LÄHITAPIOLA
VAKUUTUKSET • PANKKI • SIJOITUKSET

TARKASTUSLISTA
Tietoturvallisuus

Pilvipalvelujen turvallisuustarkastus

Pilvipalveluilla tarkoitetaan yleensä internetissä olevia palveluita, joita palvelun tilaaja voi hyödyntää osana omaa tietojenkäsittelyään joko omien palvelujensa tuottamiseen, käyttämiseen tai edelleentoimittamiseen omille käyttäjilleen. Palvelut ovat dynaamisia sekä skaalautuvia ja niissä hyödynnetään yleensä virtualisointitekniikkaa. Pilvipalveluissa on vaihtoehtoisia palvelumalleja. Näitä ovat esimerkiksi julkinen pilvi ja yksityinen pilvi. Julkisessa pilvessä kuka tahansa voi ostaa pilvestä palvelukapasiteettia. Yksityisessä pilvessä palvelu rajoittuu vain yhden yrityksen sisälle ja on toteutettu vaikkapa yrityksen omassa konesalissa pilviteknologiaa käyttäen.

Pilvipalvelun luonteeseen kuuluu myös, että siitä on eri palveluluokkia, joista tunnetuimmat ovat SaaS (Software as a Service), PaaS (Platform as a Serviece) ja IaaS (Infrastructure as a Service). Nämä tarkoittavat eri teknologia-asteita, jolla palvelu on toteutettu. SaaS vastaa lähinnä valmista ohjelmaa, jota voidaan käyttää, kun taas IaaS antaa käyttäjälle vapauden valita järjestelmien alusta- ja toteutusteknologiaa ja PaaS on näiden välissä oleva teknologia, jolla voidaan työvälineillä räätälöidä omia sovelluksia.

Pilvipalvelun käyttöönottoa tulee aina arvioida kriittisesti. Onko tietojenkäsittelytoiminta sellaista, että se voidaan siirtää pilveen? Mitä seurauksia on, jos palvelu ei toimikaan? Oheisessa listassa on muutamia tarkastuskohteita, jotka on hyvä käsitellä ennen palvelun aloitusta.

TOIMENPIDE	Tarkastettu	Ongelma
Lainsäädäntö palveluun liittyen		
Missä maassa järjestelmän tiedot fyysisesti sijaitsevat?	☐	☐
Minkä maan lainsäädännön alainen pilvipalvelun tarjoaja on?	☐	☐
Minkä maan lainsäädäntöä palvelun toteuttamisessa noudatetaan?	☐	☐
Rajoittavatko lainsäädäntö tai solmitut sopimukset käytettyjen tietojen siirtoa maan rajojen tai EU:n ulkopuolelle tai yleensä kolmannen osapuolen haltuun (esimerkiksi pilvipalveluun)?	☐	☐
Pilvipalvelun palveluntarjoajan maine ja asema		
Onko palveluntarjoaja tunnettu, vakiintunut ja maineeltaan luotettava yritys?	☐	☐

TOIMENPIDE	Tarkastettu	Ongelma
Onko tiedossa keskeneräisiä oikeus- tai riitatapauksia, joilla voi olla vaikutusta palvelun laatuun tai sisältöön?	☐	☐
Käyttääkö palveluntarjoaja toiminnassaan alihankkijoita ja miten on varmistauduttu heidän toimintansa turvallisuudesta?	☐	☐
Onko palveluntarjoaja julkaissut tietoturvallisuuspolitiikkansa?	☐	☐
Onko palveluntarjoajalla käytössään tietoturvallisuuteen liittyvä sertifiointi?	☐	☐
Auditoidaanko palvelua säännöllisesti ulkopuolisen tarkastajan toimesta?	☐	☐
Tietojen varmistaminen		
Miten on huolehdittu palvelussa olevien tietojen varmistamisesta? Onko tiedot varmistettu toisessa sijainnissa olevaan konesaliin tai muuhun turvalliseen säilytyspaikkaan?	☐	☐
Miten palvelussa voi palauttaa aikaisempia tietoja tai tilanteita? Voiko tietoja palauttaa itse vai vaatiiko se palveluntarjoajan toimintaa?	☐	☐
Voiko tietoja palauttaa yksi kerrallaan, vai vaatiiko palautus koko tietyn ajankohdan tilanteen palauttamisen?	☐	☐
Luottamuksellisuuden säilyttäminen		
Miten ja kuka hallitsee pilvipalvelussa olevia käyttöoikeuksia? Myönnetäänkö käyttöoikeudet itse omille käyttäjille vai tarvitaanko palveluntarjoajan toimenpiteitä?	☐	☐
Onko palvelussa mahdollista rajoittaa käyttäjien oikeuksia palveluun joko käytettävän ajan tai toimintojen osalta (esim. vain lukuoikeudet)?	☐	☐
Onko tietojen katselusta, käytöstä tai muutoksista mahdollisuus saada lokitietoja?	☐	☐
Miten palveluntarjoaja on erottanut julkisessa pilvessä olevat, järjestelmää käyttävät eri asiakkaat ja heidän tietonsa toisistaan?	☐	☐
Käyttääkö palvelu suojattua (esim. https-) yhteyttä sekä kirjautumisessa että itse istunnon aikana?	☐	☐
Vaatiiko palvelu riittävän turvallisen salasanan käyttäjältä? Onko salasanalle asetettavissa vaikeustaso ja voimassaoloaika, jonka jälkeen se on vaihdettava?	☐	☐
Miten pilvipalvelun palveluntarjoajan omaa henkilökuntaa valvotaan epärehellisen toiminnan varalta?	☐	☐
Tietojen siirtäminen		
Onko tiedot mahdollista saada palvelusta koneellisessa muodossa massasiirtona jotain yleisesti tuettua formaattia käyttäen?	☐	☐
Jos palvelusta luovutaan, miten tiedot saadaan luotettavasti tuhottua palvelusta?	☐	☐
Käytön kustannukset		
Mitä ja millä perusteella palvelusta veloitetaan (esimerkiksi kk-maksu, käyttäjämäärä, tapahtumamäärä, käyttöminuutit)?	☐	☐
Mitä toimintoja normaaliin palvelumaksuun sisältyy?	☐	☐
Esiintyykö käytön yhteydessä usein toimenpiteitä, joista peritään erillinen veloitus?	☐	☐

TOIMENPIDE	Tarkastettu	Ongelma
Tietojen käytettävyys		
Kuinka tärkeää on, että tiedot ovat jatkuvasti käytettävissä? Miten pilvipalvelun käyttökatkon sattuessa voidaan toimia?	☐	☐
Onko pilvipalvelu hajautettu siten, että sama on palvelu käytettävissä, vaikka varsinainen palvelinkeskus ei pysty toimimaan normaalisti?	☐	☐
Miten yrityksessä voidaan toimia, jos pilvipalvelu ei syystä tai toisesta ole käytettävissä? Onko olemassa varajärjestelyjä?	☐	☐
Miten palvelussa on varauduttu palvelunestohyökkäyksiin?	☐	☐
Miten palvelussa on varauduttu haittaohjelmiin?	☐	☐
Onko palveluntarjoajalla riittävät henkilö- ja laiteresurssit palvelun tarjoamiseksi kaikissa olosuhteissa? Onko tämä vaatimus sisällytetty sopimuksiin?	☐	☐
Vastuut		
Kuka käyttäjäorganisaatiossa ”omistaa” pilvipalveluun siirretyn tiedon ja niiden käsittelyprosessit?	☐	☐
Kenen on vastuu, jos palvelun toiminta estyy tai palvelu toimii virheellisesti?	☐	☐
Mikä on palveluntarjoajan vastuu, jos luottamuksellista tietoa paljastuu palveluntarjoajasta tai hänen työntekijästään tai yhteistyökumppanistaan johtuvasta syystä?	☐	☐
Onko palvelun toimimattomuudesta, tietovuodosta tai virheellisestä toiminnasta mahdollisuus saada koituneita vahinkoja vastaava korvaus? Onko korvaus vain nimellinen?	☐	☐