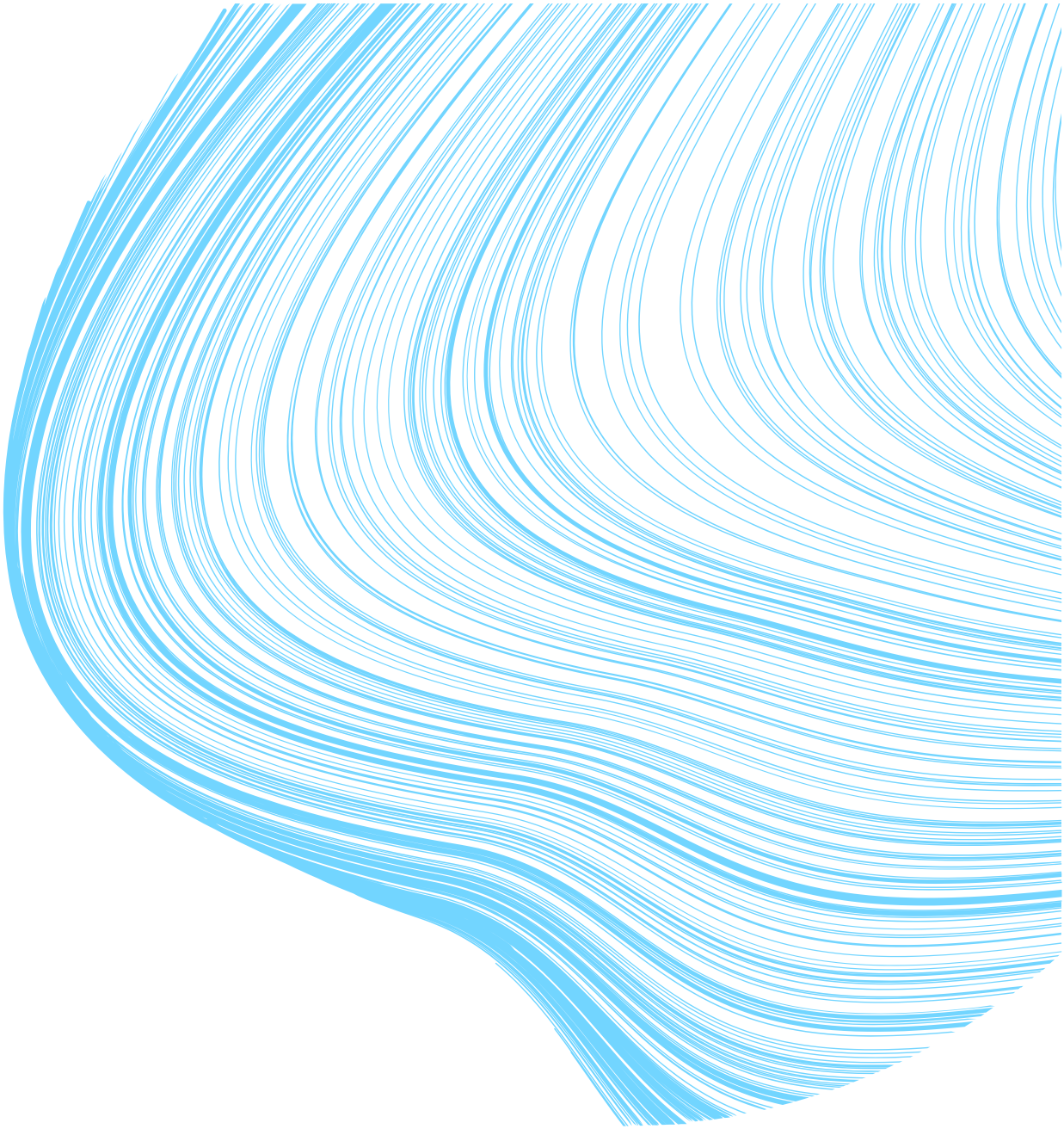


Cirrus-hanke
Esimerkkikäyttötapaus

Versio 1.0

DigiFinland

Sisällysluettelo

Sisällysluettelo 1
1. Johdanto 2
2. Yhteenveto ja johtopäätökset 2
3. Esimerkkitapauksen yleiskuvaus 5
4. Esimerkkitapauksen osa-alueet ja riskit 6
4.1. Tietoliikenne 6
4.2. Tietokannat 10
4.3. Kubernetes 12
4.4. Salausavaimet 13
4.5. Käyttäjähallinta 15
4.6. Muut huomioitavat asiat 19
5. Erityishuomioita lokituksesta ja valvonnasta 25

1. Johdanto

Tämä dokumentti esittelee Cirrus-hankkeen teknologiaesimerkkitapaukseen liittyvän toimittajavuoropuhelun havainnot ja johtopäätökset. Vuoropuhelut käytiin pilvipalveluntarjoajista AWS:n, Googlen, Microsoftin ja Oraclen kanssa. Dokumentti esittelee esimerkkitapauksen arkkitehtuurin ja siihen kytkeytyvät teknologiat osa-alueittain.

Kaikissa esimerkkitapaukseen liittyvissä kappaleissa on kappaleiden lopussa kuvattu oleellisia riskejä. Käytyjen toimittajavuoropuheluiden pohjalta on myös esitetty riskejä rajoittavia kontrolleja. Riskit liittyvät henkilötiedon käsittelyyn, mutta tässä niiden vaikuttavuutta ja todennäköisyyttä ei ole arvioitu tietosuojavaltuutetun toimiston vaikutusten arvioinnin ohjeen mukaisesti rekisteröidyn näkökulmasta.

GDPR:n osalta pyrittiin löytämään ja kartoittamaan artikla 5, kohta 2:n mukaisen osoitusvelvollisuuden toteutumista, sekä artiklan 25 mukaisen sisäänrakennettua ja oletusarvoista tietosuojaa, artiklan 28 ja 32 mukaisia turvallisuuteen liittyviä teknisiä ja organisatorisia toimenpiteitä kuten

a) henkilötietojen pseudonymisointi ja salaus;
b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;
c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;
d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi

GDPR:n resitaalissa numero 81 sanotaan muun muassa seuraavaa, huomioiden, että sertifiointimekanismi liittyy GDPR:n art 42 ja 43, sekä käytännenesäännöt GDPR:n artiklaan 40 ja 41, eikä siis mihin tahansa sertifiointeihin:

”Jotta voidaan varmistaa, että henkilötietojen käsittelijä noudattaa tämän asetuksen vaatimuksia rekisterinpitäjän puolesta suorittamassaan käsittelyssä, rekisterinpitäjän olisi antaessaan käsittelytoiminnat henkilötietojen käsittelijän tehtäväksi käytettävä ainoastaan sellaisia henkilötietojen käsittelijöitä, joilla on antaa riittävät takeet erityisesti asiantuntemuksesta, luotettavuudesta ja resursseista, jotta ne voivat panna täytäntöön tämän asetuksen vaatimusten mukaiset tekniset ja organisatoriset toimenpiteet, käsittelyn turvallisuus mukaan lukien. Sitä, että henkilötietojen käsittelijä noudattaa hyväksyttyjä käytännesääntöjä tai hyväksyttyä sertifiointimekanismia, voidaan käyttää osoittamaan rekisterinpitäjälle asetettujen velvollisuuksien noudattamista.”

2. Yhteenveto ja johtopäätökset

Pilvipalvelun käyttöön liittyvät riskit ovat olemassa, mutta samanlaisia riskejä on myös perinteisiä konesaleja käytettäessä. Pilvipalveluntarjoajat ovat suuria toimijoita, joilla on resursseja kehittää jatkuvasti palveluita, resursseja ja ominaisuuksia, jotka pienentävät ja poistavat riskejä mm. turvallisuuteen liittyen. Toimittajat parantavat jatkuvasti pilven turvallisuusominaisuuksia uusilla teknologisilla valinnoilla ja ratkaisuilla. Konesaliin voidaan käytännössä toteuttaa samat asiat, mutta se vaatii usein resursseja, joita asiakkailla ei välttämättä ole riittävästi, kuten osaamista, aikaa ja rahaa.

Jaetun vastuun malli rajaa tietoturvavastuiden jakautumisen pilvipalveluntarjoajan ja asiakkaan välillä. Tässä mallissa pilvipalveluntarjoaja vastaa pilven turvallisuudesta infrastruktuurin osalta, joka koostuu mm. fyysisistä datakeskuksista, laitteistoista ja fyysisistä verkoista (Security of the Cloud).

Asiakas puolestaan ottaa vastuun tietojensa, sovellusten, identiteetin ja pääsynhallinnan turvaamisesta sekä tietoturva-asetusten määrittämisestä käyttämiensä pilvipalveluiden sisällä (Security in the Cloud). Tämä yhteistyöhön perustuva lähestymistapa tarjoaa asiakkaille etuja, kuten lisääntyneen turvallisuuden, joustavuuden, skaalautuvuuden ja kustannustehokkuuden.

Jaetun vastuun malli mahdollistaa myös joustavamman varautumismahdollisuuden kehittyviin tietoturvauhkiin, ja molemmat osapuolet osallistuvat pilviympäristön yleiseen tietoturvaan. Muistettava on kuitenkin, että asiakkaan vastuulla on toiminta pilvessä, eli jaetun vastuun malli ei poista asiakkaan vastuuta. Myös kolmannen osapuolen ratkaisujen hyödyntäminen voi tulla ajankohtaiseksi ratkaisusuunnittelussa, mutta ne sisältävät omat riskinsä. Ulkopuoliset ratkaisut voivat lisätä turvallisuusriskiä, jos ne eivät ole turvallisia tai integroidu saumattomasti. Samoin kolmannen osapuolen ratkaisujen riskinä voi olla jatkuvan kehittämisen ja ylläpidon puute tai päättyvä elinkaari. Tämä voi johtaa vanhentuneisiin ominaisuuksiin, joista seuraa useita tietoturvariskejä, kuten esimerkiksi haavoittuvuuksia.

Pilvipalvelut mahdollistavat dynaamisen skaalautuvuuden, jossa resursseja voidaan lisätä tai vähentää tarpeen mukaan. Tämä tuo kustannustehokkuutta ja joustavuutta liiketoiminnalle ja auttaa osaltaan varautumaan ja varmistamaan toiminnan myös poikkeustilanteessa, kuten DDoS -hyökkäyksen aikana. Toisaalta, vaikka pilvipalvelut tarjoavat valmiita ratkaisuja moniin tarpeisiin, on tärkeää valita oikeat resurssit ja konfiguraatiot liiketoiminnan vaatimusten mukaisesti. Ohjelmistokehityksessä resurssit tulisi aina valita työkuorman perusteella, eikä toisinpäin. Tämä on valtava etu pilvessä, sillä pilvipalvelutarjoajilla on tarjolla resurssit eri työkuormiin, jotka ovat tarkoitettu ja optimoitu tiettyihin käyttötarkoituksiin. Pilvipalvelutoimittajien suosituksia ja ohjeita hyödyntämällä voidaan myös hallita esimerkiksi salaisuuksien ja käyttöoikeuksien hallintaan liittyviä riskejä. Kaiken kaikkiaan on mahdollista saavuttaa turvallinen lopputulos sekä nopeuttaa ohjelmistokehityksen kehitysprosessia, jonka ansiosta prosessi aina vaatimustenhallinnasta tuotantojulkaisuun saadaan optimoitua ja tuotettua arvoa asiakkaalle. Automatisoinnissa on huomioitava tarkasti turvallisuusnäkökulmat, jotta varmistetaan etteivät automaattiset prosessit itse aiheuta turvallisuusriskejä.

Selvitystyöhön valittu esimerkkitapaus havainnollistaa pilvipalveluiden riskien tunnistamista ja niiden hallintaa. Alla on esitetty tiivistetysti eri osa-alueiden keskeisimmät huomioitavat näkökulmat:

Tietoliikenne: *Turvallisen ja tehokkaan tiedonsiirron varmistaminen on ratkaisevaa pilvipalveluissa, koska se muodostaa eri komponenttien, resurssien ja palveluiden välisen vuorovaikutuksen ja liikenteen perustan. Tiedonsiirron riskeihin, kuten haavoittuvuuksiin, liittyy vakavia tietoturvauhkia. Näiden riskien torjunta edellyttää proaktiivisia toimenpiteitä, kuten vahvoja ja ajantasaisia salausprotokollia, suojattuja verkkoja monikerrosarkkitehtuureineen, sekä aktiivista valvontaa tietoturvauhkien, luvattoman pääsyn ja toimintahäiriöiden vähentämiseksi.*

Tietokannat: *Tietokannat ovat keskeisessä asemassa kriittisten tietojen hallinnassa ja niihin liittyy erityisiä riskejä, kuten luvaton käyttö, mahdolliset tietomurrot ja muut tietoturvapuutteiden tuomat uhat. Monitasoisen arkkitehtuurin ottaminen käyttöön on ratkaisevan tärkeää näiden riskien tehokkaaseen pienentämiseen. Resurssien erottaminen erillisiksi tasoiksi, jossa tietokanta sijaitsee suojattuna taustalla ja pääsy tietokantaan sallitaan vain Kubernetes-palvelulta, lisää suojakerroksia ulkoisia uhkia vastaan. Tehokkaaseen riskienhallintaan sisältyy parhaiden käytäntöjen noudattaminen, pilvitietoturvapalveluiden käyttö ja huomioiminen, kuten verkkosovellusten palomuurit ja salaustoimenpiteet, sekä palvelun ulko- että sisäpuolella.*

Kubernetes: *Vaikka Kubernetes toimii tehokkaana alustana konttisovellusten hallintaan ja skaalautuvuuden varmistamiseen, sen integrointi palveluihin tuo esiin näkökohtia, jotka vaativat huomiota. Kubernetes-klusterien turvallisuuden varmistaminen on ensiarvoisen tärkeää. Riskit voivat johtua haavoittuvuuksista, ohjaustason virheellisistä määrityksistä tai resurssien luvattomasta käytöstä. Parhaiden käytäntöjen, kuten*

roolipohjaisen pääsynhallinnan (RBAC), pod-suojauskäytäntöjen ja säännöllisten turvatarkastusten ottaminen käyttöön on tärkeää näiden riskien vähentämisessä. Monikerroksisen arkkitehtuurin merkitys piilee sen kyvyssä tarjota ylimääräinen suojakerros. Erottelemalla resurssit erillisiin tasoihin mahdolliset tietoturvahäiriöt rajoitetaan tiettyihin kerroksiin, mikä rajoittaa niiden vaikutusta ja vähentää riskejä tietoturvan osalta. Tämä toteutustapa ei ainoastaan suojaa luvattomalta käytöltä tai tietomurroilta ja -vuodoilta, vaan myös parantaa koko palvelun suorituskykyä ja luotettavuutta myös mahdollisten tieturvahyökkäysten aikana.

Salausavaimet: *Salausavaimilla on keskeinen rooli salassa pidettävien tietojen turvaamisessa, ja tämän alueen riskit voivat johtua riittämättömistä avainten hallintakäytännöistä, luvattomasta pääsystä avaimiin, avainten käytön toimintojen oikeuksista tai salausalgoritmien heikkouksista. Suojattu avainten hallinta, mukaan lukien säännöllinen kierrättäminen ja turvallinen tallennus, on elintärkeää näiden riskien tehokkaalle vähentämiselle. Lisäsuojaa voidaan saavuttaa laitteistoturvamoduuleilla (HSM) tai pilvipohjaisilla avaintenhallintapalveluilla.*

Käyttäjähallinta: *Käyttäjähallinta on kriittinen tekijä pilvipalvelujen turvallisuuden, vaatimustenmukaisuuden ja toiminnan eheyden varmistamisessa. Riskit voivat johtua riittämättömästä pääsynvalvonnasta, vaarantuneista valtuutustiedoista tai heikosta käyttöoikeuksien hallinnasta. Vahvojen käytäntöjen luominen, mukaan lukien vähimmän oikeuden periaate, monivaiheinen tunnistautuminen ja käyttäjien, oikeuksien ja mekanismien säännöllinen tarkistaminen, on ratkaisevan tärkeää näiden riskien tehokkaassa vähentämisessä. Vähimmän oikeuden periaatteen toteuttaminen tehostaa tietosuojaa rajoittamalla käyttäjien pääsyä vain välttämättömiin resursseihin minimoiden samalla turvallisuusriskejä sekä niiden vaikutuksia. Käyttäjähallintaan kuuluu myös käyttäjien toimien jatkuva lokitus ja valvonta, mikä on olennainen osa riskienhallintaa koska ilman niitä järjestelmiin ja käyttäjien tekemiin toimenpiteisiin ei ole näkyvyyttä. Lokeihin ja seurantatietoihin perustuvan automaation hyödyntäminen vähentää riskien toteutumisen todennäköisyyttä ja joissain tapauksissa ehkäisee riskien realisoitumisen.*

Muut huomioitavat asiat: *Edellä mainittujen osa-alueiden lisäksi tehokas riskienhallinta pilvipalveluissa ulottuu myös muihin alueisiin, kuten katastrofipalautukseen, tietokannan ja muiden tietojen väärinkäytön estämiseen, ohjelmistokehityksen julkaisuputkiin, ympäristön ja resurssien tilojen näkyvyyteen, tuotantotietojen käyttämiseen ja elinkaarihallintaan. Holistinen lähestymistapa, jossa yhdistyvät määritellyt turvallisuuskäytännöt, vaatimustenmukaisuustoimenpiteet ja ennakoiva seuranta koko pilviekosysteemissä, on olennainen osa riskienhallintaa. Riskien tunnistaminen ja vähentäminen eri alueilla antaa organisaatioille mahdollisuuden parantaa yleistä pilviturvallisuutta ja varmistaa palveluidensa luotettavuuden ja luottamuksellisuuden.*

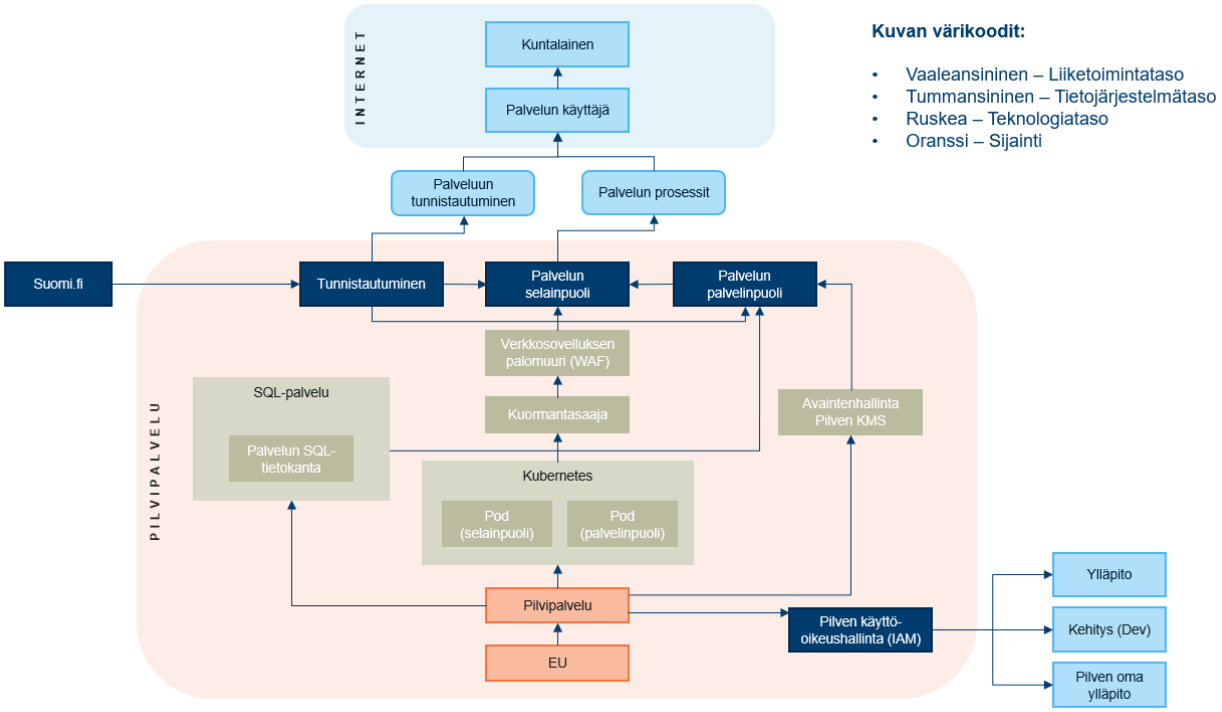
Riskienhallinta pilvipalvelun yhteydessä palvelee olennaisia lakeihin, määräyksiin ja ohjeistuksiin liittyviä tarkoituksia. Ensinnäkin se varmistaa tietosuojaa, yksityisyyttä ja turvallisuutta koskevien lakisääteisten vaatimusten noudattamisen. Velvoittavan sääntelyyn kuten GDPR liittyen riskienhallinta auttaa organisaatioita tunnistamaan riskejä kuten haavoittuvuuksia pilvipalveluissa, mukauttamaan tietoturvavalvontaa alan standardien kanssa sekä täyttämään sopimusvelvoitteet. Tämä järjestelmällinen lähestymistapa ei ainoastaan auta estämään oikeudellisia seurauksia ja säännösten mukaisia seuraamuksia, vaan auttaa myös rakentamaan kestävyyttä häiriöitä vastaan. Se auttaa myös valmistautumaan auditointeihin, jotka usein edellyttävät hyvin dokumentoituja turvallisuuskäytäntöjä.

Lisäksi riskienhallinta tukee organisaatioita saavuttamaan asetetut turvallisuusvaatimukset. Riskienhallinnan menettelyillä on keskeinen rooli pilvipalveluntarjoajien osaamisen arvioinnissa, palvelutason sopimusneuvotteluissa sekä pilvipohjaisten toimintojen turvallisuuden ja saatavuuden, sekä toiminnallisuuden varmistamisessa. Integroimalla riskienhallinnan pilvistrategiaansa organisaatiot voivat navigoida oikeudellisissa monimutkaisissa asioissa, parantaa tietosuojaa ja hyödyntää pilviteknologian etuja,

joiden yhteisvaikutuksella pilvipalveluiden tuottama hyöty voi tuoda mukanaan merkittäviä liiketoiminnallisia hyötyjä.

3. Esimerkkitapauksen yleiskuvaus

Teknologian esimerkkitapaus perustuu nykyaikaiseen Internet-palveluun. Tyypillisesti tällainen palvelu kehitetään hyödyntäen Git-versionhallintaa (esim. GitHub), jossa kehittäjien yhteistyö ja muu tiimityöskentely on optimoitua. Tehokkaasti rakennettu ja hoidettu ympäristö mahdollistaa organisaatiolle tehokkaan ja toimivan DevOps-mallisen toimintatavan tietojärjestelmän osalta.



Versionhallintapalvelusta ohjelmisto paketoidaan sopiviin kontteihin (container), jotka asetetaan ajoon konttiajoympäristöön (esimerkissä Kubernetes-ympäristöön). Selainpuolelle (frontend) ja palvelinpuolelle (backend) voi olla erilliset kontit, minkä lisäksi niitä voidaan Kubernetesin avulla skaalata sekä ylös, että alas lähes rajattomasti.

Kubernetes tarjoaa konttien hallinnan, tarjoten muun muassa tietoliikenteen podeille ja nodeille, joissa kontit ovat ajossa. Yhdessä nodessa voi olla useampi pod. Lisäksi Kubernetes tarjoaa mahdollisuuden ulkoiseen kuormantasaajaan. Tässä esimerkissä Kubernetes otetaan kokonaisuudessaan pilvipalveluna, jolloin Kubernetesin Plane on kokonaan pilvipalveluntarjoajan hallussa. Tällöin asiakkaan ei tarvitse huolehtia Kubernetesin päivityksistä ja toiminnasta. Asiakkaan pitää kuitenkin osata ajaa konttejaan Kuberenetesin podeissa.

Selainpuoli käsittää Internet-palvelun selaimessa toimivan osuuden, joka voi olla SPA-tyyppinen (Single Page Apps) tai SSR-tyyppinen (Server Side Rendered Sites) tai SSG-tyyppinen (Static Site Generator). Tässä esimerkissä on selainpuolen ajateltu olevan SPA-tyyppinen, jolloin selain tekee itse sovelluksen ja sen logiikan, kun taas palvelinpuoli on vain rajapintana ja logiikkana tiedon varastointiin. Lisäksi palvelinpuoli huolehtii pääsynvalvonnasta tietoon. Selainpuoli käyttää palvelinpuolen palveluita suojatusti HTTPS-yhteyden yli, mikä mahdollistaa AES-tasoisen salauksen näiden välisessä tietoliikenteessä.

Esimerkkitapauksessa käyttäjä tunnistetaan vahvasti, käyttäen Suomi.fi tunnistusjärjestelmää. Tunnistettu käyttäjä päästetään tekemään tietojärjestelmän prosessin mukaisia asioita itse järjestelmään, esimerkiksi täyttämään lomaketietoa tai lukemaan raportteja.

Esimerkkitapauksessa käytetään tietojen varastointiin pilvipalveluntarjoajan SQL-pohjaista pilvitietokantapalvelua, jolloin tietokantapalvelimen ylläpito tulee kokonaan pilvipalvelun tarjoajalta. Näin asiakkaan ei tarvitse päivittää tai muutenkaan ylläpitää itse tietokantapalvelinta, eikä tarvitse huolehtia sen skaalautuvuudesta tai riittävyydestä.

Esimerkissä tiedot salataan ja salausavaimia on ajateltu säilöttävän pilvipalvelutarjoajan salausavainten hallintapalvelussa.

Tällä tavoin rakennettu palvelu käsittää tyypillisesti DevOps-maailmassa omat pilviympäristönsä kehitykselle (Dev), testaukselle (Test), vastaanottotestaukselle ja liiketoiminnan kehitykselle (Staging) sekä tuotannolle (Prod). Huomioitavaa on, että ympäristöjä voidaan ohjata niin sanotuista CI/CD-putkista. Ympäristöjen ei tarvitse olla samankaltaisia tai edes samassa pilvessä. Kehitys-, testaus- ja vastaanottotestausympäristö voivat olla esimerkiksi kevyemmällä ympäristöllä verrattuna tuotantoympäristöön.

4. Esimerkkitapauksen osa-alueet ja riskit

Tämä luku esittelee esimerkkitapauksen eri osa-alueet, sekä esimerkinomaisesti näihin kytkeytyviä riskejä, sekä mahdollisia riskienhallintakeinoja. Riskien arviointi tulee tehdä aina käyttötapauskohtaisesti, joten esitettyjä riskejä ja riskienhallintakeinoja ei tule lähestyä tyhjentävänä listauksena.

4.1. Tietoliikenne

Pilvipalveluissa tiedonsiirto muodostaa eri komponenttien ja palveluiden välisen vuorovaikutuksen perustan, jolloin myös riskit realisoituessaan voivat aiheuttaa vakavia tietoturvauhkia. Turvallisen ja tehokkaan tietoliikenteen varmistaminen on välttämätöntä, mutta se tuo mukanaan omat riskinsä. Nämä riskit sisältävät haasteita, jotka liittyvät tiedonsiirron turvallisuuteen, mahdollisiin verkon, resurssien ja niiden välisen liikenteen haavoittuvuuksiin ja yleiseen luotettavuuteen.

Olipa kyseessä tiedonsiirto pilvipalvelun sisällä, vuorovaikutus Kubernetes-klusterin sisällä tai käyttäjien ja sovellusten välinen liikenne, koko järjestelmän ja palvelun turvaaminen on ratkaisevan tärkeää. Tietoliikenteen riskit voivat ilmetä mahdollisina tietoturvaloukkauksina, luvattomina pääsyinä tai palveluhäiriöinä. Ennakoivat toimenpiteet, mukaan lukien vahvat salausprotokollat, suojatut verkot monikerrosarkkitehtuureineen ja aktiivinen valvonta, ovat välttämättömiä näiden riskien vähentämiseksi.

Tietoliikenneriskien käsitteleminen sisältää tekniset ratkaisut ja ulottuu käytäntöihin, pääsynvalvontaan ja vaatimustenmukaisuustoimenpiteisiin. Priorisoimalla tietoliikenteen turvallisuuden ja eheyden organisaatiot voivat vahvistaa pilvi-infrastruktuuriaan mahdollisia uhkia vastaan, mikä varmistaa liikenteen luottamuksellisuuden ja luotettavuuden.

Tunnistetut riskit	Riskienhallintatoimenpiteet
Salaamattomat yhteydet ulkopuolelta. HTTP:n uudelleenohjausta HTTPS:aan pidetään yleisesti hyvänä tietoturvakäytäntönä tietojen luottamuksellisuuden ja eheyden varmistamiseksi. Vaikka tämä käytäntö parantaa turvallisuutta, on kuitenkin tärkeää ottaa huomioon mahdolliset riskit ja haasteet, jotka liittyvät HTTP -> HTTPS-uudelleenohjauksen toteuttamiseen pilvipalveluissa. Yksi riski on joutua Man-in-the-Middle (MitM) -hyökkäyksen kohteeksi uudelleenohjauksen aikana, jolloin hyökkääjä asettuu kahden kommunikoivan osapuolen väliin (asiakas ja palvelu) siepatakseen ja/tai muuttaakseen niiden välillä kulkevaa dataa. Näin ollen hyökkääjä pystyy esimerkiksi sieppaamaan liikenteen ja myös mahdollisesti saamaan selville käyttäjän käyttäjätunnuksen, sekä salasanan.	Pakotetaan pelkät HTTPS –yhteydet mahdollisiksi palveluun. Tämä voidaan toteuttaa esimerkiksi asettamalla palvelun ensimmäiseksi kontaktipisteeksi sisällönjakeluverkostot (Content Delivery Network, CDN) tai kuormantasaajan, ja konfiguroimalla ne hyväksymään pelkästään HTTPS-liikenne internetin yli. Näin ollen asiakas joutuu kirjoittamaan osoitepalkkiin "**Error! Hyperlink reference not valid.**...", jotta yhteys on mahdollinen. Tämä saattaa aiheuttaa tietämättömyyttä asiakkaissa, sillä jos he kirjoittavat vanhojen tapojen mukaisesti "**Error! Hyperlink reference not valid.**...", palveluun pääsy estyy. Asianmukaiset käyttäjien koulutus- ja valistuskampanjat voivat auttaa ratkaisemaan tämän huolen.
Salaamattomat yhteydet palvelun sisäpuolella aiheuttavat turvallisuusriskejä, jotka voivat vaarantaa tietojen ja järjestelmän eheyden ja luottamuksellisuuden sekä saatavuuden. Tiedon salaaminen levossa on elintärkeää, jotteivat käyttäjät tai resurssit voi lukea levyille tallennettuja salassa pidettäviä tietoja. Jotkin säädökset, kuten PCI DSS (Payment Card Industry Data Security Standard), vaativat, että palvelun sisäiset yhteydet ovat suojattuja. Salaamattomat yhteydet kasvattavat riskiä komponenttien välisen liikenteen salakuunteluun.	Järjestelmät voidaan suunnitella ja toteuttaa turvallisiksi myös tiedon salauksen osalta. Ulkopuolelta tuleva liikenne voidaan pakottaa salatuksi, mutta myös järjestelmän sisäinen liikenne voidaan konfiguroida siten, että vain salattuja yhteyksiä käytetään komponenttien väliseen tiedonsiirtoon. Jos palvelussa käytetään resursseja, jotka vaativat tiedonsalauksen purkamista, kuten verkkosovelluksen palomuuria (WAF, Web Application Firewall), ne puretaan ja uudelleen salataan ko. resursseissa. Näin saadaan keskeytymätön salaus luotua päätepisteiden välille. Riskiä voidaan lisäksi hallita ja pienentää käyttämällä yksityisiä verkkoja, päätepisteitä ja yksityisiä linkkejä tapauksissa, joissa liikenne muuten kulkisi internetin yli pisteestä toiseen. Tällaisia tapauksia on esimerkiksi objektivarastot, jotka ovat pilvipalveluntarjoajilla ns. maailmanlaajuisia palveluita ja oletusarvoisesti liikenne niihin kulkee internetin yli. Yksityisillä linkeillä ja päätepisteillä liikenne esimerkiksi virtuaalikoneen ja objektivaraston välillä saadaan kulkemaan pilvipalveluntarjoajien runkoverkkojen kautta ilman, että liikenne kulkee julkisen internetin kautta.
Vanhentuneet protokollat: **SSL/TLS-protokollien vanhentuneiden tai suojaamattomien versioiden ja heikkojen salauspakettien käyttö voi altistaa haavoittuvuuksille** ja sitä kautta tietoturvauhkille. Salassa pidettävät tiedot vaativat aina vahvan suojan. TLS-protokollat tarjoavat luottamuksellisuuden, eheyden ja usein aitouden suojan tiedoille, kun niitä siirretään verkon yli. Vanhentuneissa protokollissa, kuten SSLv2, SSLv3 ja TLS:n aikaisemmissa versioissa (esim. TLS 1.0, TLS 1.1), on tunnettuja tietoturva-aukkoja. Nämä haavoittuvuudet voivat antaa hyökkääjille	Luodaan prosessit, jolla voidaan varautua ja vaihtaa nykyaikaisimpiin saatavilla oleviin TLS/SSL-versioihin, kuten TLS 1.2 ja TLS 1.3 (suositeltavin). Pilvipalveluntarjoajat päivittävät protokollien käyttömahdollisuuksia poistamalla vanhentuneita protokollia tarjoamastaan mutta asiakkaan tehtäviä suositeltavia riskinhallintakeinoja ovat mm. päivittää säännöllisesti palvelut käyttämään moderneja uudempia protokollia, luomalla käytänteet vanhentuneiden

mahdollisuuden käyttää hyväkseen protokollan heikkouksia ja vaarantaa tietojen luottamuksellisuuden ja eheyden. Vanhentuneissa protokollissa käytetään usein heikompia salausalgoritmeja ja avainten pituuksia, joten niiden salaus on helpompi murtaa kuin uusien ajantasaisten protokollien.	protokollien estämiseksi sekä korjaamalla proaktiivisesti vanhentuneisiin protokolliin liittyviä riskejä. Näitä tukemaan on suositeltavaa suorittaa säännöllisiä turvallisuusarviointeja, jotta tunnistetaan ja sitä kautta voidaan korjata vanhentuneiden protokollien käyttöön liittyvät haavoittuvuudet. Lokitus, valvonta ja hälytykset, sekä mahdollinen automaatio tukevat erinomaisesti riskien hallintaa. Tarkastelemalla käytettäviä SSL/TLS -yhteyksiä voidaan tunnistaa ja löytää vanhentuneita protokollia käyttäviä kohtia ja niiden avulla voidaan tehdä välittömästi tarvittavat toimenpiteet asian korjaamiseksi.
Vanhentuneet tai virheelliset varmenteet saattavat johtaa palveluhäiriöihin ja mahdollisiin tietoturvaongelmiin. Digitaalisten varmenteiden, kuten TLS/SSL-sertifikaattien, tarkoitus on varmistaa palvelun tai palvelun omistajan henkilöllisyys ja salata yhteys asiakkaan (selaimen) ja palvelimen (palvelu) välillä. Vanhentuneilla varmenteilla on sekä tietoturva-, että muita riskejä, kuten maine- ja taloudellisia riskejä. Jos varmenne on vanhentunut, se todennäköisesti vaikuttaa käyttäjän haluun käyttää palvelua ja jos palvelussa käsitellään esimerkiksi salassa pidettäviä tai maksutietoja, käyttäjä ei todennäköisemmin anna näitä tietoja palveluun. Tietoturvariski sisältää useammanlaiset hyökkäykset, kuten man-in-the-middle, sekä tietojenkalasteluriskit. Vanhentuneen tai viallisen varmenteen takia on korkea riski joutua man-in-the-middle -hyökkäyksen kohteeksi, jolloin hyökkääjä voi siepata ja varastaa käyttäjän ja palvelun välistä liikennettä ja tietoja. Tietojenkalasteluriski kasvaa siinä suhteessa, että vanhentuneen tai puuttuvan varmenteen takia on vaikea varmistaa, onko palvelu turvallinen ja hyökkääjä voi luoda esimerkiksi kopion palvelusta ja näin huijata käyttäjiä väärään palveluun.	Pilvipalveluntarjoajilla on käytössä palvelut varmenteiden hallintaan, jotka sisältävät varmenteen automaattisen uusimisen. On syytä huomata tämän koskevan vain pilvipalveluntarjoajien hallinnoimia varmenteita. Jos organisaatio on itse tuonut varmenteet (import) palveluun, pilvipalveluntarjoajat eivät voi automaattisesti uusia niitä. Silloin asiakkaan on itse uusittava varmenne hankkimalla uusi varmenne myöntäjältä ja tuotava se manuaalisesti pilvipalveluntarjoajan varmenteiden hallintaan. Eri pilvipalveluntarjoajille saattaa olla eri käytäntöjä varmenteiden uusimiseen. Esimerkiksi AWS:n certificate managerissa (ACM) luotu varmenne uusitaan automaattisesti vain DNS –validoiduille varmenteille. Email-validoiduille varmenteille ei ole automaattista uusimista, vaan varmenteen vanhenemisesta lähetetään ilmoitus sähköpostiosoitteeseen, jolle validointi on tehty. Suositeltavaa on luoda hälytykset varmenteiden vanhenemisesta. Näin ollen pystytään tekemään tarvittavat toimenpiteet ennen kuin varmenteet vanhenevat ja riskit mahdollisesti realisoituvat.
Jos SSL/TLS-varmenteissa käytetty yksityinen avain vaarantuu, se voi johtaa salassa pidettävien tietojen sieppaamiseen ja salauksen purkamiseen. Jos hyökkääjä saa yksityisen avaimen haltuunsa, se mahdollistaa liikenteen salakuuntelun ja hyökkääjä voi purkaa salatun liikenteen, jolloin kyseessä on todellinen turvallisuusriski. Vaarantunut yksityinen avain antaa hyökkääjille mahdollisuuden suorittaa Man-in-the-Middle -hyökkäyksiä. Näin olleen hyökkääjä voi siepata ja manipuloida käyttäjien ja palveluiden välistä liikennettä, mikä voi johtaa tietojen peukalointiin, haitallisen sisällön lisäämiseen tai salakuunteluun. Tämä voidaan tehdä mm. pyytämällä käyttäjää todentamaan uudelleen ja siten luovuttamaan esimerkiksi salasanansa tai muun todentamiseen käytetyn tiedon tai liittämällä haittaohjelmia liikenteen mukaan.	Yksityisten avainten suojaaminen on ratkaisevan tärkeää salatun viestinnän turvallisuuden ylläpitämiseksi. Pilvipalvelun julkisia varmenteita käytettäessä esimerkiksi AWS ei anna mahdollisuutta tallentaa yksityistä avainta, jos varmenne on AWS:n hallinnoima. Jos yksityinen avain on vaarantunut, varmenne on syytä peruuttaa. Jos pilvipalveluntarjoajan hallinnoimaa varmennetta ei voida tuhota vaan pitää peruuttaa, asiakas ei välttämättä pysty sitä itse tekemään. Se saattaa vaatia pilvipalveluntarjoajan teknisen tuen toimenpiteitä. Jos varmenne on hankittu 3.osapuolelta, varmenne peruutetaan ilmoittamalla 3.osapuolelle ja toimitaan siihen liittyvän prosessin mukaan.

SSL/TLS-kättelyprosessiin kohdistuvat **DDoS-hyökkäykset** voivat kuormittaa palvelimet ja palvelun, mikä johtaa palvelun heikkenemiseen tai palvelun estoon.	DDoS:n lieventämisstrategioiden toteuttaminen on ratkaisevan tärkeää saatavuuden kannalta. DDoS suojauskeinoja ovat mm. rajoittaa alaa, mihin voidaan hyökätä, ja tässä käyttötapauksessa kuormantasaajien ja mahdollisesti sisällönjakoverkkojen hyödyntäminen estävät suoran pääsyn julkisesta internetistä muihin resursseihin, kuten Kubernetes –palveluun sekä tietokantaan. Skaalautuvuuden suunnittelu on osa hyökkäyksiin varautumista. Mahdollisen hyökkäyksen tapahtuessa hyvin suunniteltu ja toteutettu palvelu voi jatkaa toimintaansa, jos palvelun osat pystyvät vastaamaan hyökkäyksen aikaiseen liikenteeseen ja kuormaan. Monikerrosarkkitehtuuri ja palvelun resurssien skaalautuminen auttavat toimimaan hyökkäyksen aikana ja vähentävät hyökkäyksen tietoturvariskejä sekä parantavat saatavuutta. Esimerkiksi pilvipalveluiden kuormantasaajat ovat hallinnoituja palveluita ja skaalautuvat automaattisesti hyökkäyksen aikana ja siihen integroitu WAF ja/tai muut ratkaisut auttavat estämään vaarallisen liikenteen pääsyä eteenpäin. Applikaatiotasolla oleva Kubernetes-kerros skaalautuu erikseen. Jos liikenne tulee kuormantasaajalta Kubernetekseen niin järkevällä skaalauksella applikaatiotaso jatkaa toimintaansa myös hyökkäyksen aikana. Tietokanta on myös hallinnoitu palvelu ja pääsy siihen on monikerrosarkkitehtuurissa rajoitettu vain applikaatiokerrokselle, joten senkin automaattinen skaalaus auttaa järjestelmää pysymään toimintakunnossa hyökkäyksen aikana. Tähän voisi yleisenä ohjeena sanoa, että on erittäin tärkeää tehdä toimenpiteet hyökkäyksien estämiseksi mutta yhtä tärkeää myös tehdä toimenpiteitä hyökkäyksen vaikutusten minimoimiseksi.
Tietojen siirto EU/ETA alueen ulkopuolelle GDPR:n vastaisesti. Julkiset pilvipalveluntarjoajat tarjoavat maailmanlaajuisia palveluita ja useimmissa tapauksissa asiakas päättää siirtääkö tietoja maantieteellisten rajojen yli esimerkiksi tietoja replikoimalla tai varmuuskopioimalla. Sisällönjakeluverkot (Content Delivery Network, CDN) ovat kuitenkin resurssiryhmä, jonka käyttö pitää varmistaa GDPR:n osalta. Sisällönjakeluverkot ovat maailmanlaajuisesti hajautettuja palveluita tietojen tallentamiseksi välimuistiin nopeammin kuluttajille saataviksi. Jos sisällönjakeluverkkoja on suunniteltu otettavaksi käyttöön, on syytä varmistua, ettei esimerkiksi GDPR –vaatimuksia rikota.	Jostain syystä julkiset pilvipalvelun tarjoajat eivät tarjoa helposti löydettävää dokumentaatiota tiedon tallentamisen osalta koskien GDPR-asetusta, joten asiakkaan on syytä varmistaa ennen sisällönjakeluverkon käyttöönottoa mahdolliset GDPR riskit palvelun osalta.

Sisällönjakeluverkkojen käytössä on riski, että vaikka itse palvelu ja järjestelmä sijaitsevat EU/ETA-alueella niin tieto saatetaan tallentaa välimuistiin myös muihin maanosiin, kuten esimerkiksi Pohjois-Amerikkaan. Vaikka pilvipalveluntarjoajat tarjoavat mekanismeja ja ohjeita sisällön tarjoamisen rajoittamiseksi vain EU/ETA -alueella, tieto voi silti olla tallennettuna sisällönjakeluverkossa alueen ulkopuolella.	

4.2. Tietokannat

Järjestelmissä ja palveluissa tietokannat ovat keskeisessä asemassa kriittisten tietojen hallinnassa ja tallentamisessa. Tietokantojen käyttöön liittyy kuitenkin sellaisia riskejä, jotka vaativat huolellista harkintaa ja varautumista suunnitelmien, toteutukseen ja valvonnan näkökulmista. Tietokantoihin liittyviä riskejä ovat luvaton käyttö, mahdolliset tietomurrot ja tallennettujen tietojen yleisen turvallisuuden ja eheyden vaarantuminen. Nämä riskit voivat johtua mm. väärin määritetystä pääsynvalvonnasta, riittämättömistä salauskäytännöistä tai tietokannan muuhun toteutukseen ja suojaukseen liittyvistä puutteista.

Monitasoisen arkkitehtuurin käyttöönotto on ratkaisevan tärkeää näiden riskien vähentämiseksi tehokkaasti. Monikerrosarkkitehtuuri sisältää resurssien erottamisen erillisiin kerroksiin, jolloin tietokanta sijaitsee suojattuna taustalla ja pääsy tietokantaan hyväksytään vain Kubernetes -palvelulta. Tämä erottelu auttaa suojaamaan tietokantaa suoralta ulkopuoliselta pääsyltä ja lisäämään ylimääräisiä suojakerroksia mahdollisia uhkia vastaan.

Väärin määritettyihin pääsynhallintajärjestelmiin, riittämättömiin salauskäytäntöihin tai tietokannan hallintajärjestelmän haavoittuvuuksiin liittyviä riskejä voidaan käsitellä tehokkaammin ottamalla käyttöön monitasoinen lähestymistapa, sekä hyödyntämällä pilvipalveluntarjoajien turvallisuutta parantavia palveluita, kuten esimerkiksi verkkosovelluksen palomuurit, tiedon salaukset sekä palvelun ulko-, että sisäpuolella jne.

Tietokantojen suojaaminen ei ole pelkästään tekninen huolenaihe vaan se sisältää myös tiukkojen pääsykäytäntöjen, salausprotokollien ja jatkuvan valvontakäytännön käyttöönoton. Hyvin suunniteltu monitasoinen arkkitehtuuri varmistaa, että mahdolliset tietoturvauhat rajoittuvat tiettyihin tasoihin, mikä pienentää tietoturvahäiriöiden vaikutusta tietokantoihin ja järjestelmään ylipäätään.

Tunnistetut riskit	**Riskienhallintatoimenpiteet**
Käytettäessä tietokantapalvelua, **tietoliikenteen suojaaminen vaarantuu.**	Pilvipalveluntarjoajat tarjoavat mahdollisuuden kytkeä SSL/TLS salaus tietokantapalveluihin päälle, jolloin tietoliikenne salataan palvelimen ja asiakkaan välillä.
DDoS, SQL injektiot jne. ulkopuolelta, turvallisuusriskit, tietomurto sekä palvelunesto. Hyökkäykset koskevat myös tietokantoja ja vaikka tietokannat sijoitetaankin internetin yli saavuttamattomiksi, hyökkäyksissä yritetään vaikuttaa myös niihin.	Monikerrosarkkitehtuurilla voidaan pienentää hyökkäyksen riskiä tietokantoihin. Verkkosovelluksen palomuurien integrointi kuormantasaajiin ja/tai sisällönjakeluverkkoihin (Content Delivery Network, CDN) auttaa esimerkiksi sql injektoiden havaitsemisessa ja estämisessä. Niissä hyökkääjä lisää haitallista SQL –koodia keskustellessaan sovelluksen kanssa. Mikäli sovelluksessa on haavoittuvuus, niin hyökkääjä voi saada tietokannasta salassa pidettäviä tietoja, muuttaa tietokannan sisältöä tai suorittaa hallintatoimia tietokannassa.

	Verkkosovelluksen palomuurit mahdollistavat sääntöjen integroimiset osaksi palomuuria (esim. OWASP Top10), sekä IP-osoitteiden ja maantieteellisten sijaintien sulku- ja pääsylistaukset. Näillä sulku- ja pääsylistauksilla voidaan palveluun pääsy sallia esimerkiksi vain tietyistä maista, jolloin voidaan rajoittaa käyttäjien pääsy mahdolliseksi esimerkiksi vain Suomesta. Jos käyttäjä yrittää käyttää palvelua Suomen ulkopuolelta, verkkosovelluksen palomuuri estää liikenteen ja näin ollen estää pääsyn palveluun.
Tietokantapalvelun pääkäyttäjän tunnukset saadaan selville, joka muodostaa tietovuoto- ja turvallisuusriskin. Kun tietokanta luodaan, pääkäyttäjälle luodaan käyttäjätunnus ja salasana. Pääkäyttäjän oikeudet ovat laajat, yleensä sillä on enimmäiskäyttäjäoikeudet. Siksi näiden tunnusten suojaaminen on tärkeää, sillä niiden vuotaminen vääriin käsiin voi johtaa vakaviin tietoturvaongelmiin. Riskiä lisäävät liian helposti arvattavat käyttäjätunnukset ja salasanat.	Jotta Pääkäyttäjän käyttäjätunnus ja salasana eivät ole helposti arvattavissa, organisaatioiden tulisi luoda käytännöt ja sisäiset vaatimukset pääkäyttäjän tunnuksille. Monet pilvipalveluntarjoajat antavat oletuskäyttäjätunnuksen palvelua luotaessa, mutta sen vaihtaminen voi olla järkevää, sillä hyökkääjän tietäessä oletuskäyttäjätunnuksen tehtäväksi jää enää salasanan selvittäminen. Salasanan tulisi olla riittävän pitkä ja vaikeasti arvattava ja tunnukset on talletettava paikkaan, joka vastaa vaatimuksia ja pienentää tietoturvauhkan mahdollisuutta. Tietoturvauhka voi tulla ulkopuolisen murtautujan ohella myös organisaation sisältä, joten tunnusten tallennuspaikan valinta on tärkeää ja keskeistä on myös huolehtia pääsynvalvonnasta ko. paikkaan.
Tietokannan tuhoutuu vahingossa tai vahingoittamistarkoituksessa, mikä on operatiivinen-, maine-, liiketoiminnan jatkuvuus sekä tietoturvariski. Tietokannat ovat kriittinen osa järjestelmiä ja tietokannan tietojen menettämisellä on suuret seuraukset, sillä jos tietoja ei voida palauttaa, on vaarassa jopa liiketoiminnan jatkuvuus. Siksi tietokantojen, ja muiden kriittisten tietovarastojen suojaaminen on välttämätöntä.	Luodaan käytännöt ja prosessit, joilla estetään tietokannan tuhoaminen sekä mahdollisen tuhoamisen aiheuttamat haitat. Tietojen suojaaminen varmistetaan esimerkiksi pääsynhallinnalla, käyttämällä automaattisia ja manuaalisia varmuuskopioita sekä testaamalla palautusprosesseja.
Tietokantapalveluun päästään internetin yli, jolloin palvelun yleinen turvallisuus vaarantuu ja syntyy tietovuotoriski. Jos tietokanta on toteutettu siten, että siihen on mahdollista päästä suoraan internetistä, tietoturvariski kasvaa oleellisesti ja seuraukset voivat olla massiiviset mm. operatiivisen toiminnan, maineen, liiketoiminnan jatkuvuuden kannalta.	Voidaan todeta, että tietokantaan ei ole syytä päästä suoraan internetistä. Se on siksi suojattava huolellisesti ja tähän pilvipalveluntarjoajilla on tarjolla keinoja mm. verkkoarkkitehtuurin, verkon suojausryhmien (Network Security Groups), suojausryhmien (Security Groups), palomuurien, salausprotokollien, auditointien ja lokituksen sekä hallinnoitujen palveluiden ominaisuuksien osalta. Monikerrosarkkitehtuurilla voidaan estää suora pääsy tietokantaan ja tässä esimerkkikäyttötapauksessa pääsy on syytä sallia vain Kubernetes-palvelusta.

4.3. Kubernetes

Kubernetes toimii tehokkaana alustana konttisovellusten hallintaan ja niiden skaalautuvuuden varmistamiseen. Kubernetesin liittäminen osaksi palvelua tuo kuitenkin mukaan uusia huomioitavia näkökohtia. Kubernetes -riskit liittyvät konttipohjaisten työkuormien turvalliseen käyttöön, konfigurointiin ja organisointiin.

Kubernetes-klusterien turvallisuuden varmistaminen on ensiarvoisen tärkeää. Riskit voivat johtua kuvien (images) haavoittuvuuksista, Kubernetes-ohjaustason (control plane) virheellisistä määrityksistä tai salassa pidettävää tietoa sisältävien resurssien riittämättömästä suojaamisesta. Näiden riskien torjumiseksi tehokkaasti on syytä noudattaa parhaita käytäntöjä, kuten roolipohjaista pääsynhallintaa (RBAC), pod-tietoturvakäytäntöjä ja säännöllisiä tietoturvatarkastuksia.

Myös Kubernetesin osalta olennainen strategia järjestelmän turvallisuuden parantamiseksi on monikerrosarkkitehtuuri. Tämä lähestymistapa sisältää resurssien jäsentämisen erillisiksi tasoiksi, jolloin palvelun selainpuoli toimii asiakkaiden käyttöliittymänä ja Kubernetes toimii sovelluskerroksessa kommunikoiden mm. tietokannan kanssa. Liikenne kulkee käyttöliittymästä kuormantasaajan kautta Kubernetesiin ja Kuberneteksesta tietokantaan.

Monitasoisen arkkitehtuurin hyöty piilee sen kyvyssä tarjota ylimääräinen suojakerros. Erottelemalla resurssit erillisiin tasoihin, mahdolliset tietoturvahäiriöt rajoitetaan tiettyihin kerroksiin, mikä pienentää niiden vaikutusta ja vähentää riskejä myös tietoturvan osalta. Tämä toteutustapa ei ainoastaan suojaa luvattomalta käytöltä tai tietomurroilta ja -vuodoilta, vaan myös parantaa koko palvelun suorituskykyä ja luotettavuutta mahdollisten tieturvahyökkäysten aikana.

Tunnistetut riskit	Riskienhallintatoimenpiteet
Tiedot ja liikenne eivät pysy salattuna palvelun sisällä. Jos järjestelmän sisäistä liikennettä ei ole salattu, se altistaa eri resurssien ja palvelujen välisen viestinnän mahdollisille tietoturvariskeille. Ilman salausta luvattomat tahot voivat siepata ja salakuunnella palvelun sisäistä liikennettä, joka yhdessä muiden tietoturvapuutteiden kanssa voi olla kriittinen riski. Jos murtautuja pääsee järjestelmän sisälle, hän pystyy salakuuntelemaan ja sieppaamaan liikennettä vaivattomasti ja tietomurron ohella myös peukaloimaan tietoa. Tämä voi johtaa salassa pidettävien tietojen, tunnistetietojen tai muiden kriittisten tietojen vaarantumiseen. Tietojen salaus palvelun sisällä voi olla myös sääntelyn vaatimuksena. Näiden vaatimusten noudattamatta jättäminen voi johtaa oikeudellisiin seurauksiin.	Palvelun sisäisen liikenteen salaaminen pystytään toteuttamaan pilvipalveluntarjoajien tarjoamilla mekanismeilla aina internetin pääsypisteestä taustapalvelimiin saakka. Kuormantasaajat tukevat erilaisia prosesseja tiedon salauksen ja purkamisen suhteen. Jos kuormantasaajaan integroidaan Web Application Firewall, salaus puretaan ennen WAF:n prosessia ja salataan uudelleen eteenpäin lähetettäessä. Kuberneteksen ingress tukee SSL/TLS passthrough aktivointia, jolloin salaus voidaan viedä aina palvelinkerrokseen asti ja tämän avulla saadaan tiedot pidettyä salattuna myös Kubernetes –palvelussa aina tietokantaan saakka.
Haavoittuvien kuvien (image) käyttö voi johtaa tietoturvaloukkauksiin ja pohjakuvissa (base image) olevien haavoittuvuuksien hyödyntämiseen.	Kubernetes-palvelun kuvien säännöllinen päivittäminen ja tämän prosessin liittäminen osaksi julkaisuputkea pienentää tietoturvariskiä. Jos kuvissa havaitaan haavoittuvuuksia, julkaisuputken on pysähdyttävä siihen, eikä julkaisuja viedä eteenpäin

	ennen kuin haavoittuvuudet kuvissa on tarkistettu ja korjattu.
Kubernetekseen pääsy suoraan internetistä. Kubernetes-palvelun salliminen suoraan internetista tuo mukanaan sekä tietoturva-, että operatiivisia riskejä. Tässäkään käyttötapauksessa ei ole mitään syytä päästää julkisen verkon käyttäjiä kutsumaan suoraan Kubernetes-palvelua. Kubernetes toimii tässä käyttötapauksessa taustapalveluna applikaatiokerroksessa, joten kutsujen pitäisi tulla pelkästään palvelun selainpuolelta. Jos Kubernetekseen on pääsy internetistä, se aiheuttaa suuren tietoturvariskin. Silloin siinä tapauksessa on jo ohitettu useampi suojauskerros ja –resurssi, ja riski tietomurrolle kasvaa oleellisesti. Koska Kubernetes –palvelu ei ole suunniteltu tässä käyttötapauksessa selainpuolelle, sitä ei ole mitään syytä päästää internetistä saatavaksi palveluksi.	Kubernetesin pääsy internetistä voidaan estää monikerrosarkkitehtuurilla, jolloin Kubernetes luodaan yksityiseen aliverkkoon (private subnet) ja pääsy sallitaan vain selainpuolelta ja sekin vain kuormantasaajan kautta, joka sijaitsee näiden kahden resurssin välissä.
Hyökkääjä pääsee käsiksi Kubernetekseen ja saa sen hallintaansa. Tämä tietoturvariski voi aiheuttaa tietomurron, sillä käyttötapauksessa Kuberneteksella on yhteys tietokantaan ja hyökkääjä voi päästä sitä kautta salassa pidettävään tietoon käsiksi.	Monikerrosarkkitehtuurin noudattaminen sekä Kuberneteksen turvallinen konfigurointi pienentävät mahdollisia riskejä. Näitä toimenpiteitä ovat mm. pääkäyttäjän estäminen sovellusprosesseissa (non-root), pelkkien lukutiedostojen käyttäminen, sekä etuoikeutettujen (privileged) konttien kieltäminen. Näillä toimilla vähennetään tietoturvariskiä hyökkääjän mahdollisen toiminnan seurauksena. Kun tämän lisäksi noudatetaan pilvipalveluntarjoajien parhaita käytäntöjä, sekä seurataan Well-Architected Frameworkia, riski hyökkääjän pääsemiseksi Kubernetes palveluun pienenee huomattavasti.
Salaisuuksien, kuten API-avaimien, salasanojen ja muiden salassa pidettävien tietojen heikko hallinta johtaa tietoturvariskiin, joka voi puolestaan johtaa tietomurtoon.	Salaisuuksia ja muita salaiseksi luokiteltavia tietoja varten pilvipalveluntarjoajilla on salaisuuksien hallintaresurssit. Näiden salaisuuksien tallentaminen kovakoodaamalla, tallentaminen esimerkiksi versionhallintaan jne. on riskialtis vaihtoehto. Samaan tarkoitukseen voidaan käyttää pilvipalveluiden salaisuuksien hallintaresursseja. Näitä salaisuuksien hallintapalveluita ovat mm. Azure KeyVault, AWS Secrets Manager, Google Secrets Manager ja Oracle Cloud Infrastructure Vault.

4.4. Salausavaimet

Tietoturvassa salauksella ja pääsyavaimilla on keskeinen rooli salassa pidettävien tietojen suojaamisessa. Tämän osa-alueen riskit sisältävät haasteita, jotka liittyvät salausavainten ja käyttöoikeustietojen turvalliseen luomiseen, tallentamiseen ja hallintaan.

Salaus ja salauksen purkaminen on keskeinen työkalu tietojen suojaamiseen sekä siirron aikana (In transit) että lepotilassa (At rest). Tietoturvariskejä syntyy yleensä riittämättömistä avainten hallintakäytännöistä,

luvatta pääsystä salausavaimiin tai salausalgoritmien heikkouksista. Turvallinen salausavainten hallinnan toteuttaminen, mukaan lukien säännöllinen kierrätys ja turvallinen tallennus, on ratkaisevan tärkeää näiden riskien tehokkaaksi vähentämiseksi.

Pääsyavaimet, jotka mahdollistavat vuorovaikutuksen pilvipalvelujen resurssien ja tietojen kanssa, asettavat omat haasteensa. Riskit voivat ilmetä luvattomana käyttönä, pääsyavainten vuotamisena vääriin käsiin tai käyttöoikeustietojen puutteellisina määrityksinä. Näiden riskien torjumiseksi organisaatiot seuraavat ja toteuttavat parhaita käytäntöjä, kuten roolipohjaista pääsynhallintaa (RBAC), vähimmän oikeuden periaatteita (principle of least privilege) ja suojattuja tallennusmekanismeja pääsyavaimille.

Lisäsuojaus saadaan aikaan käyttämällä laitteiston suojausmoduuleja (HSM) tai pilvipohjaisia avaintenhallintapalveluita. Nämä työkalut parantavat salausavainten turvallisuutta ja tarjoavat turvallisen ympäristön niiden luomiselle, tallentamiselle ja käytölle.

Salaus- ja pääsyavainten turvallisuuden varmistaminen ei sisällä vain teknisiä näkökohtia, vaan myös kattavia käytäntöjä, säännöllisiä tarkastuksia ja varmistuksia, sekä alan parhaiden käytäntöjen noudattamista. Organisaatiot, jotka priorisoivat näitä toimenpiteitä, vahvistavat turvallisuusinfrastruktuurinsa kestävyyttä ja suojautuvat mahdollisilta tietomurroilta ja luvattomalta pääsyltä salassa pidettäviin tietoihin.

Pilvipalveluntarjoajat tarjoavat useita keinoja pääsyavainten hallintaan. Valittavana on esimerkiksi toimittajan tai asiakaan itsensä hallinnoimat avaimet. Jälkimmäiset tarjoavat korotettua tietoturvaa, mutta lisäävät samalla monimutkaisuutta. Asiakkaan tuleekin aina tehdä riskipohjaiset päätökset avainten hallintaprosessista.

Tunnistetut riskit	**Riskienhallintatoimenpiteet**
Asiakkaan hallinnoima avain (CMK) poistetaan ja kaikki tällä avaimella salatut tiedot muuttuvat palauttamattomiksi poistamisen jälkeen. Tämä voi johtaa palvelun toiminnan heikkenemiseen ja pahimmassa tapauksessa palvelun toiminta estyy, jos tietoa ei saada palautettua.	Käyttäjä- ja pääsynhallinnalla, sekä palvelunhallintakäytännöillä (Service Control Policies, SCP) pyritään estämään avainten tuhoaminen, mutta riskin toteutumisen estämiseksi on varauduttava myös siihen, että avaimet tuhotaan. Avainten varmuuskopiointi on keino estää avainten katoamisen aiheuttamaa tiedon saatavuuden estymistä. Pilvipalveluntarjoajista Azure sekä Oracle tarjoavat suoraan varmuuskopiointimahdollisuudet asiakkaan hallinnoimille avaimille. KMS-avainten poistosta voidaan myös tuottaa hälytyksiä, jotka auttavat reagoimaan avainten poistoon. Monesti pilvipalveluntarjoajien avainten tuhoaminen ei tapahdu heti, vaan vasta jonkun ajan kuluttua poistopyynnöstä. Myös testaaminen on yksi keino varmistua mahdollisten avainten tuhoamisen haittojen varalta ja säännöllinen testaaminen on suositeltavaa, jotta voidaan varmistaa tietojen saatavuus avainten katoamisen sattuessa. Pilvipalveluntarjoajat tarjoavat myös hallinnoimansa avainpalvelut. Pilvipalveluntarjoajien hallinnoimia avaimia asiakas ei voi poistaa, mikä pienentää avainten katoamisen riskiä. Asiakkaan hallinnoimien avainten ja pilvipalvelun tarjoajien hallinnoimien avainten välinen ero antaa käyttäjille mahdollisuuden tehdä valintoja turvallisuus- ja vaatimustenmukaisuusvaatimustensa

	perusteella. Käyttäjien on tärkeää ymmärtää kuhunkin avaintyyppiin liittyvät vaikutukset ja ominaisuudet, kun arkkitehtuuria ja suojausratkaisuja suunnitellaan.
Pitkäikäiset salausavaimet lisäävät turvallisuusriskejä ja tarjoavat laajemman aikaikkunan mahdollisille tietomurroille sekä lisäävät riskiä luvattomalle käytölle. Säännöllinen avainten kierrätys on tärkeää avainten murron vaikutuksen minimoimiseksi, uhkiin reagoimiseksi tehokkaasti sekä turvallisuusstandardien ja -määräysten noudattamisen varmistamiseksi. Tämä parantaa turvallisuutta, rajoittaa altistumista luvattomalle käytölle ja vähentää sekä ulkoisiin että sisäisiin uhkiin liittyviä riskejä.	Organisaatioiden tulisi luoda käytännöt avainten kierrätykselle ja automatisoida avainten kierrätysprosessit, sekä tarkistaa ja päivittää säännöllisesti käytännöt myös kierrätysprosessien suhteen. Suuret pilvipalveluntarjoajat (AWS, Azure, GCP, Oracle) tarjoavat avainten automaattisen kierrätyksen asiakkaan hallinnoimille avaimille. Pilvipalveluntarjoajan hallinnoimille avaimille kierrätys on automaattinen, pilvipalveluntarjoajat huolehtivat avainten säännöllisestä kierrättämisestä.
Luvattomat käyttäjät pääsevät tekemään salaus- ja purkuoperaatiota salausavaimilla mikä voi johtaa salassa pidettävien tietojen vaarantumiseen, sekä muihin tietoturvariskeihin, kuten tietojen eheyden vaarantumiseen, tietojen kaappaukseen jne. Avaimten luvaton käyttö voi johtaa em. riskien realisoiduttua myös mainehaittoihin, mahdollisiin sääntelyrikkomuksiin ja jopa oikeudellisiin seurauksiin.	Näiden riskien hallinta edellyttää moninaista lähestymistapaa, jotta riskejä voidaan pienentää ja poistaa. Vahvat pääsynvalvonta- ja todennusmekanismit avaintenhallintapalveluille, vähimmän oikeuden periaate (Principle of Least Privilege), jolla rajoitetaan avaimien käyttöoikeutta ja avaimen käytön toimintojen oikeuuksia (salaus, purku jne.). Lokien säännöllisellä auditoinnilla voidaan seurata avainten käyttöä ja automaatiolla voidaan reagoida nopeasti epäilyttäviin toimintoihin. Tietoturvatestauksella voidaan todentaa avainten tietoturvan toteutuminen sekä arvioida olemassa olevien turvatoimien tehokkuutta. Näin voidaan parantaa myös avaintenhallinnan ja oikeuksien turvallisuutta.
Sisäisten käyttäjien, joilla on pääsy keskeisiin avaintenhallintapalveluihin, haitalliset toimet tai huolimattomuus. Sisäisten käyttäjien kohdalla riskit voivat olla samaa tasoa kuin edellisen kohdan kohdalla ja samat riskit nousevat esiin myös tässä.	Sisäisten käyttäjien pääsy avaimiin on nostettu erillisenä kohtana esiin, sillä usein tätä riskiä ei tunnisteta ja monesti sisäisillä käyttäjillä voi olla liian laajat oikeudet avaimiin. Hallintakeinoina toimivat samat keinot, kuin yllä olevassa riskitapauksessa.
Asiakkaan hallinnoimien avainten oikeudet määritellään väärin, jolloin avaimen käyttö estyy. Tämä riski saattaa estää palvelun käytön väliaikaisesti, mutta ei estä tiedon käyttöä lopullisesti sillä pilvipalvelun pääkäyttäjän (root user) avulla oikeudet saadaan palautettua.	Kehitystiimien osaaminen huolellisuuden ohella vaikuttaa paljon tähän riskiin. Organisaatioiden tulisi luoda käytännöt, joilla varmistetaan osaaminen myös salausavainten hallinnan osalta sekä luodaan hyvät käytännöt joilla pienennetään virheiden mahdollisuutta.

4.5. Käyttäjähallinta

Käyttäjähallinta (Identity and Access Management, IAM) on kriittinen osa pilviturvallisuutta. Sillä on keskeinen rooli turvallisuuden, vaatimustenmukaisuuden ja toiminnan varmistamisessa. Pilven käyttäjähallinta kattaa käyttäjätunnusten, käyttöoikeuksien ja todennusmekanismien hallinnan. Riskejä voi

aiheutua riittämättömästä pääsynvalvonnasta, vaarantuneista valtuustiedoista tai käyttäjien oikeuksien huonosta hallinnasta. Vahvojen käytäntöjen luominen sisältää vähimmän oikeuden periaatteen, monivaiheisen tunnistautumisen (MFA/2FA) sekä säännölliset tarkastukset käyttäjien ja näiden oikeuksien osalta. Myös käyttäjähallinnan integrointiin sekä federointiin tulee kiinnittää huomiota.

Kyky toteuttaa pienimmän käyttöoikeuden periaatetta parantaa tietosuojaa. Se auttaa rajoittamaan käyttäjille vain tarvittavat käyttöoikeudet minimoiden samalla riskejä. Käyttäjähallinnassa on tärkeää kyetä pienentämään riskien toteutumisen todennäköisyyttä sekä myös varautua toimenpiteisiin riskien realisoituessa. Käyttäjien tekemien toimintojen lokitus ja valvonta ovat oleellinen osa riskienhallintaa. Ilman niitä järjestelmiin ja käyttäjien tekemiin toimenpiteisiin ei ole näkyvyyttä. Automaation hyödyntäminen lokituksesta ja monitoroinnista saatavan tiedon perusteella voi pienentää riskin toteutumisen todennäköisyyttä ja joissain tapauksissa jopa estää sen kokonaan.

Tunnistetut riskit	Riskienhallintatoimenpiteet
Organisaation entisen käyttäjän tunnukset/avaimet ovat edelleen aktiiviset. Tunnusten ja/tai pääsyavaimien tahaton tai tahallinen käyttö voi aiheuttaa merkittäviä tietoturvariskejä, kuten esimerkiksi tietovuotoja ja –murtoja, tietojen menetystä, vaatimustenmukaisuusrikkomuksia ja palvelun estoja.	Näitä riskejä voidaan hallita mm. luomalla käytännöt, joilla hallinnoidaan käyttäjiä ja tunnukset poistetaan heti kun niille ei ole tarvetta. Käytäntöjä voivat olla mm. säännölliset tarkastukset ja läpikäynnit, automaation lisääminen valvontaan ja poikkeaminen havaitsemiseen.
Pääsyavaimien tallentaminen julkisesti aiheuttaa merkittäviä tietoturvariskejä pilviympäristössä. Jos avaimet ovat julkisesti saatavilla esimerkiksi tallennettuna IaC -koodiin tai versionhallintaan, haitalliset toimijat voivat mahdollisesti käyttää niitä hyväkseen päästäkseen luvattomasti pilvipalveluiden resursseihin. Kyseessä on suuri tietoturvariski, jonka poistaminen on ensiarvoisen tärkeää.	Näiden riskien vähentämiseksi on erittäin tärkeää noudattaa parhaita käytäntöjä pääsyavaiten suojaamiseksi. Parhaita käytäntöjä on esimerkiksi noudattaa Least Privilege -periaatetta, missä käyttäjille ja resursseille annetaan vain ne käyttöoikeudet, joita he/ne tarvitsevat. Säännöllinen IaC -koodin sekä versionhallinnan skannaaminen ovat myös avainasemassa kun halutaan vähentää riskiä avainten julkisesta saatavuudesta. Avaimien säännöllinen kierrättämisvelvoite tai tekninen pakotus kierrättämiseen vähentävät tietoturvariskejä. Monet pilvipalveluntarjoajat tarjoavat työkaluja ja palveluita avainten kierrätyksen automatisoimiseksi. Monitoroinnilla ja lokituksella voidaan saada pääsyavainten luvaton ja haitallinen käyttö kiinni ja automatisoinnilla esimerkiksi deaktivoida tai tuhota pääsyavaimet.
Liian laajat käyttöoikeudet esim. kehitys- ja ylläpitotiimien sekä muiden sidosryhmien jäsenille aiheuttavat merkittäviä turvallisuusriskejä. Riskit voivat liittyä tietomurtoihin ja –vuotoihin, palvelun toiminnallisuuteen sekä lisätä hyökkäysriskin vaaraa.	Riskiä voidaan hallita toteuttamalla pilvipalvelutarjoajien parhaita käytäntöjä kuten Least Privilege –periaatetta, ryhmien ja roolien käyttöä, sekä monitoroimalla ja auditoimalla tapahtumia. Ryhmien ja roolien käyttö helpottaa hallintaprosessia, sillä kaikki pääsy pilvijärjestelmiin ja –alustoihin pakotetaan ryhmäkohtaisiin oikeuksiin ja rooleilla annetaan vain väliaikaiset oikeudet resursseihin.
Samoilla tunnuksilla pääsy eri ympäristöihin, esim. kehitys-, laadunvalvonta- ja tuotantoympäristöihin aiheuttaa merkittäviä riskejä.	Pilvipalveluntarjoajien parhaita käytäntöjä toteuttamalla voidaan pienentää tai jopa estää riskin toteutuminen. Keskitetty hallinnointi käyttäjä- ja pääsynhallinnalle, sekä ympäristökohtaisten roolien ja ryhmien käyttö on

Esimerkiksi tuotantoympäristön tietoihin mahdollistava pääsy suurentaa tietovuotojen ja –murtojen riskiä, mutta voi vaikuttaa myös järjestelmän ja palvelun saatavuuteen, jos käyttöoikeuksia käytetään joko tahallisesti tai tahattomasti väärin.	suositeltavaa sekä hallinnallisesta, että riskien hallinnan näkökulmasta.
Pääkäyttäjän (Root user, owner) **tunnusten käyttäminen**. Pilvipalveluntarjoajien käytännöissä on eroja tilien perustamisessa. Esimerkiksi AWS:ssa tilin perustamisen yhteydessä luodaan pääkäyttäjä (AWS account root user) ja tällä käyttäjällä on täydet omistusoikeudet ja käyttöoikeudet, joita ei voi muuttaa. Koska pääkäyttäjän oikeudet ovat laajat, tunnusten päätyminen vääriin käsiin voi johtaa mittaviin vahinkoihin niin turvallisuuden, maineen kuin liiketalouden näkökulmista. Jos pilvipalveluntarjoajalla on käytössä pääkäyttäjä, sen tunnuksia ja käyttöä pitää suojella kaikin tavoin, eikä päivittäisessä toiminnassa saa sallia pääkäyttäjän tunnusten käyttöä.	Pääkäyttäjän tunnuksien väärinkäyttöriskin pienentämiseksi tai jopa estämiseksi, on erittäin tärkeää suojata tunnukset, luoda prosessit niiden käytölle, sekä toteuttaa pilvipalveluiden tarjoajien parhaat käytännöt. Näitä ovat esimerkiksi pääkäyttäjän pääsyavainten tuhoaminen, jolla varmistetaan ettei pääkäyttäjän identiteettiä voida käyttää kuin hallintakonsolin kautta, jolloin komentorivi- ja SDK-käyttö on estetty. Pääkäyttäjälle tulee luoda vahva salasana ja salasana tulee vaihtaa säännöllisesti. Myös pääkäyttäjien tunnuksien yhteydessä tulee ottaa käyttöön monivaiheinen tunnistautuminen. Suositeltavaa on myös lisätä usean henkilön hyväksynnän vaativa prosessi, jos pääkäyttäjän tunnuksia on käytettävä. Prosessi voi koostua esimerkiksi muodostamalla ryhmä pääsynvalvojia, joilla on pääsy salasanaan, ja toinen ryhmä pääsynvalvojia, joilla on pääsy MFA-laitteeseen. Jokaisen ryhmän edustajan on oltava paikalla, jotta pääkäyttäjän tunnuksilla voidaan kirjautua sisään. Tämän lisäksi on suositeltavaa luoda hälytys, joka lähettää ilmoituksen vaatimusten mukaiseen paikkaan, esim. sähköpostiin tms., kun pääkäyttäjän tunnuksilla kirjaudutaan sisään.
Pääsyavainten kierrätysvaatimus puuttuu, jolloin avaimet ovat pitkäikäisiä mikä aiheuttaa useita tietoturvariskejä. Pääsyavaimia käytetään komentoriveillä sekä ohjelmistokehityspaketeissa (Software Development Kit, SDK). Pitkäikäisten avainten käyttö lisää mm. avaimien paljastumisen riskiä jopa niiden tahattoman jakamisen takia. Näin ollen avaimet joko tahallisesti tai tahattomasti haltuunsa saanut voi käyttää niitä mikä on suuri riskitekijä tietomurtojen, palvelun toiminnallisuuden ja muiden osa-alueiden näkökulmista.	Luotamalla prosesseja pääsyavainten kierrätykselle, voidaan varmistua, että avaimet ovat vain lyhyen aikaa käytettävissä. Tällä pienennetään riskejä. Avainten kierrätysvaatimus on yleisesti ottaen automatisoitavissa joko suoraan pilvipalveluntarjoajien omilla mekanismeilla, kuten roolipohjaisilla käyttöoikeuksilla tai melko vaivattomasti luomalla oma prosessi ja toteutus esimerkiksi IAM -käyttäjien avainten kierrätykseen.
Varastetut tai vaarantuneet tunnistetiedot voivat johtaa luvattomaan käyttöön. Tunnistetietoja voivat olla esimerkiksi käyttäjätunnus ja salasana tai pääsyavaimet. Tämä voi johtaa jopa pitkäaikaiseen tietoturvariskiin, sillä havaitsemattomana poikkeamana hyökkääjä voi toimia pitkänkin ajan saamillaan tunnuksilla. Tämä voi aiheuttaa monia eri tietoturvapoikkeamia, kuten tietomurtoja, haittaohjelmien levittämistä ja muuta palvelua uhkaava toimintaa palvelun tai johtaa sen toimimattomuuden.	Organisaatiot voivat suojautua ja pienentää vaarantuneiden tunnusten käytön riskejä laajemmalla strategialla ja varautumalla poikkeamiin ennakolta sekä pienentämällä realisoituneen riskin vaikutuksia. Monivaiheisella tunnistautumisella sekä pienimmän käyttöoikeuden periaatteella pystytään riskiä pienentämään jo huomattavasti niin ennakoidun kuin realisoituneenkin riskin tapauksessa. Muita hallintakeinoja ovat mm. tunnusten säännöllinen kierrätys, jatkuva valvonta ja lokitus, mutta myös jatkuvat turvallisuusarvioit ja auditoinnit, sekä

	organisaation sisäiset turvallisuuskoulutukset ovat avainasemassa. Tunnusten säännöllisellä kierrättämisellä voidaan estää tunnusten väärinkäyttö kun taas lokituksen ja monitoroinnin avulla voidaan havaita epäilyttävää toimintaa. Turvallisuuskoulutus on tärkeää paitsi teknisen näkökulman osalta, mutta myös organisaation toimintakulttuuriin vaikuttamisessa. Näin turvallisuudesta tulee automaatio ja itsestäänselvyys.
Liian lyhyet ja helposti arvattavat salasanat, jolloin ne voidaan todennäköisemmin murtaa siihen kehitetyillä työkaluilla. Heikkojen ja helposti arvattavien salasanojen käyttäminen tuo merkittäviä turvallisuusriskejä. Hyökkääjät voivat käyttää hyväkseen heikkoja salasanoja, mikä voi johtaa luvattomaan käyttöön, tietomurtoihin ja muihin tietoturvaloukkauksiin.	Salasanojen pituuden, merkkien jne. vaatimukset riittävälle tasolle sekä salasanojen säännöllinen kierrätys sekä palveluun kirjautumis-, että IAM-käyttäjien kirjautumisprosesseissa. Pilvipalveluntarjoajat tarjoavat yleensä joko oletusarvoisen salasanavaatimuksen, sekä kustomoitavat salasanavaatimukset IAM -käyttäjille.
Muiden identiteettien, kuten CI/CD putken **avaimet/tunnukset ovat saatavilla.** Tietoturvariski voi tulla jopa pilvipalveluntarjoajan ulkopuolelta, sillä julkaisuputkia voidaan pystyttää myös kolmannen osapuolen palveluntarjoajan palveluihin, kuten GitHub, GitLab, Bitbucket jne. Julkaisuputkilla pitää olla riittävät oikeudet ympäristöihin, joihin julkaisuja tehdään (kehitys, testi, tuotanto jne.). Siksi näiden tunnusten ja/tai avaimien paljastuminen joko sisäpuolisille (esim. kehittäjät) tai ulkopuolisille tahoille johtaa samanlaisiin tietoturvauhkiin, kuin IAM -käyttäjien avaintenkin paljastuminen.	Pääsyjä palveluihin, joissa julkaisuputket ovat, pitää rajoittaa sallimalla pääsy vain heille, joille pääsy on välttämätön. Pienimmän käyttöoikeuden periaatteella voidaan rajoittaa sallittuja toimintoja. Palveluntarjoajien mahdollisuudet ja prosessit ovat laajat, joten riippuu palveluntarjoajasta, minkälaiset mekanismit ovat mahdollisia. Pääsyavainten käyttöä julkaisuputken palveluntarjoajan ja pilvipalvelun välillä saatetaan pystyä myös hyödyntämällä esimerkiksi OpenID Connect -todennusprotokollaa. Jos pääsyavaimia kuitenkin joudutaan käyttämään, ne pitäisi pyrkiä tallettamaan niin, että niihin ei päästä käsiksi ja julkaisuputket konfiguroitava siten, etteivät avaimet näy lokeissa.
CI/CD putken oikeudet ovat liian laajat. Liian laajojen oikeuksien myöntäminen julkaisuputkille (CI/CD) tai niihin integroiduille työkaluille pilviympäristössä aiheuttaa samoja merkittäviä turvallisuusriskejä, kuin muidenkin käyttäjien tai roolien liian laajat käyttöoikeudet - lähestymiskulma on vain erilainen. Julkaisuputken tehtävänä on mm. asennusten ja konfiguraatioiden tekeminen ympäristöihin. Siksi liian laajoilla oikeuksilla voi olla riskinä, että kriittinen tieto voidaankin tuhota putkessa sisältäen myös disaster recovery -menettelyt. Silloin operatiivinen-, maine-, liiketoiminnan jatkuvuus sekä tietoturvariskit nousevat esiin.	Julkaisuputkien ja muiden integraatioiden tunnuksista on pidettävä yhtä hyvää huolta kuin muistakin käyttäjätunnuksista. Käytössä tulee siksi olla vastaavat hallintakeinot, kuten säännöllinen kierrätys, vähimmän oikeuden periaate, roolipohjaiset pääsyt ympäristöihin. Tämän lisäksi pääsyavainten hallintaan on kiinnitettävä erityistä huomiota, jolla estetään tarpeeton pääsy avaimiin. OpenIdD Connect (OIDC) protokollan hyödyntäminen on yksi keino integroida julkaisuputket pilviympäristöihin. Se poistaa tarpeen julkaisuputkien pääsyavainten käytölle, joten pienentää myös riskiä liian laajojen oikeuksien osalta. Tällöin integraatio pilviympäristön ja julkaisuputken välillä ei vaadi pääsyavaimia, jolloin julkaisuputken käyttöoikeuksien väärinkäytön riski pienenee. Esimerkiksi GitHub Actions ja GitLab tukevat OIDC –todennusta.

Julkaisuputken itsessään tekemillä mahdollisten haitallisten toimenpiteiden lisäksi hyökkääjän saadessa tunnukset haltuunsa, tietoturvariski nousee esille. Hyökkääjä pääsee tunnusten avulla käsiksi palvelun resursseihin aiheuttaen mm. Tietomurtojen, haitallisen koodin lisäämisen, palvelun konfiguraatiomuutosten ja tiedon eheyden riskejä.	
IAM käyttäjän oikeus muuttaa oikeuksia, joko omia tai toisen käyttäjän, luo merkittäviä tietoturvariskejä. Tällöin pääsy esimerkiksi salassa pidettävään tietoon mahdollistuu. Oikeuksien muuttaminen voi vaikuttaa myös palvelun turvallisuuteen, sillä riskinä voi olla, että käyttäjä pääsee omia oikeuksia muuttamalla muuttamaan myös palvelun resurssien ominaisuuksia. Silloin esimerkiksi kriittiset turvallisuusmekanismit vaarantuvat ja näin ollen palvelusta tulee haavoittuva.	Käyttäjien oikeudet pitää määritellä siten, ettei heillä ole pääsyä muuttamaan omia tai muiden käyttäjien oikeuksia. Kaikki pilvipalvelutarjoajat keräävät lokitietoa API-kutsuista, jolloin voidaan luoda automaattisia hälytyksiä, jos käyttäjien oikeuksia muutetaan. Näin ollen riskiin pystytään reagoimaan välittömästi ja tekemään tarvittavat toimenpiteet oikeuksien palauttamiseksi ennalleen.
Epäilyttäviä toimintoja tai turvallisuushäiriöitä ei seurata ja niihin ei reagoida. Näin ollen väärinkäytöstä ei huomata ajoissa, eikä tapahtuman vaikutusta pystytä lieventämään ja/tai estämään.	Lokitus ja valvonta ovat erittäin tärkeä osa pilvipalveluiden turvallisuutta ja ne liittyvät useaan osa-alueeseen, kuten turvallisuuteen, suorituskykyyn, vaatimustenmukaisuuteen ja palvelun toiminnallisuuteen. Käyttäjänhallinnan näkökulmasta lokitus ja valvonta vaikuttavat suoraan kykyyn havaita ja reagoida mm. tietoturvapoikkeamiin, epätavallisten käyttäjätapahtumien havaitsemiseen, sekä säädösten noudattamisen varmistamiseen. Esimerkiksi GDPR ja HIPAA edellyttävät organisaatioita seuraamaan käyttäjien toimintaa ja tarvittaessa raportoimaan niistä. Lokitus auttaa myös varautumaan tietoturvariskeihin ja poikkeamiin ja muun muassa automatisoituja mekanismeja hyödyntämällä niitä voidaan jopa estää. Tärkeä osa lokienhallintaan on niiden elinkaaren hallinta, millä voidaan vaikuttaa kustannusoptimoinnin ohella myös jäljitettävyyteen.

4.6. Muut huomioitavat asiat

Pilvipalveluiden - samoin kuin on-prem -palveluidenkin osalta - riskienhallinta on monitahoinen haaste. Se ulottuu myös tässä esimerkkikäyttötapauksessa käsiteltyjen tietoliikenteen, tietokantojen, Kubernetesin, salaus- ja pääsyavaimien sekä käyttäjähallinnan ulkopuolelle. Vaikka nämä alueet ovat ratkaisevan tärkeitä on muistettava että pilviympäristöt sisältävät myös useita muita mahdollisia riskejä.

Sellaiset näkökohdat kuten Disaster Recovery, tietokantojen käytön estäminen, ohjelmistokehityksen julkaisuputket, ympäristöjen tilan näkyvyys, tuotantotietojen käyttö kehitys- ja testaustyössä, resurssien lokitus ja elinkaaren hallinta, sekä liikenteen ja tiedonsiirron hallinta ovat yhtä tärkeitä. Nämä mainitut riskialueet sisältävät näkökohtia, jotka liittyvät pilvitoimintojen luotettavuuteen, suorituskykyyn, turvallisuuteen, tehokkuuteen ja operatiiviseen toimintaan.

Näiden riskien tehokas torjuminen edellyttää kokonaisvaltaista lähestymistapaa, joka yhdistää määritellyt ja toteutetut turvallisuuskäytännöt, vaatimustenmukaisuustoimenpiteet ja ennakoivan seurannan koko

pilviekosysteemissä. Tunnistamalla ja vähentämällä riskejä eri alueilla organisaatiot voivat parantaa yleistä pilvitietoturvaa ja varmistaa digitaalisen infrastruktuurinsa luotettavuuden ja luottamuksellisuuden.

Riskien tunnistaminen tässä dokumentaatiossa käsiteltyjen osa-alueiden osalta ei tarkoita sitä, että tämä on kaiken kattava tunnistettujen riskien ja niihin varautumisen ohje. Pilvipalvelut, kuten myös on-prem -palvelut, sisältävät myös muita riskejä mutta myös mahdollisuuksia. Riskienhallinnassa tulee myös huomioida inhimillinen näkökulma erityisesti kehittäjien sekä järjestelmän ylläpitäjien ja pääkäyttäjien osalta.

Pilvipalveluiden tarjoajien, kuten Amazon Web Services, Google Cloud Platform , Microsoft Azure ja Oracle Cloud auttavat organisaatioita riskien hallinnassa. Kaiken ytimessä on jaetun vastuun malli (Shared Responsibility Model) ja sitä tukevat suuret ja kohdennetut resurssit, sekä modernit teknologiat. Asiakkaan on kuitenkin aina ymmärrettävä niiden tarkoitus ja osattava itse kantaa vastuunsa valituista ratkaisuista.

Tunnistetut riskit	Riskienhallintatoimenpiteet
Pilvitenantin tietoturvapolicyt (pilven tietoturvan kontrollerisäännöstö) ovat jääneet määrittelemättä tai päivittämättä.	Uusia pilvipalveluita käyttöönotettaessa tai merkittävien muutosten yhteydessä on pidettävä pilven tietoturvan kontrollerisäännöstön katselmointilaisuuksia.Niissä organisaation omien pilvitietoturva-asiantuntijoiden sekä mahdollisten ulkoisen tahojen kanssa käydään yksityiskohtaisesti läpi säännöstöt.
Kolmannen osapuolen pilvitietoihin pääsyyn liittyy riski, jossa luvattomat osapuolet pääsevät käsiksi myös pilveen tallennettuihin luottamuksellisiin tai salassa pidettäviin tietoihin. Tämä voi johtaa mm. tietoturvaloukkauksiin tai salassa pidettävien asiakastietojen vaarantumiseen, mistä voi olla seurauksena mainevaurio ja oikeudelliset seuraukset.	Pilvipalveluissa voidaan hyödyntää salausta ja kehittyneitä virtualisointitekniikoita, kuten AWS Nitro (AWS), virtualisoitujen ympäristöjen eristämiseen ja suojaamiseen, millä voidaan vähentää riskiä 3.osapuolen pääsystä tietoihin. Nitro –teknologiaa voidaan käyttää sekä Kubernetes –palvelussa, että relaatiotietokantapalvelussa.
Disaster recovery –prosessia ei ole ja/tai sen tarvetta ei ole tunnistettu. Disaster recovery on prosessi, jolla organisaatio pyrkii ennakoimaan ja käsittelemään teknologiaan liittyviä katastrofeja. Sen tarkoituksena on katastrofin sattuessa palauttaa järjestelmä toimintakuntoon vaatimusten mukaisessa ajassa ja toimintakunnossa. Tapahtumia, jotka vaikuttavat järjestelmän toimintakykyyn, ovat esimerkiksi järjestelmän maantieteellisellä alueella tapahtuvat luonnonilmiöt (tulvat, maanjäristykset jne.), teknologian aiheuttamat viat, inhimilliset virheet, sekä muut tahallinen tai tahaton järjestelmän toimintaan vaikuttavat toimenpiteet. Disaster recovery keskittyy järjestelmän palautumiseen suuren katastrofin tai häiriötapahtuman jälkeen. Korkea käytettävyys (High availability, HA) pyrkii tarjoamaan jatkuvan ja keskeytymättömän järjestelmän saatavuuden minimoimalla normaalin toiminnan häiriötilanteet. Molemmat strategiat ovat keskeisiä osia	Disaster recovery –prosessiin liittyvät olennaisesti RPO ja RPO, jotka määrittävät, kuinka nopeasti järjestelmän täytyy olla toimintakunnossa (=RTO), sekä kuinka paljon tietoa voidaan menettäää katastrofin sattuessa (=RPO). Järjestelmät on rakennettu erilaisiin käyttötarkoituksiin, joten RPO ja RTO ovat aina yksilöllisiä. DR-suunnitelmassa pitää tunnistaa RTO ja RPO, joiden pohjalta tehdään DR-strategia (backup and restore / pilot light / Warm standby / Multi-site active-active). Näiden perusteella suunnitellaan ja toteutetaan tekninen toteutus järjestelmän palautukseen katastrofin sattuessa, jolla varmistetaan vaatimuksenmukainen toipuminen. Disaster recovery –prosessissa kriittisinä kohteina on tietokannat ja tietovarastot, sillä monesti ne ovat järjestelmien kannalta elintärkeitä ja tiedon varmuuskopiointi, sekä mahdollinen replikointi on määriteltävä. Myös muut resurssit ja kerrokset tulee huomioida, kuten palvelun selainpuoli ja palvelinpuoli, kubernetes –palvelu, avaintenhallinta, sekä

kattavassa liiketoiminnan jatkuvuussuunnitelmassa mutta on syytä huomioida, että Disaster recovery ja korkea saatavuus tarkoittavat kontekstissaan eri asioita.	käyttöoikeuksien hallinta, sillä ilman näitä järjestelmää ei pystytä palauttamaan toimintaan. Yleisperiaatteena disaster recoverylle on, että mitä pienemmät vaatimukset ovat RPO:lle ja RTO:lle, sitä vaativampi DR strategia on. Disaster recovery pitää ottaa aina huomioon järjestelmäkehityksessä ja kehittää DR-strategiaa jatkuvasti kunnes vaatimukset täytetään, eli aloittaa esimerkiksi varmuuskopioinnista ja palautuksesta ja kehittää siitä eteenpäin tiukempien vaatimusten mukaisesti.
Disaster recovery –prosessi on olemassa mutta sitä ei testata säännöllisesti. Disaster recovery -testaus on kriittinen osa kestävän ja luotettavan palautusstrategian ylläpitämistä pilvessä. Se auttaa organisaatioita validoimaan suunnitelmansa, tunnistamaan ja korjaamaan heikkouksia sekä varmistamaan, että ne ovat hyvin valmistautuneita toipumaan mahdollisista häiriöistä ja suojelemaan liiketoiminnan jatkuvuutta.	Luodaan DR testaussuunnitelma ja valvotaan, että sitä toteutetaan vaatimusten mukaan (varmistetaan mm. varmuuskopioiden, snapshottien, konttien imaget, lisenssien ja järjestelmän toimivuus). Testaamisella varmistetaan RPO- ja RTO tavoitteiden täyttyminen, pyritään tunnistamaan DR-prosessin puutteet ja heikkoudet, osoittamaan mahdollinen vaatimustenmukaisuus sekä mahdollistamaan myös jatkuvan parantamisen prosessi.
Pääsy tietokantaan estyy, jolloin palvelu on mahdollisesti alhaalla. Tietokannan suorituskykyyn ja luotettavuuteen vaikuttavat mm. liikenteen määrien muutokset sekä alla olevan infran (serverit, datacenterit jne.) viat. Pilvipalveluntarjoajien hallinnoitujen palveluiden hyödyntäminen auttaa varautumaan ja reagoimaan näihin muutoksiin ja vikoihin, sillä skaalautuvuus, vikasietoisuus ja käytettävyys on tyypillisesti sisäänrakennettu palveluun. Näin ollen pilvipalveluntarjoajat tarjoavat ominaisuuksia hallinnoitujen palveluiden kautta ja asiakkaiden on helppo ottaa ominaisuudet käyttöön, millä pyritään varmistamaan tietokannan suorituskyky ja luotettavuus.	Kun hallinnoitu tietokantapalvelu, tässä tapauksessa relaatiotietokantapalvelu, otetaan käyttöön, oletuksena luodaan ensisijainen tietokanta, joka toimii siis ensisijaisena instanssina. Tämän lisäksi on syytä varautua palvelun jatkuvuuteen luomalla toissijainen kopio (secondary replica). Toissijainen kopio luodaan toiseen availability zoneen ja sen tarkoituksena on toimia mm. varatietokantana, jos ensisijainen tietokanta vikaantuu. Kun tietokantaa kutsutaan DNS-nimellä, DNS failover tapahtuu automaattisesti ensisijaisesta tietokannasta toissijaiseen ilman, että asiakkaan täytyy tehdä konfiguraatiomuutoksia. Ensisijainen tietokanta replikoi tiedot automaattisesti toissijaiseen tietokantaan ja vian tapahtuessa automaattinen failover tapahtuu ns. pellin alla, jolloin pilvipalveluntarjoaja hoitaa prosessin. Hallinnoitujen palveluiden ominaisuuksia voidaan yleisesti ottaen ottaa helposti käyttöön ilman suuria konfiguraatio- ja/tai implementaatiomuutoksia mikä on hallinnoitujen palveluiden etuja.
Liika tietokannan kuormitus vaikuttaa suorituskykyyn negatiivisesti. Tietokannan suorituskyky on oleellinen tekijä palvelussa ja on pyrittävä varautumaan suorituskyvyn ylläpitoon tietokantaan kohdistuvien luku- ja kirjoitusoperaatioiden muutoksissa. Hallinnoiduissa palveluissa skaalautuvuus on yksi tekijä suorituskyvyn ylläpidossa, mutta myös ensisijaisen tietokannan suojelemisella saadaan suorituskykyä.	Suorituskykyä ylläpidetään mm. luomalla ensisijaisesta tietokannasta lukukopioita (read replica), tietokantayhteyksien jakamisella (connection pooling, proxy), sekä välimuistien käyttämisellä. Lukukopioiden avulla lukuoperaatiot voidaan ohjata erillisiin kopioihin, jolloin ensisijaiseen tietokantaan kohdistuu vain kirjoitusoperaatiot. Tietokantayhteyksien jakamisella tarkoitetaan proxyn käyttämistä tietokannan edessä niin, että liikenne asiakkaalta tietokantaan kulkee proxyn kautta. Silloin

	proxy vastaan tietokantayhteyksien muodostamisesta, poistamisesta ja jakamisesta. Näin ollen vikatilanteiden riski pienenee yhteyksien osalta. Välimuistin käyttäminen tietokantojen yhteydessä parantaa suorituskykyä ja luotettavuutta, sillä kyselyistä saatavat vastaukset tallennetaan välimuistiin, jolloin ne ovat nopeammin saatavilla seuraavalle kysyjälle. Näin ollen myös tietokantaa suojellaan, sillä vastauksia voidaan palauttaa suoraan välimuistista ilman, että jokaisen kyselyn täytyy käyttää tietokantaa.
Kehitysputki ei varmista turvallisuutta. Ohjelmistokehityksen kehitysprosessiin olennaisena osana kuuluvat kehitysputket (CI/CD) auttavat asiakkaita kehittämään ominaisuuksia, sekä julkaisemaan niitä tuotantoon optimaalisesti, jolloin asiakkaalle tuotettava arvo saadaan parhaimmassa tapauksessa maksimoitua. Kehitysprojekteissa on kuitenkin riskinä, ettei turvallisuuden varmistusta ole huomioitu riittävästi ja turvallisuuspoikkeamiin ei reagoida, jolloin tietoturvariskit kasvavat. Jos esimerkiksi CI/CD putket sisältävät paljon manuaalisia prosesseja, julkaisutiheys heikkenee huomattavasti ja samaan aikaan turvallisuusriskit kasvavat.	Sisällyttämällä myös turvallisuuteen keskittyvät vaiheet ja laatuportit CI/CD-putkiin, voidaan palvelun turvallisuutta parantaa koko kehitystyön elinkaaren ajan. Automatisoinnin lisääminen julkaisuprosessiin lisää turvallisuutta ja parantaa mm. ohjelmiston laadunvarmistusta. Yleisesti ottaen automaatiotasoa pitäisi kasvattaa kehitysprojektin edetessä ja sen tärkeyttä ei monesti ymmärretä. Yksi syy tähän voi olla prosessin vaatimat resurssit ja jos automatisoinnin tuomaa arvoa ei tunnisteta, siihen panostaminenkin jää vähäiseksi.
Näkyvyyttä ympäristöjen tilasta ei ole tai sitä ei seurata. Näkyvyyden puute ympäristöihin ja järjestelmiin aiheuttaa merkittäviä riskejä IT-järjestelmille. Näkyvyys on ratkaisevan tärkeää IT-infrastruktuurin luotettavuuden, suorituskyvyn ja turvallisuuden hallinnan kannalta. Jos ympäristön tilasta ei ole näkyvyyttä, emme voi tietää nykyistä suorituskykyä, emmekä voi varautua tai tehdä toimenpiteitä joko ennakoitaviin tai jo olemassa oleviin järjestelmää koskeviin riskeihin.	Valvonta ja lokitus ovat avainasemassa näkyvyyttä koskevien riskien suhteen ja myös tapahtumiin reagoiminen automaattisilla prosesseilla vaikuttaa riskien hallitsemiseen. Suorituskykyyn, tietoturva- ja muihin tapahtumiin liittyvän tiedon kerääminen ja analysointi edellyttää valvontatyökalujen käyttöönottamista. Keskitetty lokienhallinta antaa mahdollisuuden reagoida poikkeamiin ja tietoturvahäiriöihin, sekä tehdä ennakoivia, sekä jo tapahtuneisiin tapahtumiin liittyviä toimenpiteitä. Dashboardit antavat näkyvyyden lokeista saatavaan tietoon. Automaation hyödyntäminen voi auttaa tunnistamaan malleja, poikkeavuuksia ja trendejä tehokkaammin, jolloin tietoturvapoikkeamiin pystytään reagoimaan jo ennalta. Automatisointia hyödyntämällä voidaan myös poistaa tietoturvapoikkeamia.
Testausympäristössä on tuotantodataa. Tuotantodatan käyttäminen muissa ympäristöissä on todellinen turvallisuusriski. Riskit liittyvät ensisijaisesti tietosuojaan, tietoturvaan, vaatimustenmukaisuuteen ja mahdollisiin tahattomiin seurauksiin, kuten tuotantodatan eheyteen liittyvät muutoksiin.	Tuotantoympäristöjen ulkopuolella on käytettävä muuta kuin tuotantodataa. Data voi olla tuotannonkaltaista ja sitä voidaan saada esimerkiksi tiedon maskauksella ja anonymisoinnilla, jolloin salassa pidettävä tieto piilotetaan samalla sen rakenteet ja suhteet säilyttäen. Tuotannonkaltaista dataa käytettäessä tiedoista voidaan puhdistaa ja poistaa salassa pidettävät tiedot. Lisäksi voidaan käyttää vain osajoukkoa tuotantodatasta. Nämä ovat vain esimerkkejä tuotannonkaltaisen tiedon hyödyntämisessä, eikä voida käyttää ohjeena. Kunkin

	organisaation on itse luotava käytännöt datan käyttämiseen eri ympäristöissä ja mekanismit datan saamiseen. Yleisenä ohjeena tässä voidaan kuitenkin todeta, ettei tuotantodataa pitäisi käyttää muissa ympäristöissä.
Resurssien ja palveluiden lokitus, valvonta ja lokitiedon elinkaaren hallinta ovat puutteellisia. Mikäli hallintaprosessi on puutteellinen, dokumentissa jo mainittujen riskien lisäksi vaatimustenmukaisuus on vaarassa. Esimerkiksi tietomurtojen ja –vuotojen osalta lokit ovat kriittisessä roolissa, sillä niiden perusteella voidaan todeta mitä on tapahtunut, milloin on tapahtunut ja missä on tapahtunut. Jos lokeja ei ole kerätty kaikilta tarvittavilta osin tai sen elinkaarenhallinta on puutteellista, riskinä voi olla, että ei pystytä todentamaan tietoturvapoikkeamia.	Järjestelmäkehityksessä on tunnistettava kaikki kohdat, joista lokit on kerättävä ja tunnistettava myös niiden elinkaaren hallinnan vaatimukset. Toisin sanoen missä lokeja on säilytettävä ja kuinka kauan ne on pidettävä tallessa. Näin ollen pystytään täyttämään mahdolliset säädösten vaatimat vaatimukset, sekä selvittämään mahdollisesti jo tapahtuneet tietoturvapoikkeamat.
Hallinnointiliikennettä ja operatiivista liikennettä ei ole eroteltu toisistaan. Tämä voi aiheuttaa useampia riskejä, kuten turvallisuusriskin, säädösten ja määräysten noudattamattomuuden. Operatiivinen liikenne tässä tapauksessa tarkoittaa järjestelmän toiminta käyttäjän näkökulmasta, eli palvelun käyttämistä. Hallinnointiliikenne tarkoittaa järjestelmän ylläpitäjien toimintaa järjestelmässä. Nämä liikenteet on syytä erottaa toisistaan ja yleisesti ottaen hallinnointiliikenteen sallimista internetin yli on syytä välttää, sillä internetin yli kulkeva liikenne kasvattaa aina tietoturvariskejä ja tämä liikenne voidaan usein reitittää esimerkiksi VPN:n tai muun yksityisen yhteyden kautta. Yksi tapa hallita hallinnointiliikennettä on käyttää ns. Bastion Hosteja eli hyppypalvelimia, jotka toimivat yhdyskäytävinä järjestelmän resurssien ja internetin välillä ja tarkoituksena on mahdollistaa mahdollisimman turvallinen ylläpito. Bastion hosteihin kuitenkin kohdistuu hyökkäyksiä samoin kuin muihinkin internetin yli saatavilla oleviin palveluihin, joten ylläpito- ja hallinta pitäisi sallia vain yksityisten putkien kautta.	Hallinnointiliikenne tulee erottaa operatiivisesta liikenteestä. Bastion Hostit tulee suojata kuten muutkin järjestelmän palvelun resurssit. Myös pilvipalvelutoimittajien hallinoituja palveluita, kuten AWS Session Manager tulee harkita. Pilvipalveluntarjoajilla on yleisesti erityyppisiä ratkaisuja hallinnointiliikenteen mahdollistamiseksi ilman, että tarvitsee avata pääsyä internetin yli.
DevOps-prosessien turvattomat käytännöt voivat paljastaa IAM-ja muut tunnistetiedot.	Käyttämällä automaatiotyökaluja, kuten AWS Secrets Manageria tai Azure Key Vaultia on mahdollista toteuttaa turvallinen kirjautumistietojen ja muiden salassa pidettävän tiedojen tallennus. Salassa pidettävän tiedon päätyminen myös CI/CD putkien lokeihin tulee estää.

5. Erityishuomioita lokituksesta ja valvonnasta

Lokitus ja valvonta ovat olennaisia komponentteja, jotka palvelevat monia tarkoituksia. Niiden merkitys on ratkaisevassa roolissa turvallisuuden parantamisessa, suorituskyvyn optimoinnissa, vaatimustenmukaisuuden varmistamisessa sekä vianetsinnässä.

Turvallisuuden varmistamisen yhteydessä lokitus ja valvonta mahdollistavat uhkien nopean tunnistamisen ja niihin vastaamisen. Reaaliaikainen näkyvyys toimintoihin on välttämätöntä poikkeamien tai luvattoman käytön nopeassa havaitsemisessa. Lisäksi nämä käytännöt edistävät vaatimustenmukaisuuden noudattamista. Monet toimialat edellyttävät erityistä standardien, vaatimuksien ja säädösten noudattamista. Pilvipalveluntarjoajat tarjoavat erilaisia työkaluja vaatimustenmukaisuuden täyttämiseksi.

Suorituskyvyn optimointi on toinen tärkeä näkökohta. Valvonta varmistaa optimaalisen resurssien käytön tunnistamalla pullonkaulat, varmistamalla tehokkaan toiminnan ja ylläpitämällä resurssien ja palvelujen suorituskykyä. Vianmääritystä helpottaa lokien tarjoama historiallinen tapahtumakirjaus, joka auttaa ongelmien ja vikojen syiden tunnistamisessa.

Lokeihin liittyy kuitenkin myös luontaisia riskejä. Luotujen lokien määrä voi aiheuttaa haasteita merkityksellisen tiedon hallinnassa ja keräämisessä. Tasapainon löytäminen perusteellisen lokituksen ja lokianalyysin tehokkuuden välillä on ratkaisevan tärkeää. Lokien tallentaminen lisää myös kustannuksia, mikä edellyttää tarkkaan harkittavaa tasapainoa yksityiskohtaisen lokituksen ja siihen liittyvien kulujen välillä. Lisäksi lokit voivat sisältää arkaluonteisia tietoja, mikä edellyttää tiukkoja toimenpiteitä niiden suojaamiseksi ja pääsyn rajoittamiseksi valtuutetuille henkilöille, sekä mahdollisesti vaadittavilta osin lokien anonymisointeja ja/tai pseudonymisointeja.

Lokitukseen tulisi sisältyä pääsytietojen, sovellustoimintojen, infrastruktuurin suorituskyvyn, verkkokäyttäytymisen ja turvallisuuteen liittyvien tapahtumien tallentamisen. Nämä osa-alueet tarjoavat yhdessä kattavan kuvan koko järjestelmästä.

Lokien elinkaarimalli käsittää niiden reaaliaikaisen luomisen, yhdistämisen eri lähteistä keskitettyyn tietovarastoon, säilytysaikojen määrittämisen vaatimustenmukaisuuden ja toiminnallisten tarpeiden perusteella, lokien arkistoinnin pitkäaikaista säilytystä varten ja säännöllisen tarpeettomien lokien poistamisen. Lokituksen osa-alueiden tehokas elinkaarenhallinta on tärkeää historiallisten tietojen, vaatimustenmukaisuusstandardien, tallennustehokkuuden, sekä kustannusten optimoinnin kannalta missä tahansa laskentaympäristössä, olipa se sitten tai pilvessä tai perinteisissä konesaleissa.