Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

TEEMU HYVÄRINEN

Pilvipalveluiden tietoturva

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2024

TIIVISTELMÄ

Hyvärinen, Teemu: Pilvipalveluiden tietoturva
Opinnäytetyö, AMK
Tietojenkäsittelyn tutkinto-ohjelma
Toukokuu 2024
Sivumäärä: 38

Opinnäytetyön tarkoituksena on rakentaa ja opetella oman pilvipalvelun käyttöä, oman palvelun hyötyjä sekä haittoja verraten olemassa oleviin palveluihin. Työssä käydään läpi mitä pilvipalvelut ovat, niiden tietoturvaperustoja sekä kuinka ne liittyvät pilvipalveluiden perusteisiin ja niiden käyttöön.
Lisäksi opinnäytetyössä esitellään pilvipalveluiden luomisen eri toteutusvaihtoehtoja, toimintamalleja sekä eri tietoturvaan liittyviä vaihtoehtoja. Työssä käydään läpi pilvipalveluiden käyttämiseen liittyviä riskejä ja ongelmia.

Opinnäytetyö alkaa työn tavoitteiden esittelyllä sekä pilvipalveluiden tarkoituksien läpikäynnillä. Työssä käytetyt lyhenteet ja termit käydään läpi ja avataan lukijalle. Pilvipalveluiden toimintamallien jälkeen työssä käsitellään tietoturvaa yleisesti, sekä erikseen pilvipalveluiden tietoturvaa ja sen merkityksellisyyttä. Työn edetessä verrataan itse rakennettua pilvipalvelua, jo valmiina oleviin palveluihin, niiden eroavaisuuksia ja käsitellään niiden kannattavuutta mahdollisimman optimaaliseksi käyttäjän omiin tarpeisiin. Työn lopussa vertaillaan kuuden pilvipalvelun tietoturvia sekä niihin liittyviä ominaisuuksia.

Pilvipalveluiden käyttö kasvaa todella nopeasti ja valittavat palvelut tulevat mukana, tämän takia oikean palvelun valinta on tärkeä oman toiveiden mukaan. Tietoturva otetaan nykyisinä vuosina enemmän huomioon ja tietoturva-aukot saadaan korjattua nopealla aikataululla. Tietoturvaa opetetaan jokaiselle ja aukkojen estäminen on tämän takia helpompaa, eikä virhe tietoturva-aukot ole niin yleisiä.

Opinnäytetyön tuloksena voidaan todeta, että oman pilvipalvelun etuja ovat palvelun täysi hallinta, sen mukautettavuus sekä tietoturvaratkaisut. Itse rakennetun pilvipalvelun voi räätälöidä täsmälleen käyttäjän tarpeiden sekä taitojen mukaan. Lisäksi pilvipalvelun hallinnointiin käyttäjä tarvitsee syvää teknistä osaamista. Valmiin palvelun etuja ovat helppokäyttöisyys, niiden yleinen luotettavuus ja kattavat tietoturvaominaisuudet. Valmiin palvelun haittoja ovat rajoitetut mukautusmahdollisuudet sekä kokoaikainen riippuvuus palveluntarjoajasta. Voidaan todeta, että valinta tietoturvan kannalta oman pilvipalvelun ja valmiin ratkaisun välillä riippuu käyttäjän tarpeista, mahdollisesta budjetista sekä teknisestä osaamisesta.

Avainsanat: pilvipalvelu, pilviturva, tietoturva

ABSTRACT

Hyvärinen, Teemu: Security in cloud services
Bachelor's thesis
Degree programme
May 2024
Number of pages: 38

The purpose of the thesis is to build and learn to use a personal cloud service and to compare its benefits and drawbacks with existing services. The thesis will cover what cloud services are, their basic security principles and how these principles relate to the fundamentals and use of cloud services. Additionally, the thesis will present different implementation options for creating cloud services, operating models, and various security-related alternatives. The risks and issues related to using cloud services will also be discussed.

The thesis begins with an introduction to the objectives and purposes of the work. The abbreviations and terms used in the thesis will be explained and clarified for the reader. After discussing the operating models of cloud services, the thesis will cover general security concepts, specifically focusing on the security of cloud services and its significance. The pros and cons of cloud services will be discussed. As the work progresses, a self-built cloud service will be compared to existing services, highlighting their differences and evaluating their feasibility to best suit the user's needs. The thesis will conclude with a comparison of the security and features of six different cloud services.

The use of cloud services is growing rapidly and with it, the number of available services. Therefore, choosing the right service according to personal needs is crucial. In recent years, security has become more of a priority and security vulnerabilities are being addressed quickly. Security education is provided to everyone, making it easier to prevent vulnerabilities and as a result, security breaches are less common.

As a result of this thesis, it can be concluded that the advantages of having your own cloud service include full control of the service, its customizability, and security solutions. A self-built cloud service can be tailored exactly to the user's needs and skills. Additionally, managing the cloud service requires deep technical expertise from the user. The advantages of a ready-made service include ease of use, general reliability, and comprehensive security features. The disadvantages of a ready-made service are limited customization options and constant dependence on the service provider. It can be concluded that, from the security perspective, the choice between your own cloud service and a ready-made solution depends on the user's needs, possible budget, and technical expertise.

Keywords: cloud service, cloud security, cybersecurity

SISÄLLYS

1 JOHDANTO

1.1 Tavoitteet ja tarkoitus

Opinnäytetyön tavoitteena on oman pilvipalvelun rakentaminen ja tietoturvan testaaminen. Lisäksi tavoitteena on verrata työstä saatua tulosta jo olemassa olevien pilvipalveluiden tietoturvaan. Myöhemmin opinnäytetyössä vertaillaan palveluita esimerkiksi niiden ominaisuuksien, tietoturvan ja käyttäjähallinnan osalta. Seuraavassa alaluvussa tutustutaan työssä käytettäviin lyhenteisiin sekä termeihin (taulukko 1).
Johdanto-luvun jälkeen työssä esitellään yleisesti pilvipalveluita, niiden historiaa sekä pilvipalveluiden mahdollisia toiminta- ja toteutusmalleja. Seuraavaksi kerrotaan yleisesti tietoturvasta ja sen vaikutuksesta pilvipalvelun valitsemiseen, yleisesti mahdollisista riskeistä sekä uhkista.

Opinnäytetyön tarkoitus on arvioida pilvipalveluiden tietoturvaa ja sen mahdollisia ominaisuuksia. Opinnäytetyön tarkoituksen mahdollistamiseksi rakennetaan oma pilvipalvelu käyttämällä virtuaalikonetta ja FileCloud -palvelua. Olen valinnut opinnäytetyön aiheen oman kiinnostuneisuuden sekä ammatillisen kehittymisen vuoksi. Opinnäytetyön aiheen valintaan vaikutti myös tämän tutkinnon opinnoista kerääntyneen kiinnostuksen pilvipalveluihin sekä tietoturvaan.

1.2 Opinnäytetyön tutkimusongelma

Opinnäytetyön tarkoituksena on saada vastaus kysymyksiin, ovatko pilvipalvelut turvallisia, sekä kuinka luotettavia pilvipalvelut ovat. Lisäksi työssä on tarkoitus selvittää, onko turvallisempaa rakentaa oma pilvipalvelu vai käyttää valmiiksi tarjolla olevia pilvipalveluita. Viimeisimpänä pohdin kuinka käyttäjän pitäisi tehdä valinta sekä mitä positiivisia ja negatiivisia puolia pilvipalveluiden vaihtoehdoissa on.

1.3 Lyhenteet ja termit

Taulukko 1. Opinnäytetyössä käytettävät lyhenteet ja termit selitteineen

Lyhenne	Termi	Selite
IaaS	Infrastructure as a Service	Infrastruktuuri palveluna. Palveluntarjoaja tarjoaa virtuaalisia IT-infrastruktuuripalveluita internetin välityksellä.
CaaS	Container as a Service	Kontti palveluna. Palveluntarjoaja tarjoaa konttien hallintapalveluita internetin välityksellä.
PaaS	Platform as a Service	Pilvialusta palveluna. Palveluntarjoaja tarjoaa kehitysalustan ja ympäristön.
SaaS	Server as a Service	Ohjelmisto palveluna. Ohjelmistot toimitetaan internetin kautta palveluna.
MFA	Multifactor Authentication	Monivaiheinen todennus, on tietoturvamenetelmä, minkä avulla käyttäjän henkilöllisyys varmennetaan tunnistautumistekijällä.
Zero Knowledge Encryption	Nollatiedon salaus	Tietoturvateknologia, jossa palveluntarjoaja ei pääse käsiksi tai näe käyttäjän tietoja, vaikka tiedot olisivat palveluntarjoajan palvelimilla.
Zero trust	Ei luottamusta	Tietoturvamalli, järjestelmän sisällä ei luoteta kehenkään, riippumatta käyttäjästä tai laitteesta.

End to End	Päästä päähän	Tietoturvamenetelmä, jossa tiedot salataan lähettäjän laitteella ja pysyvät salattuina, kunnes saapuvat vastaanottajan laitteelle.
Phishing	Kalastelu	Hyökkääjä yrittää huijata uhria paljastamaan henkilökohtaisia tietoja.
AWS	Amazon Web Services	Maailman johtava pilvipalvelualusta, joka tarjoaa laajan valikoiman pilvipalveluita.
Hybrid	Hybridi	Yhdistää paikalliset IT-resurssit ja pilvipalvelut muodostaen integroidun ja yhtenäisen IT-ympäristön.
Serverless	Palvelimeton	Palveluntarjoaja hallinnoi automaattisesti palvelininfrastruktuuria ja resursseja.
IoT	Internet of Things	Fyysisten laitteiden verkkoon, jotka ovat varustettu antureilla, ohjelmistoilla ja muilla teknologioilla.
EC2	Elastic Compute Cloud	Pilvilaskentapalvelu, joka mahdollistaa skaalautuvien ja resursseilta joustavien virtuaalipalvelimien käytön.
S3 Bucket	Simple Storage Service	AWS tarjoama pilvitallennuspalvelu, joka mahdollistaa suurien tietomäärien tallentamiseen ja hakemisen internetin kautta. ”Bucket” ämpäri on yksikkö, johon data tallennetaan.

2 PILVIPALVELUT

2.1 Mikä on pilvipalvelu?

Pilvipalvelu eli tietotekniikan resurssipalvelut ovat verkkoyhteyden välityksellä tarjottavia tietojenkäsittely- ja tallennuspalveluita sekä tietoliikennepalveluita. Pilvipalveluiden tarjonta on laaja ja monipuolinen käyttäjän eri tarpeille. Pilvipalveluiden asiakkaita ovat yksityishenkilöt ja yritykset. Osa palveluista ovat maksullisia ja osa maksuttomia. (Kyberturvallisuuskeskus, n.d, s. 5)

Pilvipalvelu on palvelumalli, jossa tarjotaan mahdollisuus jakaa tietoteknisiä resursseja tietoverkkojen yli helposti usean käyttäjän kanssa. Yhteydensaanti on tehty helpoksi ja toimintamallin voi muokata käyttäjän tarpeiden mukaiseksi. Pilven resurssien hallinta ja kulujen optimointi on tehty helpoksi. (Kybertuvallisuuskeskus, n.d, s. 5)

2.2 Pilvipalveluiden toteutusmallit

Kappaleessa käydään läpi pilvipalveluiden toteutusmalleja. Toteutusmalleista annetaan yleistä tietoa ja käyttötapoja. Toteutusmalleja on erilaisia, koska käyttäjän mukaan palvelulta vaaditaan erilaisia ominaisuuksia.

2.2.1 Yksityinen pilvipalvelumalli

Yksityisellä pilvipalvelulla tarkoitetaan, joko internetin tai yksityisen sisäisen verkon kautta tarjottavia laskentapalveluita vain valituille käyttäjille suuren yleisön sijaan. Yksityinen pilvipalvelu tarjoaa yrityksille myös monia julkisen pilven etuja mukaan lukien itsepalvelun, skaalautuvuuden sekä joustavuuden – lisähallinnan ja räätälöinnin. Räätälöinti on saatavilla omistetuista resursseista paikan päällä isännöidyn laskentainfrastruktuurin kautta. Yksityiset pilvet tarjoavat lisäksi korkeamman tason tietoturvaa ja yksityisyyttä yrityksen palomuurien, että sisäisen isännöinnin kautta varmistaakseen, että sekä toiminnot ja

arkaluontoiset tiedot eivät tule kolmansien osapuolien saataville. Yksi haittapuoli yksityisessä toteutusmallissa on, että yrityksen IT-osasto on kokonaan vastuussa pilven hallinnan kustannuksista sekä on vastuussa sen ylläpidosta. Yksityisten pilvienpalveluiden käyttö vaatii samat henkilöstö-, hallinta- ja ylläpitokulut kuin perinteisetkin palvelinkeskukset. (Azure, n.d.c.)

Yksityisessä pilvessä voidaan suorittaa kahta pilvipalvelumallia. Ensimmäinen palvelu on Infrastruktuuri palveluna (IaaS), jonka avulla yritys käyttää palvelun infrastruktuuriresursseja, kuten laskentaa, verkkoa ja tallennusta. Toinen toimintamalli on alusta palveluna (PaaS), jonka avulla yritys pystyy toimittamaan kaiken yksinkertaisista pilvipohjaisista sovelluksista kehittyneisiin yrityssovelluksiin. Yksityisiä pilvipalvelumalleja sekä julkisia pilvipalvelumalleja voidaan yhdistää hybridipilven luomiseksi. (Azure, n.d.c.)

Jos käyttäjän tietoturvan vaatimukset ovat erittäin korkealla tasolla ja vaativat, yksityinen pilvi on hyvä ratkaisu yritykselle. Yksityisen pilvipalvelumallin ylläpitämiseen vaaditaan yritykseltä erityisen paljon resursseja.

2.2.2 Julkinen pilvipalvelumalli

Julkinen pilvipalvelun toteutusmalli määritellään kolmannen osapuolen julkisessa internetissä tarjoamaksi palveluksi. Palvelut ovat kaikkien saatavilla niille, jotka haluavat ostaa tai käyttää niitä. Palvelun voi yleensä valita ilmaisena tai maksullisena tilauksena, jolloin asiakas maksaa käyttökohtaisesti. (Azure, n.d.d.)

Julkiset pilvipalvelumallit voivat säästää yrityksiltä kalliita kustannuksia, toisin kuin yksityiset pilvipalvelumallit. Yksityisen pilvipalvelumallin omistamisen mukana voi aiheutua kustannuksia esimerkiksi paikallisen laitteiston ja sovellusinfrastruktuurin ostamisesta, hallinnasta ja ylläpidosta. Palvelun tarjoaja on vastuussa kaikesta järjestelmien hallinnasta ja ylläpidosta. Julkisen pilvipalvelun käyttöönotto on nopeampaa ja on muokattavissa lähes rajattomasti skaalautuvalla alustalla. Jokainen yrityksessä oleva työntekijä voi käyttää samaa

sovellusta toimiston tai konttorin millä tahansa laitteella, kunhan heillä on internet-yhteys. Julkisten palveluiden tietoturvallisuutta on esitetty ongelmallisena, jos kolmannen osapuolen palveluntarjoaja ei huolehdi korkeasta tietoturvan tasosta. Julkinen pilvi voi kuitenkin oikein toteutettuna olla yhtä turvallinen kuin tehokkaimmin hallittu yksityinen pilvitoteutus. Tämä kuitenkin velvoittaa, että palveluntarjoaja käyttää asianmukaista suojausmenetelmää, kuten esimerkiksi tunkeutumisen havainnointi- ja estojärjestelmää (IDPS) (Azure, n.d.d.)

2.2.3 Hybridi pilvipalvelumalli

Hybridi pilvipalvelumalli yhdistää yksityisen- sekä julkisen pilven, mikä mahdollistaa tietojen jakamisen niiden välillä. Hybridipilvi tarjoaa monia etuja ja mahdollisuuksia, mutta myös haasteita ja harkintaa vaativia aspekteja. Hybridipilvi tarjoaa useita tietoturvatoimia, mutta sen hallinta on monimutkaisempaa. On varmistettava, että molemmat ympäristöt, yksityinen ja julkinen pilvipalvelumalli ovat tietojenkäsittelyltä turvattuja sekä tietoturvapolitiikat ovat johdonmukaisia koko infrastruktuurissa. Hybridipilvi tarjoaa tehokkaan ja joustavan tavan hallita tietojenkäsittelyä ja palvelinkapasiteettia, mutta vaatii huolellista suunnittelua ja jatkuvaa tarkkailua varmistaakseen, että sekä sääntelyvaatimukset että korkea tietoturvan taso säilytetään.
(Azure, n.d.b.)

2.3 Pilvipalveluiden toimintamallit

Pilvipalvelut tarjoavat erilaisia toimintamalleja. Toimintamallit voidaan jakaa kolmeen pääluokkaan: IaaS, PaaS ja SaaS. Toimintamallit tarjoavat eri tasoista hallintaa, joustavuutta ja palveluita. Toimintamallin valinta riippuu käyttäjän tarpeista. Kuvassa 1 vertaillaan toimintamallien hallinnointi tarpeita käyttäjän näkökulmasta.

Kuva 1. Pilvipalvelumallien hallinta vertailuna. (Vento, 2020.)

2.3.1 IaaS toimintamalli

IaaS (Infrastructure as a Service) tarkoittaa infrastruktuuria palveluna. Esimerkkinä kyseisestä toimintamallista yleisesti käytetään Amazon Web Services (AWS) ja Microsoft Azure palveluita.

Esimerkkinä palvelumallin toiminnasta on, että virtuaalikoneiden ja verkkojen ajaminen sekä konfigurointi jää käyttäjän vastuuseen. Fyysistä laitetta ei ole, mutta muualla olevaa täytyy ylläpitää. (Vento, 2020.)

2.3.2 PaaS toimintamalli

PaaS (Platform as a Service) tarkoittaa pilvialustan käyttöä palveluna. Tämä mahdollistaa ohjelmiston kehittämisen, julkaisun ja hallinnoinnin ilman omaa infraa. Yleensä PaaS-palvelusta puhutaan kehitys- ja julkaisualustana pilvessä.

Hyvänä esimerkkinä palvelun toiminnasta on pilveen perustettu tietokanta, jossa ainoastaan data on käyttäjän vastuulla, mutta palvelun ylläpito kuuluu palveluntarjoajalle. (Vento, 2020.)

2.3.3 SaaS toimintamalli

SaaS (Server as a Service) tarkoittaa ohjelmistoa palveluna. Palvelua voi nimittää jopa on-demand-ohjelmistona, joka yleensä on saatavilla selaimen kautta. SaaS-ohjelmistoja ovat esimerkiksi Office 365:n palvelut ja Gmail. Ohjelmistot ovat palveluntarjoajan toimesta täysin ylläpidettyjä. SaaS palvelun käyttämisessä asiakkaan vastuulle jää vain ohjelmiston käyttäminen. (Vento, 2020.)

2.3.4 CaaS toimintamalli

CaaS (Container as a Service) tarkoittaa kontin käyttöä palveluna. CaaS on uudempi palvelumuoto, jossa konttiteknologiaa hyödynnetään sovellusten paketoinnissa tavalla, että koodi sekä konfiguraatiot pystytään helposti ja nopeasti siirrettyä ympäristöstä toiseen. Tämä toimintamalli on vertaisiinsa nähden uudempi. (Vento, 2020.)

2.3.5 FaaS toimintamalli

FaaS (Feature as a Service) tarkoittaa funktioiden käyttöä ajoalusta palveluna. FaaS on usein toiseksi viitattuna serverless-arkkitehtuuriin, joka on

pilvipohjainen tietojenkäsittelynmalli, jossa resurssien hajauttaminen tapahtuu palveluntarjoajan puolesta. (Vento, 2020.)

FaaS tarjoaa pilvipohjaisen sovelluskehityksen, infran ylläpito-ongelmista huolimatta. FaaS-palvelut toimivat täydellisesti ajastettuina tai funktio voidaan ajaa vain kerran päivässä. (Vento, 2020.)

Tässä toimintamallissa käyttäjä joutuu maksamaan pelkästään niistä toiminnoista, joita hän käyttää. Hyvä esimerkki FaaS-palvelusta on Azure Functions-palvelu, joka sallii skriptien ajamisen tapahtumapohjaisesti. (Vento, 2020.)

3 TIETOTURVA

3.1 Yleistä

Kyberturvallisuus on turvallisuuden osa-alue, minkä avulla tavoitellaan sähköisen ja verkotetun yhteiskunnan turvallisuutta. Kyberturvallisuuden tarkoitus on tunnistaa, ehkäistä sekä varautua sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin ja kriittisiin toimintoihin yhteiskunnassa. Kyberturvallisuusajattelu on tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen yhdistettyä ajattelua. Useat kriittiset toiminnot yhteiskunnassamme, kuten rahaliikenne, vesihuolto, lennonjohto ja energiantuotanto ovat riippuvaisia järjestelmien ja verkkoyhteyksien huolettomasta toimivuudesta. Toimintoja tukeviin järjestelmiin ja verkkoihin kohdistuvat häiriöt voivat olla esimerkiksi tietoturvakysymyksiä. Niitä voi olla esimerkiksi haittaohjelmissa tai vikaantuvissa laitteissa, jolloin häiriön vaikutus yhteiskunnan näkökulmasta muodostaa kyberturvallisuusuhan. Kyberturvallisuus on jatkuvasti kehittyvä ala, koska tietoturvauhat muuttuvat ja kehittyvät samalla kun tietojärjestelmät ja teknologia uudistuvat. Tämän takia on tärkeää, että tietoturvasta huolehditaan jatkuvasti ja että uusia tietoturvatekniikoita ja -menetelmiä kehitetään jatkuvasti. (Ulkoministeriö, n.d.)

3.2 Tietoturvan uhat ja riskit

Yksityisen käyttäjän sekä yritysten tiedot ovat tallennettuina verkon välityksellä useassa eri paikassa sekä muodossa. Verkkorikolliset pyrkivät hyödyntämään aukkoja pilvipalveluiden tietoturvassa. (F-Secure, n.d.a.)

3.2.1 Haittaohjelma

Haittaohjelmat, eli vahingolliset ohjelmistot, ovat ohjelmistokoodia, joka on suunniteltu vahingoittamaan tietokonejärjestelmiä tai niiden käyttäjiä. Lähes jokaiseen nykyaikaiseen kyberhyökkäykseen sisältyy erilaisia haittaohjelmia.

Kyberrikolliset hyödyntävät haittaohjelmia päästäkseen luvattomasti järjestelmiin ja aiheuttaakseen niissä vahinkoa. Nämä hyökkäykset voivat tehdä järjestelmistä käyttökelvottomia, tuhota tietoja, varastaa arkaluonteista informaatiota ja jopa poistaa kriittisiä tiedostoja käyttöjärjestelmästä.

Yleisiä haittaohjelmien tyyppejä ovat

- Ransomware (Kiristysohjelma) lukitsee uhrin tiedot tai laitteen. Tämän avulla kiristäjä uhkaa pitää tiedot ja laitteen lukittuna tai vuotaa tietoja julkisesti, ellei lunnaita makseta aikamääreeseen mennessä. (IBM, 2023.) Vuonna 2022 nämä hyökkäykset muodostivat 17 prosenttia kaikista kyberhyökkäyksistä IBM Security X-Force Threat Intelligence Index 2023 -raportin mukaan (IBM raportti, 2023).
- Troijan hevonen on haitallista koodia, joka huijaa käyttäjiä lataamaan sen näyttämällä hyödylliseltä ohjelmalta tai piiloutumalla laillisen ohjelmiston sisään. Esimerkkeinä ovat etäkäyttötroijalaiset, jotka luovat salaisen takaoven sekä dropper-troijalaiset, jotka asentavat lisää haittaohjelmia. (IBM Cloud, 2024.)
- Vakoiluohjelmat ovat haittaohjelmatyyppejä, jotka keräävät salaa arkaluontoisia tietoja, kuten käyttäjätunnuksia ja salasanoja. Keräyksen jälkeen ohjelma lähettää tiedot hyökkääjälle. (IBM Cloud, 2024.)
- Madot ovat itseään replikoituvia ohjelmia, jotka leviävät automaattisesti sovelluksista laitteisiin ilman ihmisen toimintaa. (IBM Cloud, 2024.)

3.2.2 Tietojenkalastelu

Sosiaalinen manipulointi, joka tunnetaan myös nimellä "ihmishakkerointi", on menetelmä, jossa yksilöitä manipuloidaan suorittamaan toimia. Toimet saattavat paljastaa luottamuksellisia tietoja, vaarantaa heidän tai heidän organisaationsa taloudellisen turvallisuuden, tai muutoin uhata henkilökohtaista tai organisaation turvallisuutta. (IBM Cloud, 2024.)

Tietojenkalastelu on sosiaalisen manipuloinnin tunnetuin ja yleisin muoto. Se hyödyntää petollisia sähköposteja, sähköpostin liitteitä, tekstiviestejä tai puheluita huijatakseen ihmisiä paljastamaan henkilökohtaisia tietoja kuten

kirjautumistunnuksia, lataamaan haittaohjelmia, siirtämään rahaa kyberrikollisille tai ryhtymään muihin toimiin, jotka voivat altistaa heidät kyberrikollisuuden uhreiksi. (IBM Cloud, 2024.)

Yleisiä tietojenkalastelutyyppejä ovat

- Spear Phishing tarkoittaa tarkasti kohdistettuja tietojenkalasteluyrityksiä, jotka manipuloivat tiettyä henkilöä käyttäen hyväksi tietoja uhrin julkisista sosiaalisen median profiileista.
- Whale Phishing puolestaan on keihästietojenkalastelun muoto, joka kohdistuu yritysten johtajiin tai varakkaisiin henkilöihin pyrkien huijaamaan heitä siirtämään rahaa tai jakamaan tietoja.
- Yrityssähköpostien kompromissit (BEC) ovat huijauksia, joissa kyberrikolliset esiintyvät johtajina tai luotettavina liikekumppaneina tavoitteenaan saada uhrit siirtämään rahaa tai jakamaan arkaluontoisia tietoja. (IBM Cloud, 2024.)

3.2.3 Palvelunestohyökkäys

Palvelunestohyökkäys on kyberhyökkäyksen muoto, jossa verkkosivusto, sovellus tai järjestelmä kuormitetaan suurella määrällä vilpillistä liikennettä, mikä tekee siitä liian hitaan suorittaa tai estää sen käytön laillisilta käyttäjiltä. Hajautettu palvelunestohyökkäys, tunnetaan myös nimellä DDoS-hyökkäys, toimii samalla periaatteella, mutta käyttää apunaan haittaohjelmia saastuttamiseen, internetiin yhdistettyjen laitteiden tai robottien verkostoa, joka tunnetaan nimellä botnet, tarkoituksenaan lamauttaa tai kaataa kohdejärjestelmä. (IBM Cloud, 2024.)

3.2.4 Internet of Things

Internet of Things (IoT) hyökkäyksessä kyberrikolliset käyttävät hyväkseen IoT-laitteiden, kuten kodin älylaitteiden ja teollisuuden ohjausjärjestelmien turvallisuushaavoittuvuuksia. Tavoitteena voi olla esimerkiksi laitteen hallinnan

ottaminen, tietojen varastaminen tai laitteen käyttäminen osana botnet-verkkoa muunlaisiin haitallisiin tarkoituksiin. (IBM Cloud, 2024.)

3.2.5 Injektiohyökkäys

Injektiohyökkäyksessä kyberrikolliset syöttävät haitallista koodia ohjelmiin tai lataavat haittaohjelmia, joiden avulla he voivat suorittaa etäkomentoja. Tämän seurauksena he pystyvät lukemaan tai muokkaamaan tietokannan sisältöä tai muuttamaan verkkosivuston tietoja. (IBM Cloud, 2024.)

Kaksi yleisintä Injektiohyökkäystyyppiä

- SQL-injektiohyökkäyksissä hakkerit käyttävät hyväkseen SQL-syntaksia manipuloidakseen identiteettejä, muokatakseen tai tuhotakseen tietoja tai saadakseen hallintaansa tietokantapalvelimen.
- Cross-site scripting (XSS) ovat hyökkäyksiä, jotka saastuttavat verkkosivustoilla vierailevia käyttäjiä, eivätkä tyypillisesti poimi tietoja tietokannasta kuten SQL-injektiohyökkäykset. (IBM Cloud, 2024.)

4 OMAN PALVELUN RAKENTAMINEN

4.1 Aloitussanat ja tarkoitus

Opinnäytteeksi päätin rakentaa oman pilvipalvelun henkilökohtaisen kiinnostuksen pohjalta sekä tavoitteena kehittää ammattitaitoa. Palveluina rakentamiseen käytin FileCloudia sekä Amazon Web Services (AWS). FileCloud on käytössä UI alustana sekä palveluna missä palvelu pyörii. Itse palvelu on sisäisesti pyörimässä Amazonin palveluissa käyttämällä EC2 palvelua ja S3 Bucketia.

Opinnäytetyön tarkoituksena oli selvittää, miten oma pilvipalvelu asennetaan, mitä hyviä ja huonoja puolia oman pilvipalvelun käytössä on. Toisena tarkoituksena opinnäytetyön tarkoitukselle ottaa selvää minkälaisia tietoturvallisuuseroja valmiiksi olevien pilvipalveluiden ja itse rakentaman pilvipalvelun välillä on.

4.2 Oman pilvipalvelun rakentamisen hyvät ja huonot puolet

Oman pilvipalvelun rakentamisessa on useita hyviä, mutta myös huonoja puolia. Käyttäjän pohtiessa oman pilvipalvelun sekä valmiiksi saatavilla olevan pilvipalvelun väliltä, käyttäjän pitäisi ottaa huomioon alla listatut huomiot.

4.2.1 Hyvät puolet itse rakentamassa pilvipalvelussa

Tietoturvaan ja yksityisyyteen voi käyttäjä sijoittaa paljon rahaa ja aikaa, jolloin pilvipalvelusta saa niin turvallisen ja yksityisen kuin itse tarvitsee. Oman pilvipalvelun ohessa voi käyttää omia tiukkoja tietoturvaprotokollia ja yksityisyyskäytäntöjä, jotka ovat suunniteltu vastaamaan omia tietoturvastandardeja ja -vaatimuksia.

Palveluiden joustavuus sekä kustomointi kuuluvat myös oman pilvipalvelun positiivisiin puoliin. Niiden avulla käyttäjä saa pilvipalvelun räätälöityä vastaamaan omia tarpeitaan ja käytettäviä resursseja.

Suorituskykyyn sekä luotettavuuden toimivuuteen oman pilvipalvelun ollessa fyysisesti lähellä, pystytään helpommin luottamaan. Tärkeä asia pilvipalveluiden toimivuudessa riippuu viiveestä ja vasteajoista. Käyttäjän lähellä oleva pilvipalvelu vähentää huomattavasti viivettä palvelimen ja käyttäjän välillä. Pilvipalvelun pienempi viive parantaa sovelluksen ja tietojensiirron nopeutta käyttäessä.

Itse rakennetussa pilvipalvelussa tiedot saadaan pidettyä omissa tiloissa. Kun pilvipalvelun ja sen infrastruktuurin on rakentanut itse, pysyvät kaikki sinne siirrettävät tiedostot lähellä ja omissa tiloissa. Tämä on suuri syy miksi monet päätyvät rakentamaan oman palvelun, sillä silloin käyttäjän ei tarvitse säilyttää pilveen päätyviä tietoja kolmannen osapuolen palveluissa, vaan ne säilyvät käyttäjällä itsellään.

4.2.2 Itse rakentaman pilvipalvelun huonot puolet

Itse rakennetussa pilvipalvelussa on myös huonoja puolia, jotka käyttäjän tulee ottaa huomioon. Ensimmäinen huono puoli itserakennetussa pilvipalvelussa on hinta. Oman pilvipalvelun rakentamiseen täytyy varata rahaa, vaikka se olisikin vain omaan käyttöön. Mitä isompi pilvipalvelu, sitä enemmän pilvipalvelun rakentamien maksaa. Palvelun rakentamiseen tarvitaan fyysiset laitteet, palvelimet sekä tila minne palvelu rakennetaan. Palvelintila tarvitsee vartioita suojatakseen palvelimia, sekä ammattilaisia seuraamaan ja hallinnoimaan tietoturvaa nopealla varoitusajalla, mikäli tietoturva haasteita ilmenee. Oman pilvipalvelun rakentamisen ja käytön kanssa käyttäjän pitää ottaa huomioon ja varautua rahallisesti laitteiden hajoamiseen tai muihin hätätilanteisiin.

- Ajankäyttö

Oman palvelun rakentamiseen menee paljon aikaa, joka alkaa jo oikean tilan valitsemisella palvelun rakentamiseen tarvittavien laitteiden tarkalla valitsemisella. Tämän jälkeen käyttäjän seuraava vaihe on näiden hankkiminen ja asentaminen. Palvelun ollessa toiminnassa pitää käyttäjän silti varata aikaa pilvipalvelun ylläpitoon, päivityksiin, mahdollisiin tarkastuksiin ja laitteiden vaihtoihin.

- Vartiointi ja tietoturva

Pilvipalvelun vartiointi ja tietoturva ovat isossa asemassa palvelun käynnistämisen jälkeen ja vievät käyttäjältä niin aikaa kuin rahaa. Koska palvelut ovat omissa tiloissa, joutuu käyttäjä itse hankkimaan tarpeelliset turvakeinot, jotta pilven tiedostot pysyvät turvassa. Tämän takia useat päätyvät ostamaan valmiin palvelun, jossa fyysisistä laitteista ja tietoturvasta huolehtiminen kuuluu palveluntuottajalle.

- Skaalautuvuus

”Skaalautuminen, eli systeemi tai entiteetti pystyy operoimaan aikaisempaa suuremmalla tehokkuudella ilman, että sen tarvitsee lisätä resursseja toiminnan pyörittämiseen” (Pulkkinen, 2017). Omassa palvelussa maksetaan fyysisestä resurssista, jota käytetään, kun taas valmiissa pilvipalvelussa käyttäjän omat tarpeet kattavat vain murto-osan palvelun mahdollisista resursseista. Esimerkiksi pilvipalvelussa käytössä olevaa muistia tai palvelun tehokkuutta voi tavallisesti kasvattaa vain muutaman asetuksen tai napin takaa ja maksamalla siitä lisää kuukausittain. (Pulkkinen, 2017.)

- Katastrofi

Itse rakennetussa pilvipalvelussa jokainen katastrofi on käyttäjän omissa käsissä ja vahingoittuneet laitteet maksetaan itse tai korjautetaan. Useimmat käyttäjät eivät ota pilvipalveluiden tietoturvaa tarpeeksi tosissaan ja uskovat yksittäisinä käyttäjinä olevansa turvassa, eivätkä ymmärrä olevansa mahdollisia tietojenkalastelun tai tietojen myyntikohteita. Tämän takia mahdolliset katastrofit ovat tärkeitä ottaa omissa pilvipalveluissa huomioon ja esimerkiksi palkata erillinen henkilö etsimään sekä korjaamaan mahdollisia tietoturva-aukkoja katastrofien välttämiseksi.

- Ylläpito

Palvelun ylläpidon kustannukset voivat yllättää käyttäjän. Mitä edistyneempi tai suurempi pilvipalvelu ja pilvitarjonta, sitä enemmän pilvipalvelu maksaa. Pilvipalvelun käynnistyessä käyttäjä joutuu maksamaan tilasta, laitteista, tietoturvasta ja ohjelmistosta. Pilvipalvelun keskeisiä kuluja ovat laitteistoinvestoinnit, sähkö, jäähdytys, ohjelmistoinvestoinnit, henkilöstön palkat ja koulutus.

5 PILVIPALVELUIDEN TIETOTURVA

5.1 Yleistä

Pilvipalveluiden tietoturva on kokoelma menetelmiä ja teknologiaa, suunniteltuna ulkoisiin sekä sisäisiin turvallisuuden uhkiin. Monet organisaatiot siirtyvät käyttämään pilvipohjaisia työkaluja ja palveluita, joten turvallisuudesta huolehtiminen on kasvava huolenaihe. Nykyaikainen tekniikka tuo paljon helpotusta organisaatioille, sekä auttavat kehittämään ominaisuuksia. Siirtyessä pilvipohjaiseen ympäristöön voi kuitenkin tulla negatiivisia ja kalliita seurauksia, jos siirtymiä ei tehdä turvalliseksi. Pilvipalveluiden yleistymisen seurauksena tietoturvavaatimusten ymmärtäminen ja ylläpitäminen on tullut entistäkin kriittisemmäksi. Tilanteessa, jossa kolmannen osapuolen pilvipalveluntarjoajat ottavat pilvipalvelun infrastruktuurin hallintaansa, ei hallinta-alueeseen kuitenkaan kuulu tietoturvaresurssien turvallisuus eikä vastuullisuus. Digitaalinen maisema kehittyy jatkuvasti ja tietoturvauhat kehittyvät niiden mukana. Tietoturvauhat voivat kohdistua jokaiseen palveluntarjoajaan, jonka takia tietoturvan tulee olla tärkeä aihealue yrityksen koosta riippumatta. (IBM, n.d.)

5.2 Pilvipalveluiden tietoturvan heikkouksia

Pilvipalvelut voivat olla turvallinen valinta tietojen säilyttämiseen, mutta käyttäjän tulee muistaa, että niihinkin sisältyy riskejä, eivätkä pilvipalvelut ole turvassa tietoturvauhilta. Pilvipalveluiden haavoittuvuuksien hallinta edellyttää kattavaa tietoturvapolitiikkaa, jatkuvaa valvontaa ja päivittämistä. Kuvassa 2 näkyy yleisimmät pilvipalveluiden tietoturvariskit.

Kuva 2. Yleisimmät tietoturvariskit (Stouffer, 2023.)

5.3 Pilvipalveluiden yleiset uhat

- Pääsynhallinta

Kuten paikalliset järjestelmät, niin myös pilvipohjaiset järjestelmät ovat vaarassa joutua tietojen katoamisen uhriksi. Tietojen menetykselle ei ole pelkästään yhtä syytä, niin voi tapahtua esimerkiksi tietomurron, luonnonkatastrofin tai järjestelmänlaajuisen toimintahäiriön seurauksena. (Stouffer, 2023.)

- Kaappaus

Pilvitilin kaappaus tapahtuu, kun hyökkääjä onnistuu saamaan toisen tilin hallintaansa. Kaappauksen kohteeksi joutuvat yleensä pilviverkot, joilla on tehottomat tietoturvaresurssit ja -protokollat. Verkkorikolliset pääsevät käsiksi tileihin käyttämällä tietojenkalastushuijauksia sekä bottiverkkoja.

Näiden avulla rikolliset tunkeutuvat järjestelmiin saastuttaakseen ja ottaakseen täyden hallinnan laitteista, kunhan he ovat saaneen hallinnan tileistä tai laitteista. Tämän avulla rikolliset saavat käsiinsä uhrin tiedostot sekä käyttäjätiedot. Jos kyseessä on yritys, myös arkaluontoiset asiakas- tai yritystiedot olla vaarassa. (Stouffer, 2023.)

- Haittaohjelmat

Haittaohjelmat ovat ohjelmistoja, jotka voidaan asentaa laitteelle käyttäjän tietämättä ja luvatta. Ne on suunniteltu häiritsemään järjestelmän toimintaa, vahingoittamaan sitä tai saamaan siitä hallinnan. Kyberrikolliset saattavat käyttää haittaohjelmia yrittäessään tunkeutua käyttäjän pilvipalveluihin. Nämä haittaohjelmat ovat suunniteltu eksyttämään pilvipalvelut uskomaan, että ne ovat osa todellista järjestelmää. Kun haittaohjelma on integroitunut pilvipalvelun kanssa, se voi vapaasti manipuloida, tuhota ja lukita tietoja mielensä mukaan. (Stouffer, 2023.)

- Sisäpiiristä johtuvat ongelmat

Toisin kuin riittämätön pääsynhallinta, sisäpiirin uhat koskevat käyttäjiä, kenellä on tarkoituksella oikeudet päästä pilviverkkoon. Nämä henkilöt saattavat ohittaa asetetut kyberturvallisuussäädökset, jotka suojaavat yksityisyyttä ja tietoja. Yleensä tämä tarkoittaa kiellettyjen verkkosivustojen käyttöä tai yrityksen ulkopuolelle levitettäviä tiedostoja. Pilvipalveluiden turvallisuus ja sen ylläpito alkaa siitä, miten hallitaan lähellä olevien ihmisten käyttäytymistä ja heidän pääsyään verkkoon. (Stouffer, 2023.)

- Palvelunestohyökkäykset

Palvelunestohyökkäykset pyrkivät kuormittamaan verkkosivusto resursseja, että oikeutetut käyttäjät eivät pääse tarvitsemiinsa palveluihin. Pilviympäristöihin hyökkäykset häiritsevät toimivuutta lähettämällä suuren määrän hyökkäyspaketteja, jotka kuormittavat tietokoneen keskusyksikköä, joka tekee verkosta käyttökelvottoman. (Stouffer, 2023.)

- Inhimilliset virheet

Kyberrikolliset hyödyntävät usein käyttäjien tietämättömyyttä ja sisäisiä turvallisuusaukkoja iskuissaan. Monet käyttäjät eivät ole tietoisia heidän tietoturvaansa liittyvistä heikkouksista, mikä voi johtaa ongelmiin. Vuonna 2022 peräti 82 prosenttia tietoturvamurroista johtui inhimillisistä erehdyksistä tai laitteiden väärinkäytöistä, kuten

- Vahingossa tartunnan sisältävän haittaohjelman lataaminen
- Heikon salasanan käyttäminen
- IP-osoitteiden altistaminen vaaralle
- Tietojen lähettäminen vahingossa väärälle vastaanottajalle
- Ohjelmistojen päivittämättä jättämisestä

Kun tietoja säilytetään julkisessa pilvipalvelussa, se lisää riskejä. Jos yksikin järjestelmän osa murretaan, kaikki verkon käyttäjät voivat olla alttiita hyökkäyksille. (Stouffer, 2023.) Kuvassa 3 löytyy lista inhimillisistä virheistä.

Kuva 3. Lista käyttäjän mahdollisista inhimillisistä virheistä. (Stouffer, 2023.)

5.4 Pilvipalvelujen tietoturvan suojelemisen ohjeita

Oikean pilvipalvelun valinta, jolla käyttäjä saa salattua tiedostot sekä tietokoneella että pilvessä on tärkeää. Salaus on käyttäjälle lupaus ja varmistus, että palveluntarjoajat tai kolmannen osapuolen käyttäjät eivät pääse käsiksi muokkaamaan tai tarkistamaan tiedostoja. (Stouffer, 2023.)

Käyttäjän ei ikinä kannata rekisteröityä mihinkään lukematta käyttäjäsopimusta kokonaan. Käyttäjäsopimus sisältää oleellisia tietoja siitä, kuinka tietoja suojataan, mitä lupia palvelulle annetaan vai antaako käyttäjä luvan palvelulle myydä tietojaan jollakin tavalla. Ennen allekirjoittamista käyttäjän kannattaa ottaa selvää perusteellisesti, mitä jokainen tietosuojakäytäntö ja sopimuslauseke tarkoittaa. Uusista päivityksistä tietosuojakäytäntöön ilmoitetaan aina niiden muuttuessa ehtojen hyväksymisen jälkeen. Silloin käyttäjän tulee lukea uudet ehdot läpi ja harkita vaikuttavatko muutokset negatiivisesti käyttäjän tietoihin.

Kaksivaiheinen todennus on tietoturvan ylläpitämiseksi tärkeää lisätä käyttöön, jos se on saatavilla. Kaksivaiheinen todennus lisää käyttäjän käyttötilille toisen todennusmenetelmän salasanan lisäksi jokaisella uudella kirjautumisella. Toisen tunnistustavan määrityksen mahdollisuus on tärkeä tarkistaa asetuksista, sillä kaikki palvelut eivät automaattisesti vaadi sen määritystä. Kuvassa 4 on esimerkki kaksivaiheisestä todennuksesta, jossa puhelimeen ilmestyy nelinumeroinen koodi tietokoneella täytettävän salasanan lisäksi.

Kuva 4: Kaksivaiheinen todennus (F-secure, n.d.b.)

Yleisiä todennusmenetelmiä kaksivaiheiseen tunnistamiseen

- Biometrinen tunnistus on teknologia, joka toimii tunnistamalla käyttäjän heidän fyysisten tai käyttäytymiseen liittyvien ominaisuuksien avulla. Biometrisiä kirjautumisia ovat esimerkiksi sormitunnistus, kasvojentunnistus, iirisskanneri tai äänen tunnistus. Biometrisiä tunnistuksia käytetään turvallisuuden ja tietoturvan parantamiseen, kuten puhelimen tai kannettavan tietokoneen avaamiseen, henkilötietoja sisältävän sovelluksen avaamiseen, henkilöllisyyden vahvistamiseen tai antamalla pääsyn järjestelmään. Biometrinen tunnistus on turvallisempi vaihtoehto tunnistautumiseen suhteessa perinteiseen salasanaan.

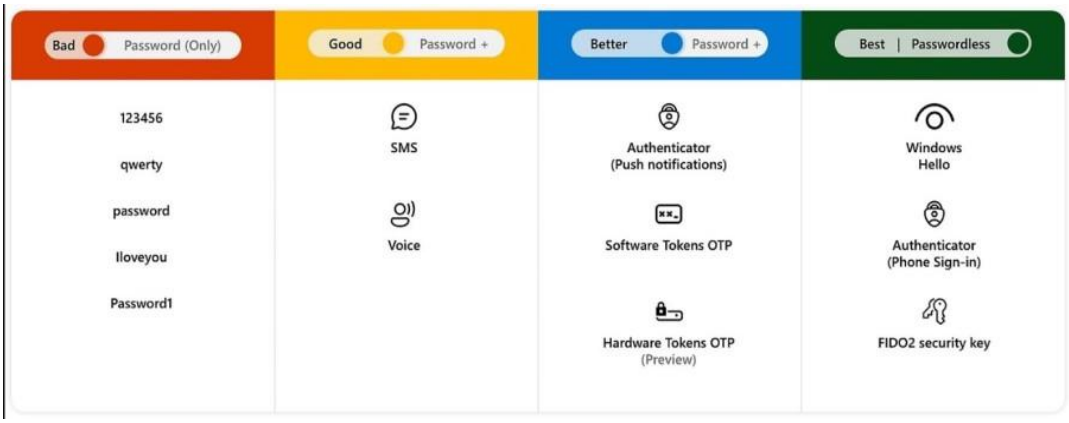
- Turvallisuuskysymykset tuovat lisäturvaa käyttäjälle lisäämällä kirjautumiseen käyttäjän valitsemia turvallisuuskysymyksiä. Turvallisuuskysymykset liittyvät useasti henkilökohtaiseen elämään. Ne ovat tietoja, joita vain harva tietää, esimerkiksi käyttäjän ensimmäisen lemmikin tai rakkauden nimi, äidin tyttönimi tai ensimmäisen kodin osoite.

- Henkilökohtaiset PIN-koodit ovat laajasti käytössä oleva todennusmenetelmä, joka suojaa henkilöllisyyttä sekä tietoja neli- tai kuusinumeroisen salaisen koodin avulla. Menetelmä tarjoaa nopean ja helpon tavan varmentaa henkilöllisyys turvallisesti.

- Väliaikainen koodi on todennusmenetelmä, jossa käyttäjälle annetaan kertakäyttöinen, rajoitetun ajan voimassa oleva koodi. Koodi on osa kaksivaiheista todennusta, joka vahvistaa käyttäjän identiteetin käyttämällä tunnettua menetelmää (salasana) ja saatua menetelmää (kertakäyttöinen koodi). Kertakäyttöinen koodi toimitetaan käyttäjälle tyypillisesti tekstiviestillä. Tästä esimerkki kuvassa 4.

- Authenticator on mobiililaitteeseen ladattava erillinen sovellus, johon lisätään käyttäjätili, jolle halutaan kaksivaiheinen todennusmentelmä. Kun käyttäjätili on lisätty sovellukseen, aina kun käyttäjä haluaa kirjautua kyseisellä käyttäjällä uudella laitteella, sovellus kysyy kertakäyttöistä PIN-koodia, joka näkyy Authenticator-sovelluksessa ja on voimassa vain hetken ajan.

Henkilökohtaisten tietojen jakaminen on riskialtista ja kattavan tietoturvan saavuttamiseksi tämä ei ole kannattavaa. Vaikka kaikki henkilökohtainen tieto ei ole käyttäjän mielestä salattavaa, vääriin käsiin joutuessaan se voi vaarantaa käyttäjän henkilöllisyyden. Henkilökohtaisia tietoja voidaan käyttää vastaamaan turvallisuuskysymyksiin, myydä eteenpäin tai voidaan käyttää henkilöllisyyden varastamisessa. Henkilökohtaisten tietojen varastaminen voi johtaa taloudelliseen petokseen, esimerkiksi avaamalla uusia luottotilejä tai tyhjentämällä käytössä olevia. Kuva 5 näyttää todennusmenetelmien vaikutusta.



Kuva 5: Todennusmenetelmiä (Bhatnagar & Kudrati, 2023.)

Arkaluontoisten tietojen tallentamista pilveen pitäisi välttää. Pilvipalvelu on yleisesti ottaen turvallinen paikka, mutta arkaluontoisten tietojen tallentamista pilveen tulee välttää, sillä ne voivat joutua ei haluttujen ihmisten käsiin tai kadota kokonaan. Väärissä käsissä arkaluontoisia tietoja voidaan käyttää kiristykseen. Rikolliset saattavat pyytää uhria maksamaan, jotta tiedot saadaan takaisin tai ettei niitä levitetä.

Luotettavan pilvipalvelun valinta omien tarpeiden mukaisesti on tärkeää tietoturvan varmistamisessa. On tärkeää valita palveluntarjoaja, joka tarjoaa sekä turvallisen tiedon tallennuksen, salauksen ja käyttöoikeuksien hallinnan. On suositeltavaa oikean palveluntarjoajan valitsemisessa, että palveluntarjoaja täyttää oleelliset tietoturvallisuusstandardit ja noudattaa voimassa olevia säädöksiä. (Bhatnagar & Kudrati, 2023.)

Tietoturvaan kuuluu paljon vastuuta, jonka ymmärtäminen on tärkeää. Tietojen siirtäminen pilvipalveluihin tuo mukanaan tärkeän ymmärryksen vastuunjaosta suojaustoimissa. Palveluiden tarjoaja vastaa pääsääntöisesti infrastruktuurin turvallisuudesta, kun taas asiakas huolehtii tallentamiensa tietojen suojaamisesta. On olennaista tietää omat velvoitteet ja toteuttaa toimenpiteet tietojen suojaukseen. Esimerkiksi siirrettäessä sovelluksia pilveen, palveluntarjoajan vastuu kasvaa, mutta asiakkaan vastuulla on edelleen tietojen, laitteiden ja identiteettien ylläpito ja suojaaminen. (Bhatnagar & Kudrati, 2023.)

Pilvipalveluiden tietoturvan kannalta seuranta sekä valvominen ovat keskeisessä roolissa luvattoman pääsyn havaitsemisessa sekä sen estämisessä. Palveluntarjoajat tarjoavat valvontapalveluita, jotka voivat hälyttää järjestelmänvalvojia epäilyttävästä toiminnasta. Säännöllisesti pilvilokien ja kirjausketjujen tarkistus on isona apuna tunnistamaan mahdolliset tietoturvauhat. Microsoft Sentinel on Microsoftin tekoälyä hyödyntävä pilvipohjainen tietoturvatietojen ja tapahtumien hallintajärjestelmä. Sentinel kykenee paljastamaan kehittyneitäkin tietoturvauhkia ja automatisoimaan niiden torjunnan. Tämä järjestelmä toimii yhtenäisenä keskuksena erilaisissa pilviympäristöissä, tehden mahdolliseksi hyökkääjien toiminnan seuraamisen ja hallinnan eri verkkoväylissä. (Bhatnagar & Kudrati, 2023.)

Zero Trust on turvallisuusstrategia ja lähestymistapa, jolla toteutetaan seuraavat turvallisuusperiaatteet. Todenna ja valtuuta pääsy aina saatavilla olevien tietopisteiden perusteella. Käyttäjillä on rajoitettu pääsy kirjautumaan järjestelmään riskipohjaisten mukautuvien käytäntöjen ja tietosuojan

avulla. Zero Trust -lähestymistavan on tarkoitus ulottua koko digitaaliseen kiinteistöön ja toimia integroituna turvallisuusfilosofiana ja end-to-end-strategiana (Bhatnagar & Kudrati, 2023.)

Identiteetti- ja käyttöoikeuksien hallinta (IAM) auttaa hallitsemaan käyttäjätietoja turvallisesti ja varmistamaan, että oikeat henkilöt saavat pääsyn vain heille kuuluvaan tietoon. Turvallista käyttöoikeuksien hallintaa pidetään olennaisena liiketoiminnan kehitykselle sekä ylläpitämään yrityksen mainetta. Identiteetti- ja pääsynhallinta ovat tärkeä osa yritysten järjestelmissä, jonka avulla varmistetaan vaatimuksien toteutuminen tietoturvan kannalta. (CGI, n.d.)

6 PILVIPALVELUIDEN TIETOTURVAN VERTAILU

Opinnäytetyön osiossa käydään läpi tietoturvan kannalta loogisimpia pilvipalveluita, niiden ominaisuuksien eroja sekä palveluiden tietoturvaan liittyviä positiivisia puolia. Vertailussa on mukana suosittuja sekä vähemmän suosittuja pilvipalveluita. Kaikki vertailussa olevat pilvipalvelut ovat erityisesti tietoturvaan erikoistuneita.

6.1 Amazon Web Service

Amazon Web Service (AWS) on ensimmäinen ja yrityksien käytetyin palveluntarjoaja listalla. Sen avulla käyttäjä voi luoda esimerkiksi virtuaalikoneita tai tietokannalle tallennustilaa. AWS noudattaa useita tietoturvaharjoitteita sekä standardeja kuten SOC 1/ISAE 3402, SOC 2, SOC 3, FISMA, DIACAP, FedRAMP, PCI DSS Level 1, ISO 9001, ISO 27001, ISO 27017 ja ISO 27018. (AWS, n.d.)

6.2 Microsoft Azure

Microsoft Azure on Microsoftin tarjoama pilvipalvelu, joka sisältää laajan tarjonnan erilaisia pilvituotteita ja tietoturvaratkaisuja. Azuren tarjontaan kuuluu virtuaalikoneita, konttipalveluita, tietokantoja ja erilaisia kehittäjä- sekä analytiikkapalveluita. Pilvipalveluiden laaja tarjonta tukevat käyttäjiä esimerkiksi sovellusten kehittämiseen, tietojenkäsittelyyn, sekä jatkuvasti kehittyviin tekoälysovelluksiin. Palvelut ovat turvallisia ja luotettavia ratkaisuja sillä ne on suunniteltu skaalautumaan liiketoiminnan tarpeiden mukaan. (Azure, n.d.a.)

6.3 Google Cloud

Google Cloud on Googlen tarjoama pilvipalvelu. Tunnettu erittäin korkeatasoisesta tietoturvasta. Tietoturva sisältää sekä fyysisen turvallisuuden että verkkoturvallisuuden, sisältäen monimutkaiset suojausprotokollat ja säännölliset

turvatarkastukset. Google Cloud hyödyntää koneoppimista tietoturvauhkien automaattiseen havaitsemiseen ja torjumiseen. Googlen tarjoama pilvipalvelu on luotettava vaihtoehto myös tiukkojen tietosuojastandardien kannalta. (Google, n.d.)

6.4 pCloud

pCloud käyttää TLS/SSL-salausta suojatakseen käyttäjien tiedostoja siirron aikana käyttäjän laitteelta palvelimelle. Tietoturva on palveluntarjoajalle tärkeä prioriteetti. Palveluntarjoaja tuottaa itse pilvipalveluiden tietoturvan omatakseen ensiluokkaiset turvatoimet. Varmistaakseen tiedostojen täydellisen säilytyksen tiedostot tallennetaan vähintään kolmelle turvalliselle palvelimelle. pCloud tarjoaa myös maksullisen salauspalvelun, joka pitää tärkeimmät tiedostosi salattuina ja suojattuina salasanalla. Asiakaspuolen salaus on yksi tarjoamista palveluista, mikä käyttäjälle tarkoittaa, että kenelläkään paitsi palvelun ostajalla ei ole avaimia tiedostojen salauksen purkamiseen. (pCloud, n.d.b.)
pCloud käyttää alan standardia 4096-bittistä RSA:ta käyttäjien yksityisille avaimille ja 256-bittistä AES:ää tiedosto- ja kansiokohtaisille avaimille. (pCloud, n.d.a.)

6.5 Mega

Mega käyttää tietoturvan varmistamiseksi nollatietämys-tekniikkaa (zero-knowledge-encryption) tiedostojen salauksessa. Nollatietämys-tekniikan avulla tiedostot ovat salattuja salausavaimen avulla, joka tarkoittaa käyttäjälle, että tiedostot sekä salausavain ovat vain käyttäjän hallussa. Lisäturvatoimena Mega tarjoaa kaksivaiheisen tunnistautumisen, joka vaatii yleisen salasanan lisäksi toisen todennuksen sisäänkirjautumisessa. Tietoturvan lisäksi Mega tarjoaa palvelun, jonka avulla pystyt palauttamaan kadonneita ja vahingoittuneita tiedostoja. Mega käyttää lisäksi versiohallintaa, jolla se mahdollistaa aikaisempien versioiden palauttamisen. Versiohallinta on täydellinen apuväline, jos tiedostot joutuvat haittaohjelman hyökkäyksen uhriksi. (Mega, n.d.)

6.6 Proton Drive

Proton Drive on erikoistunut vahvaan tietoturvaan käyttämällä erittäin edistyneitä salausmenetelmiä. Proton Drive pilvipalvelun tietoturva hyödyntää End-To-End salausta sekä Zero-Access salausta. Lisäksi pilvipalvelun tietoturvatarjontaan kuuluu esimerkiksi kaksivaiheinen tunnistautuminen, joka käyttää digitaalista allekirjoitusta tiedon eheyden varmistamiseksi. Protonin järjestelmä on esillä avoimella lähdekoodilla, jonka ansiosta jokainen käyttäjä voi itse käydä läpi pilvipalvelussa käytettävän tietoturvan vahvuudet ja heikkoudet. (Proton, n.d.)

7 POHDINTA

Opinnäytetyön tavoitteena oli opetella ja tutkia pilvipalveluiden tietoturvaa, verrata itse rakennettua pilvipalvelua valmiina palveluna ostettuun pilvipalveluun. Työn perusteella havaitsin, että käyttäjän tulee huomioida seikkoja, kuten infrastruktuuri, ohjelmisto, tietoturva sekä pilvipalvelun ylläpito. Seuraavaksi koottuna lyhyet johtopäätökset molemmista vaihtoehdoista. Oman pilvipalvelun etuja ovat palvelun täysi hallinta, sen mukautettavuus sekä tietoturvaratkaisut. Itse rakennetun pilvipalvelun voi räätälöidä täsmälleen käyttäjän tarpeiden sekä taitojen mukaan. Itse rakennetun pilvipalvelun haittoja ovat suuret alkuinvestoinnit sekä ylläpitokustannukset. Lisäksi pilvipalvelun hallinnointiin käyttäjä tarvitsee syvää teknistä osaamista.

Valmiin palvelun etuja ovat helppokäyttöisyys, niiden yleinen luotettavuus ja kattavat tietoturvaominaisuudet. Valmiin palvelun haittoja ovat rajoitetut mukautusmahdollisuudet sekä kokoaikainen riippuvuus palveluntarjoajasta.

Opinnäytetyön edetessä kehitin omaa ammatillista tietämystä pilvipalveluista sekä niiden tietoturvasta. Sain selville opinnäytetyön aikana kuinka paljon pilvipalveluun voi vaikuttaa, vaikka se olisikin kolmannen osapuolen tuottama ja turvaama. Pilvipalvelut ovat jatkuvasti suosiotaan kasvattava palvelu. Pilvipalveluiden käytön yleistyessä, yleistyvät myös niihin kohdistuvat rikokset sekä tietoturvaan liittyvät uhat. Tämän takia käyttäjän omat kriteerit täyttävä palvelu on entistä tärkeämpää. Opinnäytetyön aikana havaitsin haasteita työhön tarkoitetun palvelun valitsemisessa. Monipuolisen tarjonnan vuoksi haasteena oli löytää pilvipalveluita, jotka toisivat mahdollisimman paljon positiivisia sekä negatiivisia puolia pilvipalveluiden tietoturvasta ja pilvipalveluiden ylläpitämisestä. Haasteiden kautta opin oikean pilvipalvelun valitsemisen tärkeydestä, joka kehitti minua tutkijana.

Johtopäätöksenä työssä voidaan todeta, että valinta oman pilvipalvelun ja valmiin ratkaisun välillä riippuu käyttäjän tarpeista, mahdollisesta budjetista sekä teknisestä osaamisesta.

8 LÄHTEET

AWS. (n.d.). Security and compliance. Haettu 12.02.2024 osoitteesta https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html

Azure. (n.d.a). Azure, limitless innovation. Haettu 25.4.2024 osoitteesta https://azure.microsoft.com/en-gb/#pill-bar-products_tab0

Azure. (n.d.b). What is hybrid cloud. Haettu 20.12.2023 osoitteesta https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/what-is-hybrid-cloud-computing/

Azure. (n.d.c). What is private cloud. Haettu 20.12.2023 osoitteesta https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-private-cloud/

Azure. (n.d.d). What is public cloud. Haettu 20.12.2023 osoitteesta https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-public-cloud/

Bhatnagar, Pramiti & Kudrati, Abbas. (5.7.2023). 11 best practices for securing data in cloud services. https://www.microsoft.com/en-us/security/blog/2023/07/05/11-best-practices-for-securing-data-in-cloud-services/

CGI. (n.d.). Käyttäjä- ja käyttövaltuushallinta (IAM). Haettu 9.5.2024 osoitteesta https://www.cgi.com/fi/fi/tietoturva/kayttajahallinta

F-Secure. (n.d.a) Mitä on kyberturvallisuus? Haettu 18.05.2024 osoitteesta https://www.f-secure.com/fi/articles/what-is-cyber-security

F-secure. (n.d.b). What is two factor authentication? Haettu 18.5.2024 osoitteesta https://www.f-secure.com/fi/articles/what-is-two-factor-authentication

Google Cloud. (n.d.). Security. Haettu 25.4.2024 osoitteesta https://cloud.google.com/security?hl=fi

IBM Cloud. (25.03.2024). Types of cyberthreats. https://www.ibm.com/blog/types-of-cyberthreats/

IBM. (2023) X-Force Threat intelligence index 2023. https://mysecuritymarketplace.com/reports/x-force-threat-intelligence-index-2023/

IBM. (n.d.). What is cloud security. Haettu 18.02.2024 osoitteesta https://www.ibm.com/topics/cloud-security

Kyberturvallisuuskeskus (n.d.). Pilvipalveluiden turvallisuus. Haettu 21.12.2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Mega. (n.d.). Protecting your data and respecting your privary. Haettu 27.4.2024 osoitteesta https://mega.io/security

pCloud. (n.d.a). encryption. Haettu 27.4.2024 osoitteesta https://www.pcloud.com/features/encryption.html

pCloud. (n.d.b). Security. Haettu 27.4.2024 osoitteesta https://www.pcloud.com/features/security.html

Proton. (n.d.). Security. Haettu 27.4.2024 osoitteesta https://proton.me/drive/security

Pulkkinen, Verneri. (05.10.2017). Mitä tarkoittaa skaalautuminen https://www.inderes.fi/articles/mita-tarkoittaa-skaalautuminen

Stouffer, Claire. (11.7.2023). 23 cloud security risks, threats, and best practices to follow. https://us.norton.com/blog/privacy/cloud-security-risks

Ulkoministeriö. (n.d.). Kyberturvallisuus ja kybertoimintaympäristö. Haettu 17.2.2023 osoitteesta https://um.fi/kyberturvallisuus-ja-kybertoimintaympäristö

Vento, Jussi. (03.03.2020). Iaas, Caas, Paas, FaaS, SaaS – mitä mikäkin tarkoittaa? https://loihdecloudon.com/julkisen-pilven-palvelumallit-avattuna/

Wolford, Ben. (21.7.2023). 5 cloud storage security risks and how to avoid them. Haettu 19.12.2023 osoitteesta https://proton.me/blog/cloud-security-risks