleen skaalautuvat palvelut. Kaikkia infrastruktuurin komponentteja ei kuitenkaan ole suunniteltu tähän tarkoitukseen. Esimerkiksi pilvipalveluiden palvelimet käyttävät useita moniytimisiä prosessoreita ja tieto kulkee näiden ytimien välillä, joten on mahdollista että käyttäjä voi päästä käsiksi tietoon, joka ei ole hänen. Nämä komponentit eivät tarjoa vahvaa eristysmahdollisuutta, joten eristys joudutaan tekemään virtuaalisesti. Virtualisointi mahdollistaa pilvipalvelun tehokkaamman käytön, mutta se tuo

omia tietoturvauhkia. Virtualisointi toteutetaan Hypervisorin avulla, jotta eritys olisi mahdollisimman hyvä, mutta se ei kuitenkaan ole täydellinen. Hypervisorin käyttö mahdollistaa muun muassa virtuaalikone hyppely-hyökkäyksen (VM Hopping) ja virtuaalikone pako-hyökkäyksen (VM Escape). Virtuaalikone pako-hyökkäyksessä virtuaalikoneessa suoritetaan haitallista koodia, joka murtautuu Hypervisor-tasolle. Hypervisorin saastuttamalla saadaan koko pilvipalvelu käyttöön. Virtuaalikone hyppelyssä heikon tietoturvan omaava virtuaalikone saadaan hallintaan ja sitä hyväksikäyttämällä yritetään saada hallintaan muut virtuaalikoneet.

Kommunikaation sokeat kohdat ovat ongelmana virtuaalisessa ympäristössä, sillä perinteiset tietoverkon tietoturvalaitteet eivät näe samassa palvelimessa olevien virtuaalikoneiden keskinäistä kommunikaatiota ellei kommunikaatiota kierrätetä ulkomaailman kautta. Jos kommunikaatio kierrätetään palvelimen ulkopuolella, aiheuttaa se viivettä kommunikaatioon. Sokeat kohdat ja kierrättämisestä aiheutuva viive voidaan eliminoida virtuaalikoneella, jonka tehtävänä on valvoa ja ohjata muiden virtuaalikoneiden kommunikaatiota. Tämä virtuaalikone integroi hypervisorin kanssa, joten tämä ratkaisu ei ole ideaalinen pilvipalvelulle, koska käyttäjällä ei aina ole pääsyä hypervisor-tasolle. Pilvipalveluissa tämä on koitettu ratkaista itsepuolustavilla virtuaalikoneilla, joissa virtuaalikone itse suojaa itsensä ja sen ei tarvitse kommunikoida ulkopuolelle pysyäkseen turvallisena. Virtuaalikoneissa voi olla myös erittäin arkaluontoista tietoa, joka on suojattava hyvin, mutta myös tietoa joka on julkista tai ei-arkaluontoista ja ei tarvitse erityistä suojaamista. Tämä luo ongelman luottamuksen tasoon, kun samalla virtuaalikoneella on eritasoista suojasta vaativaa tietoa. Tätä voidaan välttää hajauttamalla yrityksen tietoja usealle palvelimille, mutta samalla se tuhoaisi virtualisoinnin tarkoituksen. Jos virtuaalikoneet osaavat puolustaa itseään, esimerkiksi tunkeilijan havaitsemisella ja estämisellä, palomuurilla, eheydellä, valvonnalla ja antivirus-toiminnoilla, ei ongelmaa pääse syntymään vaikka virtuaalikone sisältäisi eritasoista suojausta vaativaa tietoa. (Trend Micro).

Virtualisoidut ympäristöt eivät teoriassa ole yhtään vähemmän turvallisia kuin fyysiset ympäristöt, mutta käytännössä virtuaalisten ympäristön käyttö saattaa aiheuttaa tietoturvauhkia, ellei näitä etukäteen oteta huomioon. Yrityksissä virtuaalikoneita jatkuvasti otetaan käyttöön uusia, kloonataan, siirretään, ja poistetaan käytöstä vanhoja testiympäris-

töiksi, katastrofista toipumiseen, säännöllisiin huoltoihin ja tukemaan tehtäviä, joissa tarvitaan laskentatehoa. Tämän seurauksena virtuaalikoneita on aktiivisena ja ei-aktiivisena jatkuvasti ja niiden tila vaihtelee, joten myös niiden tietoturvantason ylläpito on haasteellista. Kauemmin poissa käytöstä olleen virtuaalikoneen tietoturva on voinut laskea niin alas, että sen käynnistäminen voi luoda suuren tietoturvauhan. Hyökkääjät voivat myös joissain tapauksissa käyttää hyväkseen virtuaalikoneita, jotka eivät ole edes aktiivisia tai uusia virtuaalikoneita voidaan kloonata virtuaalikoneesta, jonka tietoturva on jo valmiiksi vanhentunut. (Trend Micro).

Normaalien antivirus tai muiden vastaavien, paljon resursseja käyttävien ohjelmien, suorittaminen pilvipalvelimella voi aiheuttaa todella suuren kuorman järjestelmälle. Kun ajastettu antivirustarkistus tai ajastettu päivitys suoritetaan samaan aikaan kaikissa virtuaalikoneissa, lamauttaa se koko virtualisoinnin alapuolella olevan fyysisen laitteiston, koska sen resurssit eivät riitä. Jos tuote ei ymmärrä virtualisointia, käyttävät ne hyväkseen satunnaisuutta tai ryhmittämistä, jotta vältytään resursseista tappelemiselta. Tämä ei kuitenkaan toimi virtualisointia sisältävässä pilvipalvelimessa, sillä se ei estä resursseista taistelua tai ei auta välttämään liiallista aikaa, jonka antivirustarkistus vie. Ryhmittely ei myöskään sovi virtualisoinnin liikkuvaan luonteeseen missä uusia virtuaalikoneita luodaan ja poistetaan käytöstä jatkuvasti. Ratkaisuna voisi olla virtuaalikone, joka ymmärtää virtualisoinnin tarpeet, ja voi aikatauluttaa tarkistukset virtuaalikoneissa, jotta palvelimen resurssit ovat riittävät. Keskitetty antivirus pienentäisi huomattavasti palvelimen muistin jalanjälkeä parantaen tietoturvaa. (Trend Micro).

Joulukuussa 2015 Valven kehittämän Steam-pilvipalvelun käyttäjät joutuivat kokemaan jaetun teknologian huonommat puolet. Steam-palvelu joutui usean palvelunestihyökkäyksen kohteeksi ja jotta palvelu kestäisi hyökkäyksen, kolmannen osapuolen ylläpitämät erityiset välimuistin säännöt otettiin käyttöön. Tämän tarkoituksena oli estää palvelunestohyökkäyksen haitallinen liikenne palvelun palvelimille, mutta samaan aikaan päästää läpi normaali liikenne, jotta palvelu toimisi käyttäjilleen. Hyökkäyksen jatkuessa, jouduttiin vielä uusi välimuistin konfiguraatio ottamaan käyttöön ja tämä konfiguraatio erheellisesti näytti kirjautuneille käyttäjille Steam-kaupan vastauksia, jotka olivat luotu toiselle käyttäjälle eli käyttäjät näkivät väärän Steam-tilin tiedot omansa sijaan. Konfiguraatiovirheen seurauksena koko Steam-palvelu jouduttiin lopulta ajamaan alas ja uudet

konfiguraatiot jouduttiin testaamaan tarkkaan ennen kuin palvelu saatiin jälleen toimintaan. Konfiguraatiovirheen takia käyttäjät näkivät väärien tilien laskutusosoitteita, puhelinnumeroiden neljä viimeistä numeroa, ostohistorian, luottokorttien kaksi viimeistä numeroa sekä sähköpostiosoitteet. Steam-palvelun muuten korkeasta tietoturvasta johtuen käyttäjien kokonaiset luottokorttinumerot tai salasanat eivät näkyneet väärille henkilöille. Näkyvillä ei ollut myöskään tarpeeksi tietoa, jotta tilin väärinkäyttö olisi onnistunut. Saman palvelunestohyökkäyksen kohteeksi joutuivat myös Sonyn Playstation Network sekä Microsoftin Xbox Live (Steam 2015; Puustinen 2015).

Moni yritys olisi halukas siirtymään pilvipalveluihin, mutta eivät ole sitä tehneet johtuen tietoturvauhista. Hypervisorin tietoturvauhkien poistamiseksi voitaisiin ottaa käyttöön NoHype-malli, missä Hypervisor poistetaan kokonaan käytöstä. Tämä parantaisi pilvipalvelun tietoturvaa. Virtuaalikoneet olisivat suoraan laitteiston päällä ilman Hypervisoria, mutta virtuaalikoneiden käynnistämistä ja pysäyttämistä varten pidettäisiin hallintaohjelmisto. NoHype-mallissa virtuaalikoneet toimivat keskeytyksettä ja niillä on suora pääsy laitteiston resursseihin. Jokainen virtuaalikone saisi oman ytimen prosessorilta käytettäväkseen, jolloin eliminoituisi mahdollisuus, että käyttäjä pääsisi käsiksi toisen käyttäjän tietoihin. Pilvipalvelun toiminta ei kuitenkaan juuri heikentyisi, sillä nykyisissä prosessoreissa on jo kahdeksan ydintä ja lähivuosien aikana jo 16. Nykyisissä laitteistoissa fyysisen muistin määrä on jo 256 GB ja NoHype-mallissa tämä muisti osioitaisiin virtuaalikoneille. Virtuaalikoneen toiminta pysyisi samana, mutta osiointi selkeyttäisi multicore controllerin (MCC) toimintaa. MCC:n tehtävänä on jakaa muisti reilusti käyttäjien kesken ja NoHype-mallissa se voisi jakaa muistin suoraan prosessorien ytimien lukumäärän perusteella. Myös Ethernet-kytkimen tehtävät siityisivät palvelinkeskuksen Ethernet-kytkimelle, kun ohjelmallinen kytkin poistuisi Hypervisorin mukana. Tämä vähentäisi hallinnoinnin tarvetta ja prosessorin kuorma keventyisi. Palvelimen käynnistyessä satunnaisesti valittu prosessorin ydin käynnistetään hyper-privileged tilassa ja se toimii järjestelmänhallintana. Ydin vastaanottaa pilvipalvelun hallintaohjelmistolta käskyjä ja käynnistää ja pysäyttää virtuaalikoneita käskyjen mukaan.

3. KYSELY PK-YRITYKSILLE

Kyselytutkimuksen tarpeellisuuden idea sai alkunsa pilvipalveluiden nopeasta yleistymisestä ja niiden tuomasta suuresta hyödystä niin kuluttajille kuin PK-yrityksille. PK-yritykset ovat Suomessa myös kuin maailmalla todella tärkeä osa taloutta, mutta monesti toimivat rajallisella budjetilla ja vähällä henkilökunnalla, joten tekninen osaaminen tai tekniikan yleinen tuntemus voi olla heikompaa kuin isoilla yrityksillä. Tästä syystä halusin kartoittaa PK-yritysten mielipiteitä ja asenteita pilvipalveluiden tietoturvaa kohtaan, jotta mahdollisesti nähdään onko niissä parantamisen varaa.

PK-yrityksille suunnatun kyselytutkimuksen tarkoituksena oli selvittää, ovatko PK-yritykset huolestuneita pilvipalveluiden tietoturvasta ja onko tietoturvalla mahdollisesti osuutta syihin miksi pilvipalveluihin ei ole siirrytty. Kyselyssä kartoitettiin aluksi yleisesti PK-yritysten tarpeita pilvipalveluille ja etätyölle sekä onko pilvipalvelut tuttuja vastaajalle. Riippuen siitä oliko yrityksessä käytössä pilvipalveluita vai ei, vastaajat jaoteltiin omiin ryhmiin. Tietoturvauhkia koskevat kysymykset olivat molemmille vastaajaryhmillä samat, mutta muuta suhtautumista pilvipalveluihin koskevat kysymykset olivat keskenään erilaisia.

Kysely toteutettiin vuonna 2015 Marraskuun ja Joulukuun aikana. Ensimmäisen kerran kysely toimitettiin vastaanottajille 26. Marraskuuta ja muistutusviesti lähetettiin 16. Joulukuuta. Vastaajille ei määritelty ajankohtaa, jolloin kysely on auki. Kyselyn levityksessä saatiin apua Vaasan Yrittäjiltä. Vaasan Yrittäjillä on todella hyvät kontaktit Vaasan alueen PK-yrityksiin. Kysely toimitettiin Vaasan Yrittäjien jäsenille sähköpostitse. Kyselyssä ei kysytty vastaajilta tietoturvan teknisestä toteutuksesta, koska kyselyn tarkoituksena oli, että vastaajan ei tarvitse tuntea pilvipalveluita tai sen uhkia normaali käyttäjää tarkemmin. Kysely toteutettiin sähköisessä muodossa ja sen toteutuksessa käytettiin apuna Google Form-palvelua. Tämän ansiosta kysely oli helppo lähettää PK-yrityksille sähköisesti jakamalla linkki kyselyyn. Kyselyyn vastatakseen vastaajan ei tarvinnut kirjautua Googlen palveluihin, koska näin mahdollistettiin anonyymi ja mahdollisimman yksinkertainen vastaaminen. Haitta puolena tässä oli se, että anonyymius mahdollisti vastaamisen useaan kertaan, mutta tästä ei kyselyn aikana näkynyt mitään viitteitä.

3.1. Tulokset

Kyselyyn vastanneita PK-yrityksiä oli 91 kappaletta. Vastaajien määrä oli riittävä tekemään johtopäätöksiä kyselyn perusteella, joten vastaajien aktiivisuuteen voi olla tyytyväinen. Vastaajat ovat kuitenkin kaikki Vaasan alueelta, joten maantieteellinen sijainti on vastaajien keskuudessa hyvin rajattu. Vastaajille annettiin mahdollisuus ilmoittaa toimiala, mutta tämä ei ollut pakollista, jotta anonymiteetti säilyisi mahdollisimman hyvin. Toimialan ilmoitti 25 yritystä eli noin yksi kolmasosa vastanneista. Vastanneiden yrityksien joukossa oli muun muassa rakennusalanyrityksiä, teollisuudenalan ja markkinoinninalan. Kaiken kaikkiaan vastaajia oli todella monelta eri toimialalta, joten kyselyn tulokset kuvastavat hyvin koko PK-yrityksien kirjoa eikä ainoastaan joitain tiettyjä toimialoja. Vastaajien joukko oli todella heterogeeninen, jolloin kysely kuvastaa paremmin todellisuutta.

Kyselyn ensimmäinen osio sisälsi toimiala kysymyksen ja sen lisäksi kolme muuta yleistä kysymystä. Nämä ensimmäisen osion kysymykset olivat suunnattu kaikille vastanneille ja niiden tarkoituksena oli kartoittaa yleistä tietoa pilvipalveluista ja käytetäänkö vastaajan yrityksessä pilvipalveluita. Kaikkiin kysymyksiin vastausvaihtoehtona oli ”Kyllä” ja ”Ei” sekä toimiala-kysymykseen vastaaja sai kirjoittaa itse toimialansa tai jättää sen tyhjäksi. Tällä osiolla vastausprosentti oli 100 %, sillä kaikki kysymykset olivat pakollisia kysymyksiä eli vastaaja ei voinut niitä ohittaa. Ensimmäinen kysymys oli ”Onko yrityksessä tarvetta työskennellä etänä?” ja vastaajia kysymyksellä oli 91. Vastaajista 61 kappaletta vastasi ”Kyllä” eli 67 % kaikista vastaajista. ”Ei” vaihtoehdon valitsi siis eli 33 %. Selkeästi yli puolessa yrityksistä siis on tarvetta työskennellä etänä. Vastauksen tulosjakauma ei ole yllätys, sillä nykyaikana esimerkiksi sähköposteja joudutaan lukemaan myös työpaikan ulkopuolella ja jopa työajan ulkopuolella. Kysymys ei kuitenkaan eritellyt, että työskennelläänkö yrityksessä etänä vaan onko sille tarvetta, joten useammassa vastaajayrityksessä voidaan työskennellä etänä huolimatta ”Ei”-vaihtoehdon valitsemisesta.

Toisena kysymyksenä oli ”Ovatko pilvipalvelut teille tuttuja?”. Myös tähän kysymykseen vastasi 91 kappaletta. 85.7 % vastaajista eli 78 kappaletta vastasi kysymykseen ”Kyllä”

eli heillä oli tietoa pilvipalveluista. Pilvipalvelut eivät olleet tuttuja 13 PK-yritykselle. Tämänkään kysymyksen vastausjakaumassa ei yllätyksiä esiintynyt, sillä pilvipalvelut ovat nykyään joka puolella ja iso osa ihmisten arkea. Osa ”Ei” vastaajista saattaa myös käyttää pilvipalvelua tuntematta sitä sen tarkemmin tai edes ymmärtävän sen olevan pilvipalvelu, koska usein pilvipalvelut toimivat aivan kuten paikallinen ohjelmisto. Kolmas kysymys oli ”Käytetäänkö yrityksessä pilvipalveluita?”. 29 vastaajaa eli noin kolmasosa kysymykseen vastanneista yrityksistä ei käytetä tällä hetkellä pilvipalveluita, kun puolestaan 68.1 % vastanneista PK-yrityksistä käytetään. Huomattavasti yli puolet vastanneista siis käyttävät pilvipalveluita, mikä ei ole yllätys. Kaikki vastanneista eivät välttämättä ole täysin varmoja siitä, että käyttävätkö pilvipalveluita tai yksinkertaisesti eivät vain ole tietoisia. Tämä kysymys toimi myös jakajana ja sen avulla jaettiin vastaajat kahteen ryhmään eli pilvipalveluiden käyttäjiin ja niihin jotka eivät käytä pilvipalveluita. Tämän kysymyksen jälkeen molemmille ryhmille esitettiin eri kysymykset. Pohjimmiltaan kysymyksien sisältö oli suhteellisen samankaltainen, mutta kysymysten asettelu on hieman eri riippuen ryhmästä. Pilvipalveluiden käyttäjien kysymyksiin vastasi siis 62 kappaletta yrityksistä ja puolestaan pilvipalveluita käyttämättömien kysymyksiin vastasi 29 kappaletta.

3.1.1. Pilvipalvelua käyttämättömien vastaukset

Yrityksiä, joissa ei pilvipalveluita ole käytössä, vastasi kyselyyn 29 kappaletta. Mikään kysymyksistä ei kuitenkaan ollut pakollinen, joten kaikki kysymykset eivät välttämättä saaneet 100 % vastausosuutta. Tämä voi johtua siitä, että vastaaja ei ole ymmärtänyt kysymystä tai mikään vaihtoehto ei ole ollut sopiva. Yrityksille, joilla ei pilvipalveluita ole käytössä, kysymykset oli jaettu kahteen eri osioon. Ensimmäisessä osiossa yrityksiltä kysyttiin kolme kysymystä, jotka liittyivät yleisesti pilvipalveluihin. Toisessa osiossa kysyttiin itse tietoturvauhista.

Kysymys: ”Onko yrityksessä pohdittu siirtymistä pilvipalveluiden käyttäjäksi?”

Vastausvaihtoehtoina kysymyksessä oli ”Kyllä” ja ”Ei”. 100 % vastaajista vastasi tähän kysymykseen. Enemmistö vastaajista eli 58.6 % (17 kappaletta) vastasi, että yrityksessä ei ole pohdittu siirtymistä pilvipalveluiden käyttäjäksi. 41.1 % (12 kappaletta) puolestaan

vastasi, että yrityksessä on pohdittu siirtymistä. Vastauksen jakauma oli pienoinen yllätys, sillä monesti pilvipalveluita on ainakin pohdittu vaikka olisi todettu, että mahdollinen hyöty olisi liian pieni kustannuksiin tai muuhun vastaavaan nähden. Melkein 60 % on kuitenkin iso osuus, mutta myös näistä yrityksistä osa saattaa tulevaisuudessa siirtyä pilvipalveluihin, kun tavoitteena on kasvu tai siirtyminen uusille markkinoille.

Kysymys: ”Ovatko uutiset lisääntyneistä tietomurroista saaneet teidät kyseenalaistamaan pilvipalveluiden tietoturvaa?”.

Tässäkin kysymyksessä oli vastausprosentti täysi 100 %. Vastausvaihtoehtoina oli ”Paljon”, ”Jonkin verran” ja ”Ei yhtään”. Pilvipalveluiden tietoturvaa lisääntyneiden tietomurtojen johdosta vastaajista7 kappaletta ei kyseenalaistanut pilvipalveluiden tietoturvaa yhtään. 22 kappaletta oli kuitenkin huolissaan pilvipalveluiden tietoturvasta johtuen lisääntyneistä tietomurroista. Näistä 22 kappaleesta ylivoimaisesti isoin osa eli 16 vastaajaa tietomurrot olivat saaneet kyseenalaistamaan tietoturvaa jonkin verran. Tämä 16 vastaajaa oli myös yli puolet vastaajista koko kysymyksen osalta eli 55.2 %. Paljon huolestuneita oli 6 kappaletta. Tietomurroista puhutaan mediassa nykyään paljon ja tietomurrot voivat olla myös todella isoja ja koskettaa suurta ihmismäärää, joten on luonnollista, että niillä on myös vaikutusta PK-yrityksien mielikuviin pilvipalveluista. Vastauksien jakautumisessa ei mitään ihmeellistä ollut vaikka pienin ryhmä vastaajista oli paljon huolestuneita, mutta kokonaisuudessaan kolme neljäsosaa oli huolestuneita tietoturvasta, johtuen lisääntyneistä tietomurroista tai ainakin niiden lisääntyneestä uutisoinnista.

Kysymys: ”Mitkä seuraavista koette pilvipalveluiden eduksi?”

Vaihtoehtoja oli 11 kappaletta ja vastaajia oli 28 kappaletta. Vaihtoehtoina oli ”Datan saatavuus usealla laitteella”, ”Oman datan oleminen aina saatavilla”, ”Etätyöskentely”, ”Kilpailuetu”, ”Kustannukset”, ”Tietoturva”, ”Helppous”, ”Mahdollisuus uuteen toimintamalliin”, ”Yrityksen toimintojen tehostuminen”, ”Järjestelmien olemisen aina päivitettynä” sekä ”Muu/Other”. Suosituin etu pilvipalveluille oli vastaajien mukaan etätyöskentely, jonka koki eduksi 20 kappaletta vastaajista eli reilu 70 %. Seuraavaksi suosituimpana olivat datan saatavuus usealla laitteella sekä oman datan oleminen aina saatavilla. Molemmat vaihtoehdot keräsivät 18 vastausta eli 64.3 %. Lähelle edellisiä pääsi järjestelmien oleminen aina päivitettynä keräten 16 vastausta (57.1 %). Muut vaihtoehdot jäivät

alle 50 %, lähimmäksi pääsi helppous, joka sai 12 kappaletta vastauksia. Mahdollisuus uuteen toimintamalliin sai yrityksiltä 8 vastausta joka oli 28.6 %. Loput vaihtoehdot jäivät 10 % pintaan ja sen alle. Ainoa vaihtoehto, joka jäi kokonaan ilman ääniä, oli kilpailuetu. Tämän kysymyksen vastaukset olivat yllättäviä. Pilvipalvelut ovat yleisesti tunnettuja siitä, että ne tarjoavat kustannustehokkaita vaihtoehtoja erityisesti PK-yrityksille, joilla ei ole varaa tai osaamista sijoittaa isoihin järjestelmiin, mutta tarvitsevat laajennusta. Kuitenkin vastaajista ainoastaan 2 kappaletta näki pilvipalveluiden etuna kustannukset. Myös tietoturva sai 2 kappaletta vastauksia, vaikka yleisesti pilvipalveluiden käyttöönotto parantaa tietoturvaa yrityksissä, sillä pilvipalveluntarjoajilla on aivan eritasoiset resurssit panostaa tietoturvaan ja tämä näkyy myös asiakkaan arjessa. Vastanneista PK-yrityksistä yksikään ei uskonut pilvipalveluiden tuovat mitään etua kilpailullisesti, vaikka pilvipalvelut muuan muassa mahdollistavat PK-yrityksien laajentumisen. Vaikka 8 kappaletta vastaajista uskoi pilvipalveluiden tuovan mahdollisuuden uuteen toimintamalliin, myöskään heistä ei yksikään uskonut tämän tuovan kilpailuetua yritykselle. Harva vastaajasta osasi myös yhdistää järjestelmien olemisen ajan tasalla ja tietoturvan toisiinsa, kun ensimmäisellä oli 16 vastaajaa, mutta tietoturvalla ainoataan kaksi.

Toinen osio käsitteli ainoastaan pilvipalveluita koskevia tietoturvauhkia. Kaikki kysymykset kysyivät vastaajalta kuinka huolissaan he ovat kyseisestä tietoturvauhkasta. Kysymyksiä esitettiin 10 kappaletta ja nämä kaikki sisälsivät viisi eri vaihtoehtoa. Vastausvaihtoehdot olivat luvut 1–5 ykkösen ollessa ”En ollenkaan” ja viitosen ollessa ”Erittäin suureksi”.

Kysymys: ”Kuinka suureksi uhkaksi koette pilvipalvelun palvelukatkoksen?”

Vastaajia kysymyksellä oli 28 kappaletta 29 mahdollisesta. Palvelukatkoksesta ei ollut ollenkaan huolissaan 10.7 % vastaajista. Erittäin suurena uhkana palvelukatkosta piti puolestaan 21.4 % (11 kappaletta). Suurimpana ryhmänä oli keskivaiheen vaihtoehto 3, joka sai vastaajia 11 kappaletta (39.3 %). Yksi vastaaja valitsi vaihtoehdon 2 eli ei ollut kovinkaan huolissaan ja loput 7 kappaletta valitsi vaihtoehdon 4. Vastauksien jakautumisessa pienoinen yllätys oli se, kuinka moni oli ainakin jonkin verran huolestunut palvelukatkoksista. Palvelukatkokset voivat pahimmassa tapauksessa tarkoittaa sitä, että yrityk-

sellä ei ole pääsyä viimeisimpään versioon tiedostoistaan, jolloin myös PK-yrityksen asiakkaat voivat kärsiä. Yrityksen verkkosivut voivat myös olla pois käytöstä katkoksen ajan, jolloin esimerkiksi tuotteita ei voida myydä. Vastaajat selkeästi tiedostivat palvelukatkoksen mahdolliset haitat.

Kysymys: ”Kuinka suureksi uhkaksi koette mahdollisten toimialan standardien puutteen pilvipalveluille?”

Vastaajia kysymyksellä oli ainoastaan 27 kappaletta. Melkein puolet vastaajista (48.1 %) piti standardien puutetta jonkinlaisena tietoturvauhkana. Noin yksi kolmasosa (29.6 %) oli kuitenkin sitä mieltä, että standardien mahdollinen puute ei aiheuta mitään tai erittäin vähäisen tietoturvauhkan PK-yritykselle. Vastauksissa ei esiintynyt mitään yllättävää, vaan vastausten jakautuminen oli odotetun laista. Standardien puute voi aiheuttaa tietoturvauhan, sillä niiden puuttumisen myötä erilaisia toteutuksia on mahdollisesti useita ja tämä aiheuttaa keskinäistä yhteensopivuusongelmaa sekä mahdollisia tietoturva-aukkoja ja huolimattomuutta suojauksissa. Myös pilvipalveluntarjoajille on ongelmia omien standardien puutteessa.

Kysymys: ”Kuinka suureksi uhkaksi koette kustannusten nousun pilvipalvelun joutuessa hyökkäyksen kohteeksi?”

Yhteensä kuusi vastaajaa (21.4 %) olivat vähän tai eivät ollenkaan huolestunut kyseisestä tietoturvauhkasta. Saman verran oli erittäin paljon huolissaan. Suurin yksittäinen vastausvaihtoehto oli, kun sen valitsi vastaajista 35.7 %. Vaihtoehdot 3, 4 ja 5 kattoivat yhteensä 78,5 % vastaajista, joten PK-yritykset olivat selkeästi huolissaan kustannusten nousemisesta, jos esimerkiksi hyökkääjä ohjaa liikennettä sivuille ja tämän takia kustannukset nousevat. Uhka on uusi ja ilmestynyt pilvipalveluiden yleistymisen myötä, joten on hyvä, että PK-yritykset ovat tietoisia asiasta ja ymmärtävät uhkan vaarallisuuden.

Kysymys: ”Kuinka suureksi uhkaksi koette tietomurron yrityksen käyttämää pilvipalvelua kohtaan?”

Vastaajia oli 28 kappaletta. Jopa 17,9 % (5 kappaletta) vastaajista oli sitä mieltä, että pilvipalvelun joutuminen tietomurron kohteeksi ei ole suuri uhka yritykselle. Täsmälleen yhtä monta oli kuitenkin sitä mieltä, että se on todella suuri riski. Suurin osa vastaajista

oli sitä mieltä, että uhka on jokseenkin suuri (vaihtoehto 3) tai uhka on suuri (vaihtoehto 4). Suurin yksittäinen vaihtoehto oli 4, joka sai 32,1 % kaikista vastauksista. Yllättävää vastauksissa oli se, että melkein yksi viidesosa vastaajista ei pitänyt pilvipalvelun joutumista tietomurron kohteeksi uhkana yritykselle itselleen. PK-yritykset voivat kuitenkin varastoida pilvipalveluihin liiketoiminnalle kriittistä tietoa ja jos pilvipalveluntarjoaja joutuu tietomurron kohteeksi, voi yrityksen tiedot päätyä hyökkääjälle. Yrityksen käyttämät kirjautumistunnukset ovat vähintään vaarassa ja usein käyttäjät käyttävät samoja tunnuksia useissa palveluissa.

Kysymys: ”Kuinka suureksi uhkaksi koette Suomen tai muun valtion vakoilun?”

Kysymyksen vastausmäärä oli 28 kappaletta. 32,1 % vastaajista oli sitä mieltä, että Suomen tai muun valtion vakoilu ei ole uhka yritykselle ollenkaan ja saman verran piti vakoilua keskivakavana uhkana. Pienenä uhkana sitä piti puolestaan 21,4 % vastaajista eli 6 vastaajaa. Tätä isompana uhkana sitä piti ainoastaan 4 vastaajaa eli 14,3 % vastaajista. Vastaajien, jotka eivät pidä valtioiden vakoilua uhkana, suuri osuus voi selittyä sillä, että kaikki vastaajat ovat suomalaisia yrityksiä. Suomessa valtio on suhteellisen korruptiosta vapaa ja ihmiset yleisesti luottavat Suomen valtioon eivätkä usko sen suorittavan vakoilua omia kansalaisia tai yrityksiä kohtaan. Pilvipalveluiden palvelimet, jotka sisältävät PK-yrityksien tietoja, eivät välttämättä sijaitse Suomessa, joten niihin voi olla pääsy muilla valtioilla joko tarkoituksellisti tai salaisesti.

Kysymys: ”Kuinka suureksi uhkaksi koette pilvipalveluiden palvelimien sijainnin muussa maassa kuin Suomessa?”

Vastaajia oli 27 kappaletta. Tämä uhka oli monien vastaajien mielestä vakava, sillä erittäin suurena uhkana sitä piti jopa 22,2 % vastaajista ja isona uhkana sitä piti 33,3 %. Yli puolet vastaajista piti pilvipalvelun palvelimien sijaitsemista ulkomailla isona uhkana. Myös vaihtoehto 3 sai 5 ääntä eli 18,5 %. 7 vastaajaa ei pitänyt palvelimien sijaintia uhkana ollenkaan tai todella vähäisenä. Vastauksissa erottui selkeästi se, että vastaajat pitivät palvelimien sijaintia uhkana, elleivät ne sijaitse Suomessa. Kuten edellisen kysymyksen perusteella voitiin päätellä, PK-yritykset luottavat omaan valtioon, mutta he luottavat myös suomalaisiin yrityksiin. Jos palvelimet eivät sijaitse Suomessa, ei PK-yritys välttä-

mättä voi tietää onko heidän tietonsa turvassa ja millaisia lakeja heidän tietoon sovelletaan. Esimerkiksi jos palvelimet takavarikoidaan rikollisen toiminnan seurauksena, mihin asiakasyrityksellä tai pilvipalveluntarjoajalla ei ole osuutta, miten yritys saa tietonsa takaisin ja koska.

Kysymys: ”Kuinka suureksi uhkaksi koette pilvipalveluiden riippuvuuden internet- yhteydestä?”

Kysymyksen vastaajamäärä oli 27 vastausta. Sekä vaihtoehdot 5 että 4 saivat 22,2 % vastauksista yhteensä 12 vastausta. 33,3 % puolestaan valitsivat vaihtoehdon 3. Ainoastaan eli 2 vastaajaa oli sitä mieltä, että kyseessä ei ole uhka pilvipalveluille. Kuten palvelimien sijainti, myös riippuvuus internetistä koettiin PK-yrityksien keskuudessa isoksi uhaksi. Internet ei välttämättä aina ole toiminnassa ja sen toiminta ei ole aina riippuvainen PK-yrityksestä itsestään, joten on luonnollista, että he ovat huolissaan tästä ja pitävät sitä myös uhkana pilvipalveluille, jotka perustuvat täysin internetiin.

Kysymys: ”Oletteko huolissanne yksityisyyden heikkenemisestä käyttäessä pilvipalveluita”

Kysymykseen vastanneita PK-yrityksiä oli 27 kappaletta. Heistä jopa 12 kappaletta eli melkein puolet piti yksityisyyden heikkenemistä isona uhkana. Kuitenkin ainoastaan yksi vastaaja oli sitä mieltä, että kyseinen uhka on erittäin suuri. 4 vastaajaa (14,8 %) ei puolestaan pitänyt yksityisyyden heikkenemistä uhkana ollenkaan ja 22,2 % piti sitä pienenä uhkana. Yleisesti koetaan pilvipalvelun haittapuolena se, että samoja palvelimia käyttävät useat eri tahot, niin kuluttajat kuin yrityksetkin, sillä tämä mahdollistaa sen, että yrityksen tietoja voi päätyä vääriin käsiin vahingossa. Yrityksen tiedot voivat muutenkin olla helpommin saatavilla, kun se ei sijaitse ainoastaan yrityksen omilla koneilla omissa tiloissa. Tämä näyttäisi olevan myös PK-yrityksien huolenaiheena.

Kysymys: ”Kuinka suureksi uhkaksi koette sen, että yrityksellä ei ole IT- henkilöä jolla on vahva osaaminen pilvipalveluista?”

”Yrityksellä on IT- henkilö, jolla on vahva osaaminen pilvipalveluista” oli tässä kysymyksessä lisävaihtoehtona. Tähän kysymykseen vastasi 28 vastaajaa. Tasan puolet vastaajista oli sitä mieltä, että kyseessä on erittäin suuri tai suuri uhka yritykselle, että heillä

ei ole omaa IT-henkilö, jolla on vahva osaaminen pilvipalveluista. Molemmat vaihtoehdot saivat 7 vastausta. Ainoastaan yksi vastaaja ilmoitti, että yrityksellä on osaava IT-henkilö. Vaihtoehto 3, vastaajat pitivät keskisuurena uhkana, sai 4 ääntä ja vaihtoehto 2 puolestaan 6 ääntä. Yrityksissä selkeästi tiedostetaan, että IT-henkilön puute saattaa aiheuttaa tietoturvauhkan pilvipalveluissa. Yleisesti ottaen pilvipalvelut ovat yksinkertaisia ja helppoja ottaa käyttöön, varsinkin SaaS-mallissa, mutta niihin perehtymätön ja tekniikasta vähän tietävä voi kokea ne todella monimutkaisiksi.

Kysymys: ”Oletteko huolissanne jostain muusta liittyen pilvipalveluihin?”

Viimeisenä kohtana oli mahdollisuus sanallisesti kirjoittaa, jos vastaaja kokee tietoturvauhaksi jonkin, mitä ei ole kysymyksissä mainittu. Ainoa vastaus oli ”Vastuukysymykset mahdollisissa ongelmatilanteissa”. Vastuukysymykset ovat varmasti monen pilvipalvelua harkitsevan PK-yrityksen huolenaiheena ja suurin osa vastuukysymyksistä on määriteltynä pilvipalveluiden palvelutasosopimuksissa.

3.1.2. Pilvipalvelua käyttävien vastaukset

Pilvipalveluita käyttäviä PK-yrityksiä kyselyyn vastasi 62 kappaletta. Näiden yrityksien osalta otanta on siis huomattavasti suurempi kuin niiden yrityksien, joilla pilvipalveluita ei ole käytössä. Pilvipalveluita käyttävien yrityksien kysymyksien määrä on myös suurempi, koska heiltä on pyritty kartoittamaan myös laajemmin pilvipalveluiden tietoturvaa koskevia asenteita ja mielipiteitä. Tämän osion kysymykset eivät olleet pakollisia, joten kaikki kysymykset eivät saaneet 100 % vastausosuutta. Yleisesti tämän osion vastausprosentti oli kuitenkin hyvä, kuten oli aikaisemmassakin osiossa.

Pilvipalveluita käyttävien PK-yrityksien ensimmäinen osio sisälsi kysymyksiä yleisesti pilvipalveluiden käytöstä. Kysymyksiä esitettiin 4 kappaletta ja jokaisen kysymyksen vastausprosentti oli 100 %.

Kysymys: ”Kuinka monta pilvipalvelua yrityksellä on käytössä?”

Vaihtoehtoja kysymyksessä oli 3; 1–3, 4–6 tai Enemmän. Vastaajista 72,6 % eli 45 vastaajaa ilmoitti, että heidän yrityksellään on käytössä 1–3 pilvipalvelua. 21 % puolestaan

oli 4–6 ja ainoastaan 4 vastaajalla käytössään oli enemmän pilvipalveluita. Kysymyksessä ei nähty tarvetta kerätä tarkempaa tietoa pilvipalveluiden määrästä, vaan suuntaa antava tieto oli tarpeeksi. Suuntaa antava tieto riitti tutkimuksessa, koska tutkimuksen tarkoituksena ei ollut kartoittaa pilvipalvelun käyttöä tarkemmin.

Kysymys: ”Minkä mallista pilvipalveluja yrityksessä käytetään?”

Toisessa kysymyksessä kartoitettiin vastaajien pilvipalveluiden palvelumalleja. kysymykseen vaihtoehtoina olivat ”Julkinen pilvipalvelu”, ”Yksityinen pilvipalvelu”, ”Julkinen & yksityinen pilvipalvelu”, ”Hybridi pilvipalvelu” ja ”En tiedä”-vaihtoehto. Kysymyksen yhteydessä oli lyhyt esittelyteksti, jotta vastaajalla olisi ainakin jonkinlainen tieto pilvipalveluiden palvelumalleista. Esittelytekstistä huolimatta 6 vastaajaa, alle 10 %, ilmoitti, että heillä ei ole tietoa pilvipalvelun mallista. Suurin yksittäinen osio, 30,6 % osuudella, oli julkinen & yksityinen. Julkista pilveä käyttivät 18 kappaletta vastaajista. Yksityinen pilvi oli käytössä 19,4 % PK-yrityksistä ja hybridi pilvi pienimmällä osuudella eli 11,3 %. Yllättävän iso osa vastaajista ilmoitti käyttävänsä sekä julkista että yksityistä pilvipalvelua. Ennakko-odotuksien mukaan julkinen pilvipalvelu olisi ollut suurin vaihtoehto kyselyssä.

Kysymys: ”Ovatko käyttämänne pilvipalvelut olleet hyödyksi yritykselle?”

Vastauksissa ei ollut epäselvyyttä, kun jopa 98,4 % vastaajista ilmoitti pilvipalveluiden olleen hyödyllisiä yritykselle. Ainoastaan yksi kyselyyn vastannut ilmoitti, että pilvipalvelut eivät ole olleet hyödyllisiä.

Kysymys: ”Mitkä seuraavista koette pilvipalveluiden eduksi?”

Kysymyksessä esitettiin samat vaihtoehdot kuin aikaisemmin pilvipalveluita käyttämättömien kysymyksessä mitä he kokevat pilvipalveluiden eduksi. Vaihtoehdot olivat siis ”Datan saatavuus usealla laitteella”, ”Oman datan oleminen aina saatavilla”, ”Etätyöskentely”, ”Kilpailuetu”, ”Kustannukset”, ”Tietoturva”, ”Helppous”, ”Mahdollisuus uuteen toimintamalliin”, ”Yrityksen toimintojen tehostuminen”, ”Järjestelmien olemisen aina päivitettynä” sekä ”Muu/Other”. Pilvipalveluita käyttävien vastausosuus kysymyksessä oli 100 %. Selkeästi suurimpana etuna pilvipalveluita käyttävät pitivät datan saatavuutta usealla laitteella. Tämä vaihtoehto sai 87,1 % vastaajan äänen. Kolme seuraavaa

vaihtoehtoa, jotka kaikki olivat lähellä toisiaan osuuksien perusteella, olivat ”Helppous” (74,2 %), ”Etätyöskentely” (72,6 %) ja ” Oman datan oleminen aina saatavilla” (71 %). Näiden jälkeen ”Järjestelmien olemisen aina päivitettynä” (54,8 %) ja ”Yrityksen toimintojen tehostuminen” (53,2 %) olivat seuraavaksi isoimpina pidettyjä etuja. ”Kustannukset” 30,6 % osuudella, ”Tietoturva” 29 %, ”Mahdollisuus uuteen toimintamalliin” 24,2 % ovat myös pidettyjä etuja. ”Kilpailuetu” jäi kyselyssä viimeiseksi saaden 12,9 % vastaajan äänen. ”Muu/Other” vaihtoehto sai kaksi ääntä (3,2 %). Kaikki esitetyt edut saivat vastaajilta ääniä, osan ollessa suositumpia kuin osan. Kustannusten ja tietoturvan osuudet jäivät kuitenkin odotettua pienemmiksi, mutta kun molemmat olivat etuja kuitenkin noin 30 % vastaajista mielestäni, niin selkeästi niitä pidetään pilvipalveluiden etuna.

Seuraava osio sisälsi yhdeksän kysymystä. Melkein kaikki kysymykset saivat 100 % vastausosuuden. Osion aiheena on tietoturva yleisesti ja pilvipalveluiden osalta.

Kysymys: ”Ovatko uutiset lisääntyneistä tietomurroista saaneet teidät huolestuneeksi pilvipalveluiden tietoturvasta?”

Tähän kysymykseen kaikki 62 vastaajaa vastasi. Vaihtoehtoina oli ”Paljon”, ”Jonkin verran” ja ”Ei yhtään”. Kysymys on sama, joka esitettiin aikaisemmin PK-yrityksille, jotka eivät käyttäneet pilvipalvelua, mutta vähän eri tavalla muotoiltuna. Pilvipalvelua käyttävistä vastaajista jopa reilu 70 % vastaajista oli sitä mieltä, että uutiset lisääntyneistä tietomurroista ovat saaneet heidät jonkin verran huolestuneemmaksi pilvipalveluiden tietoturvasta. 6,5 % vastaajaa oli sitä mieltä, että he ovat paljon huolestuneempia sekä 22,6 % eli 14 vastaajaa ei ollut yhtään sen huolestuneempi, vaikka uutisissa on enemmän uutisia tietomurroista. Vastauksen jakauma oli suhteellisen odotetun lainen, kun melkein 80 % oli ainakin jonkin verran huolestuneempi.

Kysymys: ”Oletteko olleet huolissanne tietoturvasta johtuen pilvipalvelusta?”

Vaihtoehdot kysymyksessä oli samat kuin edellisessä kysymyksessä. 20 vastaajaa ei ole ollut huolestunut tietoturvasta pilvipalveluiden takia. 37 vastaajaa puolestaan oli ollut jonkin verran huolissaan ja ainoastaan 5 vastaajaa oli ollut paljon huolissaan. Vastauksien jakauma noudattaa aika hyvin edellisen kysymyksen jakaumaa, mikä oli myös odotettavissa. Kuitenkin vaihtoehdon ”Jonkin verran” vastaajista edellisessä kysymyksessä on

siirtynyt jompaankumpaan ääripäähän, valiten joko ”Ei yhtään” tai ”Paljon”. ”Ei yhtään”-vaihtoehdon osuus kasvoi suhteessa enemmän.

Kysymys: ”Koetteko pilvipalveluiden nostaneen yrityksen tietoturvaa?”

Kysymys sisälsi vaihtoehdot ”Kyllä”, ”Ei” ja ”En osaa sanoa”. Kenties jopa erittäin yllättävä oli, että yli puolet oli sitä mieltä, että pilvipalvelut eivät ole nostaneet yrityksen tietoturvaa. Kun vielä 24,2 % ilmoitti, että he eivät osaa sanoa niin ainoastaan 21 % oli sitä mieltä, että pilvipalvelut ovat nostaneet yrityksen tietoturvaa. Vastausjakaumaa voi toki selittää moni asia, joista yksi voi olla se, että yrityksen tietoturva on ollut jo aiemmin hyvällä tasolla, mutta myös se, että asiasta ei olla tietoisia. Kysymykseen kuitenkin lisättiin ”En osaa sanoa”-vaihtoehto sen takia, että ”Kyllä”- ja ”Ei”-vaihtoehdot saisivat mahdollisimman totuudenmukaisen jakauman. Tästä syystä vastauksenjakaumaa voidaan kuitenkin pitää täysin paikkansa pitävänä.

Kysymys: ”Onko pilvipalvelun käytön turvallisuutta yritetty lisätä seuraavilla asioilla?”

Tämän kysymyksen tarkoituksena oli kartoittaa, onko yrityksissä otettu huomioon pilvipalveluiden tietoturvaa ja tehty asialle jotain, jotta se olisi mahdollisimman korkealla tasolla. Vastausvaihtoehtoina olivat ”Työntekijöiden koulutuksella”, Prosesseilla”, Teknologialla”, Ei mitenkään” ja ”Muu&Other”. Yli puolessa yrityksistä ei pilvipalveluiden tietoturvaa ollut koitettu nostaa mitenkään. Kuitenkin 29 % vastaajista ilmoitti, että tietoturvaa oli teknologian avulla koitettu parantaa ja yksi neljäsosa ilmoitti, että työntekijöitä on koulutettu. Prosesseilla tietoturvan tasoa oli koitettu parantaa 11,3 % vastanneista PK-yrityksistä. Yhdessä vastaajayrityksessä oli tietoturvan tasoa koitettu parantaa muulla tavoin. ”Ei mitenkään”-vaihtoehdon ylivoimainen suosio ei yllättänyt, sillä vastaajina olivat PK-yritykset, joiden resurssit ja tietämys ovat helposti vähäisiä. Esimerkiksi työntekijän koulutus voi kuitenkin vähentää tietämättömyydestä tai huolimattomuudesta tapahtuvia tietovuotoja, joten jos yrityksessä on pilvipalveluita käytössä, niiden käyttöä tulisi myös opastaa.

Kysymys: ”Onko yrityksen tietoturvapolitiikassa otettu huomioon pilvipalveluiden käyttö?”

Vaihtoehtoina olivat ”Kyllä”, ”Ei” ja ”Yrityksellä ei ole selkeää tietoturvapolitiikkaa”. Viimeinen vaihtoehto lisättiin, koska vastaajina oli PK-yrityksiä, joten selkeää tietoturvapolitiikka ei uskottu löytyvän kaikista vastaajayrityksistä. Tämä vaihtoehto oli myös suosituin, kun 43,5 % vastaajista ilmoitti, että yrityksellä ei ole selkeää tietoturvapolitiikkaa. Samalla kuitenkin 41,9 % vastaajista ilmoitti, että yrityksen tietoturvapolitiikassa on huomioitu pilvipalveluiden käyttö. Ainoastaan 14,5 % PK-yrityksistä ei ollut pilvipalveluiden käyttöä huomioitu ainakaan vielä. Pilvipalveluiden tietoturvapolitiikan huomioonottaminen suhteellisen suuressa määrässä PK-yrityksiä oli positiivinen huomio, sillä vastausten perusteella PK-yritykset ovat ottaneet tietoturvan tosissaan ja ymmärtävät sen tärkeyden.

Kysymys: ”Kenen vastuulla koette tietoturvan olevan pilvipalveluissa?”

Vaihtoehtoina olivat ”Palvelua käyttävällä yrityksellä”, ”Pilvipalveluntarjoajalla” sekä ”Molemmilla”. Kysymyksen tarkoituksena oli ainoastaan selvittää, luottavatko PK-yritykset siihen, että tietoturvan hoitaa pilvipalveluntarjoaja yksinään tai olettavatko PK-yritykset, että tietoturva on pilvipalveluidenkin osalta heidän omalla vastuullaan. Vastauksien jakautuminen oli kuitenkin selkeä, kun 45 vastaajaa oli sitä mieltä, että vastuu tietoturvasta on pilvipalveluntarjoajan ja PK-yrityksen molempien vastuulla. Kuitenkin reilu yksi viidesosa oli sitä mieltä, että pilvipalveluiden tietoturvan vastuu on ainoastaan pilvipalveluntarjoajan ja 6,5 % oli sitä mieltä että vastuu on täysin PK-yrityksellä itsellään. Tietoturvasta ovat vastuussa molemmat, sillä kumman puolen tahansa laiminlyönti tietoturvassa voi aiheuttaa ongelmia toiselle osapuolelle. Pilvipalveluntarjoajan vastuulla on huolehtia infrastruktuurin tietoturvasta ja yleisesti pilvipalvelun tietoturvasta muun muassa tarjoamalla PK-yritykselle tietoturvaa parantavia ratkaisuja, mutta PK-yrityksen laiminlyödessä omaa vastuutaan, esimerkiksi käyttäjienhallinnassa, saattaa se vaarantaa koko pilvipalvelun.

Kysymys: ”Varmistettiinko yrityksessä pilvipalveluntarjoajan tietoturvan taso ennen palvelun käyttöönottoa?”

Tähän kysymykseen vastaajia oli 61. Vaihtoehtoina olivat ”Kyllä” ja ”Ei”. Vähän yli puolet vastaajista oli selvittänyt pilvipalveluntarjoajan tietoturvan tason ennen kuin siirtyivät palvelun käyttäjäksi. 47,5 % ei ollut selvittänyt. Vähän huolestuttavasti 29 PK-yritystä ei ole millään lailla selvittänyt pilvipalveluntarjoajan tietoturvan tasoa etukäteen, joten he eivät voi olla varmoja siitä, että heidän käyttämänsä pilvipalvelu on turvallinen. Isojen pilvipalveluntarjoajien ollessa kyseessä ongelma ei ole yleensä iso, mutta varsinkin pienempien kohdalla olisi hyvä tietoturvan taso selvittää, vaikka se saattaa olla hankalampaa.

Kysymys: ”Onko yrityksenne joutunut hyökkäyksen kohteeksi viimeisen vuoden aikana?”

Kysymyksessä oli vaihtoehtoina ”Kyllä”, ”Ei” ja ”En tiedä”. Vastaajia tähän kysymykseen oli 61 vastaajaa 62 vastaajasta. Ainoastaan kaksi kyselyyn vastannutta PK-yritystä ilmoitti, että he ovat joutuneet hyökkäyksen kohteeksi viimeisen vuoden aikana. 11 vastajaa puolestaan ilmoitti, että heillä ei ole asiasta tietoa ja 48 yritystä piti varmana, että he eivät ole joutuneet hyökkäyksen kohteeksi. Hyvänä asiana on se, että ainoastaan 2 yritystä oli joutunut hyökkäyksen kohteeksi. Hyökkäys ei kuitenkaan aina tule ilmi, joten todellisuudessa määrä voi olla myös isompi. ”Ei”-vaihtoehdon suuri osuus on ehkä pienoinen yllätys, sillä ennakkoon odotettiin suurempaa osuutta vaihtoehdolle ”En tiedä”, juurikin siitä syystä, että hyökkäys ei aina näy hyökkäyksen kohteelle itselleen.

Kysymys: ”Onko yrityksenne pilvipalveluntarjoaja joutunut hyökkäyksen kohteeksi viimeisen vuoden aikana?”

Tämä kysymys oli jatkoa edelliselle. Tähän kysymykseen olivat kaikki PK-yritykset vastanneet. Vastausten jakautuminen oli myös aivan odotettua ja ”En tiedä”-vaihtoehto sai selkeästi suurimman määrän vastauksista, 71 % vastaajaa ei ollut asiasta tietoisia. Kolmen yrityksen pilvipalveluntarjoaja oli kuitenkin joutunut hyökkäyksen kohteeksi ja 15 vastaajaa piti varmana, että heidän pilvipalveluntarjoaja ei ole joutunut. Kuten edellisessä kysymyksessä niin myös tässä on otettava huomioon se, että hyökkäys ei aina tule ilmi. Pilvipalveluntarjoajilla on kuitenkin huomattavasti paremmat valmiudet huomata hyökkäys kuin PK-yrityksellä, joten sen tuleminen ilmi on todennäköisempää. Varsinkin isommat pilvipalveluntarjoajat myös ilmoittavat tästä asiakkailleen, sillä luottamus on tärkeää

heidän toiminnalleen ja tätä voidaan myös vaatia heiltä lain tai säännöksin. Pilvipalveluntarjoajan joutuminen hyökkäyksen kohteeksi ei kuitenkaan tarkoita, että asiakkaana oleva PK-yritys itsessään olisi joutunut. Moni PK-yritys saattaa olla myös epätietoinen siitä, ilmoittaisiko pilvipalveluntarjoaja heille hyökkäyksestä ja tämän takia ovat valinneet ”En tiedä”-vaihtoehdon ”Ei”-vaihtoehdon sijasta.

Osio: Tietoturvauhat

Seuraavat kysymykset koskevat kuinka suureksi uhaksi pilvipalveluita käyttävät PK-yritykset kokevat tietoturvauhat. Tässä osiossa vastaajia oli 62 kappaletta, joista kaikki käyttävät pilvipalveluita. Jokaisen kysymyksen vastausprosentti ei kuitenkaan ole 100 %. Kysymykset sisältävät viisi eri vastausvaihtoehtoa, luvut 1–5. Luku 1 tarkoittaa kysymyksissä ”En ollenkaan” ja luku 5 ”Erittäin suureksi”.

Kysymys: ”Kuinka suureksi uhkaksi koette pilvipalvelun palvelukatkoksen?”

Tämän kysymyksen vastausprosentti oli 100 %. Vastaajista alle 10 % koki, että mahdollinen palvelukatkos pilvipalvelussa ei ole uhka ollenkaan, kun taas vajaa 15 % puolestaan koki, että palvelukatkos on erittäin suuri uhka. Noin 20 % koki palvelukatkoksen isoksi uhkaksi, kun taas yleisesti uhkaksi sen koki selkeästi isoin vastaajajoukko eli vähän reilu 40 %. 16,1 % koki palvelukatkoksen pieneksi uhaksi. Melkein 10 % osuus yrityksissä, jotka eivät koe palvelukatkosta ollenkaan uhaksi on iso osuus, kun ottaa huomioon, että pilvipalvelu ei toimi ollenkaan palvelukatkoksen aikana. Tämä tarkoittaa sitä, että yrityksellä ei välttämättä ole ollenkaan pääsyä tärkeisiin tietoihinsa. PK-yritykset, jotka eivät koe tätä uhaksi, eivät välttämättä säilö mitään tärkeää ja liiketoiminnalle kriittistä asiaa pilvipalvelussa tai eivät ainakaan koe säilyttävänsä tämän kaltaista materiaalia pilvipalvelussa.

Kysymys: ”Kuinka suureksi uhkaksi koette mahdollisten toimialan standardien puutteen pilvipalveluille?”

Tämän kysymyksen vastaajien määrä oli 61 vastaajaa. 2 vastaajaa pitivät toimialan standardien puutetta erittäin suurena uhkana ja 11 vastaajaa isona uhkana. 19 vastaajaa piti standardien puutetta keskisuurena uhkana ja pienenä uhkana 17 vastaajaa. 12 vastaajaa ei puolestaan pitänyt standardien puutetta ollenkaan uhkana. Standardien puute voi olla vielä yleistä joillain toimialoilla, johtuen siitä, että pilvipalvelut ovat suhteellisen uusi asia. Standardien kehittäminen kuitenkin tuo suojaa yritykselle, kun he tietävät kuinka toimia pilvipalvelun kanssa omalla toimialallaan ja mitä heidän tulee ottaa huomioon. Ainoastaan yksi viidesosa kuitenkin pitää tätä isona tietoturvauhkana.

Kysymys: ”Kuinka suureksi uhkaksi koette kustannusten nousun pilvipalvelun joutuessa hyökkäyksen kohteeksi?”

Kysymykseen ääripäät saivat selkeästi vähiten ääniä, kun kumpikaan ääripää ei saanut yli 10 % kannatusta. Pienenä uhkana sitä piti 30,6 % ja isona uhkana 29 %. Noin yksi neljäsosa oli sitä mieltä, että kyseessä on keskisuuri tietoturvauhka. Kustannusten noususta esimerkiksi palvelunestohyökkäyksen johdosta ei välttämättä tiedetä vielä hirveän paljon yrityksissä, sillä siitä ei ole paljoa puhuttu mediassa. Varsinkin tästä syystä PK-yritykset eivät välttämättä pidä sitä kuin pienenä uhkana. Tähän on kuitenkin enemmän aloitettu kiinnittämään huomiota, sillä pilvipalveluiden periaate on toimia niin, että liikenteen noustessa, otetaan enemmän laskentatehoa käyttöön, jotta palvelu kestää kuormituksen. Tämä laskentateho kuitenkin maksaa asiakasyritykselle.

Kysymys: ”Kuinka suureksi uhkaksi koette pilvipalvelun käytön monimutkaisuuden”.

Vastaajia 61 kappaletta. Pilvipalvelun käytön monimutkaisuuden koki erittäin suureksi uhaksi ainoastaan alle 5 % vastaajista ja isoksi uhaksi reilu 8 %. Noin 20 % piti sitä keskimääräisenä uhkana. Yli 60 % vastaajista oli sitä mieltä, että pilvipalvelun käytön monimutkaisuus ei ole ongelma ollenkaan tai on ainoastaan pieni uhka. Pilvipalvelun monimutkaisuus saattaa altistaa yrityksen arkaluontoisen materiaalin alttiiksi tietovuodolle, kun työntekijä vahingossa tai tietämättömyyttään asettaa sen julkisesti nähtäväksi. Kuitenkaan melkein yksi neljäsosa vastaajista ei koe sitä ollenkaan tietoturvauhkana. 74,2 % kuitenkin piti pilvipalvelun etuna helppoutta ja 62,3 % pitää monimutkaisuutta pienenä tai jonkin laisena tietoturvauhkana.

Kysymys: ”Kuinka suureksi uhkaksi koette tietomurron yrityksen käyttämää pilvipalvelua kohtaan?”

Kysymykseen 62 vastaajasta 2 vastaajaa ei pidä tietomurtoa yrityksen käyttämää pilvipalvelua kohtaan ollenkaan tietomurtona. Isoin yksittäinen vaihtoehdon keräämä vastaustenmäärä oli 22 vastaajaa ja se oli vaihtoehto 2 eli uhka koetaan pienenä. Ainoastaan vajaa 10 % piti uhkaa erittäin suurena ja noin yksi neljäsosa isona uhkana. Vastaavasti noin yksi neljäsosa piti uhkaa keskisuurena uhkana. Vastaajien, jotka eivät pitäneet tietomurtoa pilvipalveluntarjoajaa kohtaan uhkana tai pienenä uhkana, oli yllättävän suuri, yhteensä 38,7 % vastaajista. Vaikka PK-yritys itse ei olisi tietomurron kohteena, niin pilvipalveluntarjoaja säilöö yrityksestä tietoja, jotka voivat olla väärissä käsissä todella ikävä asia asiakkaana olevalle PK-yritykselle. Joko PK-yritykset eivät usko, että heidän tietojaan voisi tietomurron yhteydessä joutua rikollisille tai eivät usko, että niillä tiedoilla voisi tehdä mitään. Seuraukset voivat olla kuitenkin suuret PK-yritykselle, sillä joukossa saattaa olla esimerkiksi heidän omien asiakkaiden tietoja.

Kysymys: ”Kuinka suureksi uhkaksi koette Suomen tai muun valtion vakoilun?”

Melkein puolet vastaajista oli sitä mieltä, että Suomen tai muun valtion vakoilu oli ainoastaan pieni tietoturvauhka. 10 yritystä oli sitä mieltä, että se ei ole uhka ollenkaan. Suurena ja erittäin suurena uhkana valtion tason vakoilua piti yhteensä 13 % PK-yrityksistä. Kuten yrityksissä, jotka eivät käytä pilvipalveluita, myös suurimman osan pilvipalveluiden käyttäjien mielestä valtion tason vakoilu ei ole uhka ollenkaan tai iso uhka. Myös tässä saattaa syynä olla se, että vastaajat ovat Suomesta, missä valtion tason korruptio tai omien kansalaisten ja yrityksien vakoileminen ei ole tämän hetkisten tietojen valossa iso ongelma.

Kysymys: ”Kuinka suureksi uhkaksi koette pilvipalveluiden palvelimien sijainnin muussa maassa kuin Suomessa?”

Tällä kysymyksellä selvitettiin pilvipalveluiden palvelimien sijainnin vaikutusta PK-yrityksiin. Vastaukset olivat suhteellisen hajautuneita, mutta suurin yksittäinen vastausmäärä, 27,9 %, kerääntyi sille, että yritykset pitävät palvelimien sijaintia isona tietoturvauhkana. Erittäin suurena tietoturvauhkana sitä piti reilu 10 % vastaajista ja yhteensä 41 % oli sitä mieltä, että kyseessä on iso tai erittäin suuri uhka. reilu 15 % vastaajista oli

kuitenkin sitä mieltä, että kyseessä ei ole uhka yritykselle ollenkaan ja noin 20 % piti sitä vain pienenä uhkana. PK-yritykset ovat kuitenkin selkeästi huolestuneita siitä, missä pilvipalveluiden palvelimet sijaitsevat ja että he eivät välttämättä ole täysin varmoja siitä, mitä lakeja näihin palvelimiin ja samalla PK-yrityksen omiin tietoihin käytetään. Yrityksien, jotka eivät pitäneet tätä ollenkaan uhkana, osuus oli kuitenkin yllättävän suuri, sillä nykypäivänä voisi olettaa yrityksien olevan enemmän huolestuneita heidän tietonsa sijainnista.

Kysymys: ”Kuinka suureksi uhkaksi koette pilvipalveluiden riippuvuuden internet-yhteydestä?”

Myös tämä kysymys jakoi vastaajien mielipiteet. Ainoastaan 2 vastaajaa olivat sitä mieltä, että pilvipalveluiden riippuvuus internet-yhteydestä ei ole uhka, mutta loput neljä vaihtoehtoa jakoivat vastaajat keskenään suhteellisen tasaisesti. 22,6 % oli sitä mieltä, että kyseessä on pieni uhka, 24,2 % puolestaan ajattelin kyseessä olevan suurempi uhka. Isona uhkana sitä piti 27,4 % ja erittäin suurena 22,6 %. PK-yrityksille on siis selkeästi huolenaiheena se, että pilvipalvelut ovat riippuvaisia internet-yhteydestä.

Kysymys: ”Oletteko huolissanne yksityisyyden heikkenemisestä käyttäessä pilvipalveluita?”

3 vastaajaa ei ollut huolissaan siitä, että yrityksen yksityisyys heikkenisi käytettäessä pilvipalveluita. 25,8 % oli sitä mieltä, että yksityisyyden heikkeneminen on pieni riski ja puolestaan 32,3 % oli sitä mieltä, että kyseessä on keskisuuri tietoturvauhka. Noin 25 % piti sitä suurena uhkana ja reilu 10 % erittäin suurena. Vastaajien mielipiteet asettuivat suhteellisen keskelle asteikkoa ja molempien ääripäiden osuus oli pientä, mutta yrityksille on selkeästi huolenaiheena yksityisyyden heikkeneminen käytettäessä pilvipalveluita.

Kuten kysymyksissä, jotka olivat suunnattu yrityksille, joissa ei käytetä pilvipalveluita, myös pilvipalveluita käyttävien viimeinen kysymys oli ”Kuinka suureksi uhkaksi koette sen, että yrityksellä ei ole IT- henkilöä jolla on vahva osaaminen pilvipalveluista”. Myös tämä kysymys poikkesi muista kysymyksistä sillä, että normaalien vaihtoehtojen lisäksi se sisälsi vaihtoehdon ”Yrityksellä on IT- henkilö, jolla on vahva osaaminen pilvipalveluista”. Tämä lisävaihtoehto sai pilvipalvelua käyttäviltä yrityksiltä melkein 25 % vastausosuuden eli 15 yritystä ilmoitti, että heillä on käytössään IT-henkilö, jolla on vahva

osaaminen pilvipalveluista. Alle 10 % oli sitä mieltä, että tämä ei ole yritykselle uhka ollenkaan ja ainoastaan 3,2 % piti sitä erittäin suurena uhkana. Noin 20 % piti osaavan IT-henkilön puuttumista isona uhkana ja pienenä uhkana reilu 15 %. 27,4 % eli suurin yksittäinen osuus oli keskisuurella uhkalla. Pilvipalveluita käyttävillä yrityksillä yllättävän suurella määrällä on organisaatiossa IT-henkilö, jolla on tietoa ja osaamista pilvipalveluista. Muuten vastausten jakautuminen oli odotetun laista ja PK-yritykset pitävät suhteellisen vakavana uhkana osaavan IT-henkilön puutteen.

Kysymys: ”Oletteko huolissanne jostain muusta liittyen pilvipalveluihin?”

Viimeisessä kohdassa vastaajat saivat lisätä sanallisesti, jos ovat huolissaan jostain muusta uhkasta pilvipalveluita kohtaan, mitä kyselyssä ei mainittu. Tähän kohtaan tuli ainoastaan yksi sanallinen vastaus, jossa ilmoitettiin salasanojen vaihtamisen muistaminen. Salasanojen vaihtaminen säännöllisten ajanjaksojen päätteeksi on joissain palveluissa ohjelmoitu suoraan ohjelmaan tai palveluun ja ohjelma tai palvelu pakottaa käyttäjän vaihtamaan salasanansa päästäkseen jatkamaan käyttöä. Jos käyttäjällä on vahva salasana käytössään, ei sen vaihtamisesta kuitenkaan ole merkittävää hyötyä (Rubenking 2010; Cormac 2009)

3.1.3. Vastausten vertailu keskenään

Tässä luvussa vertaillaan pilvipalveluita käyttävien PK-yrityksien ja pilvipalveluita käyttämättömien PK-yrityksien antamia vastauksia. PK-yritysten mielipiteet ja asenteet voivat vaihdella sen mukaan kuinka paljon heillä on kokemusta pilvipalveluista ja ennakkotietoa. Vastauksien vertailu selkeyttää esimerkiksi sitä, onko PK-yrityksillä, joissa ei ole käytössä pilvipalveluita, jotain tiettyjä ennakkoluuloja pilvipalveluita kohtaan, joita toisen ryhmän PK-yrityksillä ei ole. PK-yrityksien suhtautuminen pilvipalveluita koskeviin tietoturvauhkiin voi myös olla yleisesti erilaista riippuen siitä, onko pilvipalvelu käytössä vai ei. Osiossa verrataan prosentuaalisia osuuksia, koska vastausryhmät olivat erikokoisia.

Etujen vertailua

Pilvipalveluiden etuja PK-yrityksiltä kysyttäessä vaihtoehdot olivat molemmilla ryhmillä samat. Vaihtoehdot olivat ”Datan saatavuus usealla laitteella”, ”Oman datan oleminen aina saatavilla”, ”Etätyöskentely”, ”Kilpailuetu”, ”Kustannukset”, ”Tietoturva”, ”Helppous”, ”Mahdollisuus uuteen toimintamalliin”, ”Yrityksen toimintojen tehostuminen”, ”Järjestelmien olemisen aina päivitettynä” sekä ”Muu/Other”. Kolme eniten vastauksia saaneet vaihtoehdot olivat molemmissa ryhmissä melkein samat. ”Datan saatavuus usealla laitteella” sai pilvipalveluita käyttävistä yrityksistä 87.1 % äänistä ja PK-yrityksistä, joissa pilvipalveluita ei käytetä, 64,3 %. Datan saatavuus usealla laitteella oli pilvipalveluita käyttävien joukossa eniten vastauksia saanut vaihtoehto. ”Etätyöskentely” oli puolestaan saanut eniten vastauksia pilvipalveluita käyttämättömien yritysten joukosta, kun 71,4 % piti sitä etuna. Pilvipalveluita käyttävien puolella etätyö nähtiin etuna 72,6 % yrityksen toimesta ja näin ollen se jäi kolmannelle sijalle. Oman datan oleminen aina saatavilla oli pilvipalveluita käyttävien yritysten joukossa reilun 70 % mielestä etu ja reilun 60 % toisessa ryhmässä. Pilvipalveluiden helppous oli toiseksi eniten ääniä saanut vaihtoehto pilvipalveluita käyttävien keskuudessa, kun se sai melkein 75 %, mutta pilvipalveluita käyttämättömien yritysten keskuudessa se keräsi ääniä ainoastaan reilu 40 %. Ero on suhteellisen suuri ja todennäköisesti selittäytyy pilvipalveluita käyttämättömien yritysten ennakkoluuloilla ja koska teknistä osaamista ei välttämättä PK-yrityksestä löydy niin moni termi voi kuulostamaan hankalalta ja saa pilvipalvelun käytön vaikuttamaan hankalalta.

Pilvipalveluita käyttävien PK-yritysten keskuudessa yli puolet oli sitä mieltä, että pilvipalvelut tehostavat PK-yritysten toimintoja ja vaihtoehto on siis etu. Kuitenkin pilvipalveluita käyttämättömien keskuudessa ainoastaan noin 10 % oli samaa mieltä. Syitä voi olla useita, joko yrityksessä ei vain uskota, että pilvipalveluista olisi mitään hyötyä ja näin ollen se ei myöskään tehostaisi toimintoja tai sitten ei vain tiedetä mitä pilvipalvelut voivat tehdä ja miten olemassa olevia toimintoja pilvipalveluun siirtämisellä voitaisiin oikeasti saada. Tämä voisi muuttua, jos PK-yrityksille kerrottaisiin tarkasti pilvipalveluiden tuomia hyötyjä ja nimenomaan miten kyseinen yritys voisi hyötyä, ei pelkästään yleisellä tasolla. Isoja eroja löytyi myös vaihtoehdoissa ”Tietoturva”, ”Kustannukset” ja ”Kilpailuetu”. Nämä kaikki edut arvioitiin pilvipalveluita käyttämättömien joukossa vain harvan

toimesta eduksi. Kilpailuetuun ei uskonut yksikään, kun taas kustannuksien pienenemiseen uskoi alle 10 % ja tietoturvaan saman verran. Pilvipalveluita käyttävien keskuudessa kilpailuetuun uskoi puolestaan reilu 10 % ja kustannuksiin sekä tietoturvaan noin kolmasosa ryhmän vastaajista. Näissä kolmessa, suhteellisen isossa asiassa, huomattavasti positiivisempia ovat ne PK-yritykset, joilla on käytössään pilvipalvelut. Tähän todennäköisesti vaikuttaa heidän henkilökohtainen kokemus asiasta, kun yritykset ovat käytännössä saaneet hyötyä näistä. Pilvipalveluita käyttämättömien keskuudessa nämä edut saattavat vaikuttaa enemmän mainospuheelta, joiden todellinen vaikutus on todella pieni.

”Mahdollisuus uuteen toimintamalliin” sai suurin piirtein saman verran ääniä molemmissa ryhmissä. Pilvipalveluita käyttävistä tämän kokivat eduksi 24,2 % ja pilvipalveluita käyttämättömien ryhmässä 28,6 % koki sen eduksi. Tässä vaihtoehdossa PK-yritykset, jotka eivät käytä pilvipalveluita, olivat positiivisempia ja kokivat tämän useammin eduksi kuin pilvipalveluita käyttävät. Molemmat ryhmät myös kokivat tämän suhteellisen hyvin eduksi ja uskovat pilvipalveluiden tuovan muutosta PK-yritysten nykyiseen toimintamalliin. Positiivisemman pilvipalveluita käyttämättömät yritykset suhtautuivat myös vaihtoehtoon ”Järjestelmien olemisen aina päivitettynä”. 57,1 % piti tätä etuna kun puolestaan pilvipalveluita käyttävien keskuudessa päivitettynä olemista piti etuna 54,8 %. Ero ei ole iso molemmissa ryhmissä pidettiin hyvin etuna ohjelmistojen olemista päivitettynä ja sen tapahtumista keskitetysti pilvipalveluntarjoajan toimesta. PK-yrityksen ei tarvitse siis itse päivittää ohjelmistojaan, jotka ovat pilvipalveluissa. ”Muu/Other” vaihtoehdon valitsi molemmissa ryhmissä reilusti alle 10 % vastaajista.

Kokonaisuudessa pilvipalveluita käyttävät olivat positiivisempia mitä tulee pilvipalveluiden etuihin. Suurimmassa osassa vaihtoehdoista pilvipalveluita käyttävät kokivat vaihtoehdot suuremmalla osuudella eduksi, kun taas pilvipalveluita käyttämättömien keskuudessa ei oltu aivan yhtä positiivisia. Monessa vaihtoehdossa kuitenkin prosentit olivat suhteellisen lähellä toisiaan, joten myös pilvipalveluita käyttämättömät olivat perillä mahdollisista eduista mitä pilvipalvelut tuovat. Suurimmat erot olivat kuitenkin yllättävissä kohdissa, kun esimerkiksi tietoturvan olevan etu uskoi pilvipalveluita käyttämättömien joukossa alle 10 %. Myös iso ero helppouden kohdalla oli erikoinen ja pilvipalveluita käyttämättömien keskuudessa oltiin yllättävän negatiivisia näiden kahden vaihtoeh-

don suhteen. Myös se, että yksikään pilvipalvelua käyttämätön PK-yritys ei uskonut pilvipalveluiden tuovan minkäänlaista kilpailuetua oli erikoista. Syitä näihin eroihin on varmasti monia, pilvipalveluita käyttävät saattavat yliarvioida mahdollisia etuja vaikka todellisuudessa etu olisi todella merkityksetön ja käyttämättömien keskuudessa voi olla kyse osaltaan tietämättömyydestä, kun ei ole ollut tarvetta asiaan perehtyä tai ei ole osaamista. Kustannusten ja tietoturvan osalta odotettiin kuitenkin suurempaa osuutta pilvipalvelua käyttävien keskuudessa, vaikka noin 30 % onkin suhteellisen korkea osuus. Nämä vaihtoehdot olivat kuitenkin viimeisinä, jos vaihtoehtojen osuuksia verrataan keskenään.

Tietoturvauhkien vertailua

Pilvipalveluiden palvelukatkokset molemmat ryhmät kokivat suurin piirtein samansuuruiseksi tietoturvauhaksi. Noin 10 % molemmista ryhmistä oli sitä mieltä, että palvelukatkos ei ole uhka ollenkaan, mutta 33,9 % pilvipalvelun käyttäjistä ja 46,4 % pilvipalveluita käyttämättömistä Pk-yrityksistä oli sitä mieltä, että kyseessä on erittäin suuri tai suuri tietoturvauhka. Pilvipalveluita käyttävät yritykset olivat vastauksissaan yllättävän välinpitämättömiä palvelukatkosta kohtaan, kun heidän vastausjakaumaa verrataan toiseen ryhmään. Standardien puutteeseen toimialalla molemmat ryhmät vastasivat myös suhteellisen samalla tavalla. Suurin ero vastauksien jakautumisessa tulee kuitenkin siinä, että pilvipalveluita käyttävät yritykset pitivät standardien puutetta huomattavasti vähäpätöisempänä tietoturvauhkana kuin PK-yritykset, jotka eivät käytä pilvipalveluita. Melkein puolet pilvipalvelua käyttävistä oli sitä mieltä, että standardien puute ei ole uhka tai se on pieni uhka. Vastaavasti alle 30 % pilvipalvelua käyttämättömien ryhmästä oli samaa mieltä. Ero on siis todella iso, mutta suurin osa yrityksistä, jotka eivät käytä pilvipalvelua, olivat sitä mieltä, että kyseessä on keskinkertainen uhka ja suurena tai erittäin suurena uhkana standardien puutetta pitivät melkein täysin samansuuruiset ryhmät.

Uhka: Kustannusten nousu hyökkäyksen johdosta

Kustannuksen nouseminen pilvipalvelun joutuessa hyökkäyksen kohteeksi kysymyksen vastaukset jatkavat osittain samaa kaavaa, kun pilvipalvelua käyttävät PK-yritykset arvioivat uhan pienemmäksi kuin vastaavasti pilvipalvelua käyttämättömät PK-yritykset. Noin 40 % pilvipalvelua käyttävistä arvioi, että kustannusten nousu hyökkäyksen takia ei ole ollenkaan riski tai ainoastaan pieni kun taas pilvipalvelua käyttämättömistä reilu 50 % arvioi, että kyseessä on erittäin suuri tai suuri uhka. Pilvipalvelua käyttävistä uhkaa pitivät erittäin suuren tai suurena 33,8 % ja pilvipalvelu käyttämättömistä pienenä tai ei uhkana ollenkaan 21,4 %.

Uhka: Tietomurto

Pilvipalveluntarjoajan joutuminen tietomurron kohteeksi kysymyksessä suurin eroavaisuus oli molemmissa ääripäissä. Pilvipalvelua käyttävät yrityksistä ainoastaan 3,2 % oli sitä mieltä, että kyseessä ei ole PK-yritykselle itselleen uhka ja vastaavasti pilvipalvelua käyttämättömissä yrityksissä jopa 17,9 % oli sitä mieltä, että kyseessä ei ole uhka. Erittäin suurena tietoturvauhkana pitävien määrässä oli myös eroa, kun pilvipalvelua käyttävien keskuudessa 9,7 % piti uhkaa erittäin suurena ja 17,9 % oli osuus pilvipalvelua käyttämättömien kesken. Suurena ja keskisuurena uhkana pitävien osuus oli samaa koko luokkaa molemmissa ryhmissä, mutta pienenä tietoturvauhkana pitävien osuus oli selkeästi suurempi pilvipalvelua käyttävien keskuudessa kuin pilvipalvelua käyttämättömien. Pilvipalveluja käyttämättömien keskuudessa mielipiteet olivat uhasta huomattavasti jyrkemmät kuin pilvipalvelua käyttävien.

Uhka: Suomen tai muun valtion vakoilu

Suomen tai muun valtion vakoilu huolestutti PK-yrityksiä molemmissa ryhmissä suhteellisen samalla lailla mitä tulee PK-yrityksiin, jotka pitivät uhkaa keskisuurena, suurena tai erittäin suurena. Pilvipalveluita käyttämättömien keskuudessa näiden kolmen vaihtoehdon osuus oli 46,4 % ja pilvipalveluja käyttävien 34,2 %. Isoin ero osuuksissa syntyi kuitenkin niiden välille, jotka pitivät valtioiden vakoilua uhkana ja niiden jotka pitivät sitä vain pienenä uhkana. Pilvipalvelua käyttävien keskuudessa pienenä uhkana vakoilua pitivät melkein puolet ja ei ollenkaan uhkana vain reilu 15 %. Vastaavat osuudet pilvipalvelua käyttämättömien keskuudessa pienenä uhkana vakoilua pitivät noin 20 % ja ei ollenkaan uhkana reilu 30 %.

Uhka: Pilvipalveluiden palvelimien sijainti muualla kuin Suomessa

Pilvipalveluiden palvelimien sijainnin muissa maissa kuin Suomessa osuuksien jakautuminen molemmissa ryhmissä oli hyvin samankaltaista. Erot osuuksien välillä olivat todella pieniä, suurimman eron ollessa 9,1 % ja ero oli erittäin suurena uhkana pitävissä, kun pilvipalveluja käyttämättömien keskuudessa uhka arvioitiin vakavammaksi. Sama tilanne on myös seuraavan kysymyksen osuuksien jakaumissa eli ” Kuinka suureksi uhkaksi koette pilvipalveluiden riippuvuuden internet-yhteydestä”. Eroja osuuksissa esiintyi, mutta suurin yksittäinen ero oli 9,1 % ja se oli keskisuurena uhkana pitävien osuudessa. Muuten osuudet olivat hyvin lähellä toisiaan ja mielipiteet PK-yrityksien molemmilla ryhmillä hyvin samankaltaiset.

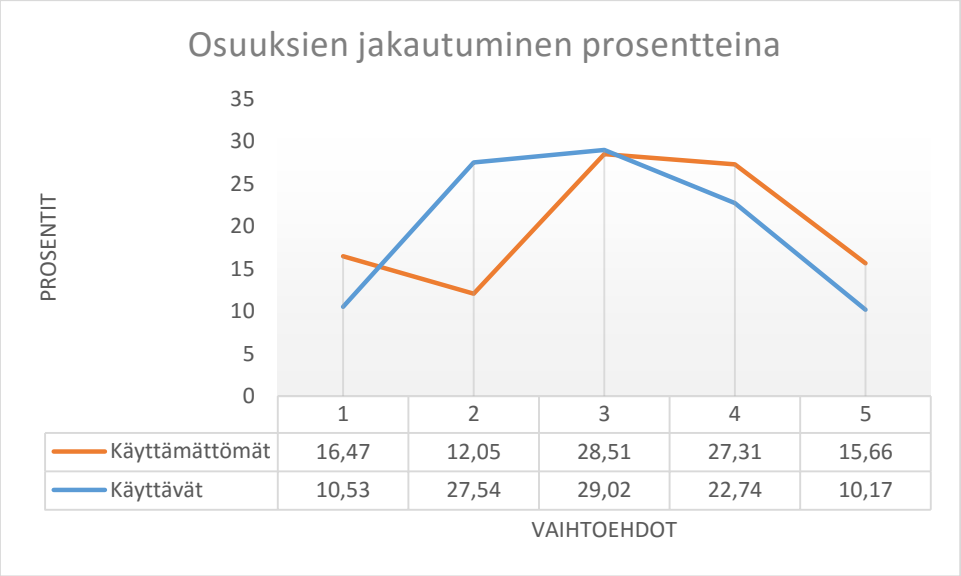
Uhka: Yksityisyyden heikkeneminen

Yksityisyyden heikkenemisestä pilvipalveluita käytettäessä enemmän huolissaan olivat pilvipalveluita käyttävät PK-yritykset, joskin ero niitä käyttämättömiin oli ainoastaan 7,6 % eli ei kovin merkittävästi isompi. Paljon huolissaan yksityisyyden heikkenemisestä oli kuitenkin 44,4 % pilvipalveluita käyttämättömien joukossa, kun vastaavasti 25,8 % oli samaa mieltä pilvipalveluita käyttävien joukosta. Noin 10 % enemmän ei kuitenkaan pitänyt yksityisyyden heikkenemistä uhkana ollenkaan pilvipalveluita käyttämättömistä kun pilvipalveluita käyttävistä ainoastaan 4,8 % oli tätä mieltä.

Uhka: Osaavan IT-henkilön puute

Viimeisessä kysymyksessä eli ”Kuinka suureksi uhkaksi koette sen, että yrityksellä ei ole IT- henkilöä jolla on vahva osaaminen pilvipalveluista” oli lisävaihtoehto ” Yrityksellä on IT- henkilö, jolla on vahva osaaminen pilvipalveluista” ja tässä oli arvatenkin iso ero kahden ryhmän välillä. Pilvipalveluita käyttävien keskuudessa noin yksi neljäsosa ilmoitti, että heillä on vahvaa pilvipalveluosaamista omaava henkilö yrityksessä, kun taas pilvipalvelua käyttämättömien keskuudessa vastaava luku oli reilusti alle 5 %. PK-yrityksillä, joilla ei käytössään ole pilvipalvelua, ei tietenkään ole erityistä tarvetta IT-henkilölle, jolla on osaamista pilvipalveluista. Iso ero oli myös osuuksissa, jotka olivat erittäin huolissaan tietoturvauhasta. Pilvipalvelua käyttämättömien PK-yrityksistä 25 % oli sitä mieltä, että ovat erittäin paljon huolissaan ja vastaavasti pilvipalveluita käyttävien keskuudessa ainoastaan 3,2 % oli samaa mieltä. Suureksi uhaksi tai keskisuureksi uhaksi

osaavan IT-henkilön puutteen koki pilvipalvelua käyttävistä yrityksistä 46,8 % ja toisesta ryhmästä 39,3 % eli siinä erot aavistuksen tasoittuvat.

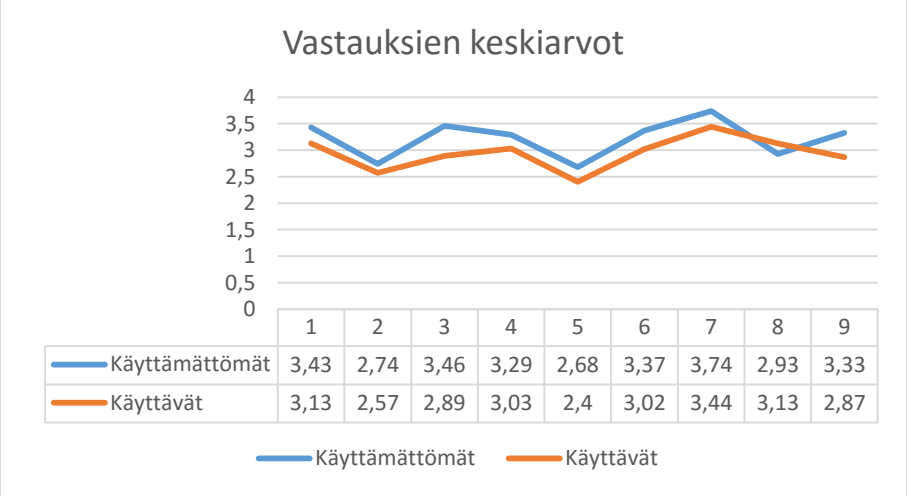


Kuva 6. Molempien ryhmien osuuksien jakautuminen prosentteina vaihtoehdoissa.

Kuvasta 6 voidaan nähdä, että PK-yrityksien suhtautuminen tietoturvauhkiin poikkesi erityisesti vaihtoehdon 2 kohdalla, kun tämä oli huomattavasti suositumpi vaihtoehto ehto pilvipalveluita käyttävien joukossa kuin PK-yrityksien, jotka eivät käytä pilvipalveluita. Kuvasta huomaamme myös selkeästi kuinka pilvipalveluita käyttävien mielipiteet loivenevat mitä vakavampaan suuntaan asteikolla mennään. Kuitenkin vaihtoehto 1 eli vaihtoehto missä uhkaa ei pidetä uhkana on suositumpi pilvipalveluita käyttävien keskuudessa.

Kuten kuvasta 7 huomataan, keskimäärin pilvipalveluita käyttämättömät PK-yritykset pitivät eri tietoturvauhkia vakavampina kuin PK-yritykset, jotka käyttivät pilvipalveluita. Samaan aikaan kuitenkin pilvipalveluita käyttämättömät PK-yritykset olivat useammin sitä mieltä, että kyseessä ei ole uhka ollenkaan eli olivat valinneet vaihtoehdon 1. Ääripäiden vaihtelu oli siis suurempaa tässä ryhmässä kuin pilvipalveluita käyttävien. Suurin yksittäinen ero löytyy vaihtoehdosta 2 eli tietoturvauhkaa pidetään uhkana, mutta ainoastaan pienenä. Pilvipalveluita käyttävät PK-yrityksien vastauksista 27,54 % sijoittui tähän,

ollen toiseksi suurin osuus häviten vain 1,48 % suurimmalle eli vaihtoehdolle 3. Pilvipalveluita käyttämättömien osuus vaihtoehdossa 2 oli kuitenkin vain 12,05 % eli eroa oli jopa 15,49 %. Pilvipalveluiden ääripäiden pienempi osuus voi johtua siitä, että heillä on toiseen ryhmään verrattuna enemmän kokemusta ja tietoa aiheesta, kun taas pilvipalveluita käyttämättömien joukossa saattaa olla enemmän vaikutusta ennakkoluuloilla ja esimerkiksi median otsikoista, joissa voidaan liioitella tietoturvauhkia, jotta saadaan ihmiset kiinnostumaan uutisesta. Pilvipalveluita käyttämättömien ryhmän suurempi osuus vaihtoehdon 1 eli ei ollenkaan uhka osalta saattaa selittäytyä sillä, että uhkasta ei ole tarkkaa tietoa, joten sitä ei osata arvioida täysin realistisesti, jolloin sitä ei pidetä myöskään uhkana. Sama koskee myös pilvipalveluita käyttäviä PK-yrityksiä.



	1	2	3	4	5	6	7	8	9
Käyttämättömät	3,43	2,74	3,46	3,29	2,68	3,37	3,74	2,93	3,33
Käyttävät	3,13	2,57	2,89	3,03	2,4	3,02	3,44	3,13	2,87

Kuva 7. Kyselyn vastauksien keskiarvot molemmista ryhmistä.

3.1.4. Pilvipalvelun määrän vaikutus

Kyselyssä pilvipalveluita käyttäviltä PK-yrityksiltä kysyttiin heidän käyttämien pilvipalveluiden lukumäärää. Vaihtoehtoina oli 1–3, 4–6 tai enemmän. Ylivoimaisesti eniten vastauksia sai vaihtoehto 1–3, kun 45 vastaajaa 62 vastaajasta valitsi tämän. 13 vastaajaa ilmoitti, että heillä on käytössään 4–6 pilvipalvelua ja neljä, että heillä on enemmän. Tässä kappaleessa tutkintaan onko tällä vaikutusta PK-yrityksien vastauksiin eli voidaanko asenteissa ja mielipiteissä nähdä muutoksia sen perusteella, kuinka monta pilvipalvelua PK-yrityksellä on käytössään. Johtuen enemmän vaihtoehdon pienestä vastaajamäärästä, tämän ryhmän vastaukset eivät ole aivan yhtä tilastollisesti pitäviä kuin kahden muun.

Pilvipalveluiden tietoturva yleisesti

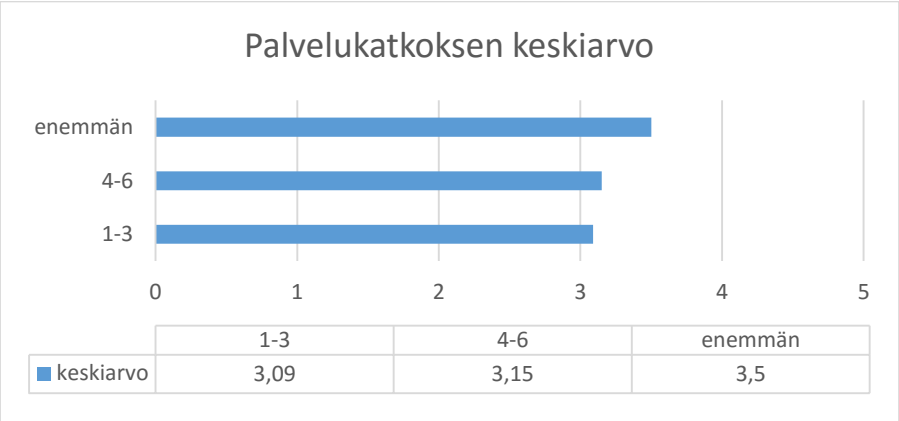
Tarkasteltaessa kokevatko pilvipalveluita käyttävät PK-yritykset pilvipalveluiden nostaneen tietoturvan tasoa reilu 25 % PK-yrityksistä, joilla oli 1–3 pilvipalvelua käytössään, oli sitä mieltä, että pilvipalvelut ovat nostaneet tietoturvan tasoa. 4–6 pilvipalvelua käyttävien PK-yrityksien keskuudessa tätä mieltä oli ainoastaan alle 8 %. Kun ”En osaa sanoa”-ryhmän koko oli 1–3 pilvipalvelun PK-yrityksissä alle 30 % ja 4–6 pilvipalvelun PK-yrityksessä noin 15 %, niin ero oli todella suuri. Enemmän kuin kuutta pilvipalvelua käyttävien PK-yrityksien keskuudessa 25 % oli sitä mieltä, että tietoturvan taso on parantunut ja 75 % vastaavasti koki että ei ole parantunut. 4–6 pilvipalvelun ryhmässä ei jostain syystä ole juurikaan koettu, että pilvipalvelut olisivat nostaneet tietoturvan tasoa.

Kun PK-yrityksiltä kysyttiin varmistivatko he pilvipalvelun tietoturvan tason ennen kuin ottivat palvelun käyttöön, 1–3 pilvipalvelua käyttävien PK-yrityksien keskuudessa vähän reilu puolet ilmoittivat näin tehneensä. 4–6 pilvipalvelun ryhmässä ei kuitenkaan jääty kauaksi tästä luvusta, kun reilu 45 % ilmoitti myös varmistaneensa pilvipalveluntarjoajan tietoturvan tason ja enemmän pilvipalveluita käytössä olevien ryhmässä jopa 75 %. Tämä vaikutti olevan kaikille tärkeätä huolimatta siitä, montako pilvipalvelua PK-yrityksellä oli käytössään. Tietoturvapolitiikan osalta eroa kuitenkin syntyi jonkin verran. 1–3 pilvipalvelua käyttävien ryhmässä noin 30 % ilmoitti, että pilvipalvelut ovat otettu huomioon yrityksen tietoturvapolitiikassa, mutta melkein 50 % ilmoitti, että heillä ei ole ollenkaan tietoturvapolitiikkaa. 4–6 pilvipalvelun ryhmässä jopa melkein 60 % ilmoitti, että pilvipalvelut ovat huomioitu tietoturvapolitiikassa, kun puolestaan 35 % ilmoitti, että heillä ei ole tietoturvapolitiikkaa. Enemmän kuin kuusi pilvipalvelua ryhmässä 75 % ilmoitti, että

pilvipalvelut ovat huomioitu tietoturvapolitiikassa. Kysymyksen vastauksien perusteella voidaan nähdä, että mitä enemmän pilvipalveluita yrityksellä on käytössään, sitä varmemmin se on myös huomioitu tietoturvapolitiikassa ja sitä varmemmin yrityksellä yleensä on olemassa oleva tietoturvapolitiikka. Erot olivat myös aika suuria ja voidaan myös olettaa, että vastauksissa korreloi PK-yrityksien koko eli mitä enemmän pilvipalveluita käytössä, sitä suuremmalla todennäköisyydellä isompi yritys.

Palvelukatkokset

Palvelukatkos huolestutti pilvipalveluiden käyttäjiä sitä enemmän mitä enemmän heillä oli pilvipalveluita käytössään. 1–3 pilvipalvelua käyttävien PK-yrityksien mielestä palvelukatkokset olivat suurin piirtein keskisuuri uhka, kun heidän vastauksien keskiarvoksi muodostui 3,09 asteikolta 1–5. Noin 35 % heistä oli sitä mieltä, että uhka oli keskisuuri ja noin 35 % piti sitä vielä vakavampana. Vastaavasti 4–6 pilvipalvelua käyttävien keskuudessa palvelukatkos sai keskiarvoksi 3,15 eri aavistuksen isompi kuin aikaisemmassa ryhmässä. Suurin ero oli joukossa, joka ei pitänyt palvelukatkosta ollenkaan uhkana, kun se oli vajaa 5 % pienempi. PK-yritykset, joilla oli enemmän kuin 6 pilvipalvelua käytössään, pitivät palvelukatkosta suurempana uhkana, kun heidän vastauksiensa keskiarvo oli 3,5 ja heistä ei yksikään antanut uhkalle pienempää arvosanaa kuin 3.

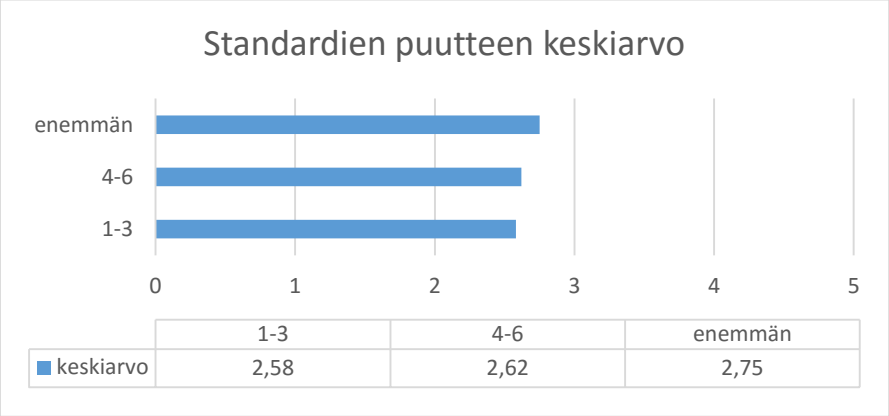


Kuva 8. Palvelukatkoksien vastauksien keskiarvo.

Toimialan standardien puute

Standardien puutteesta kysyttäessä erot ryhmien välillä olivat hyvin samansuuntaiset kuin ne olivat palvelukatkoksien osalta. Pienempänä uhkana toimialan standardien puutetta

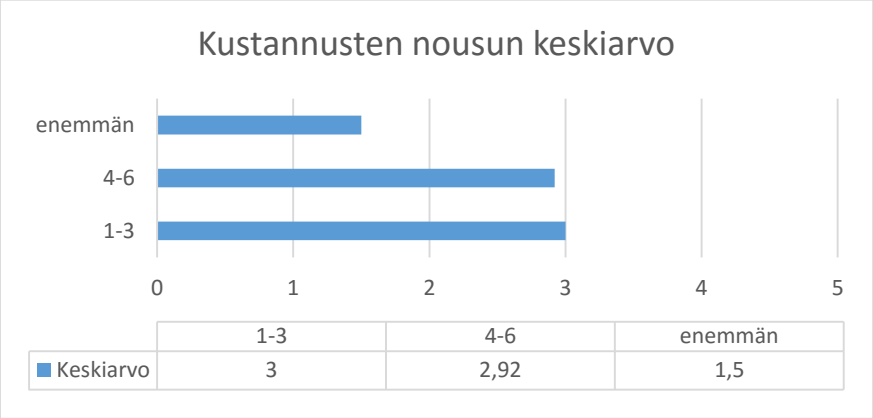
pitivät PK-yritykset, joilla oli käytössään 1–3 pilvipalvelua. Tämän ryhmän vastauksien keskiarvo oli 2,58. Vastaavasti 4–6 pilvipalvelua käyttävien PK-yrityksien vastauksien keskiarvo oli 2,62, joten se oli todella vähän suurempi. Enemmän pilvipalveluita käytössään pitävien PK-yrityksien keskiarvo oli puolestaan 2,75, joten se oli jälleen selkeästi suurempi kuin kahden aikaisemman ryhmän. Vastauksien jakautuminen eri vaihtoehdoille oli ryhmien välillä hyvin samansuuntaista, kenties suurimpana erona oli se, että 1–3 pilvipalvelua käyttävien suurimpana vaihtoehtona oli 2 kun se oli muissa ryhmissä 3.



Kuva 9. Toimialan standardien puutteen vastauksien keskiarvot.

Kustannusten nousu hyökkäyksen johdosta

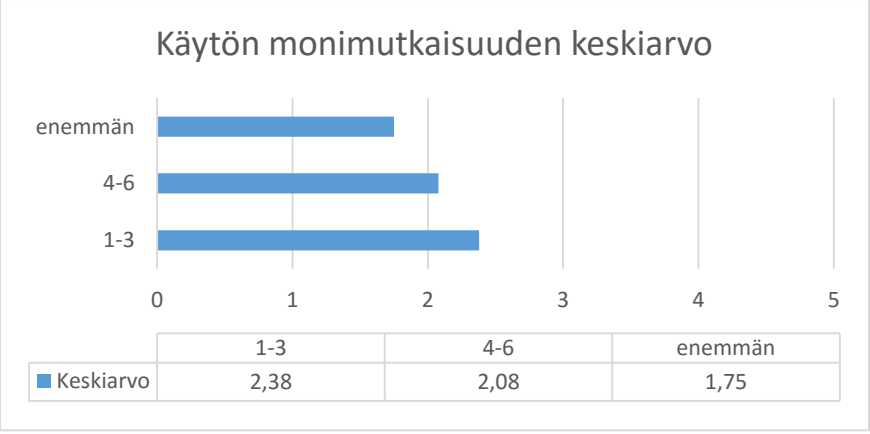
Kustannusten nousu hyökkäyksen johdosta poikkeaa kahdesta aikaisemmasta tietoturvauhasta vastauksien jakauman perusteella. Vakavimpana uhkana tätä pitävät 1–3 pilvipalvelua käyttävien ryhmä, kun heidän vastauksiensa keskiarvo on tasan 3. Jälleen 4–6 pilvipalvelua käyttävien ryhmä on aivan tasoissa edellisen ryhmän kanssa, mutta tällä kertaa heidän keskiarvonsa on vähän pienempi, kun se on 2,92. Vähiten uhkana kustannusten nousua hyökkäyksien johdosta pitävät PK-yritykset, joilla on yli 6 pilvipalvelua käytössään. Heidän keskiarvonsa on 1.5 ja yksikään ei pitänyt uhkaa edes keskisuurena, kun puolestaan 4–6 pilvipalvelua käyttävien keskuudessa eniten vastauksia oli kerännyt keskisuuri uhka.



Kuva 10. Kustannuksien nousu hyökkäyksen johdosta keskiarvot.

Pilvipalvelun käytön monimutkaisuus

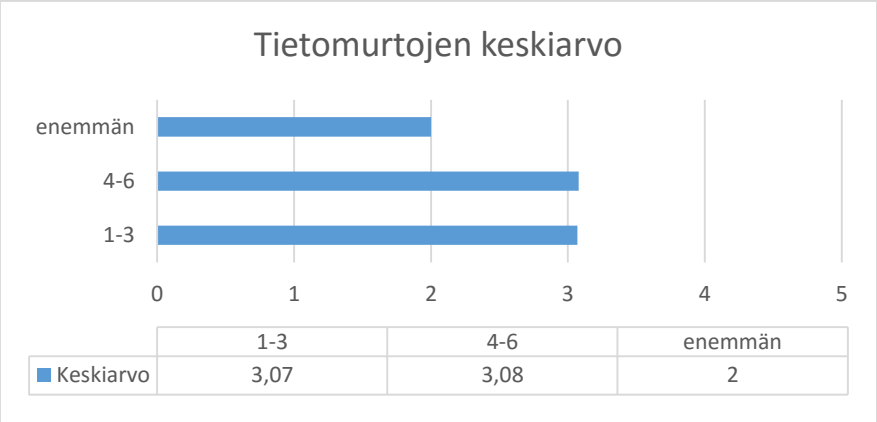
Kuten kustannusten nousussa, myös pilvipalvelun monimutkaisuus koettiin yleisesti ottaen suuremmaksi ja vakavammaksi uhkaksi PK-yrityksien, joilla on käytössään 1–3 pilvipalvelua, keskuudessa. Heidän vastauksiensa keskiarvo oli 2,38, kun se oli seuraavassa ryhmässä eli 4–6 pilvipalvelua 2,08. Myös tätä uhkaa pitivät vähiten uhkana PK-yritykset, joilla oli käytössään yli 6 pilvipalvelua. Ainoastaan 1–3 pilvipalvelua ryhmässä oli uhalle annettu vastauksia vaihtoehdolle erittäin suurena uhkana. PK-yrityksistä, joilla on käytössään 4–6 pilvipalvelua, melkein 40 % oli sitä mieltä, että kyseessä ei ole uhka ollenkaan, joka on todella suuri osa.



Kuva 11. Pilvipalveluiden käytön monimutkaisuuden keskiarvot.

Tietomurrot

Tietomurtojen osalta sekä 1–3 pilvipalvelua käyttävien ryhmä että 4–6 pilvipalvelua käyttävien ryhmä oli käytännössä samaa mieltä. 1–3 pilvipalvelua käyttävien ryhmän vastauksien keskiarvo oli 3,07 ja 4–6 pilvipalvelua käyttävien keskiarvo 3,08, joten voidaan sanoa, että eroa heidän välillään ei ollut yhtään. Heidän vastauksien jakautuminen poikkesi kuiten hieman toisistaan, kun 4–6 pilvipalvelua ryhmässä ei yksikään ollut sitä mieltä, että kyseessä olisi erittäin suuri uhka, mutta puolestaan keskisuuri ja iso uhka saivat enemmän kannatusta kuin toisessa ryhmässä. Reilu 10 % puolestaan 1–3 pilvipalvelua ryhmässä oli sitä mieltä, että kyseessä oli erittäin suuri uhka. Enemmän kuin 6 pilvipalvelua käyttävien PK-yrityksien keskuudessa uhka sai keskiarvoksi 2 eli uhkaa pidettiin selkeästi pienempänä uhkana kuin muissa ryhmissä.

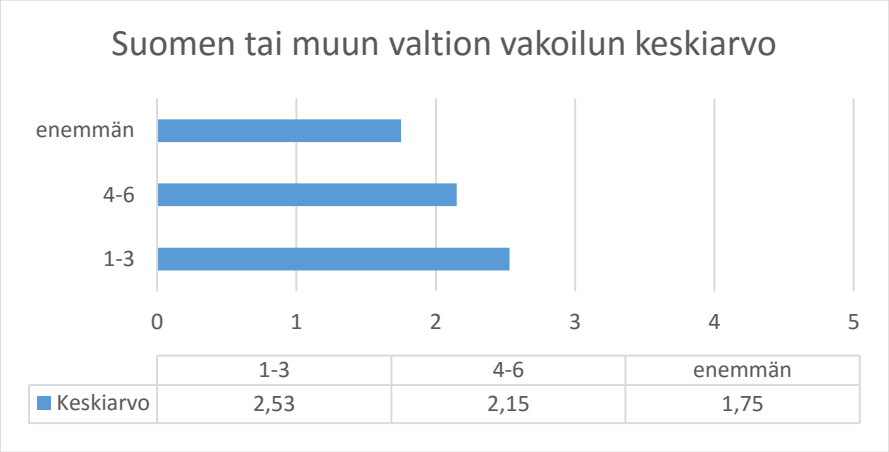


Kuva 12. Tietomurtojen keskiarvot.

Suomen tai muun valtion vakoilu

Valtion suorittamassa vakoilussa ero kahden pienemmän eli 1–3 pilvipalvelua ja 4–6 pilvipalvelua oli suurempi kuin aikaisimmissa kysymyksissä. 1–3 pilvipalvelua ryhmässä keskiarvo oli 2,53 ja puolestaan 4–6 pilvipalvelua ryhmässä ainoastaan 2,15. Ero ei ole iso tämänkään kysymyksen vastauksissa, mutta jakautuminen on suurempaa. Yli 60 % PK-yrityksistä, jotka käyttävät 4–6 pilvipalvelua, olivat sitä mieltä, että kyseessä on ainoastaan pienehkö uhka eli valitsivat vaihtoehdon kaksi. Tämä oli suurin yksittäinen vaihtoehto myös 1–3 pilvipalvelua ryhmässä, mutta tässä ryhmässä ainoastaan 40 % PK-

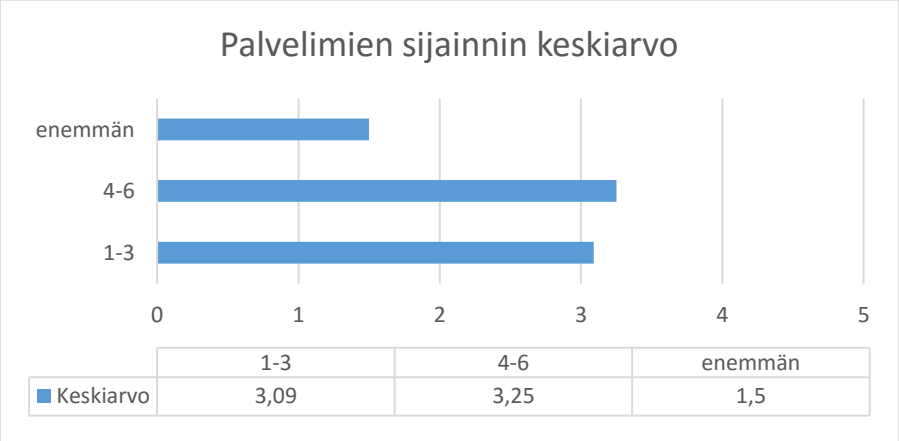
yrityksistä valitsi tämän. Enemmän kuin kuusi pilvipalvelua käyttävien PK-yrityksien vastauksien keskiarvo oli 1,75 eli jälleen huomattavasti pienempi kuin muilla ryhmillä.



Kuva 13. Suomen tai muiden valtioiden vakoilun keskiarvot.

Pilvipalveluiden palvelimien sijainti

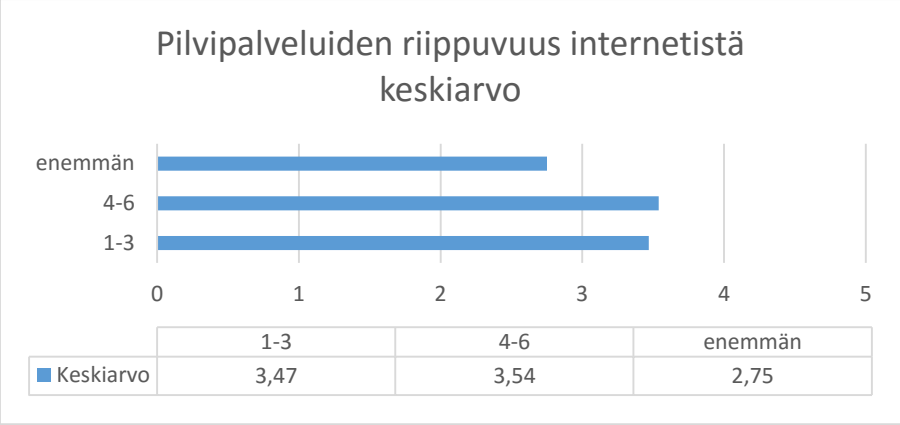
Pilvipalveluiden palvelimien sijtain on ensimmäinen kysymys, jossa kaikista eniten huolestunut on PK-yritykset, joilla on käytössään 4–6 pilvipalvelua. Heidän vastauksiensa keskiarvo oli 3,25. Tämä oli aavistuksen isom kuin 1–3 pilvipalvelua käyttävien ryhmän 3,09. Jälleen kerran nämä ryhmät olivat siis suhteellisen lähellä toisiaan ja vaikka eroa oli, oli se todella pientä. Kuitenkin ryhmä, jolla on enemmän kuin kuusi pilvipalvelua käytössään, erottuu jälleen joukosta, sillä heidän vastauksiensa keskiarvo oli ainoastaan 1,5 eli jälleen selkeästi pienin.



Kuva 14. Pilvipalveluiden palvelimien sijainnin vastauksien keskiarvot.

Pilvipalveluiden riippuvuus internetistä

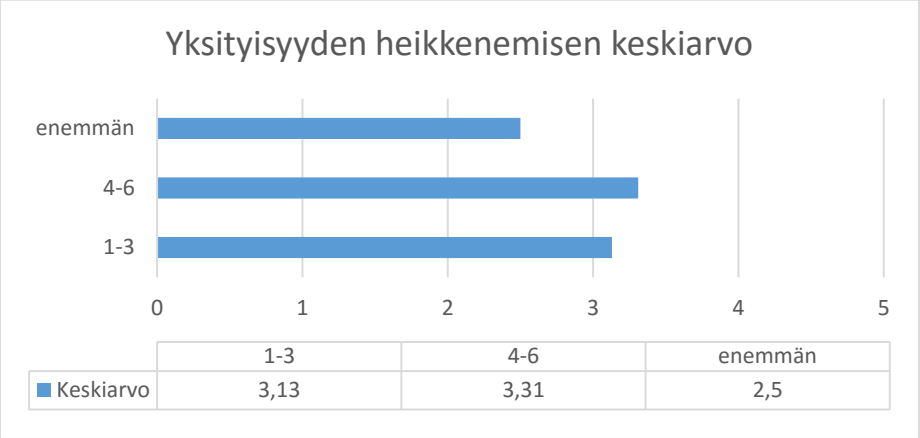
Pilvipalveluiden riippuvuudesta internetrista kysyttäessä keskimmäinen ryhmä eli 4–6 pilvipalvelua eli toista kysymystä putkeen ryhmä, joka piti uhkaa vakavimpana. Heidän vastauksiensa keskiarvo oli 3,54 kun se oli pienemmässä ryhmässä eli 1–3 pilvipalvelua käyttävien joukossa 3,47. Tämä kysymys ei jakanut ryhmiä niin suuresti kuin aikaisemmat, kun PK-yritykset, joilla oli käytössään enemmän kuin kuusi pilvipalvelua, oli suhteellisen samaa mieltä muiden ryhmien kanssa. Heidän vastauksiensa keskiarvo oli 2,75, joten jälleen selkeästi pienempi, mutta ei niin kaukana muista.



Kuva 15. Pilvipalveluiden riippuvuuden internetistä vastauksien keskiarvot.

Yksityisyyden heikkeneminen käytettäessä pilvipalveluita

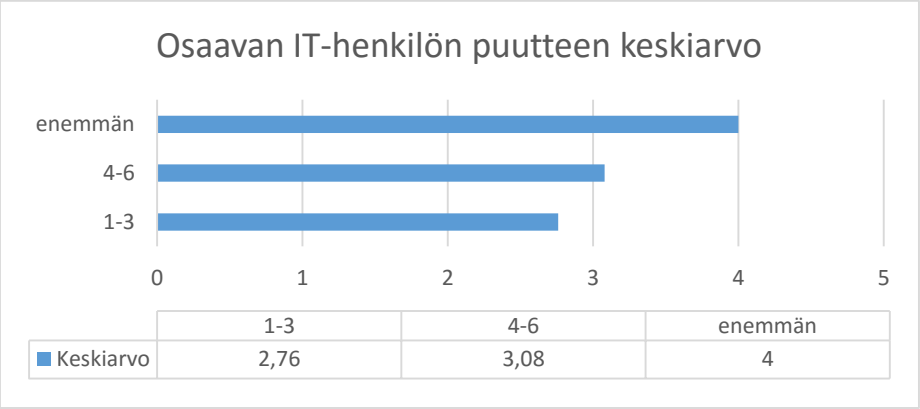
Kaksi pienintä ryhmää olivat jälleen ne tässä kysymyksessä ne, jotka pitivät yksityisyyden heikkenemistä vakavimpana uhkana. Tässä kysymyksessä kuitenkin PK-yritykset, jotka käyttivät yli kuutta pilvipalvelua olivat jälleen vähän lähempänä muita ryhmiä. Yli kuusi pilvipalvelua käyttävien vastauksien keskiarvo oli 2,5 kun seuraavaksi pienin keskiarvo oli 3,13 ja se oli 1–3 pilvipalvelua käyttävien keskiarvo. 4–6 pilvipalvelua oli jälleen suurin, 3,31, mutta ei niin suuri että isoa eroa olisi tullut 1–3 pilviaplvelua käyttävien ryhmään. Suurin yksittäinen ero oli 1–3 pilvipalvelua käyttävien vaihtoehdossa 2, joka sai melkein 30 % ryhmän äänistä ja vastaavasti 4–6 pilvipalvelua käyttävien ryhmässä vaihtoehto sai ainoastaan noin 8 %.



Kuva 16. Yksityisyyden heikkenemisen vastauksien keskiarvot.

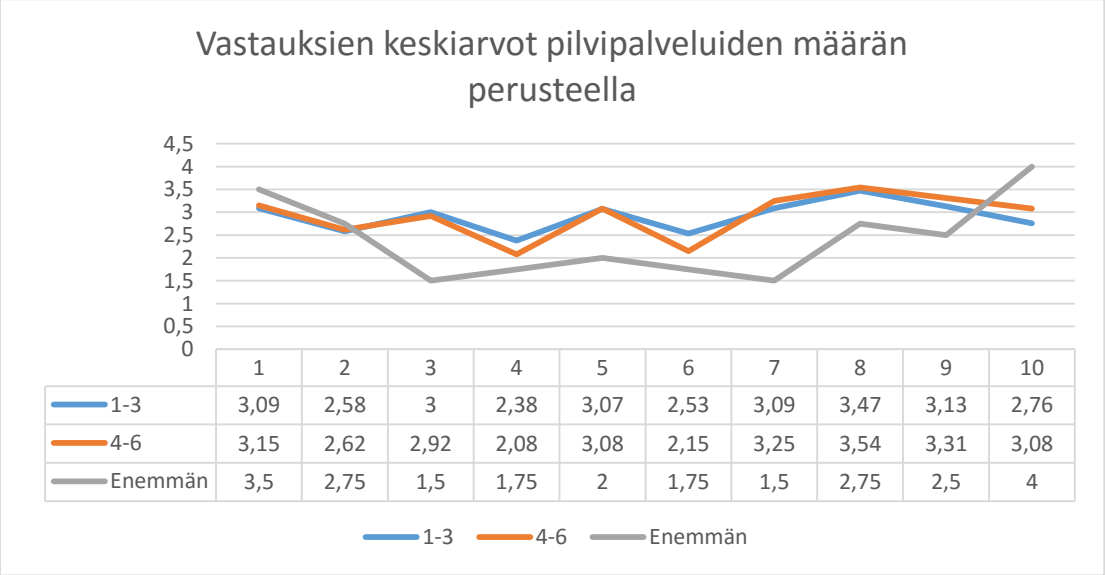
IT-henkilön, jolla vahvaa osaamista pilvipalveluista, puute

Enemmän kuin kuusi pilvipalvelua käyttävien ryhmä on osaavan IT-henkilön puutteesta kaikista eniten huolissaan. Heidän vastauksien keskiarvo on 4, mutta tämä johtuu siitä, että ainoastaan yksi PK-yritys, jolla on käytössään yli kuusi pilvipalvelua ei vastannut tähän kysymykseen, että heillä on yrityksessä osaava IT-henkilö. Jälleen kuitenkin kaksi muuta ryhmää olivat erittäin lähellä toisiaan kun 1–3 pilvipalvelua käyttävien ryhmän keskiarvo oli 2,76 ja vastaavasti 4–6 pilvipalvelua käyttävien ryhmän keskiarvo 3,08. Mielenkiintoisesti melkein 25 % PK-yrityksistä, joilla oli käytössään 1–3 pilvipalvelua, ilmoitti, että heillä on yrityksessä IT-henkilö, jolla on osaaminen pilvipalveluista. Vastaavasti 4–6 pilvipalvelua ryhmässä tämä luku oli ainoastaan vajaa 8 %, joten ero oli tässä todella suuri. Vähemmän yllättävästi melkein kaikki PK-yritykset, joilla on käytössään yli kuusi pilvipalvelua, ilmoitti, että heillä on osaava IT-henkilö.



Kuva 17. Osaavan IT-henkilön puutteen vastauksien keskiarvot.

Kokonaisuutta kun katsotaan ei eroa synny juurikaan pienimmän ja keskimmäisen ryhmän eli 1–3 pilvipalvelua ja 4–6 pilvipalvelua välille. Kun vastauksien keskiarvoa katsotaan näiden ryhmien välillä kaikkien kysymysten osalta, ovat käytännössä ryhmien vastaukset identtiset. Eroja syntyy vastauksien jakautumisessa jonkin verran, jokin vaihtoehto voi olla paljonkin suositumpi toisessa ryhmässä kuin toisessa, mutta kokonaisuudessaan ne ovat linjassa toistensa kanssa. Kuten kuvasta 18 voidaan huomata, näiden kahden ryhmän kuvaajien liike on melkein identtistä ja ainoastaan pieniä eroja syntyy. Puolestaan isoimman ryhmän eli PK-yritykset, joilla on käytössään enemmän kuin kuusi pilvipalvelua, asennoituminen ja mielipiteet eroavat hyvinkin paljon muista ryhmistä. Tämä ryhmä oli selkeästi pienin, joten myös vaihtelu on isompaa, mutta koska erot olivat suuret melkein jokaisessa kysymyksessä, voidaan päätellä, että nämä PK-yritykset suhtautuvat yleisesti ottaen lievemmin eri tietoturvauhkiin mitä pilvipalvelut kohtaavat. Ainoaina poikkeuksina tähän tekevät kysymykset 1 ja 10 eli palvelukatkokset ja osaavan IT-henkilön puute. Palvelukatkoksen osalta enemmän kuin kuutta pilvipalvelua käyttävien ryhmä oli aavistuksen vakavammin suhtautuva ja osaavan IT-henkilön puutteen osalta aika paljon vakavammin suhtautuva. Kuitenkin melkein jokaisella PK-yrityksellä, joilla oli enemmän kuin kuusi pilvipalvelua käytössään, oli palveluksessa IT-henkilö, jolla oli osaamista pilvipalveluista, joten tämä kysymys voidaan jättää huomioimatta vastauksien vähyyden takia.



	1	2	3	4	5	6	7	8	9	10
1-3	3,09	2,58	3	2,38	3,07	2,53	3,09	3,47	3,13	2,76
4-6	3,15	2,62	2,92	2,08	3,08	2,15	3,25	3,54	3,31	3,08
Enemmän	3,5	2,75	1,5	1,75	2	1,75	1,5	2,75	2,5	4

Kuva 18. Kaikkien ryhmien kaikkien vastauksien keskiarvot.

Kun kyselyllä kerätylle aineistolle lasketaan Pearsonin korrelatiokerroin, kuvasta 19 huomataan, että pilvipalvelun määrän (KPL) ja muun aineiston välillä ei ole merkittävää riippuvuutta keskenään. Pearsonin korrelaatiokerroin on positiivisesti merkittävä, kun saatu luku on lähellä 1 ja negatiivisesti merkittävä, kun luku on lähellä -1. Kyselyn aineiston korrelaatiokerroin on molemmin puolin lähellä lukua 0, joten tästä voidaan tehdä päätelmä, että näillä ei ole juurikaan riippuvuussuhdetta. Tämä sama voidaan päätellä myös kovarianssin luvusta. Kun tarkastellaan Sig. (2-tailed) osiota, voidaan huomata, että luvut ovat suhteellisen eriarvoisia. Sig. (2-tailed) kertoimen avulla voidaan päätellä onko muuttujien välillä merkittävää tilastollista korrelaatioa ja tällöin luvun tulisi olla 0.05 tai alle. Kyselyn aineiston Sig. (2-tailed) kertoimet ovat kuitenkin järjestään huomattavasti suurempia, joten voidaan tehdä päätelmä, että muuttujilla ei ole tilastollisesti merkittävää korrelaatiota toisiinsa. Muuttujien lukujen vaihtelu ei siis ole riippuvainen siitä, miten toisen muuttujan luvut vaihtelevat.

		Vakoilu	Palvelukatkos	Standardit	Kustannukset	Monimutkaisuus
KPL	Pearsonin korrelaatio	-.143	.107	.115	-.175	-.157
	Sig. (2-tailed)	.268	.406	.376	.174	.226
	Sum of Squaresand Crossproducts	-5.484	4.613	4.541	-6.984	-6.230
	Kovarianssi	-.090	.076	-076	-.114	-.104
	N	62	62	61	62	61

		Tietomurrot	Sijainti	Internet riippuvuus	Yksityisyys	IT-henkilön puute
KPL	Pearsonin korrelaatio	-.017	-.138	-.065	-.043	.143
	Sig. (2-tailed)	.893	.289	.614	.738	.332
	Sum of Squaresand Crossproducts	-.694	-6.311	-2.823	-1.710	4.000
	Kovarianssi	-.011	-.105	-.046	-.028	.085
	N	62	61	62	62	48

Kuva 19. Kyselyn vastauksien korrelaatiot pilvipalveluiden lukumäärään.

3.1.5. Vertailu muihin tutkimuksiin

Tässä osiossa tarkastellaan kyselyssä saatuja vastauksia ja verrataan niitä muihin ulkomailla tehtyihin tutkimuksiin. Tämän osion tarkoituksena on saada aikaiseksi vertailua vastaako tämän kyselyn tulokset ulkomailla tehtyjä tutkimuksia eli onko PK-yrityksillä ulkomailla vastaavat asenteet ja mielipiteet pilvipalveluista ja niiden tietoturvasta kuin

tämän tutkielman PK-yrityksillä. Vertailua hankaloitti kysymysten asettelu, sillä eri tutkimuksissa saatetaan käyttää erilailla muotoiltuja kysymyksiä, joten täyttä yhtäläisyyttä ei kaikissa kysymyksissä voi vertailun osalta vetää.

European Network and Information Security Agency (ENISA) teki vuonna 2009 kyselytutkimuksen PK-yrityksille pilvipalveluihin liittyen ja olivat keränneet 74 vastausta julkaistessaan kyselyn ”An SME perspective on Cloud Computing” tuloksia. ENISAn kyselyyn vastannaista PK-yrityksistä noin 25 % käytti julkista pilveä. Tämä on lähellä oman kyselytutkimuksen tuloksia, kun 29 % vastasi käyttävänsä julkista pilveä. Yksityistä pilveä puolestaan käytti ENISAn tutkimuksen mukaan 15,1 % kun 19,4 % ilmoitti tutkielman aiheena olevassa kyselyssä käyttävänsä yksityistä pilveä.

Eri uhista kysyttäessä ENISA käytti 4 vaihtoehdon asteikkoa eli vaihtoehtoja oli yksi vähemmän kuin tutkielman aiheena olevassa kyselytutkimuksessa. Yksityisyydestä kysyttäessä ENISAn kyselyyn vastanneista PK-yrityksistä ei yksikään ollut sitä mieltä, että kyseessä ei ole uhka. Vastaavasti 4,8 % pilvipalveluita käyttävistä tutkimuksen aiheena olevaan kyselyyn vastasi, että kyseessä ei ole uhka PK-yritykselle. ENISAn kyselyssä vastaajat olivat enimmäkseen erittäin huolissaan tai pitivät sitä jopa esteenä pilvipalveluiden käyttämiselle, kun puolestaan tähän kyselyyn vastanneet yritykset eivät olleet läheskään yhtä huolissaan asiasta. Sama trendi on näkyvissä myös palvelukatkoksien osuuksissa, ENISAn kyselyyn vastanneet PK-yritykset olivat huomattavasti kriittisempiä kuin tutkielman kyselyyn vastanneet. Selkeästi tasaisempi jaottelu oli nähtävissä kysymyksessä ” Kuinka suureksi uhkaksi koette pilvipalveluiden palvelimien sijainnin muussa maassa kuin Suomessa” ja ENISAn vastaavassa kysymyksessä missä kysyttiin epäjohdonmukaisuuksia eri maiden lainsäädännössä. Molempien kysymyksien vastausten jakautumisessa oli ääripäät saaneet pienimmät edustukset.

Rackspacen vuonna 2015 tekemässä tutkimuksessa ”The anatomy of a cloud migration” he kysyivät yrityksiltä, miksi yritykset siirtyvät pilvipalveluihin. 61 % heidän kyselyyn vastanneista ilmoitti, että yksi syy on IT-kustannusten pieneneminen. Tämä on jopa 30,4 % enemmän kuin tutkielman kyselyyn pilvipalveluita käyttävistä ilmoitti. Parantuneen tietoturvan Rackspacen tutkimuksessa ilmoitti syyksi 38 % vastanneista, joka oli enemmän kuin tutkielman kyselyn 29 %. Kilpailuedun mainitsi tutkielman kyselyssä eduksi

12,9 %, kun Rackspacen tutkimuksessa 22 % ilmoitti, että yksi syy pilvipalveluun siirtymiselle oli pysyminen kilpailijoiden mukana. 24,2 % tutkielman kyselyyn vastanneista oli sitä mieltä, että mahdollisuus uuteen toimintamalliin oli etu, kun taas Rackspacen tutkimukseen vastanneista 37 % oli sitä mieltä, että pilvipalvelut mahdollistivat tai nopeuttivat uutta innovaatiota. Rackspacen vastaajista 88 % oli sitä mieltä, että yrityksen tavoitteet pilvipalveluista täyttyi ainakin osittain ja reilusti yli puolet olivat sitä mieltä, että ne täyttyivät täysin. Tutkielman PK-yrityksistä 98,4 % oli sitä mieltä, että pilvipalveluista on ollut hyötyä yritykselle. Kysymykset eivät täysin vastaa toisiaan, mutta niiden sisältö on sen verran lähellä toisiaan, että niitä voidaan verrata.

Irlantilaisilta PK-yrityksiltä kysyttäessä Carcaryn, Dohertyn ja Conwayn tutkimuksessa ”The Adoption of Cloud Computing by Irish SMEs – an Exploratory Study” pilvipalvelua käyttämättömät yritykset ilmoittivat, että yksi syy mikseivät he ole siirtyneet pilvipalveluihin on IT-taitojen puute. Reilu 30 % irlantilaisista PK-yrityksistä oli tätä mieltä ja tämä voidaan rinnastaa siihen, että tämän tutkielman kyselyyn vastanneista PK-yrityksistä, jotka eivät käytä pilvipalveluita, reilu 39 % oli sitä mieltä, että osaavan IT-henkilön puute yrityksessä on uhka tai iso uhka. Kyselyyn vastanneista irlantilaisista PK-yrityksistä noin puolet ei ollut pilvipalvelun käyttäjä, vastaavasti tutkielman kyselyyn vastanneista noin 32 % ei ollut siirtynyt pilvipalveluihin. Näiden kahden tutkielman otoksen perusteella suomalaiset PK-yritykset ovat vähän aktiivisemmin siirtyneet pilvipalveluiden piiriin.

Mojtaba Akbarin (2012) tekemässä tutkimuksessa ”Cloud Computing Adoption for SMEs Challenges, Barriers and Outcomes” hän suoritti kyselytutkimuksen PK-yrityksille. Hänen kyselyssään vähän alle puolet vastaajista ilmoitti, että yksi syy siirtyä pilvipalveluiden käyttäjäksi oli kustannusten aleneminen. Tämä on suhteellisen paljon enemmän kuin tämän tutkielman pilvipalveluiden käyttäjien osuus eli noin yksi kolmasosa. Kysyttäessä oliko yksi syy yksinkertaisempi hallinta ja ylläpito, Akbarin kyselyyn vastaajista noin 20 % ilmoitti asian olevan näin, joka on selkeästi pienempi kuin tämän tutkielman vaihtoehdon ”Helppous” vaihtoehdon saama osuus joka oli reilu 70 %. Vaikka kysymyksen asettelu on vähän erilainen, ero on siitä huolimatta todella iso. Pääsyn joustavuus oli 11,60 % mielestä syy siirtyä pilvipalveluihin Akbrain kyselyssä ja vastaavasti datan saatavuus usealla laitteella sai kannatusta tässä tutkielmassa melkein 90 %. Pilvi-

palvelun käytön esteeksi palvelukatkoksen näki Akbarin tutkimuksessa reilu 25 % vastaajista mikä on aika pieni luku suhteessa tämän tutkimuksen tuloksiin, kun esimerkiksi keskisuurena uhkana palvelukatkosta piti reilu 40 % pilvipalvelun käyttäjistä ja 39,3 % pilvipalvelua käyttämättömät.

Voltage Securityn tekemässä tutkimuksessa 62 % kyselyyn vastanneista yrityksistä olivat sitä mieltä, että valtio vakoilee yrityksien tietoja. Tämä prosenttiluku on vielä ajalta ennen kuin Edward Snowden julkaisi salaisia asiakirjoja, joista kävi ilmi, että Yhdysvallat vakoilee myös omia yrityksiään. Heidän kyselyyn vastanneiden yrityksien joukossa oli kuitenkin myös suuria ja todella suuria yrityksiä, jotka ovat todella tarkkoja omista tiedoistaan ja käyttävät suuria summia rahaa niiden suojaamiseksi. (Yahoo! Finance 2013). Tämän tutkimuksen kyselyn vastauksien perusteella suomalaiset PK-yritykset eivät kuitenkaan ole aivan samaa mieltä tai eivät ainakaan pidä valtioiden vakoilua uhkana omalle yritykselleen. Pilvipalveluita käyttämättömien keskuudessa melkein yksi kolmasosa ei pidä valtioiden vakoilua ollenkaan uhkana ja vastaava luku pilvipalveluiden käyttäjien keskuudessa on reilu15 % ja molemmissa ryhmässä vakoilua uhkana ei pidä ollenkaan tai pienenä uhkana yli 50 % vastaajista.

Microsoftin (2014) tekemä tutkimus osoitti hyvin päinvastaisia tuloksia kuin tämän tutkimuksen kysely. Microsoftin kyselyyn vastasi yli 500 yhdysvaltalaista PK-yritystä ja heistä 60 % ei käyttänyt pilvipalveluita tällä hetkellä. Kuitenkin 86 % kyselyyn vastanneista ilmoitti, että teknologia on tärkeää yrityksen menestykselle. 90 % vastanneista tiesi mikä pilvipalvelu on. Tämän tutkimuksen kyselyyn vastanneista yrityksistä pilvipalvelua käyttivät melkein 70 %, joten tulokset ovat melkein päin vastaiset Microsoftin tutkimuksen kanssa. Yhdysvaltalaiset PK-yritykset kuitenkin yleisesti olivat tutumpia pilvipalveluiden kanssa kuin suomalaiset PK-yritykset. Suomalaisista Pk-yrityksistä pilvipalvelut tunsi noin 85 %. Microsoftin tutkimuksen mukaan 60 % vastanneista ilmoitti, että teknologia yleisesti mahdollisti heidän kilpailun samankokoisten ja isompien yrityksien kanssa, kun vastaavasti kilpailuetuna pilvipalveluita piti tutkielman kyselyssä reilu 10 % pilvipalvelua käyttävistä ja ei yksikään pilvipalvelua käyttämättömistä.

Eurostatin (2014) mukaan Suomi on pilvipalveluiden käyttöönotossa ensimmäinen maa, sillä Suomessa yritykset ovat adoptoineet pilvipalvelut muuta Eurooppaa enemmän. Heidän mukaansa 51 % suomalaisista yrityksistä on jo siirtynyt pilvipalveluihin. Seuraavana listalla ovat Islanti (43 %), Italia (40 %), Ruotsi (39 %) ja Tanska (38 %). Koko Euroopan yritykset huomioidessa pilvipalveluihin siirtyneiden yritysten osuus on ainoastaan 19 % ja PK-yrityksistä 18 %. Suomen osuus Eurostatin tilastoissa on hyvin samankaltainen kuin tämän tutkielman kyselyn vastaajien kesken. Vastaajista 68,1 % oli siirtynyt pilvipalveluihin, joten luku oli isompi, mutta todennäköisesti ero on kaventunut viimeisen vuoden aikana ja isompi osuus suomalaisista yrityksistä käyttää pilvipalveluita. Yksityistä pilveä Euroopassa käyttävät Pk-yrityksistä 12 % ja julkista pilveä 7 %. Tämän tutkielman perusteella julkista pilveä käyttävät 29 % ja 19,4 % käyttävät yksityistä. Koko Euroopan tasolla vajavainen tietämys pilvipalveluista rajoitti 32 % PK-yrityksiä pilvipalveluiden käytössä, Suomessa pilvipalveluita käyttävien keskuudessa 46,8 % piti vastaavaa asiaa uhkana tai isona uhkana.

Suomalainen Tilastokeskus (2015) puolestaan ilmoitti, että heidän tilastojensa mukaan 53 % suomalaisista yrityksistä käyttää maksullisia pilvipalveluita. Tämä luku on todennäköisesti vielä suurempi, jos siihen lisätään PK-yrityksien käyttämät ilmaiset pilvipalvelut. Myös tämä luku on kuitenkin samaan suuntaan näyttävä kuin tämän tutkielman kyselyyn vastanneiden osuus eli 68,1 %. Saman tutkimuksen mukaan julkista pilveä käytti reilu 40 % yrityksistä ja yksityistä pilveä 14 %. Vastaavasti tämän tutkielman kyselyn jakauma oli julkisen osalta 29 % ja yksityisen 19,4 %. Julkista ja yksityistä käyttivät vielä 30,6 % tämän tutkielman mukaan. Tilastokeskuksen (2014) mukaan epävarmuus tietojen sijainnista oli melkein 30 % yrityksistä syynä siihen, että he eivät ole siirtyneet pilvipalveluiden käyttäjiksi. Tämä aiheutti huolta myös PK-yrityksissä, jotka vastasivat tämän tutkielman kyselyyn ja eivät käytä pilvipalveluita tällä hetkellä, melkein 20 % piti keskisuurena uhkana ja reilu 30 % suurena uhkana. Liian vähäisen asiantuntemuksen pilvipalveluista ilmoitti pilvipalveluun siirtymisen esteeksi 42 % Tilastokeskuksen mukaan. Myös tämä on samaan suuntaan näyttävä kuin tämän tutkielman kyselyn kysymys, jossa kysyttiin IT-henkilön puutetta, jolla on osaamista pilvipalveluista. PK-yritykset, jotka eivät käytä pilvipalvelua, 25 % arvioi kyseessä olevan erittäin suuri uhka, 25 % piti suurena uhkana ja 14,3 % keskisuurena.

4. JOHTOPÄÄTÖKSET

Johtopäätös 1: Pilvipalvelut ovat suhteellisen yleisiä suomalaisissa PK-yrityksissä

Tutkimukseni perusteella PK-yrityksissä on nykypäivänä tarvetta työskennellä etänä. Etätyöskentely on yhä enemmän arkea yrityksissä ja pilvipalvelut ovat tuoneet tähän oman helpotuksensa. PK-yritykset tietävät pilvipalveluiden olemassa olosta, joten he myös tietävät, että ne ovat yksi vaihtoehto, josta yritys voi saada todella tärkeää hyötyä liiketoiminnalleen. Tutkimukseni perusteella pilvipalvelut ovat jo nyt käytössä todella monessa yrityksessä, kun kyselyni mukaan 68,1 % PK-yrityksistä käyttävät ainakin jollain tasolla pilvipalveluita. Tutkimuksen tulos on myös linjassa muihin tehtyihin tutkimuksiin niin Suomessa kuin ulkomaillakin. Suomi on kuitenkin selkeästi edelläkävijä pilvipalveluiden käyttöönotossa Euroopassa.

Johtopäätös 2: PK-yrityksissä käytetään useimmiten julkista pilveä

Tutkimukseni mukaan suurimalla osalla pilvipalveluita käyttävistä PK-yrityksistä on käytössään 1–3 pilvipalvelua, mutta myös yrityksiä, joilla on käytössään useampia pilvipalveluita, löytyy suhteellisen suuri määrä. Yksittäisistä pilvipalveluista on eniten käytössä julkinen pilvi. Julkinen pilvi on yleisin myös yleisellä tasolla, joten sen oleminen suurin tutkimuksen kyselyssä ei yllättänyt. Kuitenkin melkein yhdellä kolmasosasta PK-yrityksistä oli käytössään sekä julkinen että yksityinen pilvi. Hybridi pilvi ei ole tutkimuksen mukaan saavuttanut vielä isoa suosiota. Pilvipalveluita käyttävät yritykset ovat kuitenkin tutkimuksen mukaan järjestään sitä mieltä, että pilvipalveluista on ollut hyötyä yritykselle, ainakin jossain määrin. Tämän tutkimuksen mukaan suurimmiksi eduiksi PK-yrityksien mielestä on noussut etätyöskentelyyn liittyvät asiat kuten datan oleminen aina saatavilla ja usealla laitteella sekä tämän helppous. Yleisesti ottaen pilvipalveluita käyttävät yritykset myös suhtautuvat positiivisemmin pilvipalveluihin etuihin ja kokevat niitä saaneensa kuin PK-yritykset, joilla ei ole käytössään pilvipalveluita.

Johtopäätös 3: PK-yrityksissä tiedostetaan pilvipalveluiden uhat

Tutkimukseni mukaan pilvipalveluita käyttävät PK-yritykset ovat yleisesti jonkin verran huolissaan pilvipalveluiden tietoturvasta. Kyselyn mukaan yritykset eivät kuitenkaan ole

ylireagoineet esimerkiksi lisääntyneeseen uutisointiin aiheesta, mutta eivät usko pilvipalveluiden olevan täysin vaarattomia. Vaikka pilvipalveluissa pyritään panostamaan asiakkaiden tietoturvaan, niin tutkimukseni mukaan yli puolet PK-yrityksistä ei kuitenkaan koe, että heidän tietoturvansa olisi parantunut pilvipalveluiden myötä.

Johtopäätös 4: Puolessa PK-yrityksistä ei ole tehty erityisiä toimia pilvipalveluiden tietoturvan parantamiseksi tai heillä ei ole tietoturvapolitiikkaa ollenkaan

Tutkimuksestani selviää myös, että noin puolet PK-yrityksistä eivät ole koittaneet lisätä pilvipalveluiden tietoturvaa itse, esimerkiksi kouluttamalla työntekijöitään. PK-yrityksien koko saattaa olla tässä rajoittavana tekijänä, mutta kyselyn perusteella ainakin osassa PK-yrityksistä koulutetaan työntekijöitä pilvipalveluiden käyttöön sekä käytetään muitakin keinoja, jotta tietoturva olisi mahdollisimman korkea. Tämä näkyy myös siinä, että kyselyn mukaan hieman alle puolet PK-yrityksistä ovat ottaneet pilvipalveluiden käytön huomioon omassa tietoturvapolitiikassaan. Tosin suurempi määrä kyselyyn vastanneista PK-yrityksistä ei omista tietoturvapolitiikkaa ollenkaan. Tutkimukseni mukaan PK-yritykset ovat selvillä pilvipalveluiden tietoturvan vastuukysymyksistä. Esimerkiksi he ovat sitä mieltä, että tietoturva kuuluu sekä PK-yritykselle että pilvipalveluntarjoajalle. Hieman yli puolet vastanneista olivat myös etukäteen selvittäneet pilvipalveluntarjoajan tietoturvan tason.

Johtopäätös 5: Pilvipalveluita käyttämättömistä PK-yrityksistä yli puolet eivät ole edes harkinneet pilvipalveluita vaikka näkevät niissä etuja

Tutkimukseni mukaan PK-yrityksistä, jotka eivät tällä hetkellä käytä pilvipalveluita, reilusti yli puolet eivät myöskään ole edes harkinneet ottavansa käyttöön pilvipalveluita. Kuitenkin samat PK-yritykset ovat sitä mieltä, että pilvipalvelut auttavat esimerkiksi etätyöskentelyssä ja pitävät pilvipalveluiden etuina muun muassa datan olemista aina saatavilla ja usealla laitteella. Erotuksena pilvipalveluita käyttäviin yrityksiin, he eivät kuitenkaan usko pilvipalveluiden auttavan kilpailullisissa tilanteissa eivätkä usko pilvipalveluiden tuovan etua kustannusten tai tietoturvan muodossa. Kokonaisuudessaan PK-yritykset, jotka eivät käytä pilvipalveluita, ovat enemmän pessimistisiä pilvipalveluiden tuomia etuja kohtaan kuin pilvipalveluita käyttävät. Syitä on monia, esimerkiksi ennakkoluulot, jotka johtuvat kokemuksen tai tiedon puutteesta. Myös pilvipalveluita käyttämättömät

PK-yritykset ovat huolestuneet pilvipalveluiden tietoturvasta enemmän, johtuen lisääntyneestä uutisoinnista.

Johtopäätös 6: Pilvipalveluita käyttävien keskuudessa vakavin uhka oli pilvipalveluiden riippuvuus internetistä ja pienin valtioiden vakoilu

Keskimäärin kaikista vakavimmaksi pilvipalveluita koskevaksi tietoturvauhaksi pilvipalvelua käyttävät PK-yritykset arvioivat pilvipalveluiden riippuvuuden internet-yhteydestä. Tämä uhka sai keskiarvokseen 3,44 asteikolla 1–5. Tämä sopii yhteen myös sen kanssa, että he kokevat pilvipalveluiden tuovan etua nimenomaan etätyöhön ja datan olemiseen aina saatavilla usealla laitteella. Kaikista pienimmäksi uhaksi pilvipalveluille he kokivat Suomen tai muun valtion suorittaman vakoilun. Tämä on ollut julkisessa tiedossa vasta muutamia vuosia, mutta jo ennen Edward Snowdenin julkistamaa NSAn suorittamaa vakoilua, yrityksien johdoissa olevat henkilöt olivat sitä mieltä, että valtio todennäköisesti vakoilee yrityksien tietoja. Suomalaisia PK-yrityksiä ei kuitenkaan tämä häiritse niin paljoa ja suurin syy todennäköisesti on siinä, että nämä yritykset toimivat Suomessa, jossa on tunnetusti erittäin pieni korruptio. Keskiarvoksi uhka sai 2,40, joten se jäi kokonaisuudessaan asteikossa pienen uhan puolelle. Yksikään uhka ei jäänyt keskiarvoltaan alle kahden, joka olisi tarkoittanut, että PK-yritykset eivät uskoisi sen olevan käytännössä uhka ollenkaan.

Johtopäätös 7: Pilvipalveluita käyttämättömien keskuudessa vakavin uhka oli pilvipalveluiden riippuvuus internetistä ja pienin valtioiden vakoilu

PK-yritykset, joka eivät käytä pilvipalveluita, pitivät tutkimukseni mukaan suurimpana uhkana pilvipalveluille niin ikään internet-yhteyden puutetta. Tutkimukseni mukaan pilvipalveluita käyttämättömät yritykset olivat kuitenkin vielä enemmän huolissaan kyseisestä uhkasta. Kun pilvipalveluita käyttävien keskuudessa keskiarvo oli 3,44, oli se tässä ryhmässä 3,74. Pienimmäksi uhkaksi myös tässä ryhmässä arvioitiin Suomen tai muun valtion suorittama vakoilu pilvipalveluita kohtaan. Syy uhan pienuuteen on varmasti sama kuin pilvipalveluita käyttävien joukossa. PK-yritykset, jotka eivät käytä pilvipalveluita, pitivät uhkaa kuitenkin hieman vakavampana kuin pilvipalveluita käyttävät, kun keskiarvo oli 2,68 ja pilvipalveluita käyttävien keskuudessa 2,44.

Johtopäätös 8: PK-yritykset, jotka eivät käytä pilvipalveluita, suhtautuvat tietoturvauhkiin vakavammin

Tutkimukseni mukaan kokonaisuudessaan pilvipalveluita käyttämättömät PK-yritykset suhtautuvat pilvipalveluiden tietoturvauhkiin vakavammin kuin PK-yritykset, jotka jo käyttävät pilvipalveluita. Jos kaikkien kysymysten vastauksien keskiarvo lasketaan, niin pilvipalveluita käyttämättömien keskiarvoksi tulee 3,22 ja pilvipalveluita käyttävien keskiarvoksi 2,94. Ero ei ole iso, mutta se on kuitenkin merkityksellinen, kun pohditaan PK-yrityksien asenteita ja mielipiteitä. Ero näkyy myös kun vertaillaan yksittäisiä kysymyksiä, sillä ainoa tietoturvauhka mihin pilvipalveluita käyttävät PK-yritykset suhtautuivat vakavammin, kuin toinen ryhmä, oli huoli yksityisyyden heikkenemisestä käytettäessä pilvipalveluita. Yksi todennäköinen syy tähän on se, että näillä PK-yrityksillä oli jo yrityksen tietoja pilvipalveluita ja kenties arkaluontoistakin, joten he saattavat myös olla huolissaan siitä ja se näkyy kysymykseen vastattaessa.

Johtopäätös 9: Pilvipalveluiden määrällä ei ole suurta vaikutusta siihen kuinka vakavasti PK-yritykset suhtautuvat tietoturvauhkiin

Kun PK-yrityksellä on käytössään 1–6 pilvipalvelua, ei yrityksen asennoituminen ja mielikuvat juurikaan eroa sen perusteella montako pilvipalvelua heillä on. Kun lukumäärä kasvaa yli kuuden pilvipalvelun, rupeaa eroa syntymään jonkin verran. Tilastollisten analyysien perusteella muuttujien välillä ei ole isoa korrelaatiota. Tällöin PK-yrityksien asennoituminen ja mielipiteet pilvipalveluiden tietoturvauhkiin alkoi lieventymään. Tähän voi olla monia syitä ja yksi niistä on se, että näillä PK-yrityksillä oli huomattavasti useammin palveluksessaan IT-henkilö, jolla on osaamista pilvipalveluista ja tämä saattaa tuoda myös luottoa tietoturvaan.

Johtopäätös 10: Suomessa ja ulkomailla PK-yritykset huolet pilvipalveluiden tietoturvasta oli suhteellisen samat

Tutkimukseni tulokset ovat hyvin samansuuntaisia kuin ulkomailla tehdyt tutkimukset. Joissain kysymyksissä oli kuitenkin havaittavissa poikkeavuuksia esimerkiksi siinä kuinka vakavasti yritykset suhtautuivat johonkin tietoturvauhkaan. Kuitenkin keskimäärin tämän tutkimuksen PK-yritykset ja muiden vastaavien tutkimuksien yritykset olivat

huolissaan samoista asioista ja olivat myös suhteellisen yhtä mieltä pilvipalveluiden tuomista eduista. Johtuen kuitenkin välillä erilaisista kysymysten asetteluista, ei täysin selkeää johtopäätöstä voida vetää tutkimuksien välille, mutta pääpiirteet katsomalla voidaan nähdä, että tulokset ovat samankaltaisia tässä tutkimuksessa ja ulkomailla tehdyissä. Myöskin eroja kuitenkin löytyi yksittäisissä kysymyksissä, kuten valtion suorittama vakoilu, missä Voltage Securityn tekemän tutkimuksen perusteella 62 % uskoi valtion vakoilevan jo ennen Snowdenin paljastusta ja tekemäni tutkimuksen perusteella suomalaiset PK-yritykset eivät joko tähän usko tai eivät pidä sitä uhkana. Suuri ero oli myös pilvipalveluita käyttävien määrässä, esimerkiksi verrattaessa Microsoftin tekemään tutkimukseen. Oman tutkimukseni mukaan pilvipalveluita käytti 68,1 % kyselyyn vastanneista, kun Microsoftin tekemässä kyselyssä yhdysvaltalaisille PK-yrityksille luku oli 40 %.

Johtopäätös 11: PK-yritykset uskoivat pilvipalveluiden olevan hyödyksi yritykselle

Tutkimukseni perusteella PK-yritykset uskoivat, että pilvipalvelut ovat hyödyksi heille. Ainakin ne tuovat mukanaan monia etuja ja etujen kirjo on laaja. Käytännön kokemus pilvipalvelusta tuo mukanaan myös enemmän uskoa ja luottoa pilvipalveluihin. Tietoturvauhkat kuitenkin tiedostetaan ja niihin suhtaudutaan suhteellisen vakavasti. Suhtautuminen ei kuitenkaan tutkimuksen perusteella vaikuttaisi menevän ylireagoinniksi, vaan on järkevää. Pilvipalveluita käyttävät PK-yritykset suhtautuvat vähän positiivisemmin yleisesti pilvipalveluihin ja tämä voi olla seurausta juurikin siitä, että he ovat käyttäneet pilvipalveluita ja tietävät miten asiat käytännössä toimivat. Samaan aikaan, jos yritys on käyttänyt jo kauemmin pilvipalvelua, ja mitään ei ole tapahtunut, niin luottamus saattaa nousta liian suureksi eikä uskota, että jotain vakavaa voisi tapahtua. Pääsääntöisesti PK-yritykset kuitenkin suhtautuvat tarpeeksi luottavasti ja tarpeeksi epäilevästi pilvipalveluihin ja niiden palveluntarjoajiin.

5. YHTEENVETO

Tutkimuksellani halusin selvittää PK-yrityksien asenteita ja mielipiteitä pilvipalveluita ja niiden tietoturvaa kohtaan. Erityisesti olin kiinnostunut miten PK-yritykset, joilla ei välttämättä ole paljoa tietoa, suhtautuvat pilvipalveluiden tietoturvauhkiin. Olin myös kiinnostunut mahdollisista eroista pilvipalvelua käyttävien PK-yritysten ja PK-yritysten, jotka eivät käytä pilvipalvelua, asenteissa ja mielipiteissä sekä näiden vertaaminen ulkomaisiin PK-yrityksiin. Koska halusin saada mahdollisimman monen PK-yrityksen vastauksen, tehtiin tutkielmaan kyselytutkimus, joka toimitettiin vastaajille sähköpostitse Vaasan Yrittäjien avulla. Ensimmäisen sähköpostin jälkeen, PK-yrityksille lähetettiin muistutussähköposti, jotta vastaajia saatiin vielä jonkin verran lisää.

91 PK-yritystä lopulta vastasi heille lähetettyyn kyselyyn. Vastaajamäärässä päästiin tutkielman tavoitteeseen, sillä vastauksia oli tarpeeksi, jotta kyselyä voidaan pitää tarpeeksi kattavana, jotta johtopäätöksiä voidaan tehdä. Pilvipalveluita käyttäviä PK-yrityksiä kyselyyn vastasi 62 kappaletta ja PK-yrityksiä, jotka eivät käytä pilvipalveluita, vastasi 29 kappaletta. PK-yrityksiä, jotka eivät käytä pilvipalvelua, olisi kuitenkin voinut olla enemmän, jotta vertailuryhmät olisivat olleet lähempänä toisiaan kokonsa puolesta.

Tutkimuksessa päästiin tavoitteeseen, sillä kyselyyn saatiin tarpeeksi vastauksia oikealta kohderyhmältä. Vastauksista pystyttiin tekemään johtopäätöksiä ja niitä pystyttiin analysoimaan sen verran kuin tutkimuskysymyksessä oli asetettu tavoitteeksi. Myös ulkomaisiin tutkimuksiin ja niiden tuloksiin vertaaminen onnistui ja vertailua saatiin tehtyä usealta taholta.

Tutkimuksen molempiin hypoteeseihin saatiin tutkimuksen avulla vastaukset. Pilvipalvelun käyttäminen lieventää PK-yrityksien asenteita ja mielipiteitä jonkin verran pilvipalveluiden tietoturvauhkia kohtaan. Kuitenkaan sillä, montako pilvipalvelua PK-yrityksellä on käytössään, ei ole tilastollista merkittävyyttä ellei pilvipalveluiden lukumäärä kasva yli kuuteen kappaleeseen. Tämän kriittisen pisteen jälkeen asenteet ja mielipiteet lieventyvät tietoturvauhkia kohtaan.

Vastauksista olisi saatu syvällisempiä, jos olisi kyselytutkimuksen rinnalla haastateltu muutamaa yritystä. Haastatteluja olisi voinut suorittaa sekä pilvipalvelua käyttävistä että niistä PK-yrityksistä, jotka eivät käytä pilvipalveluita. Näin olisi voitu saada enemmän syitä johtopäätöksille mihin tutkielmassa tultiin.

LÄHDELUETTELO

Akamai. (2015). akamai's [state of the internet report] / security. Volume 2: Number 3. Saatavana World Wide Webistä: https://www.stateoftheinternet.com/downloads/pdfs/2015-cloud-security-report-q3.pdf

Akbar Mojtaba. (2012). Cloud Computing Adoption for SMEs: Challenges, Barriers and Outcomes. Dublin Institute of Technology. Saatavana World Wide Webistä: http://arrow.dit.ie/cgi/viewcontent.cgi?article=1053&context=scschcomdis

AV Comparatives. (2015). Anti-Phishing Test. Saatavana World Wide Webistä: http://www.av-comparatives.org/wp-content/uploads/2015/08/avc_phi_201508_en.pdf

Azarnik Ahmad, Shayan Jafar, Alizadeh Mojtaba & Karamizadeh Sasan. (2012). Associated Risks of Cloud Computing for SMEs. *Open International Journal of Informatics*. Vol. 1. Saatavana World Wide Webistä: https://www.researchgate.net/publication/232724703_Associated_Risks_of_Cloud_Computing_for_SMEs

Carcary Marian, Eileen Doherty & Conway Gerard. (2014) The Adoption of Cloud Computing by Irish SMEs – an Exploratory Study. *The Electronic Journal Information Systems Evaluation*. 17:1. ISSN 1566-6379. Saatavana World Wide Webistä: http://www.ejise.com/issue/download.html?idArticle=933

Cloud Security Alliance. (2011). SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING 3.0. Saatavana World Wide Webistä: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Cook Rick. (2008). Backup and recovery basics: Testing your backups. *TechTarget*. Saatavana World Wide Webistä: http://searchdatabackup.techtarget.com/tip/Backup-and-recovery-basics-Testing-your-backups

Cormac Herley. (2009). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. *Microsoft Research*. Saatavana World

Wide Webistä: http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf

European Union Agency for Network and Information Security. (2009). An SME perspective on Cloud Computing. Saatavana World Wide Webistä: https://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey/at_download/fullReport

European Union Agency for Network and Information Security. (2009). Cloud computing: benefits, risks and recommendations for information security. Saatavana World Wide Webistä: https://www.enisa.europa.eu/media/news-items/cloud-computing-speech

European Union Agency for Network and Information Security. (2015). Cloud Security Guide for SMEs - Cloud computing security risks and opportunities for SMEs. ISBN: 978-92-9204-122-9. Saatavana World Wide Webistä: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes/at_download/fullReport

Eurostat. (2014). Cloud computing - statistics on the use by enterprises. Saatavana World Wide Webistä: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

Gold Steve. (2014). Only 6 in 10 firms say their software is always up-to-date. *SC Magazine*. Saatavana World Wide Webistä: http://www.scmagazineuk.com/only-6-in-10-firms-say-their-software-is-always-up-to-date/article/340924/

Goyal Sumit. (2014). Public vs Private vs Hybrid vs Community – Cloud Computing: A Critical Review. *I.J. Computer Network and Information Security*. 6:3. ISSN: 2074-9104. Saatavana World Wide Webistä: http://www.mecs-press.org/ijcnis/ijcnis-v6-n3/IJCNIS-V6-N3-3.pdf

Hayati Pedram. (2012). botCloud – an emerging platform for cyber-attacks. BAE Systems Stratsec. Saatavana World Wide Webistä: http://stratsec.blogspot.ro/2012/10/botcloud-emerging-platform-for-cyber.html

Identity Theft Resource Center. (2015). Breach Statistics 2005 – 2014. Saatavana World Wide Webistä: http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf

Identity Theft Resource Center. (2014). Data Breach Reports. Saatavana World Wide Webistä: http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

Kaspersky Lab. (2014). The Evolution of Phishing Attacks: 2011–2013. Saatavana World Wide Webistä: http://media.kaspersky.com/pdf/kaspersky_lab_ksn_report_the_evolution_of_phishing_attacks_2011-2013.pdf

Kaspersky Lab. (2015). Kaspersky Lab Report: Financial Cyberthreats in 2014. Saatavana World Wide Webistä: https://securelist.com/files/2015/02/KSN_Financial_Threats_Report_2014_eng.pdf

Kavis J Michael. (2014). Architecting the cloud – Design Decision for Cloud Computing Service Models (SaaS, PaaS, IaaS). New Jersey: John Wiley & Sons, Inc. 351 s. ISBN 978-1-118-82627-0.

Khan Nabeel & Al-Yasiri Adil. (2015). FRAMEWORK FOR CLOUD COMPUTING ADOPTION: A ROADMAP FOR SMES TO CLOUD MIGRATION. *International Journal on Cloud Computing: Services and Architecture*. 5:5/6. Saatavana World Wide Webistä: http://arxiv.org/ftp/arxiv/papers/1601/1601.01608.pdf

Kushner David. (2013). The Real Story of Stuxnet. *IEEE Spectrum*. Saatavana World Wide Webistä: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Liu Simon, Kuhn Rick. (2010). Data Loss Prevention. *IT Professional*. 12:2. ISSN: 1520-9202. Saatavana World Wide Webistä: http://csrc.nist.gov/groups/SNS/rbac/documents/data-loss.pdf?origin=publication_detail

Mahajan Atulay & Sharma Sangeeta. (2015). The Malicious Insiders Threat in the Cloud. *International Journal of Engineering Research and General Science* 3:2. 245–256. ISSN 2091-2730. Saatavana World Wide Webistä: URL: http://pnrsolution.org/Datacenter/Vol3/Issue2/236.pdf

Microsoft. (2014). Survey shows that most small businesses feel the need to keep up with technology, but many have yet to adopt the cloud. Saatavana World Wide Webistä: http://blogs.microsoft.com/firehose/2014/06/05/survey-shows-that-most-small-businesses-feel-the-need-to-keep-up-with-technology-but-many-have-yet-to-adopt-the-cloud/

Mojtaba Akbrai. (2012). Cloud Computing Adoption for SMEs: Challenges, Barriers and Outcomes. *Dublin Institute of Technology*. Saatavana World Wide Webistä: http://arrow.dit.ie/cgi/viewcontent.cgi?article=1053&context=scschcomdis

Motahari-Nezhad Hamid R, Bryan Stephenson & Sharad Singhal. (2009). Outsourcing business to Cloud Computing Services: Opportunities and Challenges. *Hewlett-Packard Development Company*. Saatavana World Wide Webistä: http://www.hpl.hp.com/techreports/2009/HPL-2009-23.pdf

National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology. Saatavana World Wide Webistä: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Open Group. (2012). Maximizing the Value of Cloud for Small-Medium Enterprises: Cloud Adoption Benefits for the SME and Business Case. Saatavana World Wide Webistä: http://www.opengroup.org/cloud/cloud/cloud_sme/benefits.htm

Puustinen Johanna. (2015). *Valve pahoittelee vihdoin joulupäivän tapahtumia – kaiken takana ulkopuolinen hyökkäys*. Pelaajalehti. Saatavana World Wide Webistä: http://www.pelaajalehti.com/uutiset/valve-pahoittelee-vihdoin-joulupaivan-tapahtumia-kaiken-takana-ulkopuolinen-hyokkays

Protacon. (2015). Pilvipalvelujen tietoturva puhuttaa. Saatavana World Wide Webistä: http://www.protacon.com/news/76/85/Pilvipalvelujen-tietoturva-puhuttaa/

Rackspace. (2015). THE ANATOMY OF A CLOUD MIGRATION. Saatavana World Wide Webistä: http://www.rackspace.co.uk/sites/default/files/The%20Anatomy%20of%20a%20Cloud%20Migration%20study.pdf

Rubenking Neil J. (2010). Microsoft: Changing Passwords Isn't Worth the Effort. PC Mag. Saatavana World Wide Webistä: http://www.pcmag.com/article2/0,2817,2362692,00.asp

Shagin Abby. (2012). The Risks And Benefits Of Cloud Computing. *Digitalist Magazine*. SAP. Saatavana World Wide Webistä: http://www.digitalistmag.com/technologies/cloud-computing/2012/10/25/risks-and-benefits-of-cloud-computing-020025

Shet Vinay. (2014). Are you a robot? Introducing “No CAPTCHA reCAPTCHA”. Saatavana World Wide Webistä: https://googleonlinesecurity.blogspot.fi/2014/12/are-you-robot-introducing-no-captcha.html

Steam. (2015). Update on Christmas Issues. Saatavana World Wide Webistä: http://store.steampowered.com/news/19852/

Symantec Corporation. (2014). Internet Security Threat Report 2014. Saatavana World Wide Webistä: Volume 19. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

TeamDrive. (2015). Usein kysytyt kysymykset. Saatavana World Wide Webistä: https://www.teamdrive.fi/ohjeet/

Techopedia. Data Loss. Saatavana World Wide Webistä: https://www.techopedia.com/definition/29863/data-loss

The Open Security Foundation. (2015). DataLossDB. Saatavana World Wide Webistä: http://datalossdb.org/statistics

Tilastokeskus. (2014). Puolet yrityksistä käyttää pilvipalveluja. Saatavana World Wide Webistä: http://www.stat.fi/til/icte/2014/icte_2014_2014-11-25_tie_001_fi.html

Tilastokeskus. (2015). Pilvipalveluiden käyttö yleistyy yrityksissä. Saatavana World Wide Webistä: http://www.stat.fi/til/icte/2015/icte_2015_2015-11-26_tie_001_fi.html

Trend Micro. Security Threats TO Evolving Data Centers. Saatavana World Wide Webistä: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_security-threats-to-datacenters.pdf

World Backup Day. (2015). BUT WHY SHOULD I BACKUP? Saatavana World Wide Webistä: http://www.worldbackupday.com/en/

Yahoo! Finance. (2013). 62% of Employees Believe the Government Snoops on Their Cloud Data. Saatavana World Wide Webistä: http://finance.yahoo.com/news/62-employees-believe-government-snoops-100000703.html

LIITTEET

LIITE 1.

Kyselylomake PK-yrityksille

Pro Gradu- tutkielma

Teen Pro Gradu- tutkielmaani Vaasan yliopiston Teknillisessä tiedekunnassa aiheesta "Pilvipalveluiden tietoturva PK- yrityksissä". Tutkielman tavoitteena on selvittää suomalaisten PK- yritysten pilvipalveluiden käyttöä sekä erityisesti kiinnittää huomiota pk-yritysten asenteisiin ja mielipiteisiin pilvipalveluiden tietoturvasta. Tutkielmaan vaadittava tieto kerätään kyselylomakkeella PK- yrityksiltä ja saatu tieto analysoidaan itse tutkielmassa. Kyselystä saatua tietoa verrataan myös jossain määrin ulkomailla tehtyihin vastaavanlaisiin kyselyiden tuloksiin, jotta nähdään onko tutkielman kyselyyn vastanneiden yritysten mielipiteet ja asenteet vastaavia kuin PK- yrityksillä ulkomailla.

Yhteystiedot:
Johannes Töyli
johannes.toyli@gmail.com

*Required

Pilvipalveluiden tietoturva PK- yrityksissä

Pilvi ei ole uutta teknologiaa, vaan vanhan teknologian uusi käyttötapa. Pilvi- termi onkin kielikuva, jolla viitataan internetiin. Pilven tuomat edut ovat siinä, että se on aina saatavilla, käyttäjä saa paljon lisää laskentatehoa toiminnoilleen ja suuri tallennustila. Pilvipalveluita käytetäänkin nykyään joka paikassa ja käyttäjä ei aina edes tiedosta käyttävänsä nimenomaan pilvipalvelua, sillä niiden toiminta on aivan vastaavaa paikallisesti tapahtuvan käytön kanssa.

Pilvipalveluita ovat esimerkiksi sähköpostipalvelut kuten Gmail sekä tiedon tallenuspaikat kuten Microsoftin OneDrive tai Dropbox. Pilvipalvelu on myös esimerkiksi Microsoftin Office365, joka on täysin pilvessä toimiva Office työkalupaketti.

1. **Yrityksen toimiala**
   Valinnainen

   .....

2. **Onko yrityksessä tarvetta työskennellä etänä?** *
   Mark only one oval.
   - ◯ Kyllä
   - ◯ Ei

3. **Ovatko pilvipalvelut teille tuttuja?** *
   Mark only one oval.
   - ◯ Kyllä
   - ◯ Ei

4. **Käytetäänkö yrityksessä pilvipalveluita?** *
Mark only one oval.

- ◯ Kyllä *Skip to question 5.*
- ◯ Ei *Skip to question 18.*

Pilvipalvelut yleisesti

5. **Kuinka monta pilvipalvelua yrityksellä on käytössä?**
Esimerkiksi sähköposti, tiedontallennuspaikkoja ja niin edelleen.
Mark only one oval.

- ◯ 1-3
- ◯ 4-6
- ◯ Enemmän

6. **Minkä mallista pilvipalveluja yrityksessä käytetään?**
Julkinen pilvi on yleisin ja siinä kaikki pilven käyttäjät käyttävät samaa käyttöliittymää internetissä. Yksityisen pilven ero julkiseen on siinä, että siihen pääsy on ainoastaan yksityisessä verkossa. Hybridi mallissa yhdistyy julkinen ja yksityinen malli eli osa pilven toiminnoista voi olla julkinen ja osa yksityinen.
Mark only one oval.

- ◯ Julkinen pilvipalvelu
- ◯ Yksityinen pilvipalvelu
- ◯ Julkinen & yksityinen
- ◯ Hybridi pilvipalvelu
- ◯ En tiedä

7. **Ovatko käyttämänne pilvipalvelut olleet hyödyksi yritykselle?**
Mark only one oval.

- ◯ Kyllä
- ◯ Ei

8. **Mitkä seuraavista koette pilvipalveluiden eduksi?**
   Tick all that apply.

   - [ ] Datan saatavuus usealla laitteella
   - [ ] Oman datan oleminen aina saatavilla
   - [ ] Etätyöskentely
   - [ ] Kilpailuetu
   - [ ] Kustannukset
   - [ ] Tietoturva
   - [ ] Helppous
   - [ ] Mahdollisuus uuteen toimintamalliin
   - [ ] Yrityksen toimintojen tehostuminen
   - [ ] Järjestelmien olemisen aina päivitettynä
   - [ ] Other: .....

Tietoturva

9. **Ovatko uutiset lisääntyneistä tietomurroista saaneet teidät huolestuneeksi pilvipalveluiden tietoturvasta?**
   Mark only one oval.

   - ◯ Paljon
   - ◯ Jonkin verran
   - ◯ Ei yhtään

10. **Oletteko olleet huolissanne tietoturvasta johtuen pilvipalvelusta?**
    Mark only one oval.

    - ◯ Paljon
    - ◯ Jonkin verran
    - ◯ Ei yhtään

11. **Koetteko pilvipalveluiden nostaneen yrityksen tietoturvaa?**
    Mark only one oval.

    - ◯ Kyllä
    - ◯ Ei
    - ◯ En osaa sanoa

12. **Onko pilvipalvelun käytön turvallisuutta yritetty lisätä seuraavilla asioilla?**
Voit valita useamman
Tick all that apply.

- [ ] Työntekijöiden koulutuksella
- [ ] Prosesseilla
- [ ] Teknologialla
- [ ] Ei mitenkään
- [ ] Other: .....

13. **Onko yrityksen tietoturvapolitiikassa otettu huomioon pilvipalveluiden käyttö?**
Mark only one oval.

- ◯ Kyllä
- ◯ Ei
- ◯ Yrityksellä ei ole selkeää tietoturvapolitiikkaa

14. **Kenen vastuulla koette tietoturvan olevan pilvipalveluissa?**
Mark only one oval.

- ◯ Palvelua käyttävällä yrityksellä
- ◯ Pilvipalveluntarjoajalla
- ◯ Molemmilla

15. **Varmistettiinko yrityksessä pilvipalveluntarjoajan tietoturvan taso ennen palvelun käyttöönottoa?**
Mark only one oval.

- ◯ Kyllä
- ◯ Ei

16. **Onko yrityksenne joutunut hyökkäyksen kohteeksi viimeisen vuoden aikana?**
Esimerkiksi tietomurto tai haitallienn sisäpiiriläinen kuten entinen työntekijä joka varasti arkaluontoista dataa
Mark only one oval.

- ◯ Kyllä
- ◯ Ei
- ◯ En tiedä

17. **Onko yrityksenne pilvipalveluntarjoaja joutunut hyökkäyksen kohteeksi viimeisen vuoden aikana?**
Mark only one oval.

- ◯ Kyllä
- ◯ Ei
- ◯ En tiedä

Yleiset kysymykset Pk-yrityksille, jotka eivät käytä pilvipalveluita:

Yleisesti

18. **Onko yrityksessä pohdittu siirtymistä pilvipalveluiden käyttäjäksi?**
Mark only one oval.

- ◯ Kyllä
- ◯ Ei

19. **Ovatko uutiset lisääntyneistä tietomurroista saaneet teidät kyseenalaistamaan pilvipalveluiden tietoturvaa**
Mark only one oval.

- ◯ Paljon
- ◯ Jonkin verran
- ◯ Ei yhtään

20. **Mitkä seuraavista koette pilvipalveluiden eduksi?**
Tick all that apply.

- ☐ Datan saatavuus usealla laitteella
- ☐ Oman datan oleminen aina saatavilla
- ☐ Etätyöskentely
- ☐ Kilpailuetu
- ☐ Kustannukset
- ☐ Tietoturva
- ☐ Helppous
- ☐ Mahdollisuus uuteen toimintamalliin
- ☐ Yrityksen toimintojen tehostuminen
- ☐ Järjestelmien olemisen aina päivitettynä
- ☐ Other: .....

Kysymykset tietoturvauhista pilvipalvelua käyttäville PK-yrityksille:

Uhat

21. **Kuinka suureksi uhkaksi koette pilvipalvelun palvelukatkoksen (1 = en ollenkaan, 5 = erittäin suureksi)**
Esimerkiksi pilvipalveluun ei saada yhteyttä, kun palvelimet ovat kaatuneet ja työnteko ei onnistu
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

22. **Kuinka suureksi uhkaksi koette mahdollisten toimialan standardien puutteen pilvipalveluille (1 = en ollenkaan, 5 = erittäin suureksi)**
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

23. **Kuinka suureksi uhkaksi koette kustannusten nousun pilvipalvelun joutuessa hyökkäyksen kohteeksi (1 = en ollenkaan, 5 = erittäin suureksi)**
Esimerkiksi hyökkääjä ohjaa liikennettä yrityksen internet- sivuille jolloin kustannukset nousevat
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

24. **Kuinka suureksi uhkaksi koette pilvipalvelun käytön monimutkaisuuden (1 = en ollenkaan, 5 = erittäin suureksi)**
Käyttö hankalaa, jolloin työntekijä saattaaepähuomiossa jakaa julkisesti materiaalia jota ei ollut tarkoitus
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

25. **Kuinka suureksi uhkaksi koette tietomurron yrityksen käyttämää pilvipalvelua kohtaan (1 = en ollenkaan, 5 = erittäin suureksi)**
Vaikka murto ei kohdistuisi itse yritykseen, saattaa myös heidän dataa joutua hyökkääjän haltuun murron yhteydessä
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

26. **Kuinka suureksi uhkaksi koette Suomen tai muun valtion vakoilun (1 = en ollenkaan, 5 = erittäin suureksi)**
Esimerkiksi Wikileaksin paljastukset Yhdysvaltain NSAn vakoilusta
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

27. **Kuinka suureksi uhkaksi koette pilvipalveluiden palvelimien sijainnin muussa maassa kuin Suomessa (1 = en ollenkaan, 5 = erittäin suureksi)**
Palvelimien sijaitessa fyysisesti muualla kuin Suomessa, myös sen sisältämään dataan voidaan käyttää maan paikallisia lakeja
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

28. **Kuinka suureksi uhkaksi koette pilvipalveluiden riippuvuuden internet- yhteydestä (1 = en ollenkaan, 5 = erittäin suureksi)**
Pilvipalveluiden käyttö ei onnistu, koska internet- yhteys ei toimi
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

29. **Oletteko huolissanne yksityisyyden heikkenemisestä käyttäessä pilvipalveluita (1 = en ollenkaan, 5 = erittäin paljon)**
Pilvipalveluihin tallennetaan myös arkaluontoista dataa ja siihen käsiksi pääseminen on helpompaa kuin jos se sijaitsisi ainoastaan yrityksen fyysisillä koneilla yrityksen tiloissa. Pilvipalveluiden käyttämiä palvelimia käyttävät useat henkilöt ja jopa useat yritykset.
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

30. **Kuinka suureksi uhkaksi koette sen, että yrityksellä ei ole IT- henkilöä jolla on vahva osaaminen pilvipalveluista (1 = en ollenkaan, 5 = erittäin suureksi)**
Pilvipalvelun käyttöönotto saattaa olla hankalaa ilman osaavaa IT- henkilöä
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ Yrityksellä on IT- henkilö, jolla on vahva osaaminen pilvipalveluista

31. **Oletteko huolissanne jostain muusta liittyen pilvipalveluihin?**

.....

Kysymykset tietoturvauhista PK-yrityksille, jotka eivät käytä pilvipalvelua

32. **Kuinka suureksi uhkaksi koette pilvipalvelun palvelukatkoksen (1 = en ollenkaan, 5 = erittäin suureksi)**
Esimerkiksi pilvipalveluun ei saada yhteyttä, kun palvelimet ovat kaatuneet ja työnteko ei onnistu
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

33. **Toimialan standardien puute pilvipalveluille**
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

34. **Kuinka suureksi uhkaksi koette kustannusten nousun pilvipalvelun joutuessa hyökkäyksen kohteeksi (1 = en ollenkaan, 5 = erittäin suureksi)**
Esimerkiksi hyökkääjä ohjaa liikennettä yrityksen internet- sivuille jolloin kustannukset nousevat
Mark only one oval.

- 1
- 2
- 3
- 4
- 5

36. **Kuinka suureksi uhkaksi koette tietomurron yrityksen käyttämää pilvipalvelua kohtaan (1 = en ollenkaan, 5 = erittäin suureksi)**
Vaikka murto ei ikohdistuisi itse yritykseen, saattaa myös heidän dataa joutua hyökkääjän haltuun murron yhteydessä
Mark only one oval.

- 1
- 2
- 3
- 4
- 5

37. **Kuinka suureksi uhkaksi koette Suomen tai muun valtion vakoilun (1 = en ollenkaan, 5 = erittäin suureksi)**
Esimerkiksi Wikileaksin paljastukset Yhdysvaltain NSAn vakoilusta
Mark only one oval.

- 1
- 2
- 3
- 4
- 5

38. **Kuinka suureksi uhkaksi koette pilvipalveluiden palvelimien sijainnin muussa maassa kuin Suomessa (1 = en ollenkaan, 5 = erittäin suureksi)**
Palvelimien sijaitessa fyysisesti muualla kuin Suomessa, myös sen sisältämään dataan voidaan käyttää maan paikallisia lakeja
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

39. **Kuinka suureksi uhkaksi koette pilvipalveluiden riippuvuuden internet- yhteydestä (1 = en ollenkaan, 5 = erittäin suureksi)**
Pilvipalveluiden käyttö ei onnistu, koska internet- yhteys ei toimi
Mark only one oval.

- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

40. **Oletteko huolissanne yksityisyyden heikkenemisestä käyttäessä pilvipalveluita (1 = en ollenkaan, 5 = erittäin paljon)**
Pilvipalveluihin tallennetaan myös arkaluontoista dataa ja siihen käsiksi pääseminen on helpompaa kuin jos se sijaitsisi ainoastaan yrityksen fyysisillä koneilla yrityksen tiloissa. Pilvipalveluiden käyttämiä palvelimia käyttävät useat henkilöt ja jopa useat yritykset.
Mark only one oval.

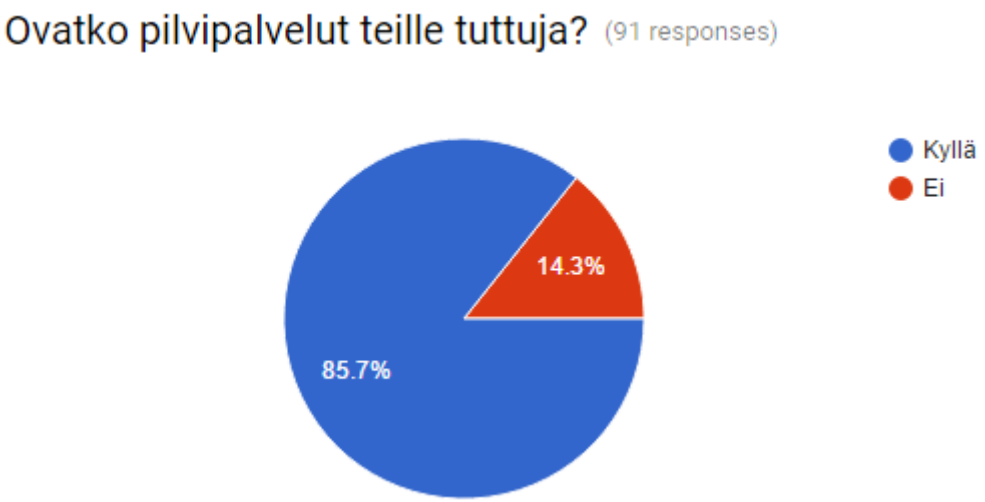
- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5

41. **Kuinka suureksi uhkaksi koette sen, että yrityksellä ei ole IT- henkilöä jolla on vahva osaaminen pilvipalveluista (1 = en ollenkaan, 5 = erittäin suureksi)**
Pilvipalvelun käyttöönotto saattaa olla hankalaa ilman osaavaa IT- henkilöä
Mark only one oval.

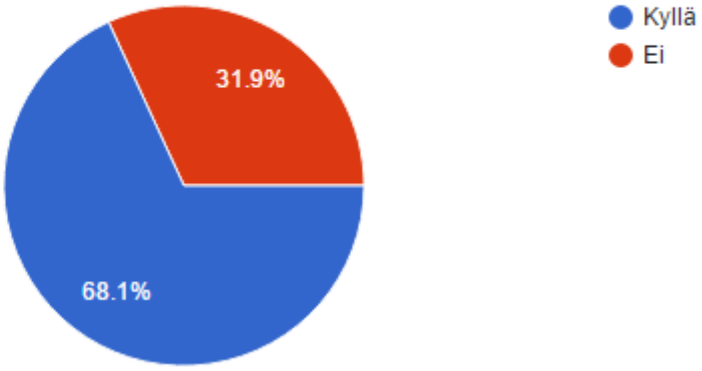
- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ Yrityksellä on IT- henkilö, jolla on vahva osaaminen pilvipalveluista

LIITE 2.

Kyselyn vastauksien jakaumat

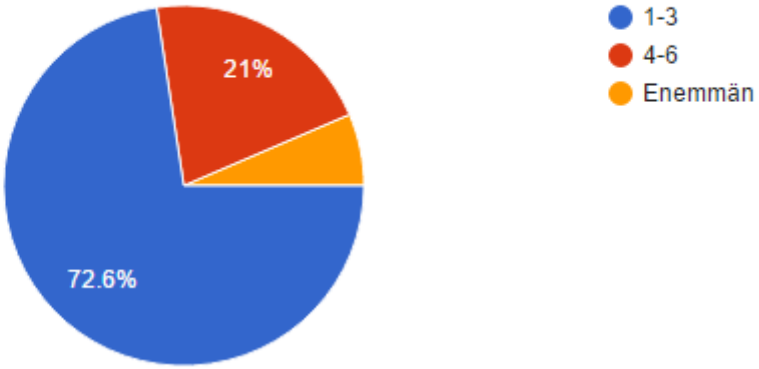


Käytetäänkö yrityksessä pilvipalveluita? (91 responses)

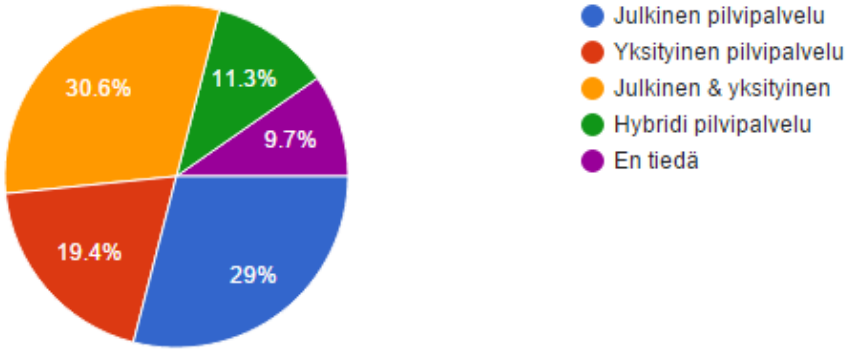


Yleiset kysymykset pilvipalveluista pilvipalveluita käyttäville yrityksille

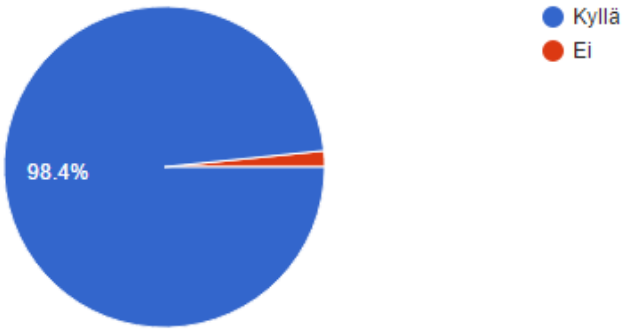
Kuinka monta pilvipalvelua yrityksellä on käytössä? (62 responses)



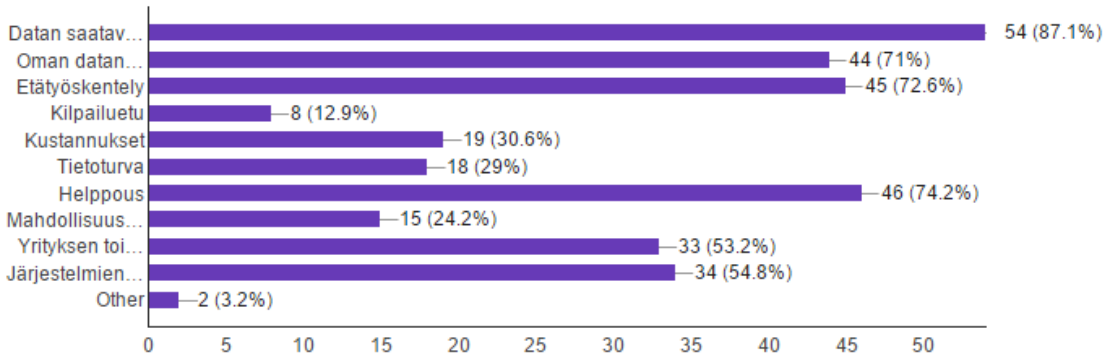
Minkä mallista pilvipalveluja yrityksessä käytetään? (62 responses)



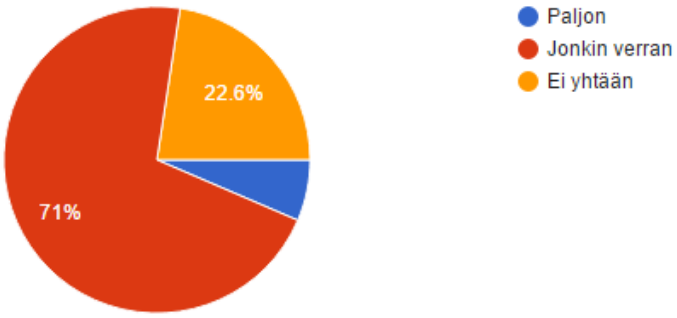
Ovatko käyttämänne pilvipalvelut olleet hyödyksi yritykselle? (62 responses)



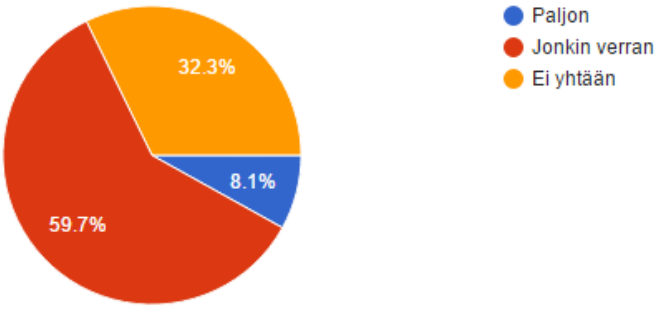
Mitkä seuraavista koette pilvipalveluiden eduksi? (62 responses)



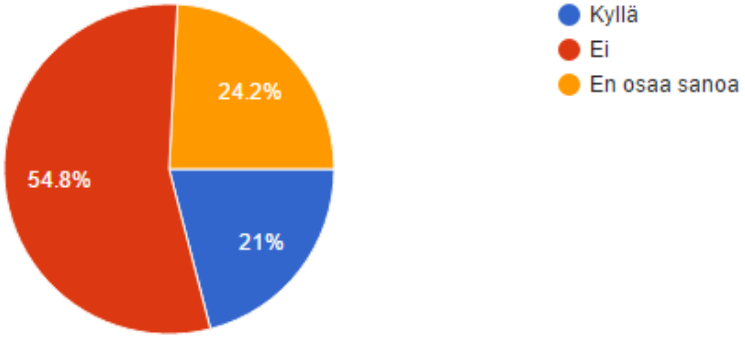
Ovatko uutiset lisääntyneistä tietomurroista saaneet teidät huolestuneeksi pilvipalveluiden tietoturvasta?
(62 responses)



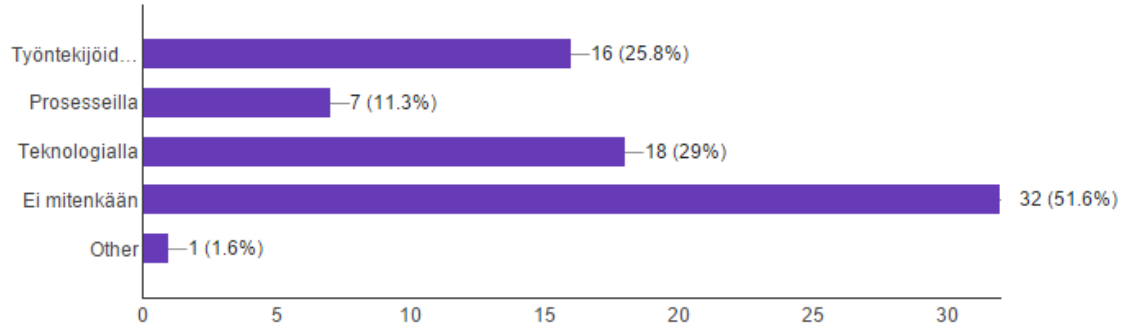
Oletteko olleet huolissanne tietoturvasta johtuen pilvipalvelusta? (62 responses)



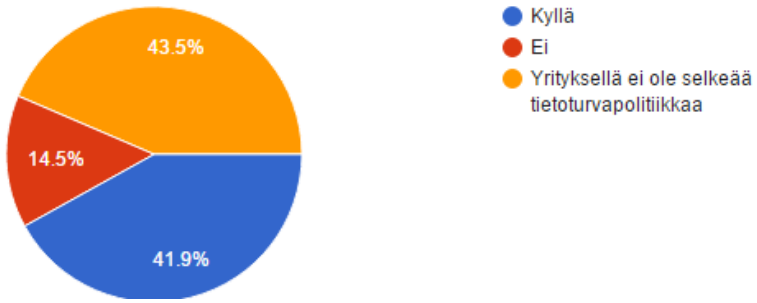
Koetteko pilvipalveluiden nostaneen yrityksen tietoturvaa? (62 responses)



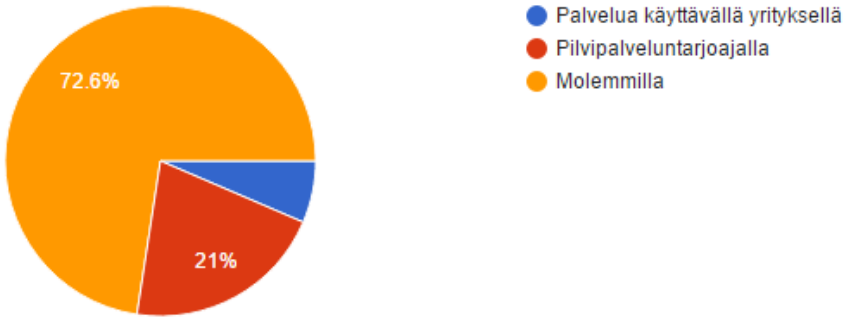
Onko pilvipalvelun käytön turvallisuutta yritetty lisätä seuraavilla asioilla?
(62 responses)



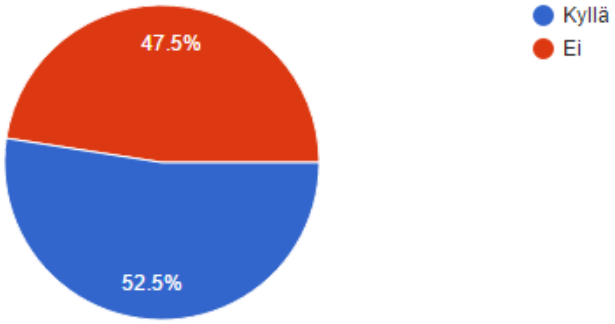
Onko yrityksen tietoturvapolitiikassa otettu huomioon pilvipalveluiden käyttö?
(62 responses)



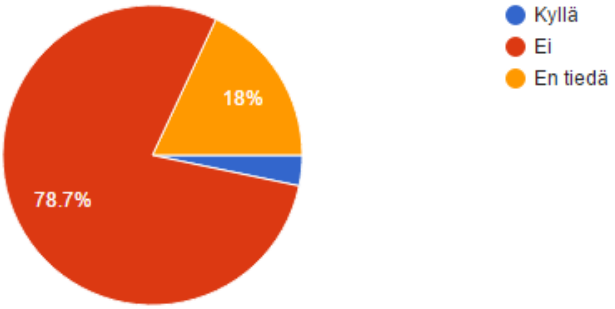
Kenen vastuulla koette tietoturvan olevan pilvipalveluissa? (62 responses)



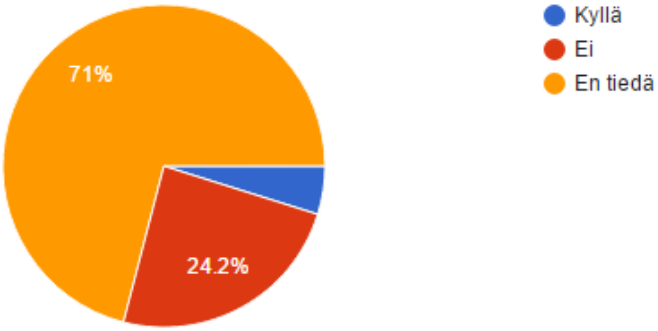
Varmistettiinko yrityksessä pilvipalveluntarjoajan tietoturvan taso ennen palvelun käyttöönottoa?
(61 responses)



Onko yrityksenne joutunut hyökkäyksen kohteeksi viimeisen vuoden aikana?
(61 responses)

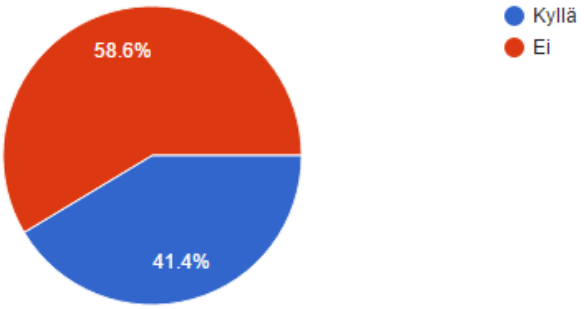


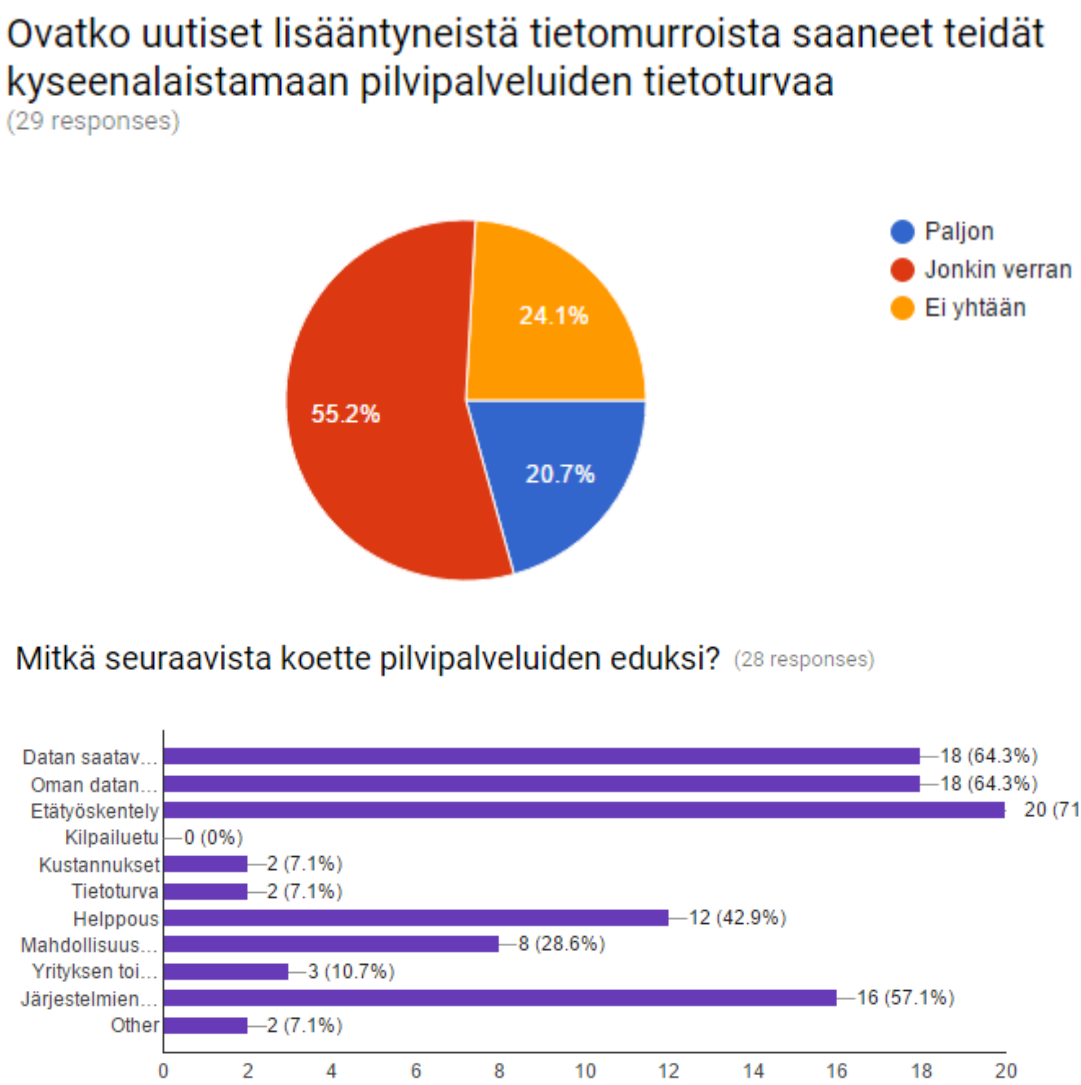
Onko yrityksenne pilvipalveluntarjoaja joutunut hyökkäyksen kohteeksi viimeisen vuoden aikana?
(62 responses)



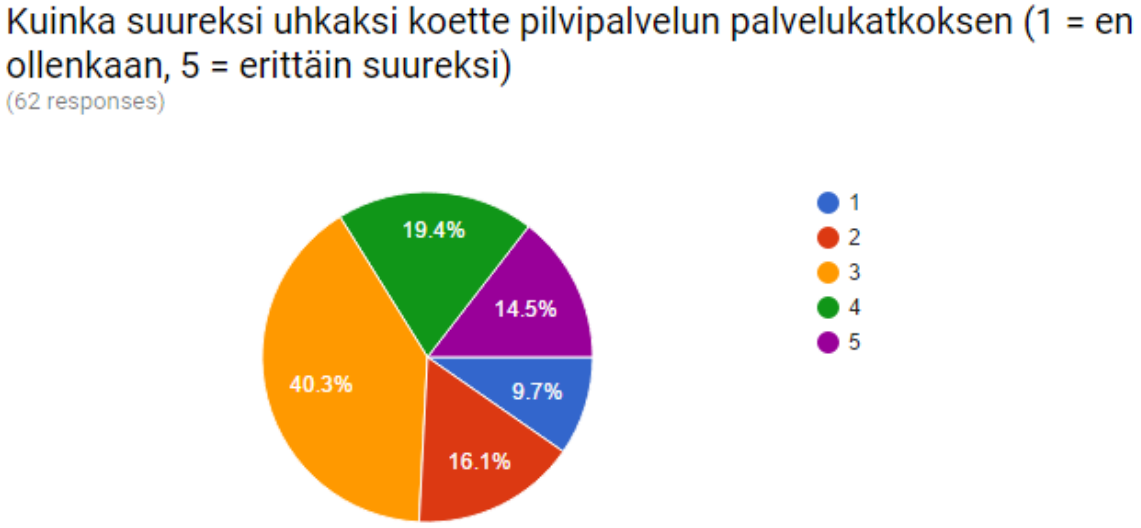
Yleiset kysymykset pilvipalveluista PK-yrityksille, jotka eivät käytä pilvipalveluita

Onko yrityksessä pohdittu siirtymistä pilvipalveluiden käyttäjäksi? (29 responses)

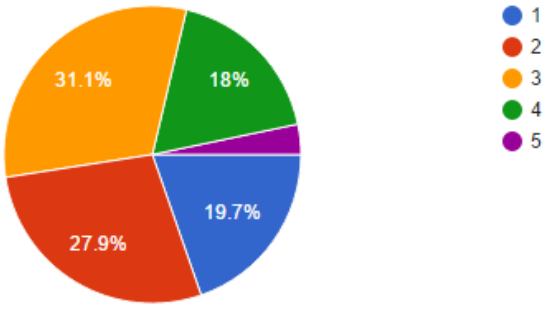




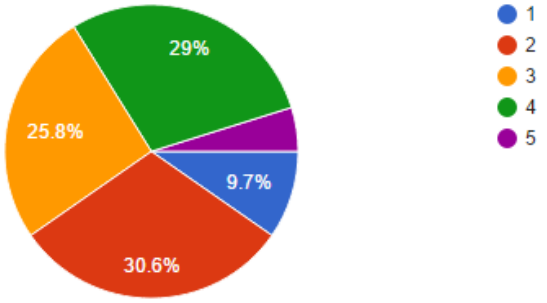
Kysymykset tietoturvauhista pilvipalveluita käyttäville PK-yrityksille



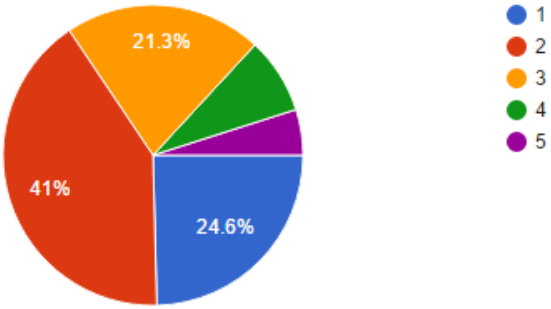
Kuinka suureksi uhkaksi koette mahdollisten toimialan standardien puutteen pilvipalveluille (1 = en ollenkaan, 5 = erittäin suureksi)
(61 responses)



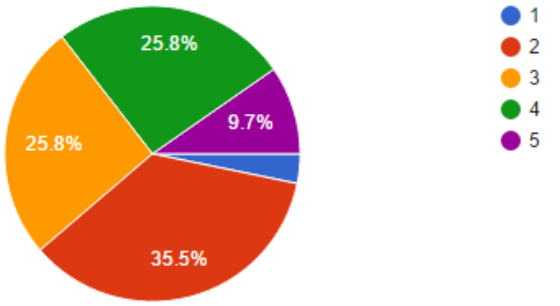
Kuinka suureksi uhkaksi koette kustannusten nousun pilvipalvelun joutuessa hyökkäyksen kohteeksi (1 = en ollenkaan, 5 = erittäin suureksi)
(62 responses)



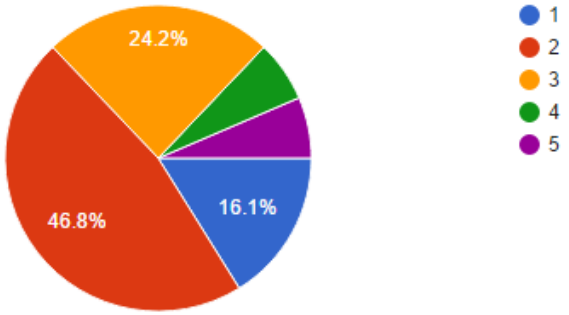
Kuinka suureksi uhkaksi koette pilvipalvelun käytön monimutkaisuuden (1 = en ollenkaan, 5 = erittäin suureksi)
(61 responses)



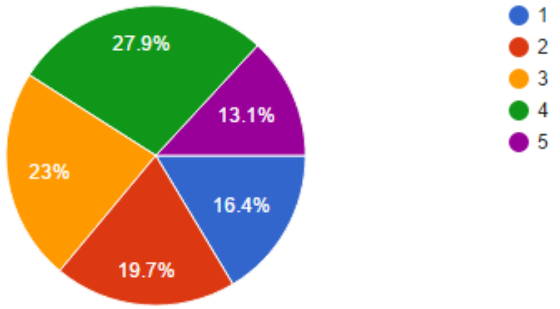
Kuinka suureksi uhkaksi koette tietomurron yrityksen käyttämää pilvipalvelua kohtaan (1 = en ollenkaan, 5 = erittäin suureksi)
(62 responses)



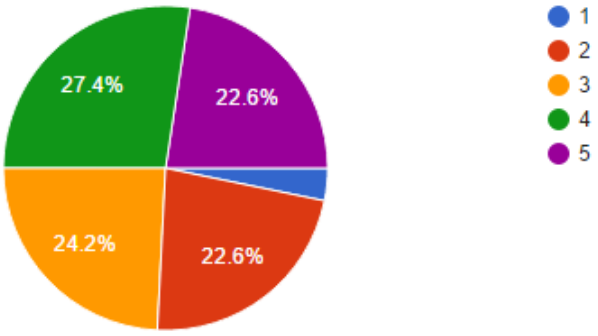
Kuinka suureksi uhkaksi koette Suomen tai muun valtion vakoilun (1 = en ollenkaan, 5 = erittäin suureksi)
(62 responses)



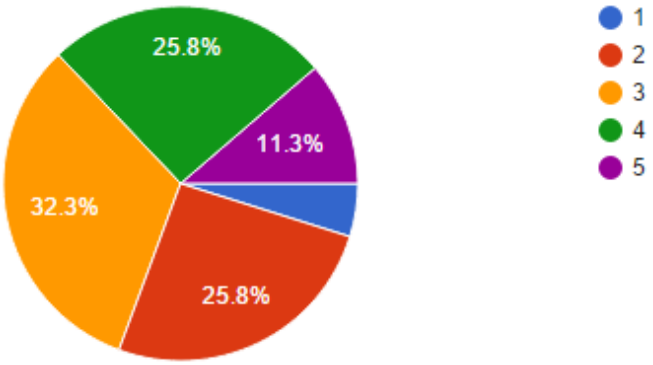
Kuinka suureksi uhkaksi koette pilvipalveluiden palvelimien sijainnin muussa maassa kuin Suomessa (1 = en ollenkaan, 5 = erittäin suureksi)
(61 responses)



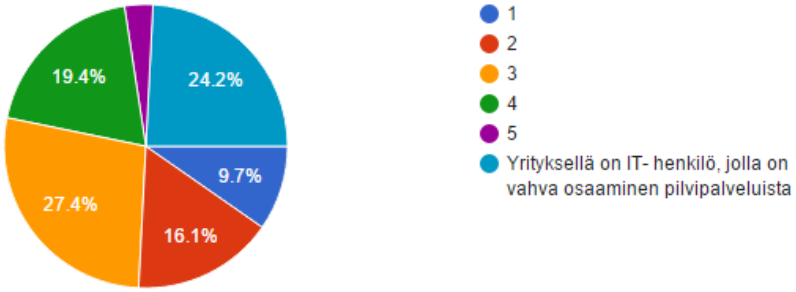
Kuinka suureksi uhkaksi koette pilvipalveluiden riippuvuuden internet-yhteydestä (1 = en ollenkaan, 5 = erittäin suureksi)
(62 responses)



Oletteko huolissanne yksityisyyden heikkenemisestä käyttäessä pilvipalveluita (1 = en ollenkaan, 5 = erittäin paljon)
(62 responses)



Kuinka suureksi uhkaksi koette sen, että yrityksellä ei ole IT- henkilöä jolla on vahva osaaminen pilvipalveluista (1 = en ollenkaan, 5 = erittäin suureksi)
(62 responses)

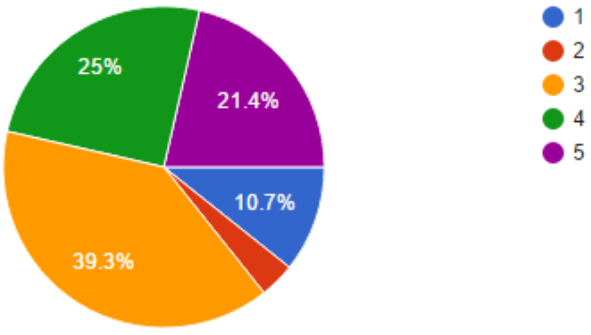


Oletteko huolissanne jostain muusta liittyen pilvipalveluihin? (2 responses)

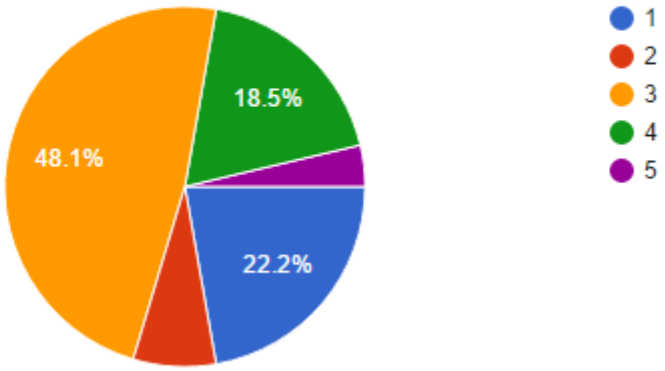
Salasanojen vaihtamisen muistamisen
En

Kysymykset pilvipalveluiden tietoturva PK-yrityksille, jotka eivät käytä pilvipalveluita

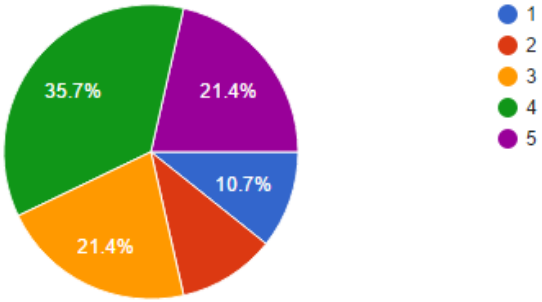
Kuinka suureksi uhkaksi koette pilvipalvelun palvelukatkoksen (1 = en ollenkaan, 5 = erittäin suureksi)
(28 responses)



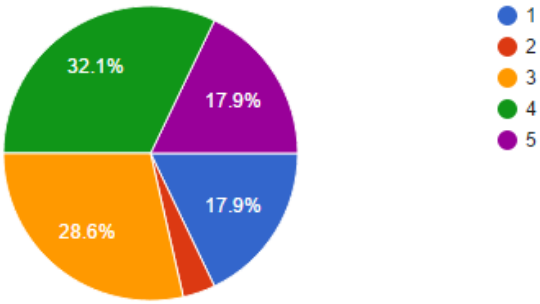
Toimialan standardien puute pilvipalveluille (27 responses)



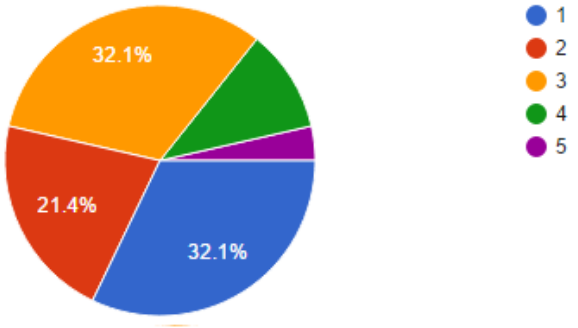
Kuinka suureksi uhkaksi koette kustannusten nousun pilvipalvelun joutuessa hyökkäyksen kohteeksi (1 = en ollenkaan, 5 = erittäin suureksi)
(28 responses)



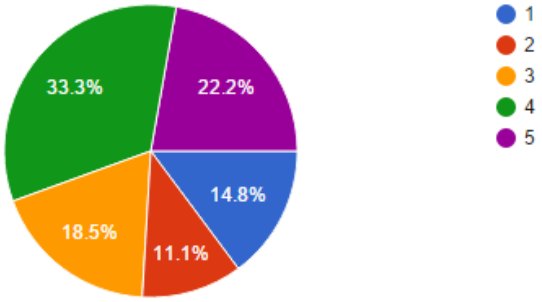
Kuinka suureksi uhkaksi koette tietomurron yrityksen käyttämää pilvipalvelua kohtaan (1 = en ollenkaan, 5 = erittäin suureksi)
(28 responses)



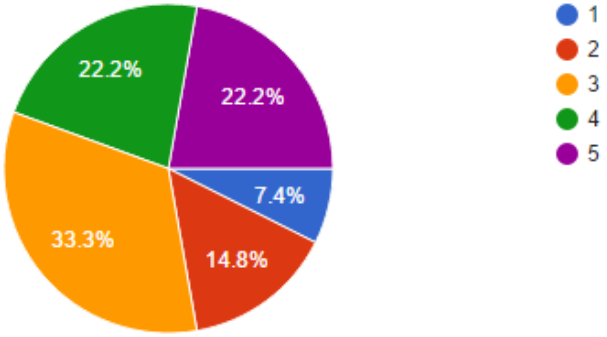
Kuinka suureksi uhkaksi koette Suomen tai muun valtion vakoilun (1 = en ollenkaan, 5 = erittäin suureksi)
(28 responses)



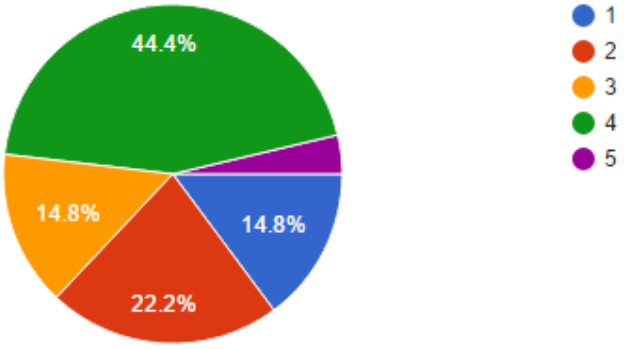
Kuinka suureksi uhkaksi koette pilvipalveluiden palvelimien sijainnin muussa maassa kuin Suomessa (1 = en ollenkaan, 5 = erittäin suureksi)
(27 responses)



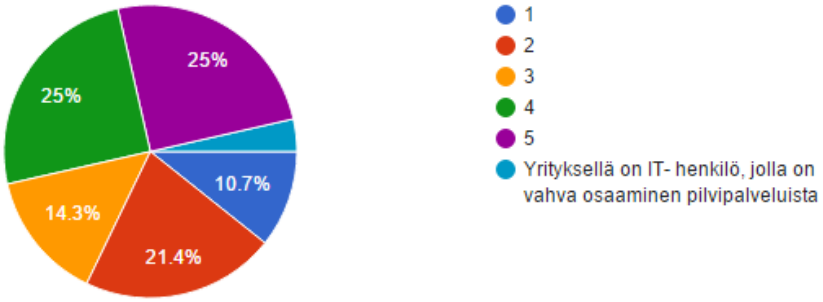
Kuinka suureksi uhkaksi koette pilvipalveluiden riippuvuuden internet-yhteydestä (1 = en ollenkaan, 5 = erittäin suureksi)
(27 responses)



Oletteko huolissanne yksityisyyden heikkenemisestä käyttäessä pilvipalveluita (1 = en ollenkaan, 5 = erittäin paljon)
(27 responses)



Kuinka suureksi uhkaksi koette sen, että yrityksellä ei ole IT- henkilöä jolla on vahva osaaminen pilvipalveluista (1 = en ollenkaan, 5 = erittäin suureksi)
(28 responses)



Oletteko huolissanne jostain muusta liittyen pilvipalveluihin? (1 response)

Vastuukysymykset mahdollisisssa ongelmatilanteissa