Pilvipalveluiden turvallisuus

Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä

Viestintävirasto
Kyberturvallisuuskeskus

Sisällysluettelo

Johdanto

Tämä on Viestintäviraston Kyberturvallisuuskeskuksen tuottama raportti pilvipalveluiden tietoturvasta. Raportti on tarkoitettu erityisesti yritysten ja muiden organisaatioiden avuksi pilvipalveluiden turvallisuutta arvioitaessa ja palveluntoimittajaa valitessa.

Raportissa keskitytään pilvipalveluntarjoajan turvallisuuteen ja valintaan vaikuttaviin tekijöihin. Esimerkiksi pilvipalveluntarjoajan fyysinen ja tekninen turvallisuus sekä henkilöstön turvaluokitukset tulisi huomioida jo palveluntarjoajaa valitessa.

Raportti käsittelee myös pilveen vietävän tiedon ja laskennan valintaa ja rajausta. Esimerkiksi henkilötietolaki asettaa rajoituksia pilveen vietävälle tiedolle. Myös turvaluokiteltu tieto edellyttää tiettyjä vaatimuksia sitä tallentavalta järjestelmältä.

Raportin sisältö

Raportti alkaa pilvipalvelujen määrittelyllä. Pilvipalvelut on laaja käsite, johon sisältyy muun muassa useita erityyppisiä toteutuksia, kuten infrastruktuuri- tai alustaresurssipalvelut.

Raportin toisessa osiossa käsitellään pilvipalveluiden toteutuksesta aiheutuvia käytäntöjä, kuten tiedon elinkaari ja tiedon omistajuus.

Raportin kolmas osio käsittelee pilveen tallennettavaan tietoon liittyviä lakien ja sopimusten aiheuttamia rajoituksia.

Raportin neljäs osa keskittyy tekijöihin, joiden perusteella pilvipalveluntarjoajan fyysistä ja teknistä turvallisuutta voi arvioida.

Raportin viides osa käsittelee muita palveluntarjoajan valintaan vaikuttavia tekijöitä, kuten palveluntarjoajan kokoa ja palvelun jatkuvuutta.

Raportin viimeisessä osassa summataan asiat, jotka on hyvä huomioida pilvipalveluntarjoajan kanssa laadittavassa sopimuksessa.

Määritelmät

Pilvipalvelut eli tietotekniikan resurssipalvelut ovat verkkoyhteyden välityksellä tarjottavia tietojenkäsittely- ja -tallennuspalveluita sekä tietoliikennepalveluita. Rajanveto pilvipalveluiden ja perinteisten etäkäytettävien tietoteknisten palveluiden välille on loppukäyttäjän näkökulmasta hankalaa, mutta palveluiden toteuttamisen, riskienhallinnan ja tietoturvallisuuden näkökulmasta on selviä eroja.

Pilvipalveluilla tarkoitetaan palvelumallia, jossa helposti säädettäviä usean käyttäjän kesken jaettuja tietoteknisiä resursseja tarjotaan tietoverkkojen yli. Yhteydensaanti pilvipalveluun on tehty mutkattomaksi. Palvelun toiminnallisuuksia voidaan kytkeä käyttöön ja pois käytöstä sekä yhdistää toisiin palveluihin nopeasti ja helposti käyttäjän tarpeen mukaan. Pilvipalvelun käytön ja kuormituksen seuranta on tehty helpoksi ja läpinäkyväksi. Tämä yhdessä helpon resurssien hallinnan kanssa mahdollistaa toiminnan ja kulujen optimoinnin [1].

Pilvipalvelut voidaan luokitella muun muassa sen mukaan, miten muotoiltua palvelua (palvelumallit) tarjotaan ja miten palvelun hankinta on järjestetty (hankintamallit). Näiden luokitusten suhdetta havainnollistetaan kuvassa 1. Pilvipalveluita voidaan tuottaa minä tahansa palvelu- ja hankintamallien yhdistelmänä.

Ohjelmistoresurssi-palvelumalli (engl. Software as a Service, SaaS) on yksinkertaisin ottaa käyttöön, mutta toisaalta käyttäjällä on vähän mahdollisuuksia vaikuttaa palvelun toteutukseen ja erityisesti sen tekniseen tietoturvaan. Ohjelmistoresurssipalvelussa palvelun tuottaja antaa asiakkaidensa käyttöön valikoituja verkon yli käytettäviä ohjelmistoja. Tyypillisiä ohjelmistoresurssipalveluita ovat verkkoselaimella käytettävät toimisto-ohjelmistot ja tallennussovellukset.

Alustaresurssipalveluissa (engl. Platform as a Service, PaaS) palvelun tuottaja tarjoaa valitsemaansa apuohjelmien ja sovelluskehitysympäristön kokonaisuutta. Palvelun käyttäjä voi toteuttaa alustan päälle omat ohjelmistonsa ja niihin omat tietoturvaratkaisunsa. Palvelun toteuttavien fyysisten- tai virtuaalisten tietojärjestelmien käyttöjärjestelmiin käyttäjät eivät kuitenkaan voi vaikuttaa.

Suurimman toimintavapauden, mutta myös suurimman vastuun käyttäjälle tarjoaa infrastruktuuriresurssipalvelu (engl. Infrastructure as a Service, IaaS). Palvelun tarjoaja antaa asiakkaidensa käyttöön yksinkertaisesti tietokoneiden laskentatehoa, tallennustilaa ja verkkoyhteyksiä. Asiakas saa itse valita tai toteuttaa kaikki ohjelmistot ja loogiset yhteydet tietokoneiden käyttöjärjestelmistä lähtien.

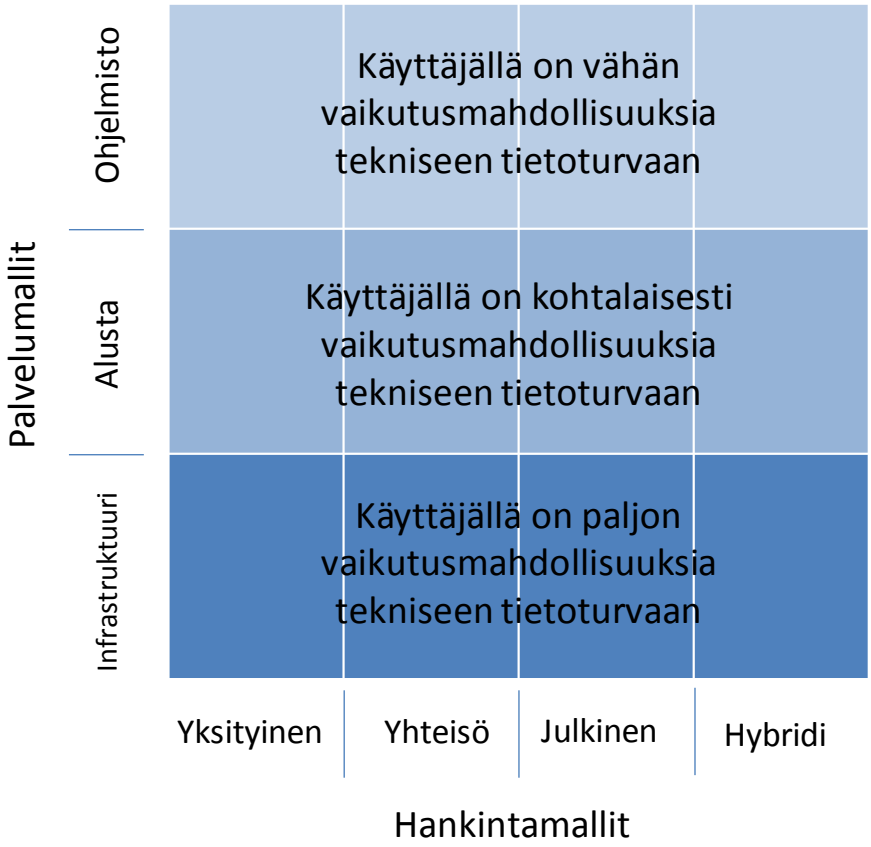
Joskus puhutaan myös verkkoliikenneresurssipalvelusta (engl. carrier cloud). Sillä tarkoitetaan infrastruktuuriresurssipalvelua, jossa verkkoinfrastruktuurin kapasiteettiin ja latenssiin on kiinnitetty erityistä huomiota.

Muita palvelumalleja, jotka ovat palautettavissa edellä mainittuihin, ovat esimerkiksi:

- Häiriöistä palautuminen (Disaster Recovery as a Service)
- Verkkoresurssit (Network as a Service)
- Lokien kirjaus (Logging as a Service)
- Maksujen käsittely (Payments as a Service)

[1] Määritelmä on omaksuttu Yhdysvaltain standardointi- ja teknologiavirasto NIST:n julkaisusta SP800-145.

- Tietoturva (Security as a Service).



Kuva 1 Palvelu- ja hankintamallit

Pilvipalveluiden hankintatapa jaetaan yleensä neljään pääluokkaan: yksityinen, yhteisö, julkinen ja hybridi.

Yksityinen pilvipalvelu on tietyn organisaation vain omaan tarpeeseensa hankkima ja käyttämä. Yksityinenkin pilvipalvelu voi olla käyttäjäorganisaation ulkopuolelta hankittu ja tuotettu. Tällöin toinen osapuoli tuottaa palvelun yksinomaan sen tilanneelle organisaatiolle.

Yhteisöpilvipalvelun infrastruktuuri on ennalta rajatun organisaatiojoukon omaan tarpeeseensa hankkima ja käyttämä. Käyttäjäyhteisöllä on tyypillisesti yhteisiä tavoitteita tai vaatimuksia pilviratkaisulle. Yhteisöpilvipalvelua voi tuottaa yksi tai useampi yhteisön jäsenistä, jokin kolmas osapuoli, tai näiden yhdistelmä.

Julkisen pilvipalvelun käyttäjäjoukkoa ei ole ennalta rajattu. Palvelun tuottaja pyörittää palvelun infrastruktuuria omissa tiloissaan.

Hybridipilvipalvelussa yhdistellään muilla hankintamalleilla tuotettuja pilvipalveluita käyttäen sovittuja rajapintoja. Eräs tyypillinen hybridipalvelu on yksityinen pilvipalvelu, jonka käsittelykapasiteetin hetkellisesti loppuessa lisäkapasiteettia otetaan käyttöön julkisesta pilvipalvelusta.

Pilvipalveluiden toimintaan liittyviä käytäntöjä

Pilvipalvelun toteutus riippuu sekä pilvipalvelua tarjoavan yrityksen ominaisuuksista että palvelusopimuksessa sovitusta palvelutasosta. Erilaisten toteutusten ja palvelusopimusten monimuotoisuus tekee vaikeaksi antaa yksiselitteisiä vastauksia pilvipalveluihin liittyvissä kysymyksissä. Esimerkiksi pilvipalveluun tallennetun tiedon maantieteellinen sijainti tai pilvipalveluun tallennetun tiedon elinkaari riippuvat palveluntarjoajasta ja palvelusopimuksesta.

Tässä osiossa käydään läpi tyypillisimpiä pilvipalveluiden tekniikkaan, lainsäädäntöön ja tietosuojaan liittyviä käytäntöjä. Niiden on tarkoitus auttaa lukijaa kiinnittämään huomiota pilvipalveluntarjoajien välisiin eroihin, ja ohjata lukija tekemään liiketoiminnan kannalta oikeita kysymyksiä pilvipalveluntarjoajalle.

1. Tiedon omistajuus ja käyttöoikeudet

Pääsääntö on, että tiedon omistajuus ja siihen liittyvät oikeudet ovat sillä henkilöllä tai organisaatiolla, joka on tuottanut tiedon alun perin esimerkiksi laatimalla pilveen tallennetun asiakirjan. Omistuksen mahdollinen siirtyminen ja käyttöoikeudet määräytyvät sovellettavan lainsäädännön ja sopimusten perusteella.

Palveluntarjoajan kanssa on hyvä sopia palveluehdoista tarkasti ja palvelun ehdot on hyvä lukea huolella. Erityisen tärkeää on huomioida tiedon hallintaan ja käsittelyoikeuteen liittyviä seikkoja. Jos yritys säilyttää pilvessä muun tiedon ohella myös liikesalaisuuksiaan, on varmistettava etteivät henkilöt, joilla ei ole oikeutta käsitellä näitä tietoja, pääse niihin käsiksi.

Käsittelyoikeuksien säilyminen vain organisaatiolla itsellään on hyvä varmistaa sopimuksin.

Palvelua käyttöönottavan organisaation voi olla järkevää sisällyttää sopimukseen mahdollinen auditointioikeus sen tarkastamiseen, että yrityksen tietoja käsitellään laaditun palvelusopimuksen mukaisesti. Arkaluonteisen tai salassa pidettävän tiedon käsittelyyn tulee kiinnittää erityistä huomiota. Tällöin arvioitavaksi voi tulla myös se, pitääkö yrityksen ja palveluntarjoajan välillä solmia salassapitoon liittyvä oma salassapitosopimus.

2. Tiedon elinkaari

Tiedon elinkaari tietojärjestelmissä alkaa siitä kun tieto luodaan ja päättyy siihen kun se ja kaikki siitä mahdollisesti tehdyt kopiot tuhotaan. Pilvipalvelussa oleva tieto on joko luotu itse pilvipalvelussa tai se on luotu käyttäjän omalla työasemalla tai tuotu siihen muualta ja ladattu pilveen.

Pilvipalvelussa tieto on tallennettuna useassa paikassa samaan aikaan eri järjestelmien muistissa, ulkoisissa massamuisteissa tai tietokannoissa. Samaan aikaan se voi olla myös liikkeellä tietovirrassa. Jos tiedolla on useita käsittelijöitä, on mahdollista että siitä on useampia kopioita käsittelijöiden paikallisissa tietojärjestelmissä tai heidän muissa tallennusvälineissään. Samoin jos tiedosto lähetetään jollekulle esimerkiksi sähköpostin välityksellä, siitä syntyy uusi kopio jolla on oma elinkaarensa joka riippuu sen vastaanottajan toimista.

Pilvipalveluiden toiminta varmistetaan useimmiten varmuuskopioinnin tai palvelun kahdentamisen avulla. Varmuuskopiointi tarkoittaa yleensä sitä, että palveluiden tietosisältö kopioidaan turvalliseen paikkaan. Palvelun kahdentaminen tarkoittaa koko palvelun replikointia toiseen paikkaan siten, että palvelu on ajan tasalla ja käytettävissä eri

paikoissa samanaikaisesti. Pilvipalveluiden varmuuskopiot tai kahdennukset voivat sijaita missä vain maapallolla, missä palveluntarjoajalla tai sen käyttämällä alihankkijalla on oma palvelinkeskus tai muuta siihen vaadittavaa kapasiteettia käytössään. Maantieteellistä hajautusta käytetään palvelun toiminnan varmistamiseksi sekä resurssien kohdentamiseksi.

Pilvipalvelun käyttäjän tuleekin varmistaa, missä hänen tallentamansa tieto sijaitsee koko sen elinkaaren aikana. Tiedon sijainnilla on vaikutusta muun muassa seuraavasti:

- Mitä tietoa kyseiseen palveluun saa tallettaa oman maan lakien puitteissa?
- Minkä maan lakia sovelletaan mahdollisissa poikkeustapauksissa?
- Onko jonkin maan viranomaisilla oikeus tutkia tätä tietoaineistoa[2]?

Tieto liikkuu eri tallennuspaikkojen välillä varmuuskopioinnin tai muun palveluun liittyvän hallinnollisen toiminnan yhteydessä tai käyttäjän käsitellessä sitä. Tällöin tieto liikkuu valon nopeudella mantereiden välillä ja tietosisältö voi käydä matkansa varrella sijaitsevien tietoliikennelaitteiden välimuistissa.

Vuonna 2013 julkisuuteen tulleiden tietojen mukaan eri maiden tiedustelupalvelut ovat salakuunnelleet mantereiden välistä tietoliikennettä sekä suurten palveluntarjoajien palvelinkeskusten välistä liikennettä. Jos itse tieto tai tietoliikenne ei ole salattu, se kulkee verkoissa selväkielisenä ja on luettavissa kolmansien osapuolten toimesta. Viimeaikainen kehitys onkin johtanut siihen, että yhä useammat pilvipalveluiden tarjoajat ovat kiinnostuneet asiakkaidensa tiedon turvaamisesta ja salauksen käyttö palveluiden ja palvelinkeskusten välisessä tietoliikenteessä on yleistymässä[3].

Kun tietoa poistetaan tietojärjestelmästä tavanomaisin menetelmin, se ei yleensä lakkaa olemasta. Käyttöjärjestelmien yleinen toimintamalli on että, kun esimerkiksi tiedosto poistetaan tallennusmedialta, sitä ei pyyhitä pois vaan ainoastaan tieto siitä poistetaan järjestelmän kirjanpidosta. Tiedoston sijainti tallennusjärjestelmässä siis merkitään vapaaksi, jolloin järjestelmä voi käyttää tiedoston käytössä olleen tilan muun tiedon tallentamiseen. Poistetuksi merkityn tiedoston sisällön voidaan kuitenkin lukea järjestelmästä erinäisillä työkaluilla niin kauan kuin sen kohdalle levypinnalle ei ole kirjoitettu jotain muuta tietoa.

Jos haluaa varmistua tiedon todellisesta tuhoamisesta, pitää se tehdä erillisellä ohjelmistolla joka ylikirjoittaa poistettavan tiedoston kohdan levypinnasta satunnaisilla merkeillä.

Pilvipalveluissa noudatetaan erilaisia käytäntöjä asiakkaan tiedon tuhoamisen suhteen. Kannattaakin tarkistaa, mitä tiedolle oikeasti tapahtuu, kun se poistetaan käyttäjän toimesta. Kannattaa myös tarkistaa mitä tiedolle tapahtuu, jos asiakassuhde päättyy tai tapahtuu jokin muu poikkeuksellinen tapahtuma, joka vaikuttaa palvelun tarjoajan toimintaan. Allokoidaanko asiakkaalta käyttöön vapautuneet resurssit seuraavalle käyttäjälle samaan tapaan kun em. käyttöjärjestelmäesimerkissä vai puhdistetaanko ne ensin vanhasta tiedosta ylikirjoittamalla tai muulla tavalla.

Kannattaa selvittää, miten elinkaarensa päähän tullut pilvipalvelun fyysinen laitteisto, johon on tallennettu asiakkaan

[2] https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland [25.8.2014]

[3] https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what [25.8.2014]

tietoja, poistetaan käytöstä: ylikirjoitetaanko laitteistojen tietosisällöt turvallisesti, tuhotaanko ne mekaanisesti vai laitetaanko ne suoraa kiertoon.

3. Missä pilveen tallennetut tiedot säilytetään?

Pilvipalveluun tallennetut tiedot voivat sijaita palvelun tarjoajasta riippuen yhdessä tai useammassa eri paikassa yhdessä tai useammassa eri maassa. Yleisesti ottaen pienemmät toimijat talletettavat tiedot paikallisesti lähellä omaa toimipistettään, jossa heillä voi olla oma konesali tai palvelinkeskus, tai he voivat vuokrata näitä resursseja ulkoiselta palveluntarjoajalta. Pilvipalvelun tarjoaja voi myös vuokrata resursseja suuremman toimijan pilvipalvelusta, ja ylläpitää siellä koko palvelua tai osaa sen toiminnallisuudesta.

Suuremmilla toimijoilla on omat konesalinsa tai palvelinkeskuksensa. Näitä voi olla eri maissa ja eri mantereilla. Yksittäisen palvelun käyttäjän voi olla mahdotonta sanoa, missä hänen tietonsa kulloinkin liikkuu tai on tallennettuna. Jos asialla on merkitystä käyttötarkoituksen kannalta, pitää se selvittää palveluntarjoajan kanssa. Osa suurista palveluntarjoajista pyrkii keskittämään pilvipalveluidensa toiminnan maantieteellisesti esimerkiksi siten, että eurooppalaisen käyttäjän tiedot pidetään Euroopassa sijaitsevissa palvelinkeskuksissa[4]. Näissäkin tapauksissa palvelun ylläpitotyötä voidaan tehdä kyseisen maantieteellisen alueen ulkopuolelta. Myös joitain osia asiakkaan tiedoista saattaa tulla tallennetuksi hänen oman kotialueen ulkopuoliseen palvelinkeskukseen, jos asiakas esimerkiksi itse käyttää palvelua oman kotialueensa ulkopuolella.

Palvelinkeskuksia sijoitetaan maantieteellisesti hajalleen ja asiakkaiden tiedot kopioidaan useampaan kuin yhteen keskukseen. Näin toimitaan erityisesti siksi, että jos yksi piste lakkaa toimimasta, palvelu voidaan keskeytyksettä tarjota toisesta palvelinkeskuksesta. Maantieteellisellä sijoittelulla on myös vaikutusta palvelun tarjoajan sekä käyttäjän toimintaan esimerkiksi sovellettavan lainsäädännön vuoksi. Samoin tällä voidaan jakaa tietoliikenteen kapasiteettiä ja ratkaista varmuuskopiointiin liittyviä ongelmia.

4. Pilvipalveluun tallennetun tiedon erottelu eri asiakkaiden välillä

Asiakkaiden tiedot voidaan erottaa pilvipalveluissa toisistaan loogisesti tai fyysisesti. Erottelu voidaan tehdä niin asiakkaan käyttämälle palvelun toimintalogiikalle kuin siinä käsitellylle ja tallennetulle tiedollekin, jos ne ovat toisistaan erillään.

Erottelua voidaan tehdä esimerkiksi seuraavin tavoin:

1. Usea asiakas käyttää samaa ohjelmistoa, mutta heidän käyttöympäristö on erotettu toisistaan ohjelmallisesti pääsynhallinnan avulla.

2. Jokaisella asiakkaalla on käytössä oma instanssi käytettävästä ohjelmasta ja ne toimivat samalla virtuaalisella tai fyysisellä palvelimella.

3. Jokaisella asiakkaalla on käytössä oma instanssi ohjelmasta, joka toimii omalla virtuaalisella tai fyysisellä palvelimella.

Fyysinen erottelu (kohta 3.) on näistä turvallisin. Loogisesti erotellussa ympäristössä on riski että asiakkaiden tietosisältö paljastuu toiselle asiakkaalle tai kolmannelle osapuolelle esimerkiksi oh-

[4] http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Geo_Boundaries.htm [25.8.2014]

jelmistovirheen, virheellisen asetuksen tai muun ylläpitotoimen johdosta.

Taustaa:

Pilvipalveluissa digitaalisessa muodossa oleva tieto on tallennettuna erilaisille massamuisteille. Toimijan ja palvelun koosta riippuen, massamuisti voi olla esimerkiksi yksittäinen kiintolevy, useasta levystä koostettu klusteri tai useasta klusterista koostettu ryhmä.

Suurilla pilvipalveluntarjoajilla tallennuskapasiteetti on valtava, minkä vuoksi niitä kutsutaan palvelinfarmeiksi. Perinteisissä tietokoneissa massamuistia hallitaan levyjärjestelmän avulla, joka on abstraktio fyysisestä tallennuslaitteesta ja jota ohjataan käyttöjärjestelmän avulla. Levyjärjestelmän peruskomponentteja ovat kansiot ja hakemistot. Suurissa pilvitallennusalustoissa massamuistia hallitaan olio-perusteisella arkkitehtuurilla, jossa jokainen tiedosto on objekti, johon liittyy sitä kuvaava metadata.

Minkälaisia tietoja pilveen voi ja kannattaa tallentaa?

Pilvipalveluihin voi tallentaa lähes rajattomasti ja mitä vain tietoa, kunhan tallennettu tietoaineisto ei loukkaa pilvipalveluntarjoajan sopimusehtoja, lainsäädäntöä tai muita sopimuksia, joihin pilvipalvelun käyttäjäorganisaatio on sitoutunut. Lisäksi tallennettavalle tiedolle on hyvä tehdä riski-hyöty-arvio.

5. Tallennettavaan tietoon kohdistuvia tai sen aiheuttamia rajoituksia

Pilvipalveluiden tarjoajat asettavat palveluiden käytölle sääntöjä ja rajoituksia. Näitä ovat muun muassa kiellot käyttää palvelua laittomiin tai moraalittomiin tarkoituksiin sekä rajoitteet palvelun resurssien käyttöön. Säännöt ja rajoitukset ovat aina palvelukohtaisia. Niitä voidaan tarkentaa palvelusopimuksessa tai palvelun käyttäjä hyväksyy ne käyttöehtoina rekisteröityessään palveluun.

Pilvipalveluiden käyttöä rajoittavat lähinnä sopimusehdot ja osaltaan myös lainsäädäntö. Näiden soveltuvuutta tulee arvioida kuitenkin aina tapauskohtaisesti. Pilvipalveluiden käyttöön ryhdyttäessä organisaation on hyvä varmistaa myös omat muut sopimusvelvoitteensa. Sopimukset voivat rajoittaa esimerkiksi tietojen siirtämistä ulkomaille. Jos käyttöön suunnitellun järjestelmän on toteutettava jonkin kriteeristön[5] mukainen suojaus- tai turvallisuustaso, täytyy ensin tutkia täyttääkö käytettäväksi suunniteltu pilvipalvelu nämä vaatimukset.

[5] Esimerkiksi PCI, ISO 27001, KATAKRI, Vahti

6. Riski-hyöty-arvio

Jos käyttötapauksessa ei ole edellä mainitun kaltaisia ulkoisia määräaviä tekijöitä tai ne eivät aseta estettä pilvipalvelun käytölle, on palvelun käyttö oman harkinnan ja riskianalyysin varassa.

Riskianalyysissä tulee ottaa huomioon, että pilvipalveluissa olevaa tietoa talletetaan tai käsitellään jonkun muun ylläpitämässä palvelussa. Tällaisessa tilanteessa on mahdollista, että tietoa katoaa, vääristyy, tuhoutuu tai joutuu tuntemattoman kolmannen osapuolen haltuun. Organisaatioiden on hyvä harkita tapauskohtaisesti, kuinka suuria nämä riskit ovat ja mitä ne tarkoittaisivat omassa tilanteessa:

- Onko palvelun käytöstä saatava hyöty riittävän suuri tilanteessa olevaan riskiin nähden?
- Ovatko kyseessä henkilökohtaiset asiat vai oma liiketoiminta?

Kolmanteen osapuoleen liittyvän riskin vuoksi ei kannata sokeasti laittaa kaikkea dataa ja laskentaa pilveen, vaikka se muutoin olisikin mahdollista. Pilvessä tietojen ja laskennan luottamuksellisuus, eheys, saatavuus tai kiistämättömyys eivät välttämättä ole yhtä hyvällä tasolla kuin tiettyä tarkoitusta varten rakennetuissa tietojärjestelmissä. On siis erittäin tärkeää valita ja rajata pilveen vietävä data ja laskenta, sillä läpikotaisesti ymmärrettyä ja loppuun asti harkittua tietojenkäsittelyä on helpompi hallita.

Riski–hyöty-arvioinnilla voidaan analysoida, mitä tietoja pilveen kannattaa siirtää ja mitkä tiedot olisi hyvä säilyttää organisaation omilla paikallisilla palvelimilla. Pilvipalveluiden käyttöönotto ja pilveen tallennettavien tietojen valinta tulisi aina perustua harkittuun päätökseen.

Pilvipalveluntarjoajan turvallisuuteen vaikuttavia tekijöitä

Pilvipalveluiden turvallisuuteen liittyy yllättävän monta tekijää, jotka eivät välttämättä näy loppukäyttäjälle. Palvelun turvallisuuteen vaikuttaa teknisen toteutuksen lisäksi myös sitä ympäröivä maailma. Esimerkiksi palvelun ylläpitohenkilöstöllä saattaa olla pääsy käyttäjän tietoihin. Lisäksi turvallisuuteen vaikuttaa ohjelmistojen, laitteistojen ja fyysisen ympäristön huolto- ja toimittajaketjut.

Kun arvioidaan pilvipalvelun turvallisuutta, on syytä arvioida myös palvelun toteutusta sekä palveluntarjoajan toimintaa. Vakavasti otettavat pilvipalveluiden tarjoajat ymmärtävät nykyään käyttäjien tarpeen varmistaa toiminnan turvallisuus ja usein ne pyrkivätkin tekemään toiminnastaan mahdollisimman läpinäkyvää.

Kannattaa tutustua mahdollisiin sertifiointeihin tai kolmannen osapuolen tekemiin auditointeihin, sekä palveluntarjoajan itse toimittamiin dokumentteihin palvelun käytännön toimista ja teknisistä toteutuksista. Kaikkia yksityiskohtia palveluntarjoajat eivät voi kuitenkaan paljastaa kilpailukyvyn säilyttämiseksi ja turvallisuuden ylläpitämiseksi.

Vinkki:

Jos on mahdollista, kannattaa varata oikeus auditoida pilvipalveluntarjoaja. Suuremmilla palveluntarjoajilla tämä ei yleensä ole mahdollista, mutta usein he ovat kuitenkin itse teettäneet auditoinnin kolmannella osapuolella, ja auditointitulokset voivat olla asiakkaan saatavilla.

7. Tekninen turvallisuus

Pilvipalvelun teknisen turvallisuuden kannalta olennaisia asioita ovat käytettävät teknologiat, toimintamallit ja periaatteet. Pilvipalvelun syvällisempää toimintaa voi olla mahdotonta tutkia, mutta jonkinlaisen kuvan saa palveluntarjoajan toimittamien teknisten tietojen avulla, mahdollisten sertifiointien tai kolmannen osapuolen tekemien auditointien tulosten perusteella sekä tutkimalla palvelua käyttäjälle näkyviltä osilta. Varovaisia johtopäätöksiä voidaan tehdä myös palveluntarjoajan muiden tuotteiden ja toimintakulttuurin ja maineen perusteella.

Turvallisen palvelun tärkeimpiä ohjelmistolle asetettavia vaatimuksia on, että käyttäjänhallinta on toteutettu luotettavasti. Tähän kuuluu palveluun rekisteröinti, rekisteröidyn käyttäjän tunnistaminen sekä käyttöoikeuksien hallinnointi. Käyttäjänhallinnan tärkein tehtävä on jakaa palvelun- ja niin ikään tiedon käyttöoikeuksia niille henkilöille, joille se kuuluu ja estää muiden asiaton käyttö.

Pilvipalveluntarjoajan ohjelmistojen päivityskäytännöt on myös hyvä selvittää. Yleensä etenkin suurilla pilvipalveluntarjoajilla ohjelmistopäivitysten käytännöt on hyvin järjestetty ja resursoitu. Asiakkaan tulee kuitenkin itse varmistaa, että päivitysmenettely toimii halutulla tavalla.

Lisäksi pilvipalvelussa, kuten missä tahansa verkkoyhteyttä hyödyntävässä ohjelmistossa, on syytä varmistaa että käytettävät yhteydet on salattu. Näin tiedon liikkuminen oman tietokoneen ja pilvipalvelun välillä on ainakin teoreettisesti suojattu. Selainpohjaista käyttöliittymää käytettäessä salauksen päällä olosta voidaan varmistua protokollan määrittävällä osoitteen etuliitteellä 'https://' tai lukon kuvasta koko osoitekentän edessä.

8. Henkilöstön turvaluokitukset

Henkilökunnalla sekä heidän työtavoillaan ja työkaluillaan on merkittävä rooli. Palvelun turvallisuutta arvioitaessa on tärkeää selvittää, minkälainen palveluntarjoajan henkilöstöpolitiikka on, ja noudatetaanko työnteon prosesseissa alan parhaita käytäntöjä. Tehdäänkö kriittisissä toiminnoissa toimiville henkilöille turvallisuusselvityksiä ja seurataanko käytännön toiminnoissa hyväksyttyjä alan standardeja? Palveluntarjoajan tulisi vaatia sama turvallisuuden taso soveltuvin osin kaikilta alihankintaketjuilta ja niiden työntekijöiltä.

Henkilöstöllä, erityisesti ylläpitäjillä ja kehittäjillä, on suora pääsy palvelun toiminnallisuuteen. Järjestelmäylläpitäjät huolehtivat palvelun päivittäisestä toiminnasta ja korjaavat mahdollisia vikatilanteita. Usein heillä on myös pääsy asiakkaan tietosisältöön. Järjestelmän kehittäjät ovat alun alkaen rakentaneet palvelun toiminnallisuuden ja tuntevat sen yksityiskohtia myöten. Useimmiten samat toimijat toimittavat myös päivityksiä ja muita korjauksia kyseisiin ohjelmistoihin.

On myös paljon muuta ylläpitohenkilöstöä, jotka toimivat välillisesti tai välittömästi palveluun kuuluvien tietojärjestelmien parissa tai läheisyydessä ja joilla on mahdollisuus vaikuttaa palvelun toimintaan.

9. Fyysinen turvallisuus

Pilvipalvelun fyysisellä ympäristöllä on myös suuri merkitys palvelun turvallisuuteen ja jatkuvuuteen. Hyvin suojattu ja valvottu ympäristö on vähemmän altis tahallisille ja tahattomille vahingoille.

Kulunvalvonnalla varmistetaan, että vain asianomaiset henkilöt asioivat alueella. Näin voidaan suojautua palveluun kohdistuvalta ilkivallalta ja minimoida muutenkin turhat vahingot. Tavanomaisiin poikkeustilanteisiin, kuten sähkön jakelun keskeytykseen, voidaan varautua varavoimalla. Vastaavasti verkkoliikenteen katkeamiseen voidaan varautua käyttämällä kahta erillistä tietoliikenneyhteyttä.

Palveluiden kahdentaminen takaa yleensä palvelun jatkuvuuden poikkeustilanteiden aikana. Jos esimerkiksi koko palvelinkeskuksen toiminta keskeytyy luonnonmullistuksen vuoksi, voidaan palvelua edelleen tarjota toisesta sijainnista.

10. Oma käyttöympäristö

Yksittäinen käyttäjä voi olla tietoturvallisuuden heikoin lenkki. Tämän vuoksi pilvipalvelun käyttöympäristöstä on pidettävä yhtä hyvää huolta kuin minkä tahansa palvelun kohdalla. Käyttöympäristö tarkoittaa koko sitä ympäristöä, jonka avulla pilvipalvelua käytetään. Tähän sisältyy erityisesti käyttäjät ja päätelaitteet, jolta palvelua käytetään sekä mahdolliset erilliset järjestelmät, jotka toimivat pilvipalvelun kanssa.

Käyttäjät tulee ohjeistaa pilvipalvelun turvalliseen käyttöön. Perinteinen turvallisuus oman päätelaitteen ja internetpalvelun käytön suhteen on tärkeää myös pilvipalvelua käytettäessä. Tärkeää on myös ohjeistaa mahdolliset rajaukset sen suhteen, mitä tietoa palveluun saa tallentaa, mihin tarkoitukseen sitä saa käyttää sekä millä laitteilla ja mistä käyttöympäristöstä palvelua saa käyttää.

Käyttäjähallinnon on myös oltava kunnossa. Tämä toteutetaan yleensä siten, että pääsynhallintaan sekä käyttöoikeuksien jakamiseen käytetään omaa käyttäjähallintaan käytettävää tietokantaa tai järjestelmää tai käyttäjätunnukset luodaan paikallisesti itse pilvipalveluun. Molemmissa toimintamalleissa on tärkeää että tunnusten luominen ja käyttöoikeuksien jakaminen on mahdollista vain siihen erikseen valtuutetuilla henkilöillä. Näiden henkilöiden tulee

tietää, millä perusteella oikeuksia jaetaan ja kuinka nämä henkilöt tulee tunnistaa ennen tunnusten tai oikeuksien aktivointia.

11. Infrastruktuuriresurssipalvelun turvallisuus

Infrastruktuuriresurssipalvelun asiakas ostaa käytännössä raakaa laskentakapasiteettia, tallennustilaa ja verkkoyhteyksiä ympäristöstä, jossa voi ajaa omia sovellusohjelmia. Ympäristö koostuu joukosta fyysisiä ja loogisia komponentteja, joista suurinta osaa ylläpitää pilvipalveluntarjoaja. Infrastruktuuriresurssipalvelun kokonaisturvallisuus määräytyykin näiden kaikkien komponenttien ja asiakkaan oman sovellusohjelman yhteistoiminnasta. Jos esimerkiksi sovellusohjelman tietoturva on huonolla tasolla ennen pilveen siirtämistä, ei pilvilaskenta sitä tule parantamaan.

Lisäksi infrastruktuuriresurssipalvelun etähallinta mahdollistaa uusia hyökkäysvektoreita. Esimerkiksi vääriin käsiin joutunut etähallintatunnus mahdollistaa pilveen siirretyn laskennan haltuunoton ja tietojen kopioinnin tai tuhoamisen, mikä saattaa johtaa koko yritystoiminnan päättymiseen.[6] Perinteisessä laskennassa tilanne vastaa fyysistä pääsyä palvelintilaan, mutta pilvilaskennassa se saattaa syntyä etähallintatunnuksen menetyksestä. Toinen hyökkäysvektori on pilvipalvelun hallintaan tarkoitetun ohjelmointirajapinnan (englanniksi Application Programming Interface, API) avaimen haltuunotto. API-avaimen avulla voi luoda uusia palveluinstansseja ja kloonata tai liittää (mount) tallennustilaa. Tämä mahdollistaa esimerkiksi uusien sovellusohjelmien ajamisen, asiakastietojen kopioinnin, pilvipalveluinstanssin hyödyntäminen muihin hyökkäyksiin tai koko virtuaalisen palvelininstanssin tuhoamisen kaikkine tietoineen.[7]

Mahdollisia tietoturvaloukkauksia on myös hankalampi tutkia infrastruktuuriresurssipalvelussa kuin omassa hallinnassa olevilla palvelimilla. Esimerkiksi jos resurssipalvelun instanssi eli virtuaalinen palvelin, käyttää ei-persistenttiä levytilaa, tuhoaa palvelun alasajo kaiken forensiikassa mahdollisesti hyödynnettävän todistusaineiston.

Myös palveluntarjoajan häiriö saattaa tuhota tietoa pysyvästi, minkä vuoksi kriittisestä tiedosta on syytä pitää varmuuskopiota pilvipalvelun ulkopuolella.

Pilvipalvelut haittaohjelmien levityksen apuvälineenä:

Kyberrikolliset ovat alkaneet levittää haittaohjelmia siten, että pahantahtoisesti muokatut verkkosivut ohjaavat käyttäjän lataamaan haittaohjelman tallennustilaa tarjoavasta pilvipalvelusta. Tässä tapauksessa pilvitallennuspalvelua, tai siihen luottavaa muuta palvelua, ei murreta, vaan tallennuspalvelusta tarjoillaan sisältöä normaaliin tapaan.

6 http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan/

7 https://speakerdeck.com/silvexis/bringing-a-machete-to-the-amazon-blackhat-eu-2014

Pilvipalveluntarjoajan valintaan vaikuttavia tekijöitä

Miten voi valita yritykselle tai organisaatiolle sopivan pilvipalvelun? Perinteisesti hankinnassa vaihtoehtojen vertailu tiivistetään hintaan ja sillä saatavaan hyötyyn. Pilvipalvelua hankittaessa on hyvä pohtia palvelusta saatavan hyödyn ja palvelun turvallisuuden lisäksi myös sekä oman että palveluntarjoajan toiminnan jatkuvuutta, palvelutasoja ja palveluntarjoajan kokoa.

12. Palvelun jatkuvuus

Useimmiten palveluntarjoaja sanoutuu irti kaikesta vastuusta koskien palvelun käytön asiakkaalle aiheuttamaa välitöntä ja välillistä haittaa. Kärjistettynä tämä tarkoittaa sitä, että jos palvelu jonain päivänä ei enää olekaan olemassa, asiakas vastaa itse toiminnan jatkuvuudesta, eikä saa korvausta mistään menettämästään aineellisesta tai aineettomasta haitasta. Tämä ei luonnollisesti ole palveluntarjoajana liiketoimintaa tekevän tahon tahtotila, mutta heilläkään ei ole kontrollia kaikesta ja myös he kehittävät toimintaansa.

Yritys saattaa esimerkiksi tulla ostetuksi ja uuden omistajan myötä toiminta voi muuttua. Palveluntarjoaja voi myös itse muuttaa toimintaansa tai ansaintalogiikkaansa asiakkaalle epäedulliseen suuntaan. Mitä paremmin varaudutaan poikkeuksellisiin tilanteisiin, sitä paremmat mahdollisuudet on selviytyä tilanteen osuessa kohdalle. Jos kyseessä on kriittinen tieto, kannattaa siitä pitää varmuuskopio myös muualla kuin pilvessä.

Palvelun käyttäjän omassa toiminnassa voi myös tapahtua ennakoituja tai ennakoimattomia muutoksia. On hyvä miettiä etukäteen, onnistuuko palveluntarjoajan vaihtaminen siten, ettei siitä koidu kohtuutonta haittaa. Tai jos palvelun käyttö halutaan lopettaa, saadaanko tietoaineisto talteen uudelleenkäytettävässä muodossa tai ylipäätään ollenkaan. Suuri osa palvelun jatkuvuuteen liittyvistä kysymyksistä selviää palvelun käyttöehdoista ja muista toiminnan kuvauksista. Niitä voidaan joissain tilanteissa tarkentaa tai jopa muuttaa palveluntarjoajan kanssa tehtävällä palvelusopimuksella.

13. Palvelutasosopimus

Omat vaatimukset palvelun toiminnalle tulee myös huomioida. Nämä määritellään yleensä palvelutasosopimusten (englanniksi Service Level Agreement tai SLA) avulla. Sopimuksessa voidaan kuvata tarkemmin palveluihin liittyvät palvelutasotavoitteet ja yksilöidä palveluntuottajan ja asiakkaan vastuut. Palvelutasosopimuksilla voidaan määritellä erilaisia mittareita ja tavoitteita, joiden alittamisesta voi seurata sanktio.

Tyypillisiä palvelutasosopimuksen avulla määriteltäviä tavoitteita ovat esimerkiksi:

1) Kuinka suuren osan ajasta palvelun luvataan toimivan ja minkälaisilla vasteajoilla?

2) Minkä tasoista käyttäjätukea on saatavilla ja minkälaiset vasteajat ovat eri viikonpäivinä ja vuorokauden aikoina?

3) Missä tietoa säilytetään ja mistä sitä voidaan ylläpitää?

14. Erikokoiset palveluntarjoajat tarjoavat erilaisia etuja

Palvelua ostaessa joutuu punnitsemaan monia kysymyksiä. Onko esimerkiksi suuren ja tunnetun monikansallisen yrityksen tarjoama palvelu luotettavampi kuin pienen paikallisen toimijan? Suuren yrityksen tarjoamassa palvelussa on useita hyviä puolia. Näillä on useimmiten vakaa talouspohja, eikä

toiminnan pitäisi kaatua ainakaan ennakoimattomaan taloudelliseen tilanteeseen. Maineriski epäonnistuessa on sellainen, että toimintaan panostetaan asianmukaisesti. Suuri toimija voi rakentaa ison ja tehokkaan infrastruktuurin ja näin ollen tarjota hyvää palvelua kilpailukykyiseen hintaan. Eri maissa toimivat palvelinkeskukset turvaavat toiminnan jatkuvuuden, vaikka yksittäisessä maassa tai sinne johtavassa runkoverkossa olisi ongelmia.

Toisaalta isossa palveluympäristössä yksittäisen asiakkaan tarpeet saattavat hautautua massan alle. Suuressa ympäristössä on paljon eritasoisia toimijoita tuottamassa ja käyttämässä palvelua, minkä seurauksena riski väärinkäyttöön tai tahattomaan haitan aiheuttamiseen kasvaa. Samoin suuri ympäristö voi olla houkuttelevampi maali haitantekijöille. Lisäksi eri maissa sijaitsevat palvelinkeskukset ovat alisteisia paikalliselle lainsäädölle.

Pienemmällä paikallisella toimijalla on koosta ja toiminnan laajuudesta aiheutuvat hyvät ja huonot puolensa. Pienen toimijan kanssa voi usein neuvotella useimmista palveluun liittyvistä asioista ja räätälöidä itselle sopivamman paketin. Pienempi palveluntarjoaja saattaa myös esimerkiksi räätälöidä halutunlaisen rajapinnan asiakkaan tietojärjestelmää varten. Paikallinen toimija voi myös näyttää asiakkaalle palvelun fyysisen ympäristön, jolloin asiakas voi varmistua missä ja minkälaisissa olosuhteissa hänen tietonsa sijaitsee. Paikallista toimijaa velvoittavat samat lait ja määräykset, joten toiminnan säännöt ovat kaikille osapuolille samat.

Pilvipalvelut sopimusten ja lainsäädännön näkökulmasta

Pilvipalvelun käyttöönotossa erilaisiin tilanteisiin voidaan varautua myös sopimuksilla. Palvelun riskiarviossa tunnistetut uhkat ja rajoitteet voidaan huomioida palvelun käyttöönottoon liittyvässä sopimuksessa. Palveluntarjoajan kanssa voidaan sopia esimerkiksi vaatimuksista ja mahdollisista sanktioista uhkatilanteisiin ja varautumiseen liittyen.

15. Tiedon käsittelyoikeuksista

Pilveen tallennettuun tietoon liittyvät käsittely- ja käyttöoikeudet määräytyvät erityisesti sopimusten perusteella. Käsittely- ja käyttöoikeuksista on syytä varmistua siis sopimalla. Näin voidaan varmistaa käyttöoikeuksien pysyminen organisaatiossa (ja mahdollisesti palveluntarjoajankin puolella) vain tietyillä henkilöillä.

Organisaation on syytä kiinnittää erityistä huomiota esimerkiksi salassa pidettävän ja arkaluonteisen tiedon käsittelyoikeuksiin. Palveluntarjoajan salassapitovelvollisuudesta voidaan laatia tarvittaessa myös oma salassapitosopimuksensa.

16. Turvallisuusvaatimukset

Palveluihin liittyvistä turvallisuusvaatimuksista on hyvä olla perillä jo silloin, kun aletaan suunnitella pilvipalveluiden käyttöönottoa. Tällöin turvallisuusvaatimuksiin tulee kiinnittää erityistä huomiota ja ne on hyvä kirjata myös sopimusehtoihin. Palveluntarjoajan tietoturvakäytännötkin on hyvä varmistaa ja selventää sopimusehdoin.

17. Häiriöt ja uhkatilanteet sekä jatkuvuuden varmistaminen

Sopimusten avulla pyritään useimmiten varautumaan poikkeaviin tilanteisiin. Riskiarvioinnissa poikkeavat tilanteet tulee arvioida ja niihin varautuminen voidaan huomioida sopimuksellisin keinoin. Sopimuksissa on hyvä ottaa huomioon myös tilanteet, joissa palveluntarjoajan toiminta jostain syystä tulee epävarmaksi tai katkeaa.

Pilvipalvelut käyttöönottavan yrityksen on hyvä varmistaa, että heillä on pääsy pilvipalveluihin tilanteessa, jossa palveluntarjoajan toiminta syystä tai toisesta lakkaa. Tällöin tietojen siirrettävyyteen ja jatkuvuuden turvaamiseen on hyvä kiinnittää huomiota.

18. Kansainvälisyys ja sovellettava lainsäädäntö

Kotimaistenkin pilvipalveluiden osalta on hyvä varmistaa palvelinten sijaintimaa. Jos palvelu on osittain tai kokonaan toteutettu ulkomailla siihen saattaa kohdistua myös ulkomaisen lainsäädännön asettamia vaatimuksia.

Ulkomaiset palveluntarjoajat luonnollisesti suosivat oman maansa lainsäädäntöä myös riitatilanteissa. Pilvipalvelut käyttöönottavan organisaation näkökulmasta helpointa on laatia palvelusopimukseen lauseke, jolla sovellettavaksi lainsäädännöksi asetetaan oma kansallinen lainsäädäntö ja riitatilanteiden varalle toimivaltainen tuomioistuin on määritelty sopimuksessa. Organisaatioiden ja palveluntarjoajien välisissä sopimuksissa tällaisesta voidaan mahdollisesti jopa sopia.

Tilanne on hankalampi kuluttajapalvelusopimuksissa, joissa sopimuksen ehdot on useimmiten ennakkoon määritelty, eikä niihin voi ehdottaa muutoksia.

Suuremmat palveluntarjoajat käyttävät useimmiten vakiosopimuksia, kun taas

pienemmät palveluntarjoajat voivat olla palveluissaan ja sopimusehdoissaan joustavampia.

19. Palvelutasosopimukset

Palvelutasosopimuksessa (SLA) voidaan kuvata tarkemmin palveluihin liittyvät palvelutasotavoitteet ja yksilöidä palveluntuottajan ja asiakkaan vastuut. Palvelutasosopimuksessa voidaan määritellä erilaisia mittareita ja tavoitteita, joiden alittamisesta voi seurata sanktio.

20. Henkilötiedot

Jos pilveen tallennetaan henkilötietoja, tulee huomioida henkilötietojen käsittelyyn liittävä sääntely. Yleissääntö tilanteeseen on, että rekisterinpitäjä ei voi ulkoistaa omaa vastuutaan.

Henkilötietoja voidaan siirtää toiseen Euroopan unionin jäsenvaltioon tai Islantiin, Liechtensteiniin ja Norjaan eli Euroopan talousalueeseen (ETA) kuuluvaan maahan samoilla perusteilla kuin niitä saa Suomessa luovuttaa tai käsitellä. Henkilötietoja voidaan siirtää EU:n tai ETA:n ulkopuolelle ainoastaan, jos kyseisessä maassa taataan tietosuojan riittävä taso[8]. EU:n komissio voi päättää, että joku unionin ulkopuolinen valtio takaa riittävän tietosuojan tason, jolloin henkilötietojen siirto on sallittua.

Euroopan unionin ja Yhdysvaltojen välillä henkilötietojen siirtoon Yhdysvaltoihin sijoittautuneille organisaatioille sovellettavaksi puolestaan tulee niin sanottu Safe Harbor -järjestelmä. Euroopan yhteisöjen komissio on päätöksellään[9] todennut Safe Harbor -järjestelmän varmistavan riittävän henkilötietojensuojan tason henkilötietojen siirroissa Yhdysvaltoihin sijoittautuneille organisaatioille.[10]

Muussa tapauksessa henkilötietojen siirto edellyttää suostumusta, elintärkeää etua tai EU:n komission hyväksymien mallisopimusten käyttämistä, jolloin vastuu henkilötietojen oikeanlaisesta käytöstä muuttuu sopimuskysymykseksi. Konsernin sisäisissä siirroissa monikansalliset yritykset voivat sitoutua Binding Corporate Rules -menettelyyn[11], jolloin sisäisiä tietoja voidaan siirtää EU:n ja ETA:n rajojen yli konsernin sisällä.[12]

Eurooppalaista henkilötietojen sääntelyä ollaan uudistamassa. Euroopan komissio on antanut ehdotuksensa uudesta tietosuojasääntelystä EU:ssa tammikuussa 2012. Keskeisenä periaatteena uudistuksessa on, että rekisterinpitäjä olisi tilivelvollinen eli vastuullinen koko käsittelyprosessin ajan seurata, että henkilötietoihin liittyviä säännöksiä noudatetaan. Uudistuksessa on haluttu korostaa myös, että alihankintatilanteessa rekisterinpitäjällä on velvoite valita sellainen henkilötietojen käsittelijä, joka antaa riittävät takeet siitä, että käsittelyyn liittyvät tekniset ja organisatoriset toimet ja menettelyt toteutetaan niin, että asetusehdotuksessa re-

[8] direktiivi 95/46/EY, 25 artikla 1 kohta
[9] (2000/520/EY)

[10] Lisätietoa asiasta löytyy Tietosuojavaltuutetun laatimasta oppaasta "Henkilötietojen siirto ulkomaille henkilötietolain mukaan ": http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/5JpRhVW1x/HENKILOTIETOJEN_SIIRTO_ULKOMAILLE_HENKILOTIETOLAIN_MUKAAN._10.6.2014pdf.pdf [viitattu 24.10.2014].
[11] Lisätietoa asiasta on saatavilla esimerkiksi Euroopan komission www-sivuilla: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm [viitattu 17.11.2014].
[12] Neuvonen 2014, s. 88.

kisterinpitäjälle asetut vaatimukset tulevat täytetyksi.

21. Keskeisimmät sopimusehdoissa huomioitavat asiat

Raportissa on käsitelty useita asioita, jotka on tilannekohtaisesti hyvä huomioida yksittäistä pilvipalvelua koskevassa sopimuksessa.

Taulukkoon 1 on koottu muistilista keskeisimmistä asioista, jotka organisaatioiden olisi hyvä huomioida pilvipalveluntarjoajien kanssa laadittavissa sopimuksissa.

Taulukko 1 Keskeiset sopimuksissa huomioitavat seikat

Asia	Käsitelty raportin osiossa
Käytettävä palvelu- ja/tai hankintamalli	Määritelmät
Kuka omistaa tiedon, kenellä on käyttö- ja käsittelyoikeus tietoon	1. Tiedon omistajuus ja käyttöoikeudet
Tiedon / palvelun / palvelimen maantieteellinen sijainti	2. Tiedon elinkaari 3. Missä pilveen tallennetut tiedot säilytetään?
Pilvipalveluun tallennettavia tietoja koskevat rajoitukset	5. Tallennettavaan tietoon kohdistuvia tai sen aiheuttamia rajoituksia 20. Henkilötiedot
Pilvipalvelua koskevat tietoturvallisuusvaatimukset	
– Tekninen, fyysinen ja henkilöstöturvallisuus	7. Tekninen turvallisuus 8. Henkilöstön turvaluokitukset 9. Fyysinen turvallisuus
– Tallennetun tiedon varmuuskopiointi	2. Tiedon elinkaari 10. Oma käyttöympäristö 11. Infrastruktuuriresurssipalvelun turvallisuus
– Tiedon salaaminen sitä siirrettäessä, tiedon tuhoaminen ja poisto tallennusmedioilta	2. Tiedon elinkaari

– Tiedon erottelu	3. Missä pilveen tallennetut tiedot säilytetään? 4. Pilvipalveluun tallennetun tiedon erottelu eri asiakkaiden välillä
– Tietoturvaloukkausten ja häiriötilanteiden käsittelyä koskevat menettelyt	11. Infrastruktuuriresurssipalvelun turvallisuus 17. Häiriöt ja uhkatilanteet sekä jatkuvuuden varmistaminen
Palvelutasot	13. Palvelutasosopimus
Palvelun tarjoaminen poikkeustilanteissa	12. Palvelun jatkuvuus 13. Palvelutasosopimus 17. Häiriöt ja uhkatilanteet sekä jatkuvuuden varmistaminen
Sopimukseen sovellettava lainsäädäntö ja oikeuspaikka	18. Kansainvälisyys ja sovellettava lainsäädäntö
Henkilötietojen käsittelyä koskevat vaatimukset	20. Henkilötiedot

Yhteenveto

Palvelun ja tietojen käytettävyys voi pilvipalvelussa olla huomattavasti parempi kuin tiettyä tarkoitusta varten omistetussa tietokoneessa. Pilvipalveluiden luonteeseen kuuluu, että niitä pääsee käyttämään vaivattomasti mistä päin maailmaa tahansa. Pilvipalvelun tarjoajalla voi myös olla paremmat resurssit tietoteknisen tietoturvan kehittämiseen ja ylläpitoon kuin asiakkailla, joiden ominta osaamisalaa ei ole tietotekniikka. Toisaalta pilvipalvelut tuovat mukanaan erilaisia tietoturvallisuuteen liittyviä tekijöitä, jotka organisaatioiden on hyvä huomioida.

Pilvipalvelun kokonaisturvallisuus muodostuu sekä palveluntarjoajan että asiakkaan tietoturvakäytännöistä ja pilveen siirrettävän sovelluksen tietoturvasta. Lisäksi pilvipalveluihin liittyy eiteknisiä riskejä, kuten palveluntarjoajan poistuminen markkinoilta. Pilvipalvelun maantieteellinen sijainti vaikuttaa puolestaan sovellettavaan lainsäädäntöön.

Pilvipalvelun käyttöönottoa harkitsevan organisaatioiden on hyvä huomioida, että pilveen siirrettävä tietosisältö saattaa asettaa reunaehtoja myös pilvipalveluntarjoajalle. Esimerkiksi henkilötietojen tallennuksesta määrää laki, viranomaistietojen tallennuksesta määrää sekä laki että sopimukset ja yritysten keskinäisten tietojen käsittelystä on saatettu sopia yritysten keskinäisellä sopimuksella.

Pilvipalveluntarjoajaa valitessa tulisi tarkastaa palveluntarjoajan turvallisuuteen vaikuttavia tekijöitä, kuten teknisen turvallisuuden taso sekä henkilöstön ja fyysisen turvallisuuden varmistaminen. Myös palveluntarjoajan koko ja palvelun jatkuvuuden varmistaminen sekä palvelusopimuksessa mainitut seikat on hyvä huomioida palveluntarjoajaa valitessa.

Jos itse tehtyyn tarkastukseen ei ole mahdollisuutta, voi pilvipalveluntarjoajan toimintaa arvioida niiden julkaisemien tietojen, kuten teknisten ratkaisujen, mahdollisten sertifiointien ja kolmansien osapuolten tekemien auditointien perusteella.

Ylipäätään organisaatioiden kannattaa miettiä, onko pilvipalveluiden käyttö riski-hyöty-arvion perusteella kannattavaa. Riskiarviota tehdessä on hyvä pitää mielessä, että pilveen voi myös ulkoistaa vain osan tiedosta. Lisäksi pilvipalvelun mahdollisiin riskeihin voidaan joissain tapauksissa vaikuttaa palveluntarjoajan kanssa laadittavalla sopimuksella.

Sanastoa

Alustaresurssipalvelu (engl. Platform as a Service, PaaS) palvelun tuottaja tarjoaa valitsemaansa apuohjelmien ja sovelluskehitysympäristön kokonaisuutta.

Henkilötieto tarkoittaa yleisesti kaikenlaista sellaista tietoa, joka voidaan yhdistää tiettyyn henkilöön.

Infrastruktuuriresurssipalvelu (engl. Infrastructure as a Service, IaaS). Palvelun tarjoaja antaa asiakkaidensa käyttöön yksinkertaisesti tietokoneiden laskentatehoa, tallennustilaa ja verkkoyhteyksiä.

Instanssi (tässä dokumentissa) infrastruktuuriresurssipalvelussa toimiva virtuaalipalvelin tai ohjelmistoresurssipalvelussa käynnissä oleva ohjelma.

Ohjelmistoresurssi-palvelumalli (engl. Software as a Service, SaaS) palvelun tuottaja antaa asiakkaidensa käyttöön valikoituja verkon yli käytettäviä ohjelmistoja.

Palvelusopimus asiakkaan ja palveluntarjoajan välinen sopimus, jossa sovitaan palveluun liittyvistä yksityiskohtaisista ehdoista, velvoitteista ja vastuista.

Palvelutasosopimus (engl. Service Level Agreement) asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot, joita mitataan erilaisilla mittareilla. Tietyn palvelutason alittamiselle voidaan palvelutasosopimuksessa määritellä sanktio.

Pilvipalvelu tietotekniikan resurssipalvelu, jossa verkkoyhteyden välityksellä tarjotaan tietojenkäsittely, tallennus sekä tietoliikennepalveluita.

Pilvipalveluntarjoaja yritys, joka myy asiakkaille omasta palvelinkeskuksesta tai isommalta pilvipalveluntarjoajalta vuokraamaansa tallennus- ja laskentakapasiteettia, tietoliikennepalveluita sekä palvelun hallintaan liittyviä toiminnallisuuksia.

Lähteet

- Are free file storage solutions a safe bet for businesses? http://www.net-security.org/article.php?id=2124
- AWS console breach leads to de-mise of service with "proven" back-up plan http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan/
- Binding Corporate Rules: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.
- Bringing a Machete to the Amazon - Blackhat EU 2014 https://speakerdeck.com/silvexis/bringing-a-machete-to-the-amazon-blackhat-eu-2014
- Cloud security threats, tips and best practices http://www.net-security.org/article.php?id=2070
- EFF's Encrypt The Web Report https://www.eff.org/encrypt-the-web-report
- ENISA Cloud Computing http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing
- Henkilötietojen siirto ulkomaille henkilötietolain mukaan http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/5JpRhVW1x/HENKILOTIETOJEN_SIIRTO_ULKOMAILLE_HENKILOTIETOLAIN_MUKAAN._10.6.2014pdf.pdf
- In re Warrant for Microsoft Email Stored in Dublin, Ireland https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland
- Neuvonen, Riku. Yksityisyyden suoja Suomessa. Lakimiesliiton kustannus, 2014.
- Skiddies turn Amazon cloud into 'crime-as-a-service' – security bod http://www.theregister.co.uk/2014/07/17/amazon_malware/
- The Role Of The Cloud In The Modern Security Architecture Date Published: 31st of July 2014 URL:http://www.net-security.org/article.php?id=2087
- Where is my data? http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Geo_Boundaries.htm

Yhteystiedot
Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki
Puh: 0295 390 100 (vaihde)
kyberturvallisuuskeskus.fi
viestintävirasto.fi