Pilvipalveluiden tietoturvauhat ja –ratkaisut finanssialalla

Turun yliopisto
Tietotekniikan laitos
LuK-tutkielma
Tietojenkäsittelytiede
Toukokuu 2026
Salla Ruismäki

TURUN YLIOPISTO
Tietotekniikan laitos

Salla Ruismäki: Pilvipalveluiden tietoturvauhat ja –ratkaisut finanssialalla

LuK-tutkielma, 35 s.
Tietojenkäsittelytiede
Toukokuu 2026

Tänä päivänä erilaisten digitaalisten ratkaisujen oletetaan olevan jatkuvasti saatavilla. Näihin lukeutuvat myös finanssialan palvelut, kuten pankit. Rahoituslaitokset ovat alkaneet hyödyntämään pilvipalveluita ratkaisuissaan tehostaakseen palveluidensa saatavuutta ja skaalautuvuutta parantaen sekä työntekijöiden että asiakkaiden käyttökokemusta. Finanssiala on taloudellisen hyödyn takia erittäin altis kyberrikollisten hyökkäyksille ja pilvipalveluiden käyttö muodostaa tarkasti säädellylle toimialalle uusia uhkia liittyen tietoturvaan.
Tässä tutkielmassa tarkastellaan, millaisia tietoturvauhkia finanssialalla on pilvipalveluissa ja miten niitä voidaan ratkaista. Tutkielman menetelmänä on kirjallisuuskatsaus, jossa tarkastellaan aihetta ajankohtaisen aineiston avulla. Aineisto analysoitiin teemoittelemalla keskeiset tietoturvauhat ja niiden ratkaisut sekä vertailemalla eri lähteissä esitettyjä näkökulmia.
Tuloksista voidaan havaita, että pilvipalvelut aiheuttavat finanssialalle monipuolisesti erilaisia tietoturvauhkia, joita myös pyritään ratkaisemaan eri keinoin. Tuloksissa nousevat uhkina esiin esimerkiksi luvaton pääsy ja tietomurrot. Ratkaisuissa puolestaan korostuvat hallinto ja vaatimustenmukaisuus, monitorointi ja identiteetin- ja pääsynhallinta. Pilvipalveluiden avulla pystytään myös suojautumaan tietoturvauhkia vastaan, esimerkiksi edistämällä tietojen saatavuutta pilviratkaisujen varmuuskopioiden avulla. Kvanttiteknologian ja tekoälyn kehittyessä niiden vaikutusta pilvipalveluiden tietoturvaan tulee seurata.

Asiasanat: pilvipalvelut, tietoturva, finanssiala

Sisällys

Kuvat

Taulukot

1 Johdanto

Finanssiala koskettaa tavalla tai toisella suurta osaa väestöstä päivittäisten pankki- ja vakuutuspalveluiden kautta aina sijoituspalveluihin. Näillä palveluilla on suora merkitys yhteiskunnalle ja yksittäisille henkilöille, minkä takia niiden suunnittelussa ja toteuttamisessa tulee ottaa erityisen tarkasti huomioon kyseisen toimialan lukuiset säädökset, kuten yleinen tietosuoja-asetus (engl. General Data Protection Regulation, GDPR), ja tietoturvaan liittyvät uhat, kuten tietomurrot.

Nykypäivänä palveluiden tulee olla aina saatavilla, minkä mahdollistaa digitaalisten palveluiden jatkuva kehittyminen. Rahoituslaitosten on arvioitu käyttäneen 622 miljardia dollaria digitaaliseen infrastruktuuriin vuonna 2023, josta 43,8 % oli pilvipalveluihin ja turvallisuuteen kohdistuneita kuluja [1]. Pilvipalveluiden käyttöönotolla rahoituslaitokset pystyvät tehostamaan esimerkiksi palveluidensa kustannustehokkuutta, saatavuutta ja skaalautuvuutta [2]. Pilvipalveluita on alettu hyödyntämään kriittisiin toimintoihin, kuten asiakkaiden tietojen säilyttämiseen ja transaktioiden prosessointiin [3].

Pilvipalveluiden tuomien hyötyjen mukana kuvaan astuu myös uusia tietoturvaan liittyviä uhkia, kuten moniasiakasympäristöjen aiheuttamat tietomurrot. Taloudellinen hyöty on motiivina 95 %:ssa rahoituslaitoksiin kohdistuvista tietomurroista.[3]. Rahoituslaitoksiin kohdistuu keskimäärin 1239 hyökkäystä viikossa, ja on tutkittu, että finanssialalla hyökkäysmallit ovat 41,6 % muita toimialoja monipuolisempia [1]. Finanssialan palvelut ovat arkaluonteisten tietojen vuoksi houkutteleva kohde ky-

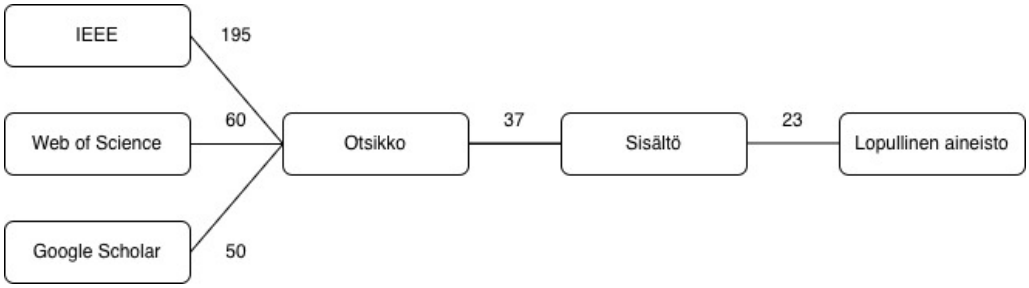
berrikollisille, ja digitaalisen kehityksen myötä myös uhat kehittyvät. Tämän takia aihetta on tärkeää tutkia jatkuvasti.

Tämän tutkielman tarkoituksena on tarkastella pilvipalveluiden tietoturvauhkia ja -ratkaisuja finanssialalla. Tutkielmasta on rajattu pois IoT-ja laitteistokategoriat sekä erilaisten haittaohjelmien erillinen käsittely. Tutkielman tutkimuskysymykset ovat seuraavat:

- TK1: Millaisia tietoturvauhkia pilvipalveluissa on finanssialalla?
- TK2: Miten finanssialan pilvipalveluiden tietoturvauhkia voidaan ratkaista?

Tutkielma on toteutettu kirjallisuuskatsauksena. Aineistoa haettiin IEEE-, Web of Science- ja Google Scholar -hakukannoista hakulauseilla ("cloud security"OR "cloud services") AND ("security threats"OR "cyber threats") AND "security solutions"AND (finance OR "financial sector"OR banking), (cloud security OR cloud service* OR cloud computing) AND (security threat* OR cyber threat* OR vulnerability* OR risk*) AND (security solution* OR security measure* OR mitigation) AND (finance OR "financial sector"OR banking OR fintech) ja "cloud security"("financial sector"OR "banking") ("threats"OR "risks") ("solutions"). Haut on tehty 7.10., 8.10. ja 17.10. ja ne on rajattu viimeisen 10 vuoden ajalle, jotta aineistojen tiedot olisivat ajantasaisia. Google Scholarissa huomioon otettiin viisi ensimmäistä sivua hakutuloksista, mikä tarkoittaa 50 hakutulosta. IEEE-hakukannasta tuloksia löytyi 195 ja Web of Science -kannasta puolestaan 60.

Kuva 1.1 havainnollistaa tiedonhaun prosessia. Aineisto rajattiin ensin otsikon perusteella, ja sen jälkeen sisällön perusteella, minkä jälkeen aineiston lopulliseksi määräksi tuli 25. Lopullista lähdemateriaalia täydennettiin esimerkiksi kirjoilla, standardeilla ja artikkeleilla.



Kuva 1.1: Aineiston tiedonhakuprosessi

Tutkielman luvussa 2 käsitellään pilvipalveluita ja tietoturvaa yleisellä tasolla. Luvussa 3 keskitytään erilaisiin uhkiin, mitä finanssialalla pitää ottaa pilvipalveluissa huomioon. Luvussa 4 tarkastellaan, millaisia ratkaisuja pilvipalveluiden tietoturvaan esitetään. Tutkielman luku 5 sisältää pohdintaa tuloksista ja mahdollisista tulevaisuuden jatkotutkimuskohteista. Viimeisenä on luku 6, joka on yhteenveto, missä myös vastataan tutkimuskysymyksiin.

2 Pilvipalvelut ja tietoturva

2.1 Pilvipalvelut

Pilvilaskennalla tarkoitetaan erilaisten IT-resurssien, kuten palvelimien, tallennustilan ja tietokantojen saatavuutta tarpeen mukaan käyttöperusteisella hinnoittelulla [4]. Pilvilaskennalla on erilaisia käyttöönottomalleja: Julkinen pilvi, yksityinen pilvi hybridipilvi ja yhteisöpilvi [5]. Julkisessa pilvessä pilvipalveluntarjoaja toimittaa palveluita käyttäjilleen julkisen internetin kautta. Palveluntarjoajalla on kaikki vastuu ja hallinta omistamistaan datakeskuksista ja laitteista, joissa sen asiakkaiden data sijaitsee. Näissä datakeskuksissa kaikki asiakkaat jakavat palveluntarjoajan infrastruktuurin. Suurimpia julkisen pilven toimittajia ovat Google Cloud, Microsoft Azure, Amazon Web Services, IBM Cloud ja Oracle Cloud. [6]

Yksityisessä pilvessä puolestaan kaikki pilvi-infrastruktuurin resurssit ovat yhden asiakkaan käytössä ja yleensä ne sijaitsevat asiakkaan omassa datakeskuksessa. Yksityinen pilvi on usein monien suurien toimijoiden, esimerkiksi terveydenhuollon ja rahoituslaitosten valinta niiden arkaluontoisten tietojen takia. Hybridipilvi on edellä mainittujen yhdistelmä. Se on joustava, kustannustehokas ja turvallinen vaihtoehto, minkä takia se onkin suuryritysten suosiossa. [6] Yhteisöpilvi on esimerkiksi jonkin ammattilaisyhteisön käytössä oleva pienempi pilvimalli. Esimerkiksi Institute of Electrical and Electronics Engineers -järjestöllä (IEEE) on yhteisöpilvi, jonka käyttöä varten tulee liittyä IEEE:n jäseneksi [5].

2.1.1 Ominaispiirteet

Pilvipalveluilla on seuraavia ominaispiirteitä:

Resurssien yhdistäminen Pilvipalveluiden yksi useista ominaispiirteistä on resurssien yhdistäminen, mikä näkyy erityisesti julkisen pilven käyttömallissa. Asiakkaat käyttävät palveluita multi-tenant-mallilla, eli fyysiset ja virtuaaliset resurssit yhdistetään ja jaetaan asiakkaille tarpeen mukaan. Näiden resurssien tarkka sijainti ei ole yleensä asiakkaiden tiedossa, vaan he tietävät vain esimerkiksi valtion tai datakeskuksen sijainnin. [7]

Nopea joustavuus Nopea joustavuus on myös ominaista pilvipalveluille. Resurssien varaaminen ja vapauttaminen on joustavaa, mikä näyttäytyy asiakkaalle käytännössä rajattomina dynaamisina resursseina, joita voi lisätä tai vähentää nopeallakin tahdilla. [7]

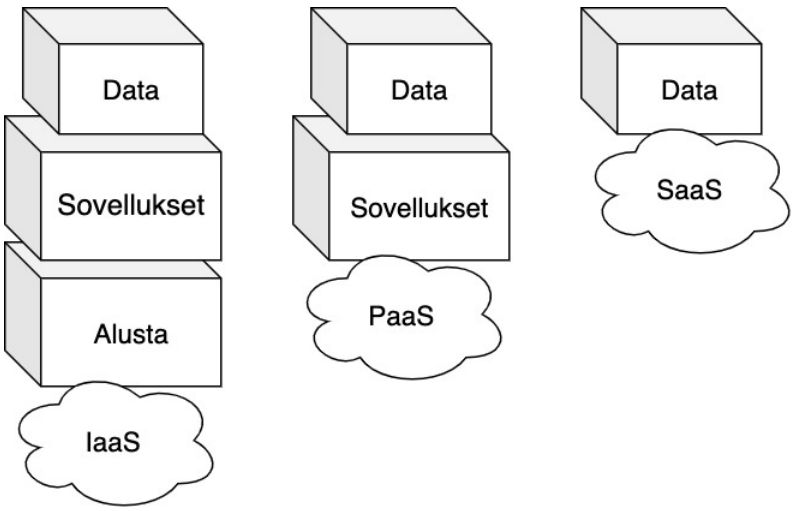
Pääsy verkon kautta Pilvipalvelut ovat yleensä käytettävissä standardilaitteilla, kuten esimerkiksi puhelimilla, tableteilla ja tietokoneilla. Käyttö tapahtuu julkisen internetin välityksellä. [7]

Palveluiden mittaaminen Pilvipalveluiden käyttöä mitataan tarkasti, mitä hyödynnetään sen laskutuksessa, mutta myös laskentatehon allokoinnissa. Laskutusta voidaan tehdä esimerkiksi tietyn resurssin käyttöajan perusteella tai käytetyn tallennustilan perusteella. [8]

On-Demand-saatavuus Pilvipalvelut ovat saatavilla asiakkaillensa verkossa ympäri vuorokauden tarpeen mukaan. Asiakkailla on mahdollisuus hankkia lisää pilvipalveluresursseja, kuten palvelinaikaa tai uusia asiakkuuksia, itsepalveluna milloin vain, mikä tehostaa hankintaprosesseja. [7], [8]

2.1.2 Palvelumallit

Pilvipalveluissa on kolme päätyyppiä, jotka ovat Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [9]. Näiden lisäksi on olemassa myös uudempia pilvityyppejä, esimerkiksi Network as a Service (NaaS), Resource as a Service (RaaS), Recovery as a Service (RaaS) / Disaster Recovery as a Service (DRaaS) ja Data as a Service (DaaS) [5]. Pilvipalvelumallien valinta perustuu asiakasyrityksen tarpeisiin, sillä jokainen pilvityyppi tarjoaa eri tasoisesti hallintaa ja joustavuutta [4]. Asiakkaan vastuu ja mahdollisuus hallita pilviympäristöään pienenee siirryttäessä kohti SaaS-mallia. Kuva 2.1 havainnollistaa kolmen päätyypin eroja. [10, s. 84]



Kuva 2.1: Palvelumallien päätyypit Bhowmikin [10] esitystä mukaillen

Infrastructure as a Service

Infrastructure as a Service (IaaS) on joustavin pääluokka ja se mahdollistaa asiakkaalleen eniten kontrollia. Se tarjoaa asiakkaalle tarvittavan infrastruktuurin, kuten esimerkiksi laskentaa, verkko-ominaisuuksia, virtualisointia ja tallennustilaa. [4], [9] Tässä palvelumallissa asiakas pitää itse huolta sovelluksien, käyttöjärjestelmän ja alustan ylläpidosta [10, s. 84].

Platform as a Service

Platform as a Service (PaaS) -mallissa pilvipalvelutarjoaja tarjoaa asiakkaalleen alustan, missä tarjoaja huolehtii laitteistosta, ohjelmistoista ja muusta infrastruktuurista. PaaS-mallin alustalla asiakas voi nopeallakin tahdilla kehittää, testata, ylläpitää ja toimittaa verkko- ja mobiilisovelluksia. Sovelluskehittäjille jää enemmän aikaa keskittyä itse ohjelmistokehitykseen, kun pilvipalvelutarjoaja on vastuussa kehitysympäristöstä. [4], [11]

Software as a Service

Software as a Service (SaaS) -mallissa asiakkaalle toimitetaan internetin kautta valmis pilvipohjainen sovellus/sovelluksia. SaaS:ssa palveluntarjoajalla on kaikki kontrolli tuotteisiin ja asiakas pääsee käyttämään niitä esimerkiksi verkkoselaimen kautta tietokoneella tai tabletilla. [11], [5] Nykypäivänä SaaS-malli on kaupallisten ohjelmistojen ensisijainen toimitusmalli ja vuonna 2023 sen markkinoiden koko on arvoltaan 273,55 miljardia dollaria. On ennustettu, että SaaS-markkinoiden laajuus kasvaa 1 228,87 miljardiin dollariin vuoteen 2032 mennessä. [6]

2.1.3 Pilvipalveluiden hyödyt finanssialalle

Pilvipalveluiden toimittajat tarjoavat rahoituslaitoksille monipuolisia ratkaisuja, joista on heille paljon hyötyä. Asiakasyritykset voivat keskittyä omaan ydintoimintaansa, kun heidän käyttämiensä sovellusten päivitykset ja ylläpito jää pilvipalveluntarjoajan vastuulle. Myös sovellusten saatavuus tarvittaessa pilvipalvelun sovelluskaupasta lisää tehokkuutta. [12, s. 46–48] Pilvipalveluiden skaalautuvuus ja joustavuus mahdollistavat rahoituslaitoksille myös vapauden skaalata omaa toimintaansa tarpeidensa mukaan. Tähän yhdistyy myös pilvipalveluiden tarjoama kustannustehokkuus, sillä pilvipalveluiden ansiosta asiakkaan ei tarvitse sijoittaa omaan infrastruktuuriinsa suuria summia. [8] Asiakasyrityksen ei tarvitse maksaa hiljaisem-

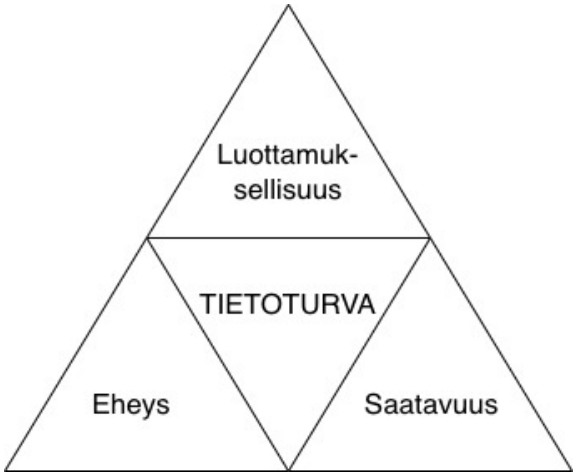
pana ajankohtana ylimääräisestä kapasiteetista pilvipalveluiden käyttöperusteisen hinnoittelun ansiosta [12, s. 46–48]. Myös turvaratkaisuiden kustannukset laskevat, sillä myös pilvipalveluiden tietoturvaratkaisuissa he voivat hyödyntää pay-as-you-go-malleja, joten he maksavat vain käyttämistään palveluista. [8]

2.2 Tietoturva

Maailma digitalisoituu vauhdilla ja samalla lisääntyy siihen liittyvät uhat. Digitalisoitumisen takia tietoturvan merkitys kasvaa, sillä yritykset ja muut tahot keräävät jatkuvasti käyttäjistään lisää tietoa sähköisiin palveluihinsa. Tietoturvan tavoite on, että vain tarkoituksenmukaiset henkilöt pääsevät käsiksi tarvitsemiinsa tietoihin. [13]

2.2.1 Tietoturvan perusperiaatteet

Tarkoituksena on turvata suojattavan tiedon saatavuus, eheys ja luottamuksellisuus. Tätä kokonaisuutta voidaan kuvata CIA-mallilla, jonka nimi tulee sanoista confidentiality (luottamuksellisuus), integrity (eheys) ja availability (saatavuus). Kuvassa 2.2 kuvataan CIA-malli yleisessä kolmiomallissa. Luottamuksellisuus tarkoittaa tiedon suojaamista siten, että sitä pääsevät tarkastelemaan vain tahot, joilla on siihen oikeus. Tiedon eheyden suojaamisella tarkoitetaan sen oikeellisuuden säilyttämistä. Sen tavoitteena on suojata tietoa luvattomalta muuttamiselta tai muuttumiselta. Tiedon saatavuudella pyritään takaamaan tietojen saatavuus aina, kun niitä tarvitaan. Saatavuutta edistetään esimerkiksi tiedonsiirtonopeudella ja ohjelmistojen avulla. [14]



Kuva 2.2: CIA-malli Petterssonin esitystä mukaillen [14]

2.2.2 Tietoturva finanssialalla

Finanssialalla tietoturvallisuuden merkitys korostuu, sillä käsiteltävä tieto on arkaluontoista. Esimerkiksi pankkijärjestelmien tietojen eheys on erittäin tärkeää ja niiden täytyy olla palautettavissa, jos ne muuttuvat hallitsemattomasti. Pankkijärjestelmät ovat muutenkin houkutteleva kohde tietoverkkorikollisille ilmiselvän taloudellisen hyödyn takia. [15, s. 20, 49] Tästä esimerkkinä voidaan pitää S-Pankkiin kesällä 2022 kohdistunutta tietoturvarikosta. 16-vuotias poika huomasi pystyvänsä kirjautumaan äitinsä verkkopankkiin ja yritti kahdesti ilmoittaa tästä haavoittuvuudesta S-Pankille. Poikaa ei otettu työntekijöiden toimesta tarpeeksi tosissaan, joten poika päätyi lopulta perumaan ilmoitukset. Myöhemmin samaa poikaa syytettiin S-Pankin asiakkaisiin kohdistuneesta tietomurto- ja petossarjasta. [16] Tässä tapauksessa rikottiin pankkijärjestelmän luottamuksellisuutta, sillä haavoittuvuus mahdollisti luvattoman pääsyn toisen henkilön pankkitietoihin. Myös järjestelmän eheys vahingoittui, toisen henkilön tililtä oli mahdollista suorittaa oikeudettomia maksutapahtumia.

Joulukuussa 2014 OP:n verkkopankin saatavuus vaarantui, kun nuoret suomalaismiehet kohdistivat siihen palvelunestohyökkäyksen. Hyökkäys esti asiakkaiden pääsyn pankkipalveluihin esimerkiksi rahannostoon ja laskujen maksamiseen uuden

vuoden aatosta loppiaiseen saakka. [17] Palvelunestohyökkäykset ovat verkkohyökkäyksiä, jotka näkyvät yksityishenkilöille esimerkiksi jonkin verkkopalvelun hidastumisena tai käyttökatkona [18]. Hyökkäyksiä käsitellään tarkemmin luvussa 3.

Finanssialan tietoturvaa edistetään ja valvotaan lakien ja määräyksien avulla. Suomessa määräyksiä ja ohjeita määrittelee ja valvoo Finanssivalvonta. Finanssivalvonta on mukana finanssialan palveluntarjoajien tietoturvan huomioinnissa jo ennen kuin varsinainen toiminta alkaa, aina siihen asti, kun palvelun toiminta lopetetaan, varmistaen tietoturvavaatimusten toteutuminen. [19]

3 Pilvipalveluiden tietoturvauhat finanssialalla

Tässä luvussa käsitellään kirjallisuuskatsauksesta ilmeneviä finanssialan tietoturvauhkia. Taulukko 3.1 kuvaa eri kategorioiden uhkien esiintymistä eri lähdeaineistoissa. Siitä voidaan havaita, että luvattomaan pääsyyn, tietomurtoihin sekä -vuotoihin ja hallintoon liittyvät uhat nousevat esiin lähes jokaisessa aineistossa jollain tasolla.

3.1 Luvaton pääsy

Luvaton pääsy (engl. unauthorized access) on yksi pilvipalveluiden tuoma tietoturvahaaste rahoituslaitoksille. [29] Luvaton pääsy voi aiheutua monesta erilaisesta syystä. Virheellinen konfiguraatio esimerkiksi pilvipalvelun palomuurissa tai muussa suojauksessa voi muodostaa reitin luvattomalle pääsylle. Myös salasanoihin ja niiden säilyttämiseen liittyvät ongelmat edesauttavat luvattoman pääsyn mahdollisuutta. Identiteetinhallinnassa väärä rooli väärälle työntekijälle aiheuttaa luvattoman pääsyn. Järjestelmien rajapinnat ja käyttöliittymät ovat mahdollinen reitti luvattomalle pääsylle, jos esimerkiksi autentikointikäyttöliittymä on suunniteltu siten, että sen voi kiertää. [40]

Myös työntekijä, joka käyttää oikeuksiaan väärin voi saada luvattoman pääsyn haluamiinsa tietoihin ja järjestelmiin. Tällainen sisäinen uhka voi nykyisen työntekijän lisäksi olla entinen työntekijä tai jokin liikekumppani. Hyökkääjät voivat

Taulukko 3.1: Lähdeaineistossa esiintyvät tietoturvauhat

Lähde	Luvaton pääsy	Palvelukatkokset	Tietomurrot ja -vuodot	Kvanttiteknologia ja APT	Konfiguraatiovirheet	Sosiaalinen manipulointi	Sisäiset uhat	Hallinto
Khan & Daniel [20]	X		X			X	X	X
L et al. [21]	X	X	X	X	X	X	X	X
Mahalle et al. [22]	X	X	X		X	X	X	X
Vadisetty [23]	X	X	X					X
Satish et al. [24]	X		X				X	X
Naik [2]	X	X	X	X	X	X	X	X
Irtaish et al. [25]	X	X	X				X	
Vinoth et al. [26]	X		X		X			X
Elzamly et al. [27]	X	X	X		X		X	X
Akhtar & Rehman [28]	X		X		X		X	X
Jim & Munira [29]	X		X				X	X
Khanfar [30]	X		X		X			X
Kulkarni [31]	X		X	X	X	X	X	X
Mamidi [1]	X	X	X	X	X		X	X
Metibemu et al. [32]	X		X	X				X
Nagarajan [33]	X	X	X		X			X
Lispector [34]	X		X	X	X			X
Rohmeyer & Ben-Zvi[35]	X	X	X		X		X	X
Shenisetty [3]	X	X	X	X	X		X	X
Sivasamy et al. [36]	X	X	X				X	X
Owolabi et al. [37]	X		X	X	X	X	X	X
Panguluri [38]	X	X	X	X		X	X	X
Madasamy [39]	X	X	X			X		X

hyödyntää myös sosiaalisen manipuloinnin keinoja saadakseen luvattoman pääsyn pilvipalveluun. Esimerkiksi tietojenkalastelulla pyritään saamaan pääsy erityisesti sellaisille tileille, joilla on laajat oikeudet pilviympäristössä. [40]

Luvattomasta pääsystä voi aiheutua suurta vahinkoa yrityksille ja niiden loppukäyttäjille. Tietovuodot, tietojen menetys, liiketoiminnan keskeytyminen, mainehaitta ja oikeudelliset seuraukset voivat aiheuttaa merkittävää taloudellista menetystä. [40]

3.2 Palvelukatkokset

Palveluiden saatavuus on rahoituslaitoksille merkittävä osa-alue huomioitavaksi, kun palveluita siirretään pilveen. Niiden on varmistettava, että resurssit riittävät korkeallekin kuormitukselle. Esimerkiksi pankkipalveluiden tulisi olla saatavilla valtuutetuille osapuolille ilman palvelukatkoksia, joten pilvipalvelun suorituskykyä tulee analysoida huolellisesti. [27] On arvioitu, että jo yhden tunnin palvelukatkos asiakkaisiin kohdistuvissa palveluissa maksaa keskimäärin 682000 dollaria [1].

Suomessa ja Pohjoismaissa yksi kasvanut uhka finanssialan palveluiden saatavuudelle on erilaiset palvelunestohyökkäykset. Palvelunestohyökkäyksissä hyökkääjä lähettää kohdesivustolle kuormittavaa liikennettä hidastaen sen toimintaa. Niistä käytetään usein nimityksiä DoS -hyökkäys (engl. Denial of Service) tai DDoS-hyökkäys (engl. Distributed Denial of Service). DoS-hyökkäys toteutetaan käyttämällä vain yhtä lähdettä, kuten esimerkiksi yksittäistä tietokonetta. [41]

DDoS-hyökkäys on hajautettu palvelunestohyökkäys, eli sen toteutustapa perustuu useista eri lähteistä tehtyyn häirintään. Useat lähteet tekevät hyökkäyksestä vaikean havaita. [22] Hyökkäyksien laajuus ja toimintatavat voivat erota toisistaan. Jotkin hyökkäykset perustuvat suureen volyymiin, jolla ylikuormitetaan kohteena olevaa palvelua, kun taas toiset hyökkäykset ovat edistyksellisempiä ja kohdistuvat suoraan kohteen infrastruktuurin tiettyyn haavoittuvuuteen. Rahoitusalan

hyökkäykset ovat usein hyvin kehittyneitä ja niiden tavoite on ajoittua palveluiden ruuhka-aikoihin, esimerkiksi kuun loppuun. Hyökkäysten tavoitteena on estää oikeiden käyttäjien pääsy kohteena olevaan palveluun, minkä taustalla voi olla esimerkiksi kosto, kiristys tai jokin muu motiivi. Pankkien arvokkaat transaktiot ovat houkutteleva kohde. [2], [3]

Yksi tunnettu DDoS-hyökkäyksiin käytetty haittaohjelma on Mirai, joka tartuttaa IoT-laitteita, kuten kotireitittimiä. Näiden tartutettujen laitteiden tai bottien verkostolla pystytään käynnistämään palvelunestohyökkäyksiä, joilla voi olla vaikutus miljooniin käyttäjiin. Mirain lähdekoodi julkaistiin vuonna 2016, jonka jälkeen se on ollut kyberrikollisten suosima pohja haittaohjelmavarianteille. Loppuvuodesta 2016 Miraita hyödynnettiin hyökkäykseen, missä sen bottiverkostolla saatiin kaadettua suuria osia Internetistä. [42], [43]

3.3 Tietomurrot ja tietovuodot

Pilvipalvelut ja finanssiala ovat potentiaalinen kohde tietomurroille ja tietovuodoille, sillä finanssialan arkaluontoinen data yhdistettynä pilvipalveluiden moniasiakasympäristöjen (engl. multi-tenant) jaettuihin resursseihin luovat useita riskejä [24].

Tietomurto on rikos, missä jokin luvaton taho pääsee varastamaan tietoja järjestelmästä, minne hänellä ei ole oikeutta päästä. Tällaisen rikoksen motiivina on yleensä taloudellinen hyöty. Hyökkäyksen kohteena voivat olla esimerkiksi: [44]:

- Henkilötiedot (kuten henkilötunnus, nimi, puhelinnumero ja kotiosoite)
- Terveystiedot (kuten potilastiedot, sairasvakuutustiedot ja henkilötiedot)
- Rahoitus- ja maksutiedot (kuten maksukorttien numerot ja maksutapahtumat)
- Immateriaalioikeudet (kuten patentit, tavaramerkit ja liikesalaisuudet)

- Toimintatiedot (kuten juridiset asiakirjat, laskut, tilinpäätökset ja myyntiraportit)
- Liiketoiminnan kannalta tärkeät tiedot (kuten lähdekoodi ja liiketoimintasuunnitelmat)

Tietovuoto voi tapahtua täysin tahattomasti, kun esimerkiksi väärä taho pääsee järjestelmässä väärään paikkaan tai tallentaa tietoja vahingossa väärään sijaintiin. Yleensä kyseessä on jokin sisäinen lähde, joka paljastaa tietoja kalastelijalle tai muu sisäinen uhka. [45] Myös kolmannet osapuolet voivat aiheuttaa tahattomia tietovuotoja. Esimerkiksi kalifornialainen terveysalan organisaatio Blue Shield vuoti vahingossa 4,7 miljoonan asiakkaansa tietoja Googlelle kolmen vuoden ajan. Syynä tähän oli Google Analytics -työkalu, jota Blue Shield käytti verkkosivujensa monitorointiin. Google Analytics:ssa oli ollut konfiguraatiovirhe, joka johti tietojen vuotoon. [46] Kuten tietomurroissa, tietovuodot aiheuttavat myös organisaatiolle suurta haittaa. [45]

3.4 Kvanttiteknologia ja edistyneet jatkuvat uhat

Tulevaisuudessa merkittävä uhka pankeille tulee olemaan kvanttitekniikoihin perustuvat kyberhyökkäykset. Tämä tulee vaarantamaan nykyisiä salausmekanismeja. [31] Esimerkiksi on odotettavissa, että esimerkiksi salausmallit RSA (Rivest–Shamir–Adleman) ja ECC (engl. Elliptic-Curve Cryptography) voidaan purkaa sekunneissa [37].

Rahoitusalan yritykset ovat usein kohteina myös edistyneille jatkuville uhille (engl. Advanced Persistent Threats, APTs). Niissä hyökkääjän tavoite on kerätä tietoja huomaamattomasti pitkiäkin aikoja. [3] On tutkittu, että keskimääräinen kokonaiskestokesto pankkiin kohdistuvalle APT-hyökkäykselle on 258 päivää, ja myös hyökkääjät hyödyntävät pilvipalveluita. Kaikki aiheutuneet kulut huomioon ottaen,

yhden hyökkäyksen kokonaislasku on keskimääräisesti 10,8 miljoonaa dollaria. [1]

3.5 Konfiguraatiovirheet

Konfiguraatiovirheet pilvipalveluissa ovat finanssialalla merkittävä uhka. Virheet voivat olla esimerkiksi ihmisen aiheuttamia tai automaation puutteesta johtuvia. Niistä voi koitua organisaatiolle laajaa vahinkoa, kuten tietomurtoja, mainehaittaa ja taloudellisia menetyksiä. Virheelliset konfiguraatiot voivat esiintyä muun muassa pilvipalvelun identiteetin- ja pääsynhallinnassa, rajapinnoissa, tallennustilassa, palomuuriasetuksissa tai lokitietojen tallennuksessa. [32]

Rikolliset voivat kohdistaa hyökkäyksensä esimerkiksi väärin konfiguroituihin pilvitietokantoihin saadakseen pääsyn taloudellisiin tietoihin [37]. Myös organisaation sisäiset uhat voivat hyödyntää konfiguraatiovirheitä saadakseen luvattoman pääsyn tietoihin, joihin heillä ei ole oikeutta [31]. Taloudellisten tietojen vuotoja voi tapahtua myös eri organisaatioiden välillä, jos niiden jakaman pilviympäristön konfiguraatiossa on virheitä [3].

3.6 Sosiaalinen manipulointi

Sosiaalinen manipulointi (engl. social engineering) perustuu käyttäjän manipulointiin. Siinä vedotaan usein uhrin tunteisiin tai pyritään muuten harhauttamaan uhria paljastamaan tietoa, jolla voidaan toteuttaa esimerkiksi identiteettirikos. Sosiaalinen manipulointi mahdollistaa rikollisille pääsyn haluamaansa tietoon, ilman että heillä täytyy olla suurta teknistä osaamista erilaisia tietoturvaohjelmia vastaan, mutta sitä voidaan myös käyttää osana teknisempää kyberhyökkäystä esimerkiksi ensin huijaamalla käyttäjältä tunnukset laitteelle ja sitten asentamalla siihen jonkin haittaohjelman. [47] Sosiaalisen manipuloinnin keinoja finanssialalla ovat esimerkiksi seuraavat:

Tietojenkalastelu

Yli 90 % finanssialan kyberhyökkäyksistä on peräisin tietojenkalastelusta (engl. phishing) [37], joka on hyökkäys, missä rikolliset tekeytyvät joksikin luotettavaksi lähteeksi esimerkiksi pankiksi, ja lähettävät asiakkaalle viestin, jossa pyydetään päivittämään esimerkiksi maksukorttitiedot. Uskottavaksi naamioitu viesti vie usein huijaussivustolle, joka tallentaa uhrin tiedot väärinkäyttöjä varten. [47] Jos maksutapahtumat eivät herätä pankissa tai asiakkaassa epäilyjä, voi kalastelu jäädä huomaamatta [22] Kalastelua voidaan tehostaa tekoälyllä, jolla pystytään harhauttamaan perinteisiä roskapostisuodattimia. [37]

Vishing

Vishing eli voice phishing on tietojenkalastelua äänimuodossa puhelimen välityksellä. Siinä on sama periaate kuin viestikalastelussa: soittaja tekeytyy esimerkiksi pankin työntekijäksi ja pyytää asiakkaalta tarvittavat tiedot, jotta voi tehdä haluamiaan tilisiirtoja. Näin luvattomat tilisiirrot saadaan näyttämään asiakkaan itse tekemiltä. [22]

3.7 Sisäiset uhat

Finanssialalla uhka voi tulla myös organisaation sisältä työntekijän tai kolmannen osapuolen kautta, jolla on pääsy pilviympäristöön [48]. Pilviympäristössä tällaisten sisäisten uhkien (insider threats) havaitseminen on yleensä hitaampaa, kuin paikallisissa järjestelmissä, joten uhka voi jäädä pitkäksikin aikaa huomaamatta, mikä lisää sen aiheuttamien vahinkojen kustannuksia [1]. Sisäinen uhan aiheuttava henkilö voi saada halutessaan paljon tuhoa aikaan. Se voi esimerkiksi [48]:

- Päästä käsiksi asiakkaiden henkilötietoihin

- Muokata pankkitilien saldoja
- Poistaa tietoja
- Aiheuttaa palvelunestohyökkäyksiä
- Vahingoittaa pankin mainetta esimerkiksi julkaisemalla haitallista sisältöä sen nimissä
- Saada sisäpiiritietoa arvopaperikaupoista

3.8 Luottamus ja hallinto

Finanssialalla on erityisen paljon vaatimuksia liittyen esimerkiksi tietojen säilyttämiseen. Pilvipalveluiden hyödyntäminen tuo toimintaan lisähaasteita, mitkä voivat muodostua organisaatioille kynnyskysymyksiksi monimutkaisuutensa vuoksi. Toimijan tulee esimerkiksi varmistaa, että heidän käyttämänsä pilvipalvelut toimivat asetettujen säädösten mukaan. Tästä tekee erityisen haastavaa se, että käytetyn pilvipalvelun sijainti voi olla sellaisella alueella, missä kyseisten säädöksien noudattaminen ei ole yleistä. [24] Pilvipalveluita ylläpitävät tahot voivat olla ulkoisia työntekijöitä esimerkiksi kustannussyistä, joten pilvipalvelua käyttävällä organisaatiolla ei ole välttämättä ollenkaan näkyvyyttä tai kontrollia siihen, keillä kaikilla on pääsy heidän ja heidän asiakkaidensa tietoihin. [22]

Säilyttääkseen asiakkaidensa luottamuksen ja turvatakseen omat tietonsa, pankkien ja muiden finanssialan toimijoiden tulee varmistaa, että heidän käyttämänsä pilvipalvelut vastaavat toimialan tiukkoihin säädöksiin. Tähän voidaan hyödyntää auditointeja ja standardeja. [49] Rahoituslaitoksia velvoitetaan noudattamaan lukuisia säädöksiä, kuten yleinen tietosuoja-asetus (engl. General Data Protection Regulation, GDPR), Payment Card Industry Data Security Standard (PCI DSS) ja ISO 27001 [31]. GDPR on Euroopan Unionin määräämä asetus, jonka tarkoitus on

ylläpitää EU:n kansalaisten tietosuojaa erityisesti henkilötietojen säilyttämisen ja prosessoinnin osalta. PCI DSS taas on suurimpien maksukorttitarjoajien määrittelemä standardi, joka keskittyy korttitietojen turvaamiseen. [2] ISO 27001 on organisaatioille suunnattu kansainvälisesti käytössä oleva standardi tietoturvallisuuden hallintaan. Se sisältää vaatimuksia, joita organisaation tulee noudattaa, jotta se voi kehittää tietoturvahallintajärjestelmäänsä (Information Security Management System, ISMS). [50] Standardeilla on suuri merkitys pilvipalveluntarjoajan valinnassa. Cloud Security Alliancen vuoden 2023 tutkimuksen mukaan rahoituslaitoksista 78 % pitää ISO 27001 -sertifikaattia välttämättömänä, kun pitää valita, mistä pilvipalveluita aletaan hankkimaan. [34]

Jos organisaatio ei onnistu noudattamaan toimialalle asetettuja säädöksiä, voi seurauksena olla suuret rahalliset menetykset. Rikkomuksista aiheutuvat sakot voivat kasvaa miljoonien dollareiden suuruisiksi ja mainehaitan aiheuttamat taloudelliset menetykset voivat olla pitkäkestoisia. Myös esimerkiksi pankin asiakkaat ja muut sidosryhmät voivat haastaa pankin oikeuteen, jos rikkomuksista on koitunut heille haittaa. Säännösten noudattamatta jättämisestä voi aiheutua myös muita kuluja liittyen esimerkiksi tutkimuksiin, rikossyytteisiin ja muihin korjaustoimenpiteisiin, jotka voivat liittyä myös turvallisuuden parantamiseen, jotta vastaavaa ei tapahtuisi jatkossa. [2]

4 Pilvipalveluiden tietoturvaratkaisut finanssialalla

Tässä luvussa tarkastellaan kirjallisuuskatsauksessa esitettyjä pilvipalveluiden tietoturvaratkaisuja finanssialalla. Taulukosta 4.1 voidaan havaita, että hallinto ja vaatimustenmukaisuus, salaus ja avaintenhallinta, monitorointi ja identiteetin- ja pääsynhallinta ovat lähdeaineistossa useasti mainittuja ratkaisukategorioita.

4.1 Salaus ja avaintenhallinta

Arkaluonteisten tietojen, kuten pankkitietojen, säilyttämiseen pilvipalveluissa vaatii suojakseen tietojen salausta (engl. data encryption) [2] Tiedot tulee salata levossa (engl. at rest) ja siirron aikana (engl. in transit). [36]. Levossa tiedot ovat tallennettuina ja siirrossa tiedot siirtyvät eri järjestelmien välillä [38]. Cloud Security Alliancen tutkimuksen mukaan jopa 83 % finanssilaitoksista hyödyntää siirron aikaista suojausta toiminnassaan, mutta levossa olevan tiedon suojaamista ei ole otettu käyttöön yhtä laajasti. [3]

Erityisesti pilvipalveluissa pitää ottaa kahden edellä mainitun lisäksi huomioon myös käytössä olevan tiedon salaus (engl. in use), sillä moniasiakasympäristöt muodostavat riskin tiedon joutumiselle vääriin käsiin. Tähän eräs menetelmä on laitteistopohjainen ratkaisu secure enclave, joka pitää tiedot salattuina myös käyttövaiheessa eristämällä ne omaan ympäristöönsä. [51] Käytössä olevan tiedon salaaminen on

monimutkaista, ja siihen hyödynnettäviä menetelmiä kutsutaan luottamukselliseksi laskennaksi (engl. confidential computing). Se luo erityisesti monipilviympäristöihin lisähaasteita ja se voi rajoittaa toimintojen skaalautuvuutta. [4] Eräs uhka käytössä olevalle tiedolle on Man-In-The-Browser (MITB), joka on hyökkäys, jonka tavoitteena on harhauttaa käyttäjää väärennettyjen verkkosivustojen avulla esimerkiksi tekemään tilisiirtoja rikollisten pankkitileille [22].

Taulukko 4.1: Lähdeaineistossa esiintyvät tietoturvaratkaisut

Lähde	Salaus ja avaintenhallinta	Identiteetin- ja pääsynhallinta	Zero Trust	Monitorointi	Tekoäly	Kyberuhkatiedustelu	Liiketoiminnan jatkuvuus	Hallinto ja vaatimustenmukaisuus
Khan & Daniel [20]	X			X	X			X
L et al. [21]	X	X	X	X	X	X		X
Mahalle et al. [22]	X	X		X			X	X
Vadisetty [23]	X	X		X			X	X
Satish et al. [24]	X			X		X		X
Naik [2]	X	X		X	X		X	X
Irtaish et al. [25]		X	X	X	X			
Vinoth et al. [26]							X	X
Elzamly et al. [27]	X	X					X	X
Akhtar & Rehman [28]	X	X		X	X			X
Jim & Munira [29]	X		X	X	X			X
Khanfar [30]	X	X		X				X
Kulkarni [31]	X	X	X	X			X	X
Mamidi [1]	X	X	X	X	X		X	X
Metibemu et al. [32]	X	X	X	X	X			X
Nagarajan [33]	X	X		X	X			X
Lispector [34]	X	X		X	X		X	X
Rohmeyer & Ben-Zvi [35]		X		X			X	X
Shenisetty [3]	X	X	X	X		X		X
Sivasamy et al. [36]	X	X		X	X		X	X
Owolabi et al. [37]	X	X	X	X	X	X	X	X
Panguluri [38]	X	X	X	X	X		X	X
Madasamy [39]	X	X		X	X		X	X

Päästä päähän -salaus (engl. End-To-End Encryption, E2EE) on salausmetodi, missä viesti salataan aina lähettäjältä vastaanottajalle asti [2]. Tämä on tärkeä suojauskeino pankkitoiminnoille ja esimerkiksi luottamuksellisille viesteille. Päästä päähän -salaus takaa, että tiedot pysyvät salattuina, vaikka viesti joutuisi tietomuron kohteeksi. Hakkereiden lisäksi edes itse palveluntarjoajalla ei ole näkyvyyttä päästä päähän salattuun tietoon. [52]

Salaamiseen hyödynnetään erilaisia salausalgoritmeja, jotka voivat olla joko symmetrisiä (engl. symmetric) tai epäsymmetrisiä (engl. asymmetric). Symmetrisessä salauksessa käytetään yhtä ja samaa avainta salaamiseen ja sen purkamiseen. Symmetrinen salaus on epäsymmetristä nopeampaa, mutta se on herkempi paljastumiselle, koska avainta tulee välittää kaikille osapuolille, mikä lisää riskiä vuodolle. [53] Yksi tunnettu ja erittäin turvallinen symmetrinen salaustekniikka on nimeltään AES-256, joka on Advanced Encryption Standard -salausmallin suurin avainkoko. Sillä on 2^{256} mahdollista avainta, mikä tekee siitä vahvan suojan hyökkäyksiä vastaan. [33]

Epäsymmetrisen salauksen toiminta perustuu avainparin käyttöön. Julkisella avaimella tieto salataan ja yksityisellä avaimella se puretaan. Käytännössä, jos henkilön julkinen avain on tiedossa, kuka tahansa voi lähettää hänelle salatun viestin, jonka vain hän voi yksityisellä avaimellaan purkaa. Tämän ansiosta purkamiseen tarkoitettua avainta ei tarvitse lähettää ollenkaan, joten ne eivät voi vuotaa lähettämisen yhteydessä. Epäsymmetrinen salaus on kuitenkin symmetristä salausta monimutkaisempi ja hitaampi toteutustapa. [53]

Eräs epäsymmetrinen salausmenetelmä on Rivest-Shamir-Adleman (RSA). Sitä käytetään erityisesti pienten tiedostojen salaamiseen, joka voi olla esimerkiksi symmetrisen menetelmän salausavain [33] Tällaista symmetristen ja epäsymmetristen mallien vahvuuksien hyödyntämistä kutsutaan hybridisalaukseksi [53].

Salauksiin merkittävästi liittyvä osa-alue finanssialalla on avaintenhallinta, joka ei ole pilvipalveluympäristöissä yksinkertaista. Avaintenhallintajärjestelmissä on tiu-

kat pääsyoikeusrajoitukset ja rahoitusalan toimijat käyttävät tähän HSM-moduuleita (engl. Hardware Security Models). [1] HSM-moduulit ovat fyysisiä laitteita, joihin voidaan tallentaa esimerkiksi moduulin luomia avainpareja. Ne tuovat avaimille kryptografista ja fyysistä turvaa hyökkäyksiä vastaan. [54] Käytössä on myös monialueellisia (engl. multiregional) avainhallintajärjestelmiä. Tämä takaa sen, että vaikka jokin pilviympäristö vaarantuisi, avaimet eivät paljastu. Riskien minimoinnin merkitys on suuri, sillä keskimääräisesti yksi alan laitos hallinnoi noin 23000 avainta useissa erilaisissa ympäristöissään. Myös kvanttikestäviä menetelmiä on alettu ottamaan käyttöön erityisesti alan johtavien organisaatioiden toimesta. [1] Useilla pilvipalveluntarjoajilla on avaintenhallintaan oma palvelunsa, esimerkiksi Azure Key Vault, Google Cloud KMS ja AWS KMS [31].

4.2 Identiteetin- ja pääsynhallinta

Pankkitietojen kaltaisten arkaluonteisten tietojen turvaamisen yksi tärkeä osa-alue on identiteetin- ja pääsynhallinta (engl. Identity and Access Management, IAM) [2]. Erityisesti monimutkaisissa pilviympäristöissä on tärkeää, että käyttäjä voidaan tunnistaa esimerkiksi ennen pankkisiirtoa [3]. Tunnistamiseen keskittyy identiteetin hallinta ja pääsynhallinnalla varmistetaan, että tunnistettu käyttäjä pääsee vain hänelle tarkoitettuihin tietoihin ja palveluihin käsiksi [38].

Yksi pääsynhallinnan mekanismeista on roolipohjainen pääsynhallinta (engl. Role Based Access Control, RBCA). Siinä käyttäjien oikeudet jaetaan organisaatiossa erilaisten roolien mukaan, joten jokaisella on pääsy vain oman työroolinsa kannalta tarpeellisiin tietoihin. [38] Tämä on pilvipohjaisissa pankkipalveluissa samaa infrastruktuuria käyttävät työntekijät, asiakkaat ja kolmannet osapuolet, joten on tärkeää, että käyttäjät näkevät vain heille tarkoitettua sisältöä [22]

Monivaiheinen tunnistautuminen (engl. Multi-Factor Authenticator, MFA) on yksi suojauskerros lisää tunnistautumiseen. Siinä käyttäjä joutuu käyttämään vähin-

tään kahta menetelmää tunnistautumiseen päästäkseen sisälle järjestelmään. Tunnistautumisen keinoja ovat salasana, biometrinen tunnistautuminen ja kertakäyttöinen koodi. Vaikka käyttäjätunnus ja salasana vuotaisivat, turvaa monivaiheinen tunnistautuminen luvattomalta pääsyltä. [2] Monivaiheisen tunnistautumisen käyttöönoton vaikutus on ollut rahoituslaitoksille merkittävä. On tutkittu, että se on vähentänyt pankkitilien väärinkäyttöä 99,9 %. [3]

4.3 Zero Trust

Pankkijärjestelmien siirtyessä pilvipalveluihin ja tietoturvauhkien kehittyessä ei voi enää olettaa, että pankin verkossa oleva käyttäjä voisi olla varmasti luotettava. Zero Trust -mallissa käytännössä jokainen käyttöoikeuspyyntö varmistetaan erikseen ja silloinkin käyttäjä saa pienimmät mahdolliset oikeudet. Tämän vähimpien mahdollisten oikeuksien periaate (engl. principle of least privilege) vähentää myös hyökkäyspinta-alaa esimerkiksi sisäisiä uhkia vastaan. Myös käyttäjän laitetta, verkkoyhteyttä ja käyttäytymistä monitoroidaan jatkuvasti, joten epäilyttävä käyttäytyminen havaitaan aikaisessa vaiheessa, mikä vähentää sisäisten uhkien mahdollisuutta. Zero Trustia kuvastaa hyvin suojausmallin perusperiaate "never trust, always verify". [31]

Zero Trustin käyttöönottoa varten organisaation IT-infrastruktuurissa täytyy ottaa huomioon muun muassa identiteetin- ja pääsynhallinta, käyttäjien jatkuva autentikointi ja erilaisten pilviympäristöjen vaatimukset. Lisäksi täytyy huomioida mikrosegmentointi, eli verkon jakaminen pienempiin osiin. [31] Mikrosegmentoinnin avulla pankkisovellusten hyökkäyspinta-ala pienenee 91,4 %, mikä vähentää esimerkiksi tietomurrosta koituvia seurauksia [1]

Vuonna 2025 astui voimaan EU:n uusi kyberturvallisuuslainsäädäntö NIS 2 -direktiivi, joka velvoittaa useita toimialoja, myös pankkialaa, ottamaan käyttöön Zero Trust -mallissakin hyödynnettyjä käytäntöjä, kuten monivaiheisen tunnistautumi-

sen ja pääsynhallinnan [55]. On tutkittu, että Zero Trust on vähentänyt tietoturvamurtoja yrityksissä jopa 71,4 %. Zero Trust -mallin käyttöönotto on hidasta, mutta silti tuoreen tutkimuksen mukaan 83,2 % pankeista tekee aktiivisesti töitä saadakseen sen toimintaan palveluissaan. [1] Käyttöönoton hitautta selittää Zero Trustin tekniset vaatimukset, joihin pankkien vanhat legacy-järjestelmät eivät välttämättä taivu. Myös kustannukset voivat nousta korkeiksi, jos organisaation täytyy hankkia toteutusta varten paljon uutta teknologiaa tai palkata Zero Trustiin erikoistuneita työntekijöitä. [31]

4.4 Monitorointi

Pilvipalveluiden suojaustason hallinnalla (Cloud Security Posture Management, CSPM) rahoituslaitokset voivat parantaa pilviympäristönsä tietoturvaa. Sen avulla hajautettuun pilviympäristöön saadaan jatkuva näkyvyys, mikä auttaa virheellisten konfiguraatioiden tunnistamisessa. [3]. CSPM tarjoaa myös jatkuvaa monitorointia, mikä tehostaa vaatimustenmukaisuutta ja tietomurtojen havaitsemista [28] Pilvipalveluiden tietoturvallisuuden hallintaan voidaan hyödyntää Security Information and Event Management -ratkaisuja (SIEM), joiden avulla rahoituslaitos pystyy keräämään pilviympäristöstään dataa, jonka avulla erilaisiin uhkiin pystytään varautumaan ajoissa. Tunkeilijan havaitsemisenjärjestelmät (Intrusion Detection Systems, IDS) keskittyvät monitoroimaan verkon toimintaa mahdollisten hyökkäysten varalta. [38]

Epäilyttävän toiminnan tarkkailu (engl. anomaly detection) on isossa roolissa pilvipohjaisissa finanssialan järjestelmissä esimerkiksi luottokorttivarkauksien ehkäisemisessä. [38] Rahoituslaitosten tulee monitoroida käyttäjiensä epäilyttävää toimintaa ja pääsyä kriittiseen dataan ja järjestelmiin, jotta vaarantuneet tilit ehditään huomata mahdollisimman ajoissa [3]. Pilvijärjestelmän, verkkoyhteyksien ja ohjelmien monitoroinnin tulee olla jatkuvaa, jotta uhat havaitaan mahdollisimman no-

peasti ja niiden seuraukset saadaan minimoitua. [2]

4.5 Tekoäly

Yksi keino tehostaa pankkisovellusten pilviturvaa jatkuvasti kehittyvien uhkien keskellä on hyödyntää tekoälyn tarjoamia mahdollisuuksia [2]. Tekoälyä hyödyntämällä pystytään tunnistamaan uhkia isoista datamääristä ja datan avulla tekoälymallit voivat oppia myös täysin uusista uhista, joita ei vielä edes tunneta [28]. Jim ja Munira 2024 havaitsivat tutkimuksessaan, että pilvipohjaisissa pankkipalveluissa merkittävä määrä hyödyntää tekoälyä epäilyttävän toiminnan monitoroinnissa ja sen on todettu parantavan monitoroinnin laatua. Laadun lisäksi tekoälyn tutkittiin vähentävän uhkien havaitsemiseen kuluvaa aikaa keskimäärin 70 % verrattuna perinteisiin menetelmiin. Samassa tutkimuksessa käsiteltiin tekoälyn hyödyntämistä vaatimustenmukaisuuden automatisoinnissa, jonka tehokkuus oli parantunut 50 % tekoälytyökalujen ansiosta. Lisäksi todettiin, että tekoälyllä parannelluilla salausmenetelmillä oli positiivinen vaikutus pilvipankkijärjestelmien tietosuojalle ja prosessien tehostamiselle. [29]

Tekoälyratkaisuiden lisäksi rahoituslaitokset voivat tehostaa tietoturvaansa lohkoketjujen tarjoamilla varmoilla ja turvallisilla kirjauksilla kaikista tapahtumista. Lohkoketjuihin tallennettavat konfiguraatiot mahdollistavat läpinäkyvyyttä, eheyttä ja jäljitettävyyttä pilvipalveluissa tapahtuviin jatkuviin muutoksiin. Näistä ominaisuuksista on hyötyä myös finanssialan vaatimustenmukaisuuden toteuttamisessa ja auditoinneissa. [28]

4.6 Kyberuhkatiedustelu

Kyberuhkatiedustelu (engl. Cyber Threat Intelligence, CTI) erityisesti organisaatioiden käyttämä menetelmä, missä analysoidaan kyberuhkia raa'asta datasta saatavan

jäsennellyn tiedon avulla. Sen ansiosta uhkia pystytään ymmärtämään paremmin ja niitä pystytään myös estämään. CTI voidaan jaotella eri tarkoituksiin: Taktinen, operatiivinen ja strateginen. Taktisen CTI:n tehtävä on auttaa organisaation tietoturvakeskuksia ennustamaan tulevia hyökkäyksiä. Operatiivista CTI:tä hyödynnetään uhkien tunnistamiseen ja turvastrategioiden määrittelyyn. Operatiivinen taso on taktista tasoa teknisempi ja siinä on tarkoitus ymmärtää uhkien käyttäytymistä tarkemmin. Strateginen kyberuhkatiedustelu on korkeatasoisinta tietoa, jonka tarkoitus on auttaa organisaation johtajia ymmärtämään kyberuhkien tapahtumia. [4]

CTI:llä on iteratiivinen elinkaari, joka koostuu toistuvista vaiheista [4]. Suunnitteluvaiheessa organisaation tietoturva-asiantuntijat määrittelevät CTI:stä saatavalle tiedolle vaatimukset. Tämän jälkeen haluttua dataa aletaan keräämään esimerkiksi OSINT-järjestelmistä (open-source intelligence) [21]. Muita mahdollisia tiedonlähteitä ovat muun muassa: sosiaalisesta mediasta ja pimeästä verkosta kerätyt keskustelut, kaupalliset lähteet, erilaiset aiheeseen liittyvät ammattilaisten yhteisöt ja tietoturvajärjestelmistä saatavat logit ja data. Kerättyä tietoa aletaan prosessoimaan esimerkiksi suodattamalla, ryhmittelemällä ja standardisoimalla ja tämän jälkeen tietoa pystytään analysoimaan. [4] Analysoitu tieto jaetaan organisaation päättäville tahoille, jotka hyödyttävät saatua tietoa turvallisuusmenetelmiin liittyvissä päätöksissä [21].

4.7 Liiketoiminnan jatkuvuussuunnittelu

Liiketoiminnan jatkuvuus (engl. business continuity) on pankkialan toiminnoissa tärkeää. Pilvipalvelut vähentävät asiakkaidensa tarvetta fyysiselle infrastruktuurille, mikä lyhentää käyttökatkoksia, koska palveluiden palautusprosessit ovat virtaviivaisempia. [23] Pilvipalveluntarjoajilla on lähtökohtaisesti useita datakeskuksia hajautetusti, mikä parantaa liiketoiminnan jatkuvuutta esimerkiksi luonnonkatastrofien tapahtuessa [35].

Liiketoiminnan jatkuvuuden suunnittelun kannalta on tärkeää ottaa huomioon katastrofipalautuminen (engl. disaster recovery) [56]. Sillä tarkoitetaan suunnitelmaa, miten organisaatio palauttaa järjestelmänsä toimintaan jonkin katastrofin tapahduttua. Katastrofi voi olla esimerkiksi laitteen vioittuminen, sähkökatkos, palvelunestohyökkäys, ihmisen tekemä virhe tai luonnonkatastrofi. [11]

Yksi katastrofipalautumisen menetelmä on tietojen varmuuskopiointi. Organisaation tiedoista säilötään toiseen sijaintiin, mistä tiedot saadaan palautettua, jos alkuperäiset tuhoutuvat. [11] Pilvipalveluiden tarjoamat automaattiset ja säännölliset varmuuskopioinnit pitävät asiakkaiden tiedot turvassa esimerkiksi, jos laitevika vaarantaa ne. [38]

Pilvipalveluntarjoajien kanssa solmittavat palvelutasosopimukset (Service Level Agreement, SLA) velvoittavat palveluntarjoajan takaamaan rahoituslaitokselle palveluiden saatavuuden ja tietoturvatason. Sopimuksen ehdot tulee neuvotella tarkasti, jotta palveluiden jatkuva laatu on taattu ja ehtojen rikkomisesta koituvat seuraamukset täytyy myös olla määriteltyinä. [2]

4.8 Hallinto ja vaatimustenmukaisuus

Finanssialan organisaatiossa hallinnon (engl. governance) ja vaatimustenmukaisuuden (engl. compliance) avulla organisaatio huolehtii, että heidän toimintansa vastaa säädöksiin, jotka varmistavat pilvipalveluiden turvallisuuden. Pilviturvallisuuden hallinto määrittelee toimintaperiaatteita, prosesseja ja organisaation rakennetta siten, että tietoturva otetaan huomioon. [22]

Kun finanssialan organisaatio päättää alkaa hyödyntämään pilvipalveluja, täytyy työntekijöiden teknisestä osaamisesta ja tietoisuudesta erilaisista kyberuhista pitää huolta. Tähän ratkaisuna toimii erilaiset koulutukset, joiden avulla nykyiset ja tulevat työntekijät voivat pitää taitonsa ajan tasalla. Esimerkiksi tietojenkalasteluun ja muihin sosiaalisen manipuloinnin keinoihin keskittyvät koulutukset turvaa-

vat organisaatiota, kun esimerkiksi pankin etulinjassa olevat työntekijät tunnistavat uhat ajoissa. [2], [24] Strategisella johtamisella, prosessien kehittämisellä ja toimintatapoja yhtenäistämällä turvallisuudesta voi tehdä osan organisaatiokulttuuria. Lisäämällä tietoturvamenetelmiä osaksi työntekijöiden päivittäisiä työtehtäviä, koko organisaation suojautuminen kyberuhkia vastaan tehostuu. [21]

Pilvipalvelut voivat edesauttaa ja tehostaa rahoituslaitoksen vaatimustenmukaisuutta. Pilviteknologiat tuovat organisaatiolle nykyaikaista infrastruktuuria ja palveluja, jotka vastaavat tuoreimpiin asetettuihin säädöksiin. [23] Useilla pilvipalveluntarjoajilla on omat työkalunsa vaatimustenmukaisuuden toteuttamiseen. Googlen Assured Workloads, AWS:n Audit Manager ja Azuren Compliance Manager tekevät säännösten noudattamisen tarkastamisesta automaattista, mikä tehostaa organisaation turvallisuutta. [31] Kun Chetwood Financial -pankki osti vuonna 2022 toisen pankkipalveluntarjoajan ja heidän oli tarkoitus yhdistää järjestelmänsä, saivat he pilvipalveluun siirtymällä käyttöön automaattiset turvallisuus- ja vaatimustenmukaisuustoiminnot. Pilvipalvelun käyttöönotto edisti pankin kykyä noudattaa säädöksiä, paransi turvallisuutta ja vähensi infrastruktuuriin liittyviä kustannuksia. [2]

5 Pohdinta

Pilvipalvelut tarjoavat finanssialalle skaalautuvia ja kustannustehokkaita ratkaisuja, joiden avulla rahoituslaitokset pystyvät kehittämään digitaalista toimintaansa. Niiden avulla on mahdollisuus tehostaa työntekijöiden prosesseja, mutta myös tehdä asiakaskokemuksesta parempi, sillä uusien innovaatioiden käyttöönotto on pilvipalveluiden joustavuuden ansiosta taloudellisempaa ja nopeampaa. [2], [38]

Tutkielmassa käy ilmi, että pilvipalvelut muodostavat finanssialalle lukuisia tietoturvaan liittyviä uhkia. Eräs aineistossa useasti esiintyvä uhka on luvaton pääsy, joka on suora uhka tietojen luottamuksellisuutta kohtaan, josta voi aiheutua suurta vahinkoa organisaatiolle ja sen asiakkaille. Luvaton pääsy voi aiheutua erilaisista syistä, esimerkiksi ihmisen tai järjestelmän virheestä.

Ihmisten muodostamat tietoturvauhat nousivat muutenkin ehkä yllättävänkin suureen rooliin esimerkiksi sisäisten uhkien ja sosiaalisen manipuloinnin yleisyytenä. Tämä korostaa organisaatioiden tarvetta panostaa teknisten ratkaisuiden lisäksi myös esimerkiksi työntekijöiden tietoturvakoulutukseen, jotta he pystyvät havaitsemaan poikkeamat ja tietojenkalasteluyritykset ajoissa. Henkilöstöä tulee sitouttaa tietoturvakulttuurin ylläpitämiseen, koska pelkät tekniset keinot eivät yksinään riitä puolustautumiseen uhkia vastaan.

Tutkielman perusteella voidaan todeta, että pilvipalveluiden uhkiin on löydetty monipuolisia ratkaisuja. Tuloksista käy ilmi, että erilaiset identiteetin- ja pääsynhallinnan mekanismit ovat yleinen tietoturvaratkaisu rahoituslaitosten pilvipalveluissa,

mikä on ratkaisu myös esimerkiksi luvattoman pääsyn uhkia vastaan. Eräs rahoituslaitoksille merkittävä lisäsuoja tunnistautumiseen on monivaiheinen tunnistautuminen, jonka on tutkittu vähentäneen pankkitilien väärinkäyttöä huomattavasti.

Zero Trust -mallin käyttöönotto vastaisi tehokkaasti luvattoman pääsyn uhkiin sekä sen avulla finanssialan organisaatiot pystyvät vastaamaan esimerkiksi EU:n NIS 2 -direktiivin vaatimuksiin. On kuitenkin syytä ottaa huomioon, että tietoturvamekanismien implementoiminen kasvattaa hyökkäyspinta-alaa, mikä voi puolestaan vaarantaa järjestelmää entisestään. Onkin tärkeää löytää tasapaino tietoturvan ja liian kompleksisen järjestelmän välillä, mikä edellyttää ratkaisuiden huolellista suunnittelua.

Kiinnostavaa on, että pilvipalveluiden avulla rahoituslaitokset pystyvät prosessien tehostamisen lisäksi myös suojautumaan tietoturvauhkia vastaan. Pilvipalvelut tehostavat liiketoiminnan jatkuvuutta, esimerkiksi varmuuskopioinnin kautta, joten ne edesauttavat rahoituslaitoksille merkittävää osa-aluetta eli tietojen saatavuutta. Pilvipalveluntarjoajat tarjoavat asiakkaillensa myös nykyaikaisia ratkaisuja esimerkiksi vaatimustenmukaisuuden toteuttamiseen, joten organisaatioiden on helpompi vastata alalle asetettuihin säädöksiin. Toisaalta herää kysymys, voiko organisaatio koskaan luottaa täysin, että käytetyn pilvipalvelun tietoturva on ajan tasalla ja kenellä on lopulta siitä vastuu.

On kiinnostava seurata, miten pilvipalvelut tulevaisuudessa kehittyvät ja millaiseksi myös uhkakenttä muovautuu jo lähivuosina. Kvanttiteknologian kehittymiseen ja sen vaikutukseen nykyisten salausmallien turvallisuuteen on tärkeää varautua. Tekoälyllä tulee olemaan rooli kvanttitekniikoiden yleistyessä esimerkiksi kvanttiturvallisten salausmenetelmien tehostamisessa, joten sen tuomat mahdollisuudet tulevat olemaan merkittäviä finanssialan pilvipohjaisille ratkaisuille kvanttihyökkäyksiä vastaan [37]. Yleisesti tekoälyn vaikutusta sekä uhkiin että ratkaisuihin on syytä seurata ja tutkia, sillä niiden kehittyminen tapahtuu nopealla tahdilla. Esimerkiksi

tekoälyllä suoritettava haavoittuvuuksien löytäminen muodostaa merkittävän uhan järjestelmille. Myös kirjallisuuskatsauksen tuloksissa tulee ottaa huomioon pilviteknologioiden jatkuva kehittyminen.

Tehostaakseen pilvipalveluidensa tietoturvaa, finanssialan toimijoiden kannattaa ennakoida ja tehdä konkreettisia toimia tietoturvallisuuden ylläpitämiseksi. Ihmiset ovat yksi suurimmista uhkista organisaatioille, joten työntekijöiden kouluttamisen merkitystä ei tule väheksyä. Organisaatioiden tulee panostaa sisäiseen tietoturvakulttuuriinsa, koska pelkät tekniset menetelmät eivät itsessään riitä puolustautumiseen uhkia vastaan. Teknisistä ratkaisuista erityisesti erilaiset identiteetin- ja pääsynhallinnan keinoja kannattaa ottaa laajasti käyttöön organisaation pilvipalveluissa luvattoman pääsyn estämiseksi. Uhkiin varautumiseen sisältyy myös tulevaisuuden uhkien tarkkailu ja teknologioiden kehittymisen seuraaminen. Finanssialan toimijoiden kannattaakin pysyä pilviturvallisuudesta ajan tasalla ja tehdä yhteistyötä pilvipalvelutarjoajansa kanssa.

6 Yhteenveto

Finanssialalla tulee ottaa toiminnassa huomioon lukuisia säädöksiä, käsiteltävän tiedon arkaluonteisuus ja merkitys yhteiskunnalle sekä yksittäisille ihmisille, minkä vuoksi tietoturva on tärkeä osa organisaatioiden toimintaa. Pilvipalvelut tuovat alalle uusia vaaroja, mutta niiden avulla tietoturvaa voidaan myös tehostaa. Tässä tutkielmassa tarkasteltiin pilvipalveluiden tietoturvauhkia ja -ratkaisuja finanssialalla.

TK1: Luvussa 3 tarkasteltiin, millaisia uhkia pilvipalveluiden käyttö tuo finanssialalle. Käy ilmi, että pilvipalvelut muodostavat useita erilaisia tietoturvauhkia liittyen luvattomaan pääsyyn. Luvattoman pääsyn voi mahdollistaa virhe pilvipalvelun konfiguraatiossa, identiteetinhallinnassa, autentikointijärjestelmässä tai salasanojen säilyttämisessä. Myös sisäiset uhat ja sosiaalinen manipulointi esitetään mahdollisina reitteinä luvattomalle pääsylle.

Palvelukatkokset ovat finanssialalla kasvava uhka, mikä aiheuttaa ongelmia työntekijöille ja loppuasiakkaille. Esimerkiksi pankkien arvokas rahaliikenne on houkutteleva kohde rikollisille, minkä vuoksi alalle kohdistuvat hyökkäykset ovat usein hyvin edistyneitä. Palvelunestohyökkäykset vaikuttavat suoraan palveluiden saatavuuteen, mikä edellyttää, että pilvipalveluiden tulisi pystyä kestämään hyökkäyksistä aiheutuvaa kuormitusta.

Tietovuodot ja -murrot ovat finanssialalla yleisiä taloudellisen hyödyn takia. Pilvipalveluiden moniasiakasympäristöt kasvattavat uhkaa, sillä jaetut resurssit voivat

mahdollistaa luvattoman pääsyn tietoihin. Hyökkäys voi kohdistua esimerkiksi henkilötietoihin tai rahoitus- ja maksutietoihin. Myös edistyvät jatkuvat uhat kohdistuvat usein rahoituslaitoksiin. Hyökkäykset voivat kestää pitkiäkin aikoja ja myös hyökkääjät hyödyntävät pilvipalveluita. Finanssialan tulee tulevaisuudessa varautua kvanttiteknologian aiheuttamiin uhkiin, sillä se tulee vaarantamaan nykyisiä yleisesti käytössä olevia salausmalleja. Siihen valmistautuminen ja suojausratkaisuiden toteuttaminen voisi olla potentiaalinen jatkotutkimuskohde.

Finanssialalla huomattava määrä kyberhyökkäyksistä perustuu tietojenkalasteluun, joka on yksi sosiaalisen manipuloinnin menetelmistä. Hyökkääjä voi esimerkiksi pankkina esiintymällä huijata uhrin luovuttamaan pankkitunnuksensa rikollisille. Pilviympäristöissä uhkien havaitseminen on yleensä hidasta, joten organisaation sisäiset uhat voivat myös saada laajasti aikaan vahinkoa, jonka kustannukset voivat kasvaa suuriksi. Sisäinen uhka voi olla organisaation oma työntekijä tai muu osapuoli, jolla on pääsy pilviympäristöön.

Finanssialaa määrittelee lait ja tiukat säädökset, kuten GDPR. Pilvipalveluita käytettäessä tuleekin palveluntarjoaja valita tarkasti sen mukaan, että vaatimustenmukaisuus toteutuu. Tämä voi olla haasteellista, jos pilvipalvelu esimerkiksi toimii alueella, missä kyseiset säädökset eivät ole laajasti käytössä.

TK2: Luvussa 4 esiteltiin erilaisia tietoturvaratkaisuja, joita rahoituslaitokset voivat hyödyntää. Yksi aineistossa usein esiintynyt ratkaisu oli salaus ja avaintenhallinta. Esimerkiksi päästä päähän -salaus on pankkitoiminnoille tehokas suoja tietomurtoja vastaan.

Monimutkaisissa pilviympäristöissä identiteetin- ja pääsynhallinnan merkitys korostuu, jotta vain tunnistettu henkilö pääsee tekemään esimerkiksi pankkisiirron tai työntekijällä on näkyvyys vain oman työroolinsa kannalta olennaisiin tietoihin. Vähimpien oikeuksien periaatetta hyödyntää myös Zero Trust -malli, jonka toiminta perustuu jokaisen käyttöoikeuspyynnön varmistamiseen ja jatkuvaan monitorointiin.

Zero Trust vastaa hyvin EU:n NIS 2 -direktiivin vaatimuksiin.

Eräs laajasti käytetty ratkaisu tietoturvan toteuttamiseen on monitorointi. Sen kohteena voi olla esimerkiksi verkkoyhteydet ja käyttäjien toiminta, jonka avulla epäilyttävä käyttäytyminen havaitaan ajoissa. Monitoroinnin laatua voidaan parantaa tekoälyn avulla ja tekoälyllä on muutenkin suuri rooli tietoturvaratkaisuiden tehostamisessa. Organisaatioiden käytössä voi olla myös kyberuhkatiedustelun menetelmiä, mikä tuottaa niille eri tasoista tietoa analysoimalla ja prosessoimalla erilaisista lähteistä kerättyä uhkiin liittyvää dataa. Tämän tiedon avulla organisaatio pystyy tekemään tietoturvaan liittyviä päätöksiä.

Liiketoiminnan jatkuvuuden turvaamiseksi pilvipalvelut tarjoavat automaattisia varmuuskopioita, joiden avulla organisaatio saa palautettua järjestelmänsä takaisin toimintaan sähkökatkoksen tai muun katastrofin sattuessa. Myös pilvipalveluntarjoajien datakeskusten hajautettu sijainti turvaa liiketoiminnan jatkuvuutta esimerkiksi luonnonkatastrofin sattuessa.

Pilvipalveluiden tarjoamilla työkaluilla finanssialan organisaatio voi tehostaa ja automatisoida toimialan tiukkaan vaatimustenmukaisuuteen vastaamista. Työntekijöiden osaaminen tulee pitää ajan tasalla, kun organisaatio siirtyy käyttämään pilvipalveluita. Erilaisiin kyberuhkiin liittyvät koulutukset pitävät organisaation tiedot turvattuina, kun työntekijät tunnistavat esimerkiksi tietojenkalasteluyritykset.

Lähdeluettelo

[1] S. Mamidi, "Privacy and Security in Cloud-Based Banking: A Technical Perspective", *IJSAT - International Journal on Science and Technology*, vol. 16, nro 1, 2025. DOI: 10.71097/IJSAT.v16.i1.2788.

[2] A. S. Naik, "Securing Banking Applications in the Cloud: Challenges and Strategies for Enhanced Security", teoksessa *2024 International Conference on Computer, Electronics, Electrical Engineering & their Applications (IC2E3)*, IEEE, 2024, s. 1–6.

[3] N. Shenisetty, "Addressing the Challenges of Data Security and Privacy in Cloud-Based Financial Systems", *Journal of Computer Science and Technology Studies*, vol. 7, nro 5, 2025. DOI: 10.32996/jcsts.2025.7.5.31.

[4] Red Hat, *What is confidential computing?* Viitattu 5. helmikuuta 2026. url: https://www.redhat.com/en/topics/security/what-is-confidential-computing.

[5] V. O. Safonov, *Trustworthy Cloud Computing*. Newark, United States: IEEE Computer Society Press, 2016.

[6] IBM, *What Is Cloud Computing?* Viitattu 23. lokakuuta 2025. url: https://www.ibm.com/think/topics/cloud-computing.

[7] P. Mell ja T. Grance, ”The NIST Definition of Cloud Computing”, *National Institute of Standards and Technology.*, 2011. DOI: https://doi.org/10.6028/NIST.SP.800-145.

[8] SSH, *Cloud Computing Services: Characteristics*. viitattu 28. lokakuuta 2025. url: https://www.ssh.com/academy/cloud/computing-services-characteristics.

[9] Google Cloud, *What is Disaster Recovery?* Viitattu 1. helmikuuta 2026. url: https://cloud.google.com/learn/what-is-disaster-recovery.

[10] S. Bhowmik, *Cloud Computing*. Cambridge: Cambridge University Press, 2017.

[11] IBM, *What is Threat Intelligence*. viitattu 1. helmikuuta 2026. url: https://www.ibm.com/think/topics/threat-intelligence.

[12] S. Kaarlejärvi ja T. Salminen, *Älykäs taloushallinto – Automaation aika*. Alma, 2018.

[13] Suomi.fi kehittäjille, *Tietoturva ja kyberturvallisuus - Kyberturvallisuuden ja digitaalisen turvallisuuden tietopankki*. viitattu 24. lokakuuta 2025. url: https://kehittajille.suomi.fi/palvelut/digiturva/tietoturva.

[14] Safestate, *Mitä tietoturvalla tarkoitetaan?*, 2023. viitattu 24. lokakuuta 2025. url: https://www.safestate.com/fi/artikkelit/mita-tietoturvalla-tarkoitetaan/.

[15] K. Rousku, *Kyberturvaopas: tietoturvaa kotona ja työpaikalla*. Helsinki: Talentum, 2014.

[16] J.-M. Mäntylä, ”16-vuotias poika päätyi mystisesti äitinsä verkkopankkiin ja siitä alkoi tapahtumasarja, joka johti S-Pankin jättisakkoihin”, *Yle Uutiset*, lokakuu 2025. viitattu 29. lokakuuta 2025. url: https://yle.fi/a/74-20189809.

[17] T. Kerkkänen, ”Motiivina hillitön pätemisen ja rahan tarve – Näin teinihakkerit kaatoivat OP:n verkkopankin”, *Yle Uutiset*, lokakuu 2016. viitattu 29. lokakuuta 2025. url: https://yle.fi/a/3-9258886.

[18] Kyberturvallisuuskeskus, *Käyttökatkot verkkopalveluissa ovat yleisiä ja usein vaarattomia*, 2023. viitattu 29. lokakuuta 2025. url: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kayttokatkot-verkkopalveluissa-ovat-yleisia-ja-usein-vaarattomia.

[19] Finanssivalvonta, *Tietoturvallisuus*. viitattu 25. lokakuuta 2025. url: https://www.finanssivalvonta.fi/finanssisektorin-toimijalle/pankki/fintech--finanssialan-innovaatiot/tietoturvallisuus/.

[20] N. Khan ja T. Daniel, *Utilizing AI and Blockchain for Cyber Threat Prediction in Financial Institutions: Tools and Techniques for Cloud Security Posture Management*, 2024. DOI: 10.13140/RG.2.2.30764.88965.

[21] A. L, R. P. Lakshmi ja S. Pavithra, ”Cybersecurity in Banking and Cloud Computing: Threats, Defenses, and Innovations”, teoksessa *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, IEEE, 2025, s. 1–6.

[22] A. Mahalle, J. Yong, X. Tao ja J. Shen, ”Data Privacy and System. Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure”, teoksessa *Proceedings of the 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design*, IEEE, 2018, s. 407–413.

[23] R. Vadisetty, ”Efficient Large-Scale Data based on Cloud Framework using Critical Influences on Financial Landscape”, teoksessa *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*, IEEE, 2024, s. 1–6.

[24] S. Satish, G. Sandeep Nadella, K. Meduri, M. Harish Maturi, F. Fatima ja H. Gonaygunta, ”Factors Influencing Trust in Cloud Adoption for Financial Services”, teoksessa *2024 International Conference on Information Technology and Computing (ICITCOM)*, IEEE, 2024, s. 60–65.

[25] B. Z. Irtaish, A. Atawnih ja A. Y. Owda, ”Zero Trust Cloud Storage and E-Payment in Local Enterprises”, teoksessa *2025 International Conference on Smart Learning Courses (SCME)*, IEEE, 2025, s. 113–119.

[26] S. Vinoth, H. L. Vemula, B. Haralayya, P. Mamgain, M. F. Hasan ja M. Naved, ”Application of cloud computing in banking and e-commerce and related security threats”, vol. 51, 2022. DOI: 10.1016/j.matpr.2021.11.121.

[27] A. Elzamly, B. Hussin ja A. S. H. Basari, ”Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study”, *International Journal of Grid and Distributed Computing*, vol. 9, nro 8, 2016. DOI: 10.14257/ijgdc.2016.9.8.13.

[28] S. Akhtar ja N. Rehman, *Enhancing Cloud Security Posture Management with Blockchain and AI: Tools, Techniques, and Best Practices for Financial Institutions*, 2024. DOI: 10.13140/RG.2.2.28667.73764.

[29] M. M. I. Jim ja M. S. K. Munira, ”The Role Of AI In Strengthening Data Privacy For Cloud Banking”, *Available at SSRN 5083379*, 2024. DOI: 10.70937/faet.v1i01.39.

[30] K. Khanfar, ”A New Conceptual Framework Modelling for Cloud Computing Risk Management in Banking Organizations”, *International Journal of Grid and Distributed Computing*, 2016. DOI: 10.14257/IJGDC.2016.9.9.13.

[31] V. Kulkarni, ”Zero Trust Security in Cloud Banking a Framework for Financial Institutions”, *International Journal of Leading Research Publication*, vol. 5, nro 3, 2024.

[32] O. C. Metibemu, T. O. Adesokan-Imran, A. J. Ajayi, O. J. Tiwo, A. T. Olutimehin ja O. O. Olaniyi, "Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications", *Journal of Engineering Research and Reports*, vol. 27, nro 3, 2025. DOI: 10.9734/jerr/2025/v27i31442.

[33] H. Nagarajan, "Assessing Security and Confidentiality in Cloud Computing for Banking and Financial Accounting", *International Journal of HRM and Organizational Behavior*, vol. 12, nro 3, 2024. viitattu 17. lokakuuta 2025.

[34] J. M. Lispector, "Comprehensive Frameworks for Ensuring Data Security and Regulatory Compliance in Financial Sector Cloud Technologies", *International Journal of Cloud Computing (IJCC)*, vol. 2, nro 2, 2024.

[35] P. Rohmeyer ja T. Ben-Zvi, "Managing Cloud Computing risks in financial services institutions", teoksessa *2015 Portland International Conference on Management of Engineering and Technology (PICMET)*, IEEE, 2015, s. 519–526.

[36] S. Sivasamy, M. Gangrade ja R. M. Rajendran, "Role of Cloud Computing and Data Security in Financial Services", teoksessa *2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)*, 2025, s. 394–399.

[37] I. O. Owolabi, C. K. Mbabie ja J. C. Obiri, "AI-driven cybersecurity in FinTech & cloud: Combating evolving threats with intelligent defense mechanisms", *International Journal of Multidisciplinary Research in Science, Engineering and Technology*, vol. 7, nro 12, 2024. DOI: 10.15680/IJMRSET.2024.0712004.

[38] N. R. Panguluri, "Cloud computing and its impact on the security of financial systems", *Computer Science and Engineering*, vol. 14, nro 6, 2024. DOI: 10.5923/j.computer.20241406.0.

[39] S. Madasamy, ”Secure cloud architectures for AI-enhanced banking and insurance services”, *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, nro 2, 2022. DOI: https://www.doi.org/10.56726/IRJMETS22745.

[40] Cloud Security Alliance, *Top Threats to Cloud Computing: The Egregious 11*. viitattu 2. helmikuuta 2026. url: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/.

[41] Nordea, *Palvelunestohyökkäys – Mitä pankin asiakkaan on hyvä tietää?* Viitattu 7. marraskuuta 2025. url: https://www.nordea.fi/henkiloasiakkaat/sinun-elamasi/turvallisuus/palvelunestohyokkays.html.

[42] Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficom, *Autoreporterin haittaohjelmahavainnot*. viitattu 18. marraskuuta 2025. url: https://kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot.

[43] Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficom, *Miraissa on tulevaisuus*. viitattu 18. marraskuuta 2025. url: https://traficom.fi/fi/ajankohtaista/blogit/miraissa-tulevaisuus.

[44] Microsoft, *Mikä on tietomurto?* Viitattu 26. tammikuuta 2026. url: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-a-data-breach.

[45] Microsoft, *Mikä on tietovuoto?* Viitattu 26. tammikuuta 2026. url: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-a-data-leak.

[46] P. Arntz, ”4.7 million customers’ data accidentally leaked to Google by Blue Shield of California”, *Malwarebytes*, viitattu 28. tammikuuta 2026. url: https:

//www.malwarebytes.com/blog/news/2025/04/4-7-million-customers-data-accidentally-leaked-to-google-by-blue-shield-of-california.

[47] IBM, *What is Social Engineering?* Viitattu 18. marraskuuta 2025. url: https://www.ibm.com/think/topics/social-engineering.

[48] A. Mahalle, J. Yong ja X. Tao, "Insider Threat and Mitigation for Cloud Architecture Infrastructure in Banking and Financial Services Industry", teoksessa *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, IEEE, 2019, s. 16–21.

[49] V. D. Bhandarkar, K. M P, S. Hashmi, D. Singh, S. Rashid Anwar ja K. Bikram, "An Intelligent AI-Enabled Cloud Security System for Certifying Information in Financial Sectors", *Journal of Internet Services and Information Security*, vol. 15, nro 2, 2025. DOI: 10.58346/JISIS.2025.I2.013.

[50] J. Santala, *ISO/IEC 27000*. viitattu 3. helmikuuta 2026. url: https://www.mv.helsinki.fi/home/jussantt/arkkitehtuuri/iso27001.html.

[51] M. Garba, *Data Encryption Best Practices for Ransomware Resilience in Financial Cloud Platforms*. viitattu 29. tammikuuta 2026. url: https://www.example.com/data-encryption-ransomware-financial-cloud.

[52] V. Nutalapati, "Implementing End-to-End Encryption in Mobile Applications: Challenges and Solutions", *International Research Journal of Engineering & Applied Sciences, IRJEAS*, vol. 9, nro 2, 2021.

[53] Valtiovarainministeriö, *Ohje salauskäytännöistä (VAHTI 2/2015)*, Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. viitattu 25. tammikuuta 2026. url: https://vm.fi/julkaisu?pubid=8703.

[54] V. Mulder, A. Mermoud, V. Lenders ja B. Tellenbach, *Trends in Data Protection and Encryption Technologies*. Springer Nature Switzerland, 2023.

[55] Euroopan Unioni, *Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555*, 2022. viitattu 28. tammikuuta 2026. url: http://data.europa.eu/eli/dir/2022/2555/oj.

[56] Google Cloud, *Backup And Disaster Recovery*. viitattu 31. tammikuuta 2026. url: https://cloud.google.com/solutions/backup-dr.