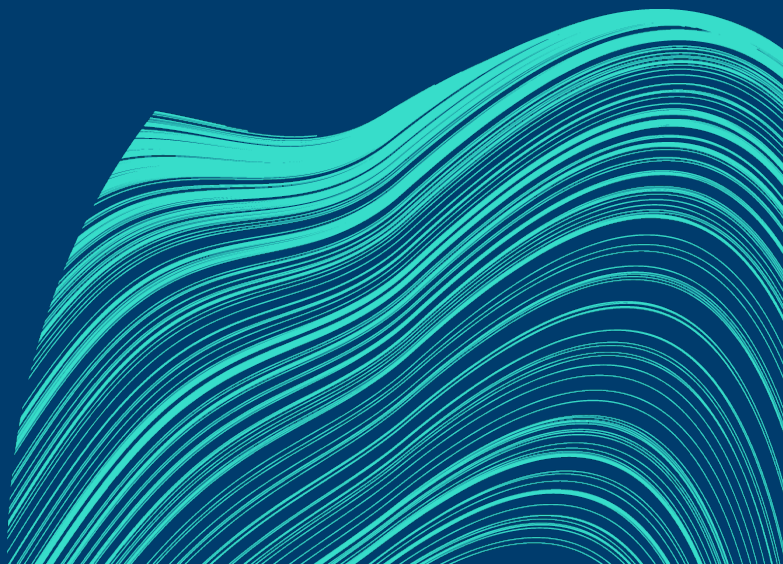
DigiFinland

Cirrus-hanke

Tekninen yhteenveto

VERSIO 1.0

15.3.2024



Sisällysluettelo

1

Johdanto

Mikä oli Cirrus-hanke ja miten sen tulokset edistävät tietosuojan huomioivaa pilvisiirtymää?

Tässä dokumentissa kuvataan julkisten pilvialustojen tietosuojan vaatimustenmukaisen käytön teknisiä mahdollisuuksia. Tavoitteena on antaa läpinäkyvää ja ajantasaista tietoa pilvipalveluteknologioista ja samalla tukea organisaatioiden julkisten pilvipalveluiden käyttöönottoa osana organisaatioiden pilvipalveluiden hallintamalleja.

Valtiovarainministeriön asettaman Cirrus-hankkeen tarkoituksena oli julkisten pilvipalvelujen toimintamalleja ja sopimusehtoja kehittämällä edistää pilvisiirtymää tietosuoja huomioiden.

Hankkeen tavoitteena oli vähentää ja poistaa (julkisten) pilvipalveluiden tietosuojaan liittyviä riskejä, neuvotella tietosuojan vaatimustenmukaisia sopimusehtoja sekä tuoda julkishallinnon vaatimuksiin yhteensovitettuja (julkisten) pilvipalveluiden toimintamalleja.

Hankkeella tavoiteltiin kansallisesti merkittäviä toiminnallisia ja kustannushyötyjä mahdollistamalla julkisen sektorin julkisten pilvipalveluiden hyödyntämistä. Hankkeen kohdetoimittajina olivat AWS, Google, Microsoft ja Oracle.

Hanketta ohjanneet tietosuojavaatimukset kuuluvat EU:n yleisen tietosuoja-asetuksen vaatimuksiin, keskeisimpiä näistä ovat oletusarvoinen ja sisäänrakennettu tietosuoja sekä rekisteröityjen oikeuksien toteutuminen. Laaja-alaisen kansallisen hyödynnettävyyden varmistamiseksi hankkeessa on keskitytty EU:n yleisen tietosuoja-asetuksen (GDPR) ja kansallisen toimialariippumattoman tietosuojasääntelyn vaatimustenmukaisuuden tavoittelemiseen.

Julkisten pilvialustojen hyödyntämisessä on huomioitava mm. seuraavia jatkuvaluonteisia tehtäviä:

Käyttäjäorganisaation osaamisen varmistaminen ja koulutus

Organisaatioiden on jatkuvasti koulutettava henkilöstöään tietosuojakäytäntöjen noudattamisessa ja valvottava, että näitä käytäntöjä noudatetaan.

Teknologian kehityksen jatkuva seuraaminen ja analysointi

Pilvipalveluiden ohella muut uudet teknologiat kuten tekoäly ja big data tuovat uusia haasteita ja mahdollisuuksia tietosuojan alueella. Organisaatioiden on arvioitava jatkuvasti, miten nämä teknologiat vaikuttavat heidän tietosuojakäytäntöihinsä.

Tietoturvariskien hallinta

Tietoturvauhkien jatkuva kehitys tarkoittaa, että organisaatioiden on jatkuvasti päivitettävä suojausstrategioitaan.

Tämän dokumentin tarkoituksena on auttaa organisaatioita näiden tavoitteiden saavuttamisessa.

Ohjeita lukijalle

Tämä dokumentti on yksi Cirrus-hankkeen lopputuloksista. Se on suunnattu ensi sijassa pilvipalveluiden käyttöönottoa suunnitteleville tai niitä jo käyttäville organisaatioille.

Tämän dokumentin tärkeimpänä kohderyhmänä ovat organisaatioiden asiantuntijat kuten esimerkiksi pilviarkkitehdit, palveluita kehittävät tahot sekä tietoturvapäälliköt ja tietosuojavastaavat.

On syytä huomata, että tämän selvityksen taustalla on ollut halu tarkastella pilvipalveluita EU:n yleisen tietosuoja-asetuksen näkökulmasta. Tietoturvallisuuden osalta on pohdittu sitä, miten eri pilvipalvelutoimittajien tietoturvallisuuden hallintakeinot tukevat rekisterinpitäjää tämän lakisääteisistä velvoitteista huolehtimisessa. Siinä mielessä tämä dokumentti eroaa aiemmista suomalaisista pilvipalveluiden tietoturvaan keskittyneistä julkaisuista.

Selvityksessä tarkastelluilla pilvipalvelutoimittajilta on saatavilla erittäin kattavaa dokumentaatiota siitä, miten juuri heidän palvelussaan voidaan toteuttaa mahdollisimman hyvää tietosuojaa sekä tietoturvallisuutta.

Kaikkia teknisiä näkökulmia ei ole mahdollista avata syvällisesti tämän selvityksen puitteissa. Uskomme kuitenkin lukijalle olevan hyödyllistä, että dokumentti osoittaa, mistä löytyy tarkempaa tietoa eri valmistajien tietosuojaa tukevista ratkaisuista.

Selvitys käsittelee pilvipalveluihin liittyvä tietosuojakysymyksiä kahden osapuolen näkökulmasta:

1. Pilvipalveluiden toimittaja eli CSP (Cloud Service Provider).
2. Pilvipalveluiden asiakas eli CSC (Cloud Service Customer).

EU:n yleisen tietosuoja-asetuksen näkökulmasta asiakas on aina vastuullinen rekisterinpitäjä ja pilvipalveluiden toimittaja on henkilötietojen käsittelijän roolissa.

Hyvin usein asiakas ei itse vastaa pilviympäristönsä operoinnista vaan tässä roolissa toimii jokin kolmas osapuoli. Silloin asiakas johtaa palvelukumppaninsa (pilvi-integraattori) toimintaa, joka puolestaan hallinnoi ja kehittää asiakkaan pilviympäristöä. Kun luette tätä dokumenttia, niin voitte mielessänne sijoittaa asiakkaan tilalle juuri teidän omaa pilviympäristöänne operoivat tahot.

Sekä asiakkaalla että toimittajalla saattaa olla myös joukko henkilötietojen alikäsittelijöitä. Nämä ovat erilaisia ulkoisia kumppaneita, jotka toimivat tavalla tai toisella asiakasorganisaation henkilötietojen käsittelijöinä tämän pilvipalveluympäristössä.

2

Pilvipalveluiden tietoturvallisuus

Mitä yleisiä ja yhteisiä periaatteita voidaan soveltaa kaikkiin pilvipalvelualustoihin?

2.1 Pilvipalveluiden käyttöönotto

Pilvipalveluiden käyttöönoton tulee tapahtua aina hallitusti, vaikka se onkin tehty teknisesti varsin helpoksi. Palveluiden käyttöönoton tulee käynnistyä organisaation ylimmän johdon strategisena päätöksenä. Aluksi eri toimittajien ja näiden palvelusopimusten vertailuun sekä sopimusneuvotteluihin tulee panostaa riittävästi. Vain näin voidaan huomioida organisaation omien tavoitteiden sekä myös velvoittavan sääntelyn huomioiminen valituilla pilvipalvelualustoilla.

Itse käyttöönoton tulee tapahtua projektimaisella lähestymistavalla. Alussa määriteltäviä asioita ovat esimerkiksi minkä tahojen toimesta ja minkälaisilla osaamisella sekä prosesseilla organisaation pilviympäristöä rakennetaan. Oleellista on myös huomioida organisaation kokonaisarkkitehtuurin linjaukset. Varsinaista toteutusvaihetta edeltää myös liiketoiminnan vaatimuksista johdettujen tietoturva- ja tietosuojatavoitteiden tarkempi määrittely sekä sovellettavien pilvipalvelun riskienhallintakontrollien valitseminen. Tietosuojan ja tietojen siirron vaikutustenarviointi (DPIA/TIA) on myös tehtävä. Vasta tämän jälkeen voidaan siirtyä varsinaiseen toteutusvaiheeseen.

Käyttöönottoprojektin valmistuessa käytön aikainen palveluiden hallinta, operointi sekä kehittäminen koko elinkaaren aikana tulee olla määriteltynä ja dokumentoituna.

Organisaation tulee laatia juuri sen omien pilvipalveluympäristöjen hallintamallin (Cloud Governance) kuvaava dokumentti, joka kattaa palveluiden käytön elinkaaren. Keskeistä on tunnistaa pilvipalvelun kriittisyys omalle toiminnalle sekä keskeiset riskit ja niiden hallintakeinot. Hallintamallissa tulee määritellä ja vastuuttaa eri osapuolten keskeiset tehtävät. Hallintamallin tulee myös olla aktiivisesti ylläpidetty koko palveluiden käytön elinkaaren ajan.

2.2 Pilvipalveluiden keskeisiä käsitteitä

Kaikista hankkeen kohdetoimittajien pilvipalveluista on tunnistettavissa joukko keskeisiä käsitteitä ja ratkaisumalleja, joiden joukosta asiakas voi valita kulloinkin sovellettavan ratkaisutavan.

Organisaatio

Organisaatio (organization) edustaa kunkin asiakkaan sitä liiketoimintaidentiteettiä, joka käyttää pilvipalvelutoimittajan palveluita. Organisaation käytössä on yksi tai useampi julkisen toimialueen nimipalvelujärjestelmän (DNS) toimialuenimi kuten organisaatio.fi. Organisaatio toimii myös pilvipalvelun tilausten säilönä.

Tenantti

Tenantti (tenant) on yksittäisen organisaation ympäristö toimittajan julkipilvialustalla. Se sisältää organisaation domainit, käyttäjät ja tilaukset.

Heti tenantin perustamisvaiheessa on käytävä läpi sen tietoturvaan vaikuttavat määrittelyt sekä tehtävä tarvittavat asiakaskohtaiset kovennukset.

Tilaukset

Tilaukset (subscriptions) ovat pilvipalvelutoimittajan kanssa tehtyjä sopimuksia yhden tai useamman pilvipalveluympäristön tai -palvelun käytöstä. Tilauksen veloitus voi perustua esimerkiksi käyttäjäkohtaiseen maksuun tai käytettyjen pilvipohjaisten resurssien kulutukseen. Tenantin alaisuudessa voi olla useita tilauksia, joihin esimerkiksi yksittäiset liiketoimintajärjestelmät voidaan sijoittaa. Etuna erillisissä tilauksissa on helpompi kustannusten kohdistaminen sekä myös lisääntyvä tietoturvallisuus. Kun järjestelmä toimii rajatummassa ympäristössä, siihen on mahdollista kohdistaa myös tarkemmin määriteltyjä tietoturvakontrolleja.

Käyttäjätilit

Käyttäjätilit ovat pilvipalveluun määriteltyjä käyttäjien identiteettejä. Ne voivat liittyä joko luonnolliseen henkilöön, mutta olla myös eri tietojärjestelmien käyttöön määriteltyjä esimerkiksi integraatiotarpeisiin. Erityisen osajoukon käyttäjätileistä muodostavat järjestelmänvalvojat, joilla on oikeus tehdä muutoksia palveluiden konfiguraatioihin, käyttöoikeuksiin sekä myös kuukausimaksullisiin tilauksiin.

Käyttöoikeudet

Käyttöoikeudet määrittelevät tietylle käyttäjätilille oikeuden käyttää määriteltyä joukkoa pilviympäristön palveluista. On huomattava, että käyttöoikeuksia on erityyppisiä. Toisaalta ne voivat kohdistua oikeuteen käyttää jotakin lisensoitua ja maksullista palvelukokonaisuutta. Toisaalta ne voivat sisältää pääsynhallinnallisen näkökulman ja avata käyttäjätilille pääsyn johonkin pilviympäristön palveluun.

Infrastruktuuri palveluna

Infrastruktuuri palveluna (IaaS, Infrastructure as a Service) on pilvipalvelun ratkaisumalli, jossa asiakas hankkii pilvestä teknologia-alustan palveluita. Näitä voivat olla esimerkiksi palvelin-, tallennus-, laskenta-, varmistus- ja tietoliikennekapasiteetti. Näiden palveluiden hyödyntäjiä ovat ICT-ylläpitäjät.

Alusta palveluna

Alusta palveluna (PaaS, Platform as a Service) on kehittämis- ja toteutusalusta, joka sisältää useita työkaluja kehittämisen ja toteutuksen tueksi. Näiden palveluiden hyödyntäjiä ovat sovellus- ja teknologiakehittäjät.

Sovellus palveluna

(Verkko)sovelluspalvelu (SaaS, Software as a Service) toteuttaa kokonaisuudessaan jonkin liiketoimintaa palvelevan tietojärjestelmän. Tyypillisesti nämä palvelut hankitaan kausitilauksena, jolloin palvelun laskutus voi perustua esimerkiksi käyttäjämäärään tai käyttöön otettujen toiminnallisten moduulien hintaan. Näitä palveluita hyödyntävät organisaatioiden loppukäyttäjät.

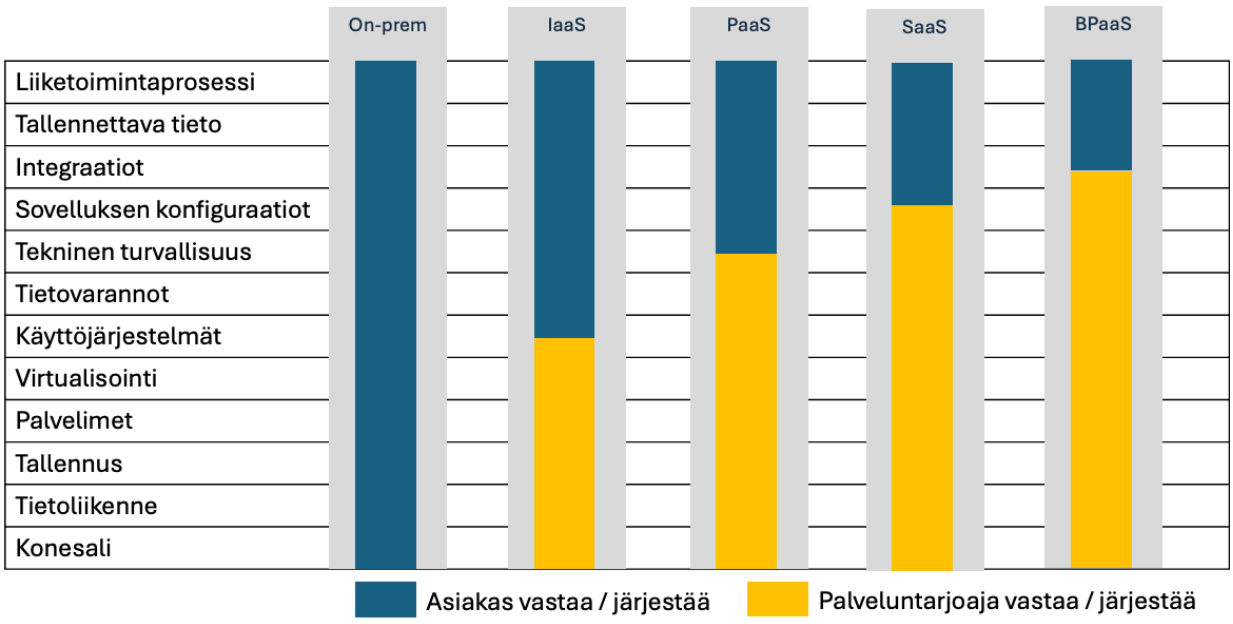
Liiketoimintaprosessi palveluna

Liiketoimintaprosessi palveluna (BPaaS, Business Process as as Service) käsittää kokonaisen palveluprosessin tai palvelun hankkimisen palveluna. Tyypillinen esimerkki on palkanlaskennan ulkoistaminen kokonaisuudessaan. Silloin ei hankita ollenkaan teknologiaa vaan käytettävät järjestelmät tulevat osana kokonaispalvelua. Näitä palveluita hyödyntävät liiketoimintavastaavat ja loppukäyttäjät.

2.3 Vastuunjako pilvipalveluissa

Pilvipalveluissa on käytössä jaetun vastuun malli (Shared Responsibility Model), joka rajaa tietoturvavastuiden jakautumisen pilvipalveluntarjoajan ja asiakkaan välillä. Tässä mallissa pilvipalveluntarjoaja vastaa pilven turvallisuudesta infrastruktuurin osalta, joka koostuu mm. fyysisistä datakeskuksista, laitteistoista ja fyysisistä verkoista. Asiakas puolestaan ottaa vastuun tietojensa, sovellusten, identiteetin ja pääsynhallinnan turvaamisesta sekä tietoturva-asetusten määrittämisestä käyttämiensä pilvipalveluiden sisällä. Toimittajan ja asiakkaan lisäksi palvelutuotantoon osallistuu tyypillisesti kummankin osapuolen taholta ulkoisia alihankkijoita sekä kumppaneita.

Tämä yhteistyöhön perustuva lähestymistapa tarjoaa asiakkaille etuja, kuten lisääntyneen turvallisuuden, joustavuuden, skaalautuvuuden ja kustannustehokkuuden. Se mahdollistaa myös joustavamman varautumisen kehittyviin tietoturvauhkiin kun molemmat osapuolet osallistuvat pilviympäristön yleiseen tietoturvaan.



* Asiakasta voi edustaa myös tämän valitsema pilvi-integraattori.

** Rekisterinpitäjän kokonaisvastuu on aina asiakkaalla itsellään.

On kuitenkin muistettava, että asiakkaan vastuulla on toiminta pilvessä, eli jaetun vastuun malli ei poista asiakkaan vastuuta palveluun tallennetun tiedon suojaamisesta. Tietosuojalainsäädännön mukainen rekisterinpitäjän kokonaisvastuu säilyy luonnollisesti aina asiakkaalla. Pilvipalvelutoimittaja toimii henkilötietojen käsittelijän roolissa ja tähän liittyvät työntekijät voivat olla sen omaa tai ulkoisten alihankkijoiden henkilöstöä.

2.4 Läpinäkyvyys turvallisuuden varmentajana

Pilvipalveluiden riskienhallinnassa oleellista on se, voiko asiakas luottaa toimittajan turvalliseen ja vaatimusten mukaiseen toimintaan. Pilvipalveluissa käytössä oleva jaetun vastuun malli johtaa siihen, että asiakkaalla ei ole suoraa näkyvyyttä toimittajan omaan toimintaan. Yksittäinen asiakas ei voi esimerkiksi mennä paikan päälle auditoimaan pilvipalvelutoimittajan datakeskusta. Varmuus sen turvallisuudesta on saatavilla ainoastaan tutustumalla toimittajan omiin kuvauksiin sekä ulkoisten auditointien tuloksiin. On huomattava, että auditoinnit eivät kuitenkaan perustu kansallisiin kriteeristöihin kuten Julkri, Katakri tai Pitukri vaan kansainvälisiin standardeihin.

Jotta asiakas voi luottaa pilvipalvelualustan turvallisuuteen tämän tulee pystyä arvioimaan palvelun toimintaa, siinä käytettyjä teknisiä ratkaisuja sekä toimittajan prosesseja.

Luottamus voi syntyä vain siten, että toimittaja kykenee riittävän läpinäkyvästi avaamaan palveluidensa tosiasiallista toimintaa. Pilvipalvelun asiakkaiden käytössä on erilaisia keinoja asioiden todellisen tilan varmistamiseksi.

Sopimusehdot

Sopimusehdot sisältävät tietoja myös siitä, millä perusteilla ja miten pilvipalvelutoimittajat käsittelevät asiakkaidensa tietoja. Vaikka ehdot on laadittu niin, että niiden tarkoituksena on hälventää asiakkaiden tietosuojahuolia, jää kokonaisuuteen kuitenkin useita ongelmallisia kohtia. Tarkastellut pilvipalvelutoimittajat saattavat joutua esimerkiksi suostumaan ulkomaisten viranomaisten tietopyyntöihin.

Toistaiseksi ei ole näyttöä siitä, että pilvipalvelutoimittajat olisivat luovuttaneet tietoja pelkkien tietopyyntöjen perusteella. Toimittajat joutuvat kuitenkin luovuttamaan tietoja oikeuden päätöksellä. Perusteena voivat olla esimerkiksi terrorismi, lapsikauppa tai organisoitu rikollisuus. Se, voiko oikeuden päätös kohdistua julkiorganisaatioon on epäselvää.

Siten pelkkien sopimusehtojen perusteella ei voida kuitata tietosuojariskejä hallituiksi, vaan henkilötietojen suojaamiseksi joudutaan soveltamaan myös teknisiä kontrolleja, kuten tietojen salausta asiakkaan omilla salausavaimilla.

Palvelukuvaukset

Palvelukuvaukset kuvaavat mistä palvelun osista toimittajien pilviympäristöt rakentuvat. Nämä kuvaukset ovat yleensä julkisia ja siten vapaasti tarkasteltavissa. Julkisten kuvausten joukosta on myös selvitettävissä esimerkiksi toimittajan palvelinkeskusten sijainti, jolloin asiakas voi määritellä ympäristönsä toimivaksi sopivalla EU-alueella. Palvelukuvausten joukosta on yhdessä sopimusehtojen kanssa löydettävissä kuvauksia myös toimittajien toimintaprosesseista sekä alihankkijoiden käytöstä.

Tekniset kuvaukset

Tekniset kuvaukset ovat kaikilla pilvipalvelutoimittajilla hyvin kattavia ja pääsääntöisesti myös julkisesti saatavilla. Näiden kuvausten perusteella on mahdollista rakentaa asiakkaan oma pilviympäristö toimittajan suosittelemalla turvallisella tavalla. Lisäksi kuvausten perusteella voidaan tehdä päätelmiä palveluiden teknisten komponenttien tosiasiallisesta toiminnasta.

Luottamukselliset kuvaukset

Luottamukselliset tai salassapitositoumuksella (NDA) saatavilla olevat dokumentit edellyttävät yleensä voimassa olevaa asiakassuhdetta pilvipalvelutoimittajan kanssa, mutta niitä voi olla saatavilla myös sopimuksen neuvotteluvaiheessa. Dokumenttien perusteella on mahdollista tehdä tarkempia päätelmiä palvelun turvallisuudesta. Luottamuksellinen dokumentaatio saattaa myös kuvata jo etukäteen palveluun tulossa olevia muutoksia tai uusia ominaisuuksia.

Ulkopuoliset arvioinnit

Ulkopuolisen tahon tekemät arvioinnit sisältävät mm. eri kriteeristöjä ja standardeja vastaan tehtyjen auditointien tulokset. Toimittajat kertovat avoimesti mitä sertifikaatteja niillä on voimassa palvelinkeskustensa osalta. Asiakkaalla on näkyvyys siihen milloin ja kenen toimesta sertifikaatti on myönnetty sekä mihin toimittajan toimintaan se kohdistuu. Näiden perusteella voidaan luottaa esimerkiksi toimittajan tietoturvallisuuden hallinnan ja myös alihankkijoiden toiminnan sisältäviin prosesseihin.

Häiriöviestintä

Häiriöviestintä kattaa kaikki toimittajan pilvipalveluihin liittyvät häiriötilanteet. Osa näistä tiedoista on julkisia ja ne kertovat esimerkiksi mihin palveluun tai konesaliin häiriö liittyy. Tarkemmat tiedot häiriön luonteesta ovat yleensä saatavilla kirjautumalla palvelun hallintaportaaliin. Portaalissa näkyy myös koskettaako häiriö juuri kyseistä asiakasta. Mikäli asiakkaan ympäristöön on kohdistunut tietoturvapoikkeama, viestitään siitä myös näiden kanavien kautta. Asiakkaan vastuulla on itse seurata näitä ilmoituksia ja varmistaa myös omien kontaktitietojensa ajantasaisuus.

Asiakkaan on yhdisteltävä useita eri tapoja varmistaakseen käyttämiensä pilvipalveluiden tietoturvallisuuden ja tietosuojan toteutumisen. Jäännösriskien pienentämiseen saatetaan joutua soveltamaan niin hallinnollisia kuin teknisiäkin keinoja. Asiakkaan luottamuksen saamiseksi toimittajat pyrkivät tekemään pilvipalveluidensa toiminnan mahdollisimman läpinäkyväksi.

Tässä selvityksessä ilmeni, että pilvipalveluiden toimittajat vastaavat yksityiskohtaisiin kysymyksiin varsin avoimesti. Asiakkaan näkökulmasta ongelmaksi muodostuu usein oikean tiedon löytäminen laajasta dokumentaatiosta.

Toimittajakohtaisissa tarkasteluissa avataan tarkemmin läpinäkyvyyteen liittyviä seikkoja sekä nostetaan esiin asiakkaan kannalta relevantteja dokumentteja tietosuojan ja tietoturvan osalta.

2.5 Pilvipalveluiden tietoturvakäytänteitä

Pilvipalvelutoimittajien toteuttaman helpon palveluiden käyttöönoton varjopuolena on se, että eurooppalaisesta näkökulmasta tarkasteltuna palveluiden oletusasetukset eivät ole riittäviä, sillä ne eivät täytä tietosuojasääntelyn vaatimustenmukaisuutta. Palvelut tarjoavat kuitenkin erilaisia välineitä, joilla nämäkin tavoitteet on mahdollista saavuttaa. Oikeiden riskienhallintakeinojen soveltaminen pilvipalvelussa on aina asiakasorganisaation omalla vastuulla.

Cloud Adoption Framework (CAF)

Cloud Adoption Framework (CAF) on toimittajien tarjoama kokoelma dokumentaatiota, käyttöönotto-ohjeita, parhaita käytäntöjä ja työkaluja, jotka tukevat pilvipalvelun turvallista käyttöönottoa.

Kaikkien toimittajien CAF:it ohjeistavat organisaatiota kyseisen toimittajan pilvipalveluun liittyvissä strategisissa päätöksissä, käyttöönoton suunnittelussa sekä myös palvelualustan hallinnassa ja käytönaikaisessa monitoroinnissa. Noudattamalla näitä ohjeita organisaation on mahdollista toteuttaa hallittava ja turvallinen pilviympäristö.

Lisätietoja:

Cloud Adoption Framework | AWS
https://aws.amazon.com/cloud-adoption-framework/

Cloud Adoption Framework | Google
https://cloud.google.com/adoption-framework

Cloud Adoption Framework for Azure | Microsoft
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/

Cloud Adoption Framework for Oracle Cloud Infrastructure (OCI) | Oracle
https://www.oracle.com/cloud/cloud-adoption-framework/

Landing Zone

Laskeutumisalue (Landing Zone) on hyvin määriteltyyn arkkitehtuuriin ja mahdollisesti useampaan pilvitiliin perustuva skaalautuva ja turvallinen ympäristö.

Laskeutumisalueen rakentaminen edellyttää organisaatiolta sekä teknisiä että liiketoiminnallisia linjauksia. Tavoitteena on mahdollistaa palvelun turvallinen ja tarpeen mukaan myös skaalautuva ja monitoimittajamalliin soveltuva organisaation pilviympäristö.

Kaikki tarkastellut pilvitoimittajat tukevat laskeutumisaluemäärityksiä.

Lisätietoja:

What is a landing zone? | AWS
https://docs.aws.amazon.com/prescriptive-guidance/latest/migration-aws-environment/understanding-landing-zones.html

Landing zone design in Google Cloud | Google
https://cloud.google.com/architecture/landing-zones

Azure landing zone architecture | Microsoft
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/#azure-landing-zone-architecture

Deploy a secure landing zone that meets the CIS Foundations Benchmark for Oracle Cloud | Oracle
https://docs.oracle.com/en/solutions/cis-oci-benchmark/index.html#GUID-89CA48AA-73E1-4992-A43F-CA5FA5CE21CD

Well-Architected Framework

Pilvipalvelutoimittajien Well-Architected Frameworkit opastavat asiakkaiden pilviarkkitehteja rakentamaan turvallisia, suorituskykyisiä, joustavia ja kustannustehokkaita ympäristöjä asiakkaan sovelluksille ja työkuormille.

Kaikki tarkastellut pilvitoimittajat tukevat kattavalla dokumentaatiollaan pilviarkkitehtien työtä.

Lisätietoja:

Well-Architected | AWS
https://aws.amazon.com/architecture/well-architected/

Cloud Architecture Framework | Google
https://cloud.google.com/architecture/framework

Azure Well-Architected Framework | Microsoft
https://learn.microsoft.com/en-us/azure/well-architected/

Best practices framework for Oracle Cloud Infrastructure | Oracle
https://docs.oracle.com/en/solutions/oci-best-practices/#GUID-5F2D2745-934E-409A-A7BA-D0976F727845

CIS Bechmarks

Organisaation pilviympäristön käynnistämisen yhteydessä on tärkeää määritellä ympäristön tietoturvalliset perusasetukset (baseline). Center for Internet Security (CIS) määrittelee ilmaisissa kriteeristöissään (bechmark) eri pilvipalvelualustoille suositeltavia turvallisuusasetuksia ja kovennuksia (hardening).

Organisaation tulisikin hyödyntää pilvipalvelutoimittajien omien ohjeiden lisäksi myös ulkopuolisia kriteeristöjä heti pilvisiirtymänsä alussa. Muutoksia palveluiden perusasetuksiin on palveluiden käytön jo alettua paljon vaikeampi tehdä ja niistä voi aiheutua turhia kustannuksia tai loppukäyttäjille näkyviä vaikutuksia.

Lisätietoja:

CIS Benchmarks List | Center for Internet Security
https://www.cisecurity.org/cis-benchmarks

Pilven tietoturvaa kontrolloivat säännöstöt

Laajojen ja monimutkaisten ympäristöjen haasteena on ihmisten kiire ja aikataulupaineet, minkä vuoksi he eivät ehdi lukea kaikkea ohjeistusta. Lisäksi yksilöiden tavat tehdä asioita poikkeavat toisistaan, jolloin turvallisessa tekemisessä voi olla suurtakin hajontaa. Siksi tuleekin soveltaa myös pilvipalveluissa käytettävissä olevia riskien hallintakeinoja.

Pilvipalveluympäristöt tarjoavat työkalut koko ympäristön osalta pakottavien säännöstöjen (policy) määrittelyyn. Niitä hyödyntämällä voidaan toteuttaa turvallisuuden kannalta kolmea keskeistä periaatetta:

1. **Automatisoi** (Automate), jolloin kaikki virheherkät ja nopeaa reagointia vaativat tehtävät automatisoidaan pilvipalvelualustan ratkaisuilla. Silloin esimerkiksi uudet käyttäjät luodaan niin, että heidän käyttöoikeutensa ovat automaattisesti oikein ja monivaiheinen tunnistaminen tulee käyttöön.

   Poikkeamatilanteessa automaatio voi lukita tietojenkalastelun uhriksi joutuneen käyttäjän tunnuksen muutamassa sekunnissa ennen lisävaurioiden syntymistä.

2. **Pakota** (Enforce), jolloin valitut tietoturvakontrollit kohdistuvat poikkeuksetta kaikkiin organisaation pilvipalvelualustalla toimiviin henkilöihin sekä myös tietojärjestelmiin. Pakottaminen tulee viedä niin tiukalle tasolle, että turvallisuuskontrollien kiertäminen ei ole mahdollista.

3. **Pienimmän käyttöoikeuden periaate** (Least Privilege), jolloin henkilöillä tai järjestelmillä on ainoastaan toiminnan kannalta tarpeelliset käyttöoikeudet. Tarpeen mukaan käyttöoikeuksia voidaan korottaa jonkin tehtävän suorittamiseksi, jonka jälkeen ne palautuvat automaattisesti alemmalle tasolle.

Yhteenveto

Yleisesti pilvipalvelut tarjoavat hyvin monenlaisia keinoja tietoturvallisuuden sekä tietosuojan varmistamiseksi. Kulloinkin sovellettavien ratkaisuiden tulee perustua riskipohjaiseen lähestymistapaan. Punaisena lankana tulisi olla se, kuinka pääsyä organisaation pilviympäristöön kontrolloidaan sekä miten siellä olevaa tietoa suojataan ja kuinka poikkeamat havaitaan ja niiden vaikutukset rajataan.

Tietosuojan kannalta tulee erityisesti tarkastella myös tiedon fyysistä tallennuspaikkaa (location) sekä sitä, ketkä pilvipalvelutoimittajan ja tämän alihankkijoiden henkilöt pääsevät käsiksi palveluun tallennettuun asiakkaan tietoon. Näihin kysymyksiin annettaan vastauksia tämän dokumentin myöhemmissä luvuissa.

2.6 Lokienhallinta pilvipalvelussa

Sääntelyn näkökulma

Viranomaisen toiminnassa lokitietojen käsittelyä koskevat velvoitteet koskevat luonnollisesti myös pilvipalveluita.

EU:n yleisen tietosuoja-asetuksen 5 artiklan toisen kohdan mukaan rekisterinpitäjän tulee pystyä osoittamaan henkilötietojen käsittelyä koskevien periaatteiden noudattaminen. Lokitietojen avulla tulee pystyä silloin osoittamaan kaikissa tilanteissa tietosuoja-asetuksen 5 artiklan 1. kohdan f-alakohdan mukainen henkilötietojen asianmukainen turvallisuus.

”niitä on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (’eheys ja luottamuksellisuus’).”

Laki julkisen hallinnon tiedonhallinnasta (906/2019) 17§ määrää:

”Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.”

Laki sähköisen viestinnän palveluista (917/2014) pykälä 145 ja siihen liittyvä voimassa oleva Liikenne- ja viestintävirasto Traficomin ohje

(Traficom/376384/03.04.05.01/2022) mukaan:

”Pilvipalveluntarjoajan kaupallinen käytäntö ei ole asianmukainen peruste vedota käsittelylokin tallentamisvelvollisuutta koskevaan poikkeusperusteeseen, koska nykyaikaisessa pilvipalvelussa lokitietojen tallentamista ei normaalisti voida pitää teknisesti mahdottomana eikä lokituksen toteuttaminen aiheuta epätavanomaisia kustannuksia. Palvelua käyttävällä yhteisötilaajalla voi usein olla käytettävissään erilaisia teknisiä keinoja lokitietojen tallentamiseen.

Yhteisötilaajalla voi olla lisämaksullisen palvelun hankkimisen lisäksi esimerkiksi mahdollisuus siirtää palvelusta lokitietoja joko erilliseen tiedostoon tai tallentaa niitä rajapinnan kautta omiin järjestelmiinsä pidempään säilytettäväksi. Lakisääteinen säilytysaika tulee ottaa huomioon myös pilvipalvelun käytön päättymisen yhteydessä.”

Voimassa olevan sääntelyn perusteella pilvipalveluiden käyttö ei vapauta organisaatiota lokienhallintaan liittyvistä vastuista. Toisaalta lokienhallinnalle asetetut vaatimukset eivät sisällä mitään sellaista, mikä ei olisi toteutettavissa myös pilvipalvelualustoilla.

Lisätietoja:

EU:n yleinen tietosuoja-asetus (GDPR) | EUR-Lex
https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504

Laki julkisen hallinnon tiedonhallinnasta | Finlex
https://www.finlex.fi/fi/laki/ajantasa/2019/20190906#a906-2019

Laki sähköisen viestinnän palveluista | Finlex
https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Liikenne- ja viestintäviraston ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta | Traficom
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Liikenne-%20ja%20viestint%C3%A4viraston%20ohje%20v%C3%A4litystietojen%20k%C3%A4sittely%C3%A4%20koskevien%20tietojen%20tallentamisesta.pdf

Tekninen näkökulma

Selvityksen aikana ilmeni, että kaikki pilvipalvelut tuottavat kattavaa lokitietoa. Lokitus koskee niin palvelun teknistä kuin palvelutuottajan oman ja alihankkijoiden henkilöiden toimintaa. Lisäksi yksittäisen asiakasympäristön sisällä syntyy myös sen käyttöön liittyvää lokia esimerkiksi kirjautumisten ja operoinnin osalta.

Pilviympäristöissä ajettavien asiakassovellusten lokitusten osalta on käytettävissä myös paljon eri vaihtoehtoja, mutta niiden soveltaminen jää asiakkaan omalle vastuulle. Lokien säilytysaikoja voidaan kasvattaa lisämaksusta oletusaikoja pidemmäksi. Maksimi lokien säilytysaika on tyypillisesti 10-12 vuotta. Lokien pitkäaikaissäilytys tapahtuu kuitenkin hitaammalla tallennusmedialla eikä se mahdollista suoria kyselyitä.

Lokeja on myös mahdollista ohjata asiakkaan omiin valvontaympäristöihin ja lisäksi pilviympäristön sisällä voidaan perustaa erillisiä lokitietojen arkistoja. Niihin pääsyä ja niiden eheyttä voidaan kontrolloida varsinaisen valvottavan palvelun ulkopuolella.

Toimittajakohtaiset tarkennukset

AWS:

AWS pilvipalveluissa on mahdollista ottaa käyttöön useita erilaisia lokienhallinnan palveluita.

CloudWatch tarjoaa kattavan ja integroidun ratkaisun AWS-resurssien ja –sovellusten valvontaan ja lokitukseen. Siihen on integroitu erilaisia tilannekuvan näyttöjä, mittareita, hälytyksiä sekä poikkeamien havainnointitoimintoja.

CloudWatch:in lisäksi CloudTrail tuo näkyvyyden käyttäjien toimintaan sekä myös API-kutsuihin AWS:n alustalla. S3 ja Kinesis –palveluihin voidaan tallentaa lokitietoja.

Lisätietoja:

Amazon CloudWatch | AWS
https://aws.amazon.com/cloudwatch/

AWS CloudTrail | AWS
https://aws.amazon.com/cloudtrail/

Amazon S3 | AWS
https://aws.amazon.com/s3/

Amazon Kinesis Data Streams | AWS
https://aws.amazon.com/kinesis/data-streams/

Google:

Cloud Logging on Googlen lokienhallinnan ratkaisu. Se mahdollistaa sekä toimittajan pilvipalvelun että myös ulkoisten lokilähteiden liittämisen. Cloud Monitoring tarjoaa näkymän lokeihin sekä mahdollistaa myös erilaiset hälytykset.

Cloud Pub/Sub mahdollistaa suurten lokitietomassojen tallentamisen sekä niiden salaamisen.

Lisätietoja:

Cloud Logging | Google
https://cloud.google.com/logging

Cloud Monitoring | Google
https://cloud.google.com/monitoring

Pub Sub | Google
https://cloud.google.com/pubsub

Microsoft:

Azure Monitor muodostaa lokidatan käsittelyyn tarkoitetun alustan. Se kerää eri lokilähteiden lokit ja mahdollistaa niiden hyödyntämisen. Esimerkiksi Log Analytics mahdollistaa kyselykielen avulla erilaiset lokimassaan kohdistuvat kyselyt. Lokit voidaan esitää myös Microsoft Sentinel SIEM-tuotteessa.

Lisätietoja:

Azure Monitor documentation | Microsoft
https://learn.microsoft.com/en-us/azure/azure-monitor/

Overview of Log Analytics | Microsoft
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview

Microsoft Sentinel documentation | Microsoft
https://learn.microsoft.com/en-us/azure/sentinel/

Oracle:

OCI Logging on Oraclen keskitetty ratkaisu sen pilvialustan ja ulkoisten lokien hallintaan. Oraclen OCI Monitoring tarjoaa lokien analyysin ja hälytykset. OCI Streaming mahdollistaa lokitiedon skaalautuvan säilytyksen sekä myös lokien salaamisen.

Lisätietoja:

Logging Overview | Oracle
https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm

Monitoring | Oracle
https://docs.oracle.com/en-us/iaas/Content/Monitoring/home.htm

Overview of Streaming | Oracle
https://docs.oracle.com/en-us/iaas/Content/Streaming/Concepts/streamingoverview.htm

Bulk Export of Audit Log Events| Oracle
https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/bulkexport.htm

2.7 Tietoturvauhkien aktiivinen ja jatkuva havainnointi sekä niihin reagointi

Pilvipalveluiden tietoturvaetu tulee toimittajien kyvykkyydestä investoida merkittävästi tietoturvallisuuteen ja siihen liittyviin palveluihin.

Kun tarkastellaan näissä palveluissa tarvittaessa käyttöön otettavissa olevia tietoturvakyvykkyyksiä, niin omiin ympäristöihin (on-premise) toteutettuna harvalla suomalaisella organisaatiolla on mahdollisuuksia samaan. Kun vielä muistetaan pilvipalveluiden tietoturvaominaisuuksien mahdollistavan myös erilaiset automatiikat esimerkiksi poikkeamiin reagoinnissa, sekä näiden sitomisen toimittajan kaikista asiakkuuksistaan keräämään kyberuhkatietoon, niin ero tulee entistä selvemmäksi.

Kolikon kääntöpuolena on toki, että harvalla organisaatiolla on myöskään rahallisia resursseja ottaa käyttöön kaikkia tarjolla olevia tietoturvaominaisuuksia. Pilvipalveluiden asiakasorganisaatiot joutuvatkin siis priorisoimaan omasta näkökulmastaan kyberriskien hallitsemiseksi tarvittavia pilvipalvelun tietoturvaominaisuuksia.

Kun asiaa tarkastellaan tietosuojan näkökulmasta, niin rekisterinpitäjän vastuu käytännössä pakottaa ottamaan käyttöön myös pilvipalveluiden lisämaksullisia tietoturvaominaisuuksia. Tämä asia on syytä huomioida kustannuksia arvioitaessa.

Yleisiä sähköisten palveluiden kyberuhkia

Jos tarkastellaan tyypillisiä digitaalisia palveluita, niin niistä on löydettävissä kolme hyvin tyypillistä tietoturvapoikkeaman syytä. Nämä ovat mahdollisia riippumatta siitä tuotetaanko palveluita omasta ympäristöstä vai pilvipalvelualustalta.

Tietojenkalastelu

Tietojenkalastelun seurauksena palvelun käyttäjätietoja päätyy kyberrikollisten tietoon. Silloin tapahtumaa estävänä hallintakeinona voidaan käyttää monivaiheisen tunnistautumisen vaatimusta. On kuitenkin mahdollista, että se onnistutaan ohittamaan. Silloin on tärkeää, että tapahtuma kyetään havaitsemaan mahdollisimman nopeasti ja automaattisesti. Edelleen on tärkeää rajoittaa lisävahingot esimerkiksi sulkemalla automaattisesti vaarantunut käyttäjätunnus.

Pilvipalvelualustat tarjoavat tietojenkalastelu-uhkaa vastaan erilaisia hallintakeinoja. Toimittajat myös kehittävät ja pitävät niitä ajantasaisena saamansa kyberuhkatiedon perusteella.

Palvelunestohyökkäys

Palvelunestohyökkäyksessä kyberrikollinen kuormittaa palvelua tavalla tai toisella niin, että se ei kykene enää kunnolla palvelemaan käyttäjiään. Palvelunestohyökkäykset ovat arkipäivää ja niitä kohdistetaan jatkuvasti myös suomalaisiin organisaatioihin.

Organisaation omaan (on-premise) ympäristöön päässeen usein hyvin voimakkaankin palvelunestohyökkäyksen vaikutuksia palveluiden toimintaan on käytännössä mahdotonta estää. Asiaa vaikeuttaa myös se, että voimakkaan verkkoliikenteen sijasta hyökkäys voikin kohdistua sovelluskerrokseen kuormittaen siten myös organisaation taustajärjestelmiä ja tietovarantoja.

Organisaatioiden julkiseen verkkoon näkyvissä palvelurajapinnoissa on niiden saatavuusuhkien torjumiseksi nykyään käytännössä otettava käyttöön erillinen verkkosovelluspalomuuri (Web Application Firewall, WAF).

Pilvipalveluiden WAF:it kykenevät torjumaan hyvin voimakkaitakin palvelunestohyökkäyksiä. Asiakasorganisaation omalle vastuulle jää konfiguroida tai ”opettaa” WAF erottamaan se mikä on normaalia palvelun käyttöä ja mikä ei. Julkipilvipalveluihin integroituvia WAF-palveluntarjoajia on muitakin kuin tässä selvityksessä mukana olleet toimittajat (esim. CloudFlare tai Fastly).

WAF:in etu on, että niihin sisältyy myös erilaisten muiden verkkouhkien torjuntakykyjä. Niinpä niiden avulla on mahdollista torjua erilaisten injektiohaavoittuvuuksien hyödyntämistä tai rakentaa nopeasti suojautumista uusien vakavien haavoittuvuuksien osalta. Usein asiakkaan ei välttämättä edes tarvitse itse tehdä mitään, vaan pilvipalvelutoimittaja lisää kaikkien asiakkaiden WAF-säännöstöön torjuntaa esimerkiksi uutta ja kyberrikollisten aktiivisesti hyväksikäyttämää haavoittuvuutta vastaan.

Haavoittuvuudet

Kaikenlaisista ICT-palveluista löytyy jatkuvasti uusia haavoittuvuuksia. Kriittisimpiä ovat sellaiset haavoittuvuudet, jotka ovat hyödynnettävissä julkisen verkon kautta ilman tunnistautumista sekä mahdollistavat pääkäyttäjäoikeuksilla mielivaltaisen komentojen suorittamisen haavoittuvassa järjestelmässä.

Kriittisten haavoittuvuuksien tapauksessa on nykyään oleellisen tärkeää, että haavoittuvuudet paikataan mahdollisimman nopeasti. Jo hyödyntämisen alla olevat kriittiset haavoittuvuudet tulee paikata tuntien (eikä päivien tai kuukauden) kuluessa niiden julkisuuteen tulosta. Joskus tuntemattomat haavoittuvuudet ilmenevät kun niiden hyväksikäytöstä havaitaan jo merkkejä. Silloin puhutaan nollapäivähaavoittuvuuksista.

Omia ympäristöjä operoivan organisaation on todella vaikeaa pitää kattavaa ja ajantasaista haavoittuvuustilannekuvaa sekä kyetä riittävän nopeaan päivityssykliin. Pilvipalvelualustoilla itse infrastruktuuri on rakennettu niin, että toimittajat kykenevät ilman asiakkaille näkyviä vaikutuksia pitämään haavoittuvuustilanteen hallinnassa. Luonnollisesti asiakkaan omien työkuormien osalta päivitysvastuu on jaetun vastaan mallin mukaisesti täällä itsellään. Siihenkin pilvipalvelut tarjoavat toki työkaluja.

Toimittajakohtaiset tarkennukset – suojautuminen

Suojautumisen tavoitteena on, että organisaatio suojaa tunnistetut kohteet, kuten tietojärjestelmät, tietovarannot ja tiedot riskienhallinnan keinoin tunnistetuilta uhilta ja riskeiltä.

AWS

Amazon GuardDuty suojaa palvelun käyttäjä- ja järjestelmäidentiteettejä jatkuvan monitoroinnin sekä koneoppimisalgoritmien avulla. Se mahdollistaa automaattiset vaarantuneisiin identiteetteihin kohdistuvat poikkeaman rajoittamistoimet.

AWS WAF on verkkosovelluspalomuuri, jonka integroituu Amazonin muihin pilvipalveluihin. Sen avulla on mahdollista määritellä erilaisia suojauspolitiikkoja, estää ja suodattaa haitallista liikennettä sekä monitoroida suojauksen toimintaa.

Amazon Inspector on haavoittuvuuksienhallinnan palvelu, joka tarkkailee asiakkaan palveluita jatkuvasti erilaisten haavoittuvuuksien varalta. Se auttaa tunnistamaan lähes reaaliaikaisesti kunkin sovelluksen aktiivisen haavoittuvuustilanteen, priorisoimaan rajoittavia toimenpiteitä sekä takaamaan mahdollisimman hyvän kattavuuden haavoittuvuuksien hallinnan osalta.

Lisätietoja:

Amazon GuardDuty | AWS
https://docs.aws.amazon.com/guardduty/

AWS WAF Documentation | AWS
https://docs.aws.amazon.com/waf/

Amazon Inspector | AWS
https://aws.amazon.com/inspector/

Google

Cloud Armor on Googlen verkkosovelluspalomuuri. Se sisältää eri tyyppisiltä palvelunestohyökkäyksiltä suojautumisen. Lisäksi sen muokattavissa olevan säännöstön avulla on mahdollista torjua muitakin verkkohyökkäyksiä.

Web Security Scanner pystyy tunnistamaan Googlen App Engine-, Google Kubernetes Engine (GKE)- sekä Compute Engine –alustoilla ajettavista sovelluksista haavoittuvuuksia. Palvelu kykenee tekemään tämän vain julkiseen verkkoon julkaistujen verkko-osoitteiden kautta.

Lisätietoja:

Google Cloud Armor Documentation | Google
https://cloud.google.com/armor/docs

Web Security Scanner | Google
https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview

Microsoft

Microsoft Entra ID Protection kykenee tunnistamaan käyttäjäidentiteettien riskejä, havainnoimaan poikkeamia sekä tekemään automaattisia poikkeamien rajoittamistoimia. Osa ominaisuuksista on lisämaksullisten korkeampien lisenssitasojen takana.

Azure Web Application Firewall on Microsoftin pilvinatiivi verkkosovelluspalomuuri. Se kykenee suojaamaan palvelunestohyökkäyksiltä sekä myös muun tyyppisiltä verkkohyökkäyksiltä.

Microsoft Defender Vulnerability Management kykenee tunnistamaan Azure-alustalla ajettavista virtuaalipalvelimista haavoittuvuuksia. Se hyödyntää tässä niille palvelimiin asennettuja Defender-päätelaitesuojauksen agentteja.

Lisätietoja:

Identity Protection | Microsoft
https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

Azure Web Application Firewall | Microsoft
https://azure.microsoft.com/en-us/products/web-application-firewall

What is Microsoft Defender Vulnerability Management | Microsoft
https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide

Oracle

Oracle Web Application Firewall kykenee suojaamaan alustalla ajettavia verkkosovelluksia palvelunestohyökkäyksiltä. Siinä on myös kykyä suojautua muilta verkkohyökkäyksiltä.

OCI Vulnerability Scanning Service kykenee tunnistamaan haavoittuvuuksia sekä palvelurajapinnoista että alustalla ajettavien konttien sisältä.

Cloud Guard on OCI:n palvelu, joka auttaa asiakkaita keskitetysti seuraamaan, tunnistamaan ja ylläpitämään tietoturva-asetuksia Oracle Cloudissa. Palvelun avulla monitoroidaan jatkuvasti mm. konfigurointiin liittyviä poikkeamia tai käyttäjien riskialttiita toimintoja. Palvelu ehdottaa, auttaa ja korjaa toiminnot annettujen sääntöjen perusteella.

Tietovarastojen keskitetty turvallisuusmonitorointi ja hallinta tapahtuu Data Safen kautta. Se tarjoaa kaikki OCI Oracle tietovarastojen suojaamiseen (ml. auditointi, käyttöoikeudet, poikkeamat) liittyvät työvälineet integroidusti yhdestä paikasta.

Security Advisor palvelu tarjoaa käyttäjille Oraclen parhaita tietoturvakäytäntöjä, mukaan lukien Security Zones -resurssien määritysvaatimukset.

Lisätietoja:

Web Application Firewall | Oracle
https://docs.oracle.com/en-us/iaas/Content/WAF/home.htm

Vulnerability Scanning | Oracle
https://docs.oracle.com/en-us/iaas/scanning/home.htm

Cloud Guard | Oracle
https://docs.oracle.com/en-us/iaas/cloud-guard/home.htm

Data Safe | Oracle
https://docs.oracle.com/en-us/iaas/data-safe/index.html

Toimittajakohtaiset tarkennukset – havainnointi ja reagointi

Havainnoinnin ja reagoinnin tarkoituksena on tunnistaa pilviympäristöstä poikkeava toiminta sekä reagoida siihen rajoittavin toimenpitein mahdollisimman nopeasti ja tehokkaasti.

Perinteisissä omien ympäristöjen (on-premise) ratkaisuissa nämä avaintoiminnot on hyvin usein erotettu toisistaan ja ne sisältävät hyvin paljon manuaalista työtä. Toisin sanoen esimerkiksi SIEM-järjestelmä nostaa esiin epäillyn poikkeaman, analyytikko tutkii sen sekä soveltaa siihen sitten ennalta määritellyn pelikirjan mukaisia poikkeamaa rajoittavia toimenpiteitä.

Pilvipalvelualustoilla havainnoinnin ja reagoinnin osalta on mahdollista hyödyntää kohtuullisin kustannuksin koneoppimista ja automaatiota, jolloin poikkeamatilanteen tapahtumisesta sen vaikutusten automaattiseen rajoittamiseen kuluva aika saattaa olla vain joitakin sekunteja. Silloin esimerkiksi käyttäytymismallien ja tunnistetietojen perusteella tietojenkalasteluun haksahtaneen käyttäjän tunnukset voivat mennä lukkoon välittömästi ennen kuin kyberrikollinen ehtii toteuttaa suunnitelmansa seuraavaa vaihetta.

AWS

AWS Security Hub sisältää Automated Security Response on AWS –toiminnallisuuden, jonka avulla on mahdollista määritellä erilaisia automaatioita ja pelikirjoja kyberuhkiin reagoimiseksi.

Lisätietoja:

Threat Detection & Response Automation | AWS
https://aws.amazon.com/solutions/security/threat-detection-response-automation/

Google

Chronicle Security Operations on Googlen tietoturvapoikkeamien käsittelyyn ja automatisointiin suunniteltu ratkaisu.

Lisätietoja:

Chronicle Security Operations | Google
https://cloud.google.com/security/products/security-orchestration-automation-response

Microsoft

Microsoft Sentinel mahdollistaa tietoturvapoikkeamien havainnoinnin ja niihin reagoinnin niin Azuressa kuin erilaisissa hybridiympäristöissäkin. Se kykenee keräämään lokeja useista eri lähteistä, tunnistamaan niistä poikkeamia sekä reagoimaan niihin automaattisesti ja erilaisten pelikirjojen mukaisesti.

Lisätietoja:

What is Microsoft Sentinel? | Microsoft
https://cloud.google.com/security/products/security-orchestration-automation-response

Oracle

Havainnointi ja reagointi sisältyvät Oraclen Cloud Guard –palveluun (kts. edellinen kohta “Suojautuminen”).

Tietoturvapalveluiden hinnoittelu

Pilvialustoilla on otettavissa käyttöön erilaisia tietoturvallisuuteen liittyviä lisäpalveluita. Toimittajien hinnoittelumallit poikkeavat toisistaan. Joitakin näiden palveluiden osia saattaa sisältyä jo perustilaukseenkin. Esimerkiksi mahdollisesti tietojenkalastelun uhriksi joutunut käyttäjä saatetaan tunnistaa ilman lisämaksua, mutta tähän liittyvät automaattiset rajoittamistoimet ovatkin lisämaksullisen tilauksen takana. Tietoturvapalveluita on mahdollista ostaa erikseen tai suurempina kokonaisuuksina.

Ennen näiden palveluiden hankintaa on syytä kirkastaa organisaation omaa kyberuhkakuvaa sekä siitä johtuvia riskejä ja vaadittuja riskien rajoittamistarpeita. Sen jälkeen tulee tutustua oman pilvipalvelualustan tarjoamiin tietoturvaominaisuuksiin sekä niiden hinnoittelumalleihin. On syytä myös huomata, että itse tietoturvaominaisuuksien lisäksi kustannuksia muodostuu kyseisen palvelun käyttämien lokitietojen tallentamisesta.

AWS

AWS Security Hub tarjoaa palvelua, jolla on mahdollista arvioida eri ominaisuuksien käyttöönotosta aiheutuvia kustannuksia. Hinnoitteluun vaikuttaa esimerkiksi se kuinka monelle palvelutunnukselle tietoturvatarkastukset kohdistuvat, paljonko niitä tehdään, paljonko on löydöksiä ja minkälaisia automaatioita rakennetaan.

Lisätietoja:

AWS Security Hub Pricing | AWS
https://aws.amazon.com/security-hub/pricing/

Google

Security Command Center -hinnoittelu riippuu esimerkiksi tarkasteltavan työkuorman tyypistä, tarvittavasta suoritinkapasiteetista tai käsiteltävästä tietomäärästä. Tähän liittyvää hinnoittelua on avattu erillisellä verkkosivulla.

Lisätietoja:

Security Command Center Pricing | Google
https://cloud.google.com/security-command-center/pricing

Microsoft

Microsoft on paketoinut suuren osan tietoturvapalveluistaan Microsoft 365 E5 perheen ohjelmistopakettiin. Valittavissa on niin tietoturvaan tarkoitettu E5 Security kuin tiedon suojaamiseen soveltuva E5 Compliance pakettikin.

Hinnoittelumallina näissä on käyttäjäkohtainen kuukausihinta. Azure-palveluiden suojaamiseen on hankittava mahdollisesti erillisiä Defender tuoteperheen paketteja.

Tietoturvan valvontaan tarkoitettu Microsoft Sentinel on hinnoiteltu tallennettujen lokien määrän perusteella. Verkosta löytyy myös epävirallinen palvelu, josta voi tutkia osaa Microsoft 365 tietoturvaominaisuuksia eri lisenssitasoilla.

Lisätietoja:

Microsoft Defender for Cloud pricing | Microsoft
https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/

Microsoft Sentinel pricing | Microsoft
https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/

Microsoft 365 Licensing | Aaron Dinnage
https://m365maps.com/

Oracle

Cloud Security Pricing -sivustolla on mahdollista arvioida OCI:n eri tietoturvapalveluiden kustannuksia. Oraclen suvereenissa pilvessä on saatavilla samat palvelut samalla hinnoittelulla kuin Oraclen globaalissa julkipilvessä. Tosin tietosuojaan liittyvät rajoitteet rajaavat tietyt ulkoiset palvelut pois (esim. Azure Interconnect -yhdyskäytävä).

Lisätietoja:

Cloud Security Pricing | Oracle
https://www.oracle.com/security/cloud-security/pricing/

Cost Estimator | Oracle
https://www.oracle.com/cloud/costestimator.html

Services available in all cloud regions | Oracle
https://www.oracle.com/cloud/public-cloud-regions/service-availability/

Tietoturvapalveluiden tietosuoja

Nykyisten tietoturvauhkien tehokas havainnointi sekä niihin vastaaminen vaatii erilaisten koneoppimisalgoritmien hyödyntämistä. Silloin yhtenä elementtinä on käyttäjien tekemien toimenpiteiden analysointi ja vertailu normaaliin. Siksi EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi tulee aina tehdä myös käyttöönotettujen tietoturvaominaisuuksien osalta.

3

Julkipilvialustojen riskit ja mahdollisuudet

Mitä riskejä ja mahdollisuuksia pilvipalveluissa on tietosuojan näkökulmasta tarkasteltuna?

Tässä luvussa kuvataan pilvipalveluihin liittyviä riskejä ja mahdollisuuksia. Tarkasteluun sisältyy sekä yleisiä että erityisesti pilvipalveluympäristöihin liittyviä riskejä painopisteen ollessa pilvipalveluympäristöissä esiintyvissä riskeissä.

Riskien arvioinnissa tulee ottaa huomioon sekä riskin todennäköisyys että sen vaikutuksen suuruus. Tämän selvityksen painopisteenä on riskien todennäköisyyden arviointi, koska riskien vaikutukset riippuvat rekisterinpitäjän pilvipalveluun tallentamien henkilötietojen ja niiden käsittelyn luonteesta.

Pilvipalveluiden käyttöönottoa harkitsevien organisaatioiden tulee omassa riskien arvioinnissaan ottaa huomioon riskien vaikutukset rekisteröidyn näkökulmasta. Tämä EU:n yleiseen tietosuoja-asetukseen perustuva vaatimus koskee kaikkea henkilötietojen käsittelyä, mutta sen merkitys korostuu pilvipalveluita käytettäessä, koska uutta teknologiaa hyödyntävä henkilötietojen käsittely voi aiheuttaa todennäköisemmin korkean riskin rekisteröidyille.

Huolellinen vaikutustenarvioinnin tekeminen sekä selkeät kriteerit rekisteröityihin kohdistuvien riskien arvioimiseksi tukevat osaltaan lain edellyttämää riskien arviointia. Lisätietoa vaikutustenarvioinnin tekemisestä ja rekisteröityihin kohdistuvien riskien arvioimisesta löytyy Tietosuojavaltuutetun toimiston vaikutustenarviointia koskevista ohjeista.

Lisätietoja:

EU:n yleinen tietosuoja-asetus (GDPR) | EUR-Lex
https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504

Vaikutustenarviointi | Tietosuojavaltuutetun toimisto
https://tietosuoja.fi/vaikutustenarviointi

3.1 Yleistä pilvipalveluiden tietosuojariskeistä

Lähtökohtaisesti pilvipalveluihin kohdistuvat samat tietosuojariskit kuin muillakin teknologioilla toteutettuihin palveluihin. Globaali toimintamalli ja uudenlainen teknologia korostavat tietosuojariskien arvioinnin merkitystä pilvipalveluissa. Mahdolliset puutteet pilvipalvelun turvallisuudessa sekä eri asiakkaiden kanssa yhteiskäytössä oleva ympäristö voivat suurentaa tietoturvaongelmien vaikutuksia ja heikentää asiakkaan mahdollisuuksia reagoida mahdollisiin alustassa oleviin puutteisiin.

Pilvipalvelut tarjoavat lähtökohtaisesti monipuoliset ja ajantasaiset työkalut tietojen suojaamiseen ja tietosuojariskien pienentämiseen. Pilvipalveluissa vastuu näiden ominaisuuksien hyödyntämisestä oikealla tavalla on asiakkaalla itsellään. Sen takia pilvipalvelun riskejä arvioitaessa on tarkasteltava kokonaisuutta, johon sisältyvät sekä pilvipalvelutoimittajan että asiakkaan vastuulla olevat toimenpiteet.

Keskeisiä erottavia tekijöitä pilvipalveluiden ja On-Premise palveluiden välillä ovat riskit, jotka liittyvät tietojen siirtoon kolmansiin maihin sekä lainsäädäntöön, mikäli pilvipalvelutoimittaja sijainnin tai omistuksen osalta sijaitsee EU/ETA-alueen ulkopuolella.

Riskien arvioinnin käytännön toteuttamisen kannalta keskeistä on riittävä läpinäkyvyys toimittajan teknologisiin ratkaisuihin ja prosesseihin sekä niiden vaatimustenmukaisuutta osoittaviin sertifikaatteihin. EU:n tietosuoja-asetuksen perusteella rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi.

3.2 Luottamuksellisuus

Luottamuksellisuus tarkoittaa sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä eikä se paljastu muille. Pilvipalveluiden tärkeimmät luottamuksellisuuteen liittyvät riskit on lueteltu seuraavassa kohdissa.

Lainsäädäntöjohdannainen riski

EU:n ulkopuolinen lainsäädäntö voi edellyttää asiakkaan vastuulla olevien henkilötietojen luovuttamista sellaisen maan viranomaisille, jotka eivät noudata EU:n tietosuoja-asetuksen asettamia vaatimuksia.

Toimittajat tekevät tyypillisesti erilaisia toimenpiteitä tietopyyntöjen vastustamiseksi, mutta niillä ei ole kattavia mahdollisuuksia vastustaa kaikkia tietopyyntöjä, vaikka ne olisivat EU:n tietosuojalainsäädännön vastaisia.

Toimittajilta saatujen tietojen mukaan viranomaisten tietoihin ei käytännössä kohdistu tällaisia EU:n lainsäädännön vastaisia tietopyyntöjä pilvipalvelualustoilla. Näiden tietojen luotettavuutta ei ole kuitenkaan mahdollista todentaa johtuen mm. tietopyynnöistä, joista ei saa kertoa eteenpäin.

Teknisesti riski on poissuljettavissa asiakastietojen kattavalla ja riittävän vahvalla salauksella sekä asiakkaan erillisellä pilvipalvelun ulkopuolella toteutetulla avaintenhallinnalla. Nämä toimenpiteet ovat kuitenkin varsin raskaita, joten niiden käyttöönotto edellyttää huolellista etujen ja haittojen punnitsemista.

Tietojen siirto 3. maahan

Pilvipalvelua käytettäessä henkilötietoja saatetaan siirtää EU/ETA-alueen ulkopuolelle tavalla, joka ei täytä EU:n tietosuoja-asetuksen V-luvussa asetettuja vaatimuksia.

Tiedonsiirtoihin liittyvien riskien hallitsemiseksi rekisterinpitäjän on selvitettävä kaikki pilvipalvelussa tapahtuvat tietojen siirrot kolmansiin maihin sekä yksilöitävä niissä käytettävät EU:n yleisen tietosuoja-asetuksen V-luvun mukaiset tiedonsiirtovälineet.

Jos tiedonsiirto perustuu EU:n yleisen tietosuoja-asetuksen 45 artiklan mukaiseen komission riittävyyspäätökseen, ei tarvita lisätoimenpiteitä. Riittävyyspäätöksen pysyvyydestä ei kuitenkaan ole täyttä varmuutta, mikä tulee ottaa huomioon päätöstä tehtäessä ja varautumisessa.

Tällä hetkellä (1Q/2024) henkilötietoja voidaan siirtää riittävyyspäätöksen nojalla sertifioituneille yhdysvaltalaisille yrityksille, jotka ovat sitoutuneet EU:n ja Yhdysvaltojen välisessä tietosuojakehyksessä sovittuihin suojatoimiin. Riittävyyspäätöstä ei voi käyttää tiedonsiirtoihin julkisen sektorin toimijoiden välillä Yhdysvaltoihin.

Mikäli riittävyyspäätöstä ei ole, tulee arvioida tiedonsiirtovälineen tehokkuutta sekä määritellä lisätoimenpiteitä tiedonsiirtojen turvallisuuden varmistamiseksi. Lisätietoja täydentävistä toimenpiteistä ja niiden riittävyyden arvioinnista löytyy Euroopan tietosuojaneuvoston suosituksesta 1/2020 sekä sen liitteestä II.

Lisätietoja:

Data Privacy Framework List | Data Privacy Framework Progran
https://www.dataprivacyframework.gov/list

Siirto tietosuojan riittävyyttä koskevan päätöksen perusteella | Tietosuojavaltuutetun toimisto
https://tietosuoja.fi/siirto-tietosuojan-riittavyytta-koskevan-paatoksen-perusteella

Tietomurto

Tietomurrossa ulkopuolinen taho saa tietoonsa asiakkaan pilvipalvelussa säilyttämiä tai käsittelemiä tietoja. Riski voi olla seurausta esimerkiksi pilvipalvelutoimittajan tarjoamien suojauskeinojen pettämisestä tai asiakkaan virheellisestä suojauskeinojen käytöstä.

Riskin todennäköisyyden arviointi pilvipalveluissa sisältää sekä eroja ja yhtäläisyyksiä suhteessa On-Premise ympäristöihin. Jälkimmäisissä asiakkaan tiedot ovat tyypillisesti jossain tarkkaan määritetyssä sijainnissa, jolloin korostuvat verkon rakenteelliseen turvallisuuteen, ympäristöjen suojattuun yhteen liittämiseen sekä konesalin fyysiseen turvallisuuteen liittyvät suojakeinot. Pilvipalvelussa tulee lisäksi tarkastella keinoja, joiden avulla eri asiakkaiden tiedot on erotettu toisistaan sekä menettelyitä, joiden avulla pääsyä kunkin asiakkaan asiakaskohtaisiin tietoihin hallitaan.

Yleisellä tasolla voidaan arvioida, että pilvipalvelut tarjoavat tehokkaita ja monipuolisia suojauskeinoja pilvipalveluissa säilytettävien ja käsiteltävien tietojen suojaamiseksi eri turvallisuuden tasoilla. Nämä keinot liittyvät esimerkiksi salaukseen, avainten hallintaan, verkkohyökkäysten torjuntaan ja palvelun monitorointiin. Toisaalta asiakkaan on vaikea saada täyttä varmuutta palvelun turvallisuudesta, koska turvallisuus on osin toimittajan vastuulla. Siten erityisesti tietosuojan kannalta kriittisemmissä

pilvipalvelutoteutuksissa tulee arvioida yksityiskohtaisesti käyttöön otettavat tekniset suojaukset sekä niiden muodostama kokonaisuus.

Toimittajan EU:n yleisen tietosuoja-asetuksen vastainen asiakkaan henkilötietojen käyttö

Toimittaja käyttää asiakkaan pilvipalvelussa käsittelemiä tai säilyttämiä henkilötietoja tavalla, joka ei ole välttämätöntä asiakkaan tilaaman palvelun tuottamiseksi.

Teknisten vuoropuheluiden yhteydessä toimittajat ovat hyvin selkeästi vakuuttaneet, että he eivät käsittele asiakkaiden pilvipalveluun tallentamia henkilötietoja muuhun kuin asiakkaan tilaaman palvelun tuottamiseen.

Teknisiä ja organisatorisia keinoja riskin pienentämiseksi ovat erilaiset salaukseen ja avaintenhallintaan liittyvät ratkaisut sekä toimittajan dokumentoimat prosessit siitä, miten, millä edellytyksillä ja missä tilanteissa he voivat käsitellä asiakkaiden palveluun tallentamia henkilötietoja.

Teknisesti on hyvin vaikea saada täyttä varmuutta siitä, että toimittajat eivät käsittele asiakkaan henkilötietoja tietosuoja-asetuksen vastaisesti. Siten riskin pienentäminen tulee ottaa riittävässä laajuudessa huomioon myös sopimuksissa.

Toimittajan EU:n yleisen tietosuoja-asetuksen vastainen palveludatan käyttö

Toimittaja käyttää pilvipalvelun käytön yhteydessä syntyviä henkilötietoja tavalla, joka ei ole välttämätöntä asiakkaan hankkiman palvelun tuottamiseksi. Palvelun käyttöön liittyvä tieto on henkilötietoa, joka väärin käytettynä voi muodostaa riskin rekisteröidylle. Pilvipalvelutoimittajat määrittelevät tyypillisesti itsensä rekisterinpitäjiksi näiden tietojen osalta, mikä heikentää asiakkaan mahdollisuuksia vaikuttaa palveludatan käsittelyyn.

Sopimuksellisten keinojen lisäksi on syytä selvittää mitä eri henkilötietoja palvelun käytön yhteydessä palvelun käyttäjästä kerätään, miten toimittaja on rajannut näiden tietojen käytön sekä mitä teknisiä suojakeinoja toimittaja on toteuttanut näihin tietoihin sisältyvien henkilötietojen suojaamiseksi. Esimerkkejä tällaisista keinoista voivat olla palveludatan pseudonymisointi tai anonymisointi. Vain jälkimmäisessä tavassa yksittäinen henkilö ei enää ole tunnistettavissa.

Lisätietoja:

Pseudonymisoidut ja anonymisoidut tiedot | Tietosuojavaltuutetun toimisto
https://tietosuoja.fi/pseudonymisointi-anonymisointi

Toimittajan henkilöstön pääsy tietoihin

Toimittajan henkilö pääsee asiakkaan pilvipalveluun tallentamiin henkilötietoihin liian laajojen pääsyoikeuksien johdosta tai ilman, että tietoihin pääsystä on sovittu asiakkaan kanssa. Tässä yhteydessä riskillä tarkoitetaan sellaista toimittajan henkilön pääsyä tietoihin, joka on vastoin toimittajan menettelyitä, eli yksittäisten toimittajan henkilöiden toiminnasta johtuvia riskejä.

Riskin pienentämiseksi pilvipalvelutoimittajat tarjoavat erilaisia keinoja kuten toimittajan sisäisiä tai asiakkaan kanssa tehtäviä luvitusprosesseja, teknisiä kontrolleja toimittajan henkilöstön luvattoman pääsyn estämiseksi, salauskeinoja sekä tietojen käytön valvontaan liittyviä keinoja. Riskin suuruuteen vaikuttaa myös se, missä laajuudessa yksittäinen toimittajan henkilö pääsee tietoihin niissä tilanteissa, kun lupa pääsyyn on myönnetty sekä miten asiakas voi kontrolloida näitä luvallisia pääsyjä.

Palvelun käytön päättäminen

Pilvipalvelun käytön päättämiseen sisältyy luottamuksellisuusriski. Arvioitavaksi tulee miten voidaan varmistaa, että toimittaja todella poistaa palveluun tallennetut tiedot. Palvelukuvaustensa perusteella nämä kertovat tietojen poistuvan lopullisesti jokin säilytysajan jälkeen (esim. 90 tai 180 päivää), mutta asiakas ei voi tästä itse varmistua. Tämä riski on mahdollista varmuudella hallita vain palveluun tallennettujen tietojen vahvalla salauksella ja asiakkaan itse hallitsemilla salausavaimilla.

3.3 Eheys

Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa. Pilvipalveluiden tärkeimmät eheyteen liittyvät riskit on lueteltu seuraavassa kohdissa.

Tietomurto

Ulkopuolinen taho muuttaa oikeudettomasti asiakkaan vastuulla olevia henkilötietoja tietomurron seurauksena. Esimerkiksi jokin ulkopuolinen taho on kyennyt ohittamaan pilvipalvelun tarjoamat tietoturvallisuuskontrollit ja muuttaa sen jälkeen henkilötietoja.

Riski liittyy luottamuksellisuuden yhteydessä esiteltyyn tietomurto-riskiin, mutta voi poiketa siitä sekä riskin todennäköisyyden että vaikutusten suhteen. Prosessit ja kontrollit, jotka mahdollistavat asiakkaan vastuulla olevien henkilötietojen muuttamisen tai poistamisen voivat olla erillisiä suhteessa tietojen katselun mahdollistaviin kontrolleihin. Lisäksi tietojen eheyteen vaikuttavat muutokset voivat aiheuttaa korkeamman riskin rekisteröidyille ja organisaatiolle kuin pelkkä tietojen luottamuksellisuuden vaarantuminen.

Tietojen eheyteen liittyvä tietomurron riski liittyy usein tietojen ylläpitosovellusten toteutukseen. Siten riskiä tarkasteltaessa tulee pilvialustan lisäksi kiinnittää huomiota myös pilvipalvelun päälle rakennetun tietoja käsittelevän sovelluksen toteutukseen.

Vahingossa tapahtuva virheellinen tietojen muuttaminen

Muutosoikeuden omaava henkilö tai palvelu muuttaa pilvipalvelussa olevia henkilötietoja virheellisesti.

Riski on samankaltainen riippumatta siitä, onko palvelu toteutettu pilvi- vai on-premise-palveluna. Riskin pienentämiseksi on mahdollista toteuttaa erilaisia tietojen oikeellisuuteen liittyviä teknisiä tarkastuksia ja prosesseja.

3.4 Saatavuus

Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Pilvipalveluiden tärkeimmät saatavuuteen liittyvät riskit on lueteltu seuraavissa kohdissa.

Tietoliikennehäiriö

Häiriö tietoliikenneyhteyksissä, joka estää täi häiritsee pääsyä pilvipalveluihin. Mikäli palvelu on suunniteltu tiettyjä yhteyspisteitä hyödyntäviksi, ne voivat muodostaa kriittisiä riippuvuuksia, jolloin palvelu ei ongelmatilanteessa ole käytettävissä.

Pilvipalvelussa olevien tietojen hyödyntäminen edellyttää toimivaa tietoliikenneyhteyttä pilvipalvelun konesalin ja käyttöpaikan välillä. Koska pilvipalvelun konesalit ovat tyypillisesti fyysisesti eri paikassa kuin tietojen käyttäjät, aiheuttaa tietoliikenne riskin pilvipalvelun käytölle. Tosin sama riski on olemassa usein myös on-premise palveluissa, mikäli tietojen käyttö ja konesalit eivät sijaitse samassa fyysisessä rakennuksessa.

Toisaalta pilvipalvelut tarjoavat monipuolisia keinoja hajauttaa tietoja useisiin eri konesaleihin sekä korkean saatavuuden tietoliikenneyhteyksiä konesalien ja tietojen käyttöpaikkojen välillä. Siten pilvipalveluiden hyödyntäminen voi myös vähentää tietojärjestelmän häiriöherkkyyttä erilaisten tietoliikennehäiriöiden suhteen.

Tietoliikennehäiriöiden riskien arvioimiseksi tulee tarkastella asiakkaan käyttöpaikkojen, pilvipalvelusta käyttöön otettavien konesalien sekä niiden välisten tietoliikenneyhteyksien muodostamaa kokonaisuutta asetettujen saatavuusvaatimuksien näkökulmasta.

Konesalin laajempi vaurioituminen

Vakavampi tapahtuma konesalin infrastruktuurissa, joka estää pääsyn konesaliin sijoitettuihin pilvipalveluihin. Yleisellä tasolla pilvipalveluiden konesaleihin liittyy samoja riskejä kuin on-premise konesaleihin. Pilvipalveluiden skaalaedusta, edistyneestä teknologiasta sekä hajautusmahdollisuuksista johtuen pilvipalvelut tarjoavat kuitenkin on-premise-konesaleja kustannustehokkaampia ratkaisuja konesalivaurioista aiheutuvilta riskeiltä suojautumiseen.

Laitteistovika

Häiriö yksittäisessä laitteessa tai pilvipalvelun infrastruktuuriin liittyvässä komponentissa, joka voi vaikuttaa kyseistä laitetta hyödyntävien pilvipalveluiden saatavuuteen.

Yleisellä tasolla voidaan todeta, että virtualisointiin perustuvat pilvipalvelut tarjoavat hyvät mahdollisuudet laitteistorikoilta suojautumiseen, minkä johdosta laitteistorikkojen seurannaisvaikutusten todennäköisyys on pieni.

Salausavaimen häviäminen

Asiakas kadottaa salausavaimen, minkä seurauksena pääsy tietoihin estyy. Riski liittyy erityisesti sellaiseen avaintenhallinnan ratkaisuun, jossa asiakas hallinnoi itse salausavaimia pilvipalvelun ulkopuolella.

Salausavainten hallinta pilvipalvelun ulkopuolella tuo lisäturvaa suhteessa pilvipalvelutoimittajaan sekä mahdollisiin lainsäädäntöjohdannaisiin riskeihin. Toisaalta salausavainten hallinta on monimutkainen prosessi, johon liittyvät riskit voivat pahimmassa tapauksessa johtaa tietoihin pääsyn estymiseen ilman että pilvipalvelutoimittajalla tai muulla taholla on mitään keinoa tietojen palauttamiseen.

Riski on syytä tunnistaa ja arvioida perusteellisesti niissä tapauksissa, kun harkitaan pilvipalvelun ulkopuolisen salausavainten hallinnan käyttöönottamista. Riskin lisäksi arvioinnissa on syytä tarkastella myös ulkopuolisen avaintenhallinnan aiheuttamaa lisätyötä sekä vaikutuksia palvelun suorituskykyyn.

Palvelun käytön päättäminen

Palvelun käytön päättämiseen sisältyy saatavuusriski. Palvelun käytön aikana tulisikin varmistua, että täydelliset asiakkaan tiedot ovat saatavissa palvelusta yleisesti käytetyssä ja koneellisesti luettavassa muodossa.

3.5 Jatkuvuus

Pilvipalvelun hallitsematon päättyminen

Pilvipalvelu tai sen jokin oleellinen osa päättyy tavalla, joka ei mahdollista palvelun jatkamista joko toisessa pilvipalvelussa tai muulla tavalla.

Esimerkiksi tilanne, jossa uutta vastaavaa palvelua ei kyetä ottamaan käyttöön riittävän nopeasti. Riski voi realisoitua erilaisista syistä johtuen, kuten esimerkiksi pilvipalveluun sovellettavan lainsäädännön muutoksista, komission riittävyyspäätösten muutoksista tai sellaisista muutoksista toimittajan käyttämissä alihankkijoissa, joita asiakas ei voi hyväksyä. Riski on luonteeltaan laaja-alainen ja se voi kohdistua sekä asiakkaan organisaatioon että suureen joukkoon rekisteröityjä, joiden palveluiden saatavuuteen riski voi vaikuttaa.

Rekisterinpitäjän tulee arvioida palvelun kriittisyys rekisteröidyn näkökulmasta sekä varmistaa tarvittaessa joko palvelun nopea siirrettävyys vaihtoehtoiseen pilvipalveluun tai palvelun tarjoaminen muulla tavalla. Palvelun siirrettävyys vaihtoehtoiseen pilvipalveluun tulee ottaa huomioon erityisesti käytettäessä pilvialustan tarjoamia uudenlaisia teknisiä kyvykkyyksiä, jotka eivät ole vakio-ominaisuuksia kaikissa pilvipalveluissa.

Lisäksi riskin hallitsemiseksi on suositeltavaa arvioida pilvipalvelutoimittajan luotettavuutta jatkuvuuden näkökulmasta sekä varmistaa sopimuksellisin keinoin, että palvelu ei pääty hallitsemattomasti.

Tietojen siirto toiselle toimittajalle ei onnistu

Pilvipalvelusta ei ole mahdollista saada ulos asiakkaan tietoja tavalla, joka mahdollistaisi niiden siirtämisen uuteen palveluun. Riski liittyy lähinnä SaaS-palveluihin. Riskin käsittelemiseksi rekisterinpitäjän tulee varmistaa, että palvelu tukee tietojen saantia pilvipalvelusta yleisesti käytetyssä ja koneellisesti luettavassa muodossa.

Laaja kansainvälinen kriisi

Kriisin seurauksena pilvipalvelun käyttö estyy ilman, että siihen voidaan vaikuttaa kansallisin toimenpitein. Riski voi liittyä esimerkiksi tilanteeseen, jossa kansainväliset tietoliikenneyhteydet eivät ole käytössä tai pilvipalvelua ei voida hyödyntää muusta laajemmasta toimintaympäristön häiriöstä johtuen.

Riski on epätodennäköinen, mutta ei täysin poissuljettu. Rekisterinpitäjän tulee arvioida riskin suuruus etenkin saatavuuden ja jatkuvuuden näkökulmasta kriittisten palveluiden osalta sekä varmistaa, että tällaiset palvelut ovat saatavilla myös laajempien häiriötilanteiden aikana.

Pilvipalvelut tarjoavat erilaisia vaihtoehtoja tietojen hajauttamiseen useisiin fyysisiin sijainteihin, minkä johdosta pilvipalvelut voivat tarjota myös perinteisiä on-premise palveluita kriisisietoisempia vaihtoehtoja tietojen saatavuuden varmistamiseksi laajan kriisin yhteydessä.

Muu palveluiden käytön estävä tilanne

Pilvipalveluihin voi liittyä myös muita yleisisiä ICT-jatkuvuusriskejä. Jokin yllättävä häiriö itse palvelualustassa, asiakkaan ympäristön muissa riippuvuuksissa (esim. integraatiot tai palvelukumppanit) saattaa johtaa jatkuvuushäiriöön. Vakavin esimerkki on johonkin tähän kokonaisuuteen kohdistuva lunnastroijalaistapaus (ransomware). Pilvipalvelualustan toimittajilla itsellään on hyvä kyvykkyys hallita tätä riskiä, joten se kohdistuu todennäköisimmin asiakkaan omalla vastuulla oleviin osa-alueisiin.

3.6 Pilvipalveluiden edut ja mahdollisuudet

Pilvipalveluiden käyttöön liittyvien riskien lisäksi ne tarjoavat myös sellaisia mahdollisuuksia, joita omissa ympäristöissä ei usein ole mahdollista saavuttaa tai vastaavien ominaisuuksien käyttöönotto tulisi todella kalliiksi. Seuraavissa kohdissa tarkastellaan pilvipalveluiden vahvuuksia.

Joustava kapasiteetti

Kapasiteetin joustavuus mahdollistaa palvelun saatavuuden myös sellaisissa tilanteissa, joissa tarve muuttuu nopeasti. Lisäksi pilvipalvelusta hankittavaa jatkuvaluonteista kapasiteettia ei tarvitse mitoittaa kuormituspiikkien mukaan, jolloin ei tarpeettomasti makseta käyttämättömästä kapasiteetista. Joustavuus on yksi suurimmista pilvipalveluiden tarjoamista edusta suhteessa on-premise ratkaisuihin. Etu korostuu sellaisissa palveluissa, joissa kapasiteetin tarve vaihtelee.

Kapasiteetin edulliset yksikkökustannukset

Edulliset laite ja lisenssikustannukset johtuen monista eri tekijöistä, kuten suurtuotannon eduista, automatisoiduista prosesseista sekä jaetun infrastruktuurin hyödyntämisestä. Kustannushyöty on suurin käytettäessä julkisia pilvipalveluita. Hyöty pienenee käytettäessä erilaisia yksityisen pilven ratkaisuja, koska tällöin menetetään jaetun infrastruktuurin mahdollistama kustannushyöty.

Edistykselliset tietoturvakontrollit

Pilvipalvelut tarjoavat edistykselliset ja monipuoliset tietoturvakontrollit verrattuna esimerkiksi on-premise konesalien tarjoamiin kontrolleihin. Tämä johtuu mm. pilvipalvelutoimittajien mahdollisuuksista resursoida tietoturvallisuuden kehittämiseen.

Mahdollisuus on tavallaan kaksijakoinen. Yhtäältä pilvipalvelut hoitavat monia tietoturvallisuuteen liittyviä asioita automaattisesti. Lisäksi pilvipalvelualustat tarjoavat monipuolisia mahdollisuuksia asiakkaiden käyttöön. Näiden kyvykkyyksien tehokas hyödyntäminen edellyttää kuitenkin riittävää osaamista joko asiakkaalta tai palvelun hallinnan ulkoistamista yhteistyökumppanille.

Teknologian kehittymisestä saatavat hyödyt

Monet uudet teknologiat tulevat nopeammin tarjolle pilvipalveluiden kautta. Tämä tuo uusia mahdollisuuksia asiakkaille. Toisaalta uudet teknologiat tuovat myös uusia riskejä, jotka on otettava huomioon pilvipalveluiden ominaisuuksia käyttöönottaessa.

Palveluiden nopea käyttöönotto

Pilvipalvelut mahdollistavat nopeat käyttöönotot koskien sekä uusia pilvipalveluita, pilvipalvelun kapasiteetin laajennuksia, että ohjelmistopäivityksiä. Nopea käyttöönotto helpottaa asiakkaan toimintaa muutostilanteissa. Lisäksi uusien tietoturvapäivitysten nopea käyttöönotto parantaa osaltaan pilvipalveluiden tietoturvallisuutta.

Lisätietoja:

Vaikutustenarviointi | Tietosuojavaltuutetun toimisto
https://tietosuoja.fi/vaikutustenarviointi

Suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi, Versio 2.0 | European Data Protection Board
https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_fi.pdf

4

Julkipilvialustojen tietoturva-arkkitehtuurit

Mitä erityispiirteitä tarkasteltujen toimittajien julkipilvialustojen tietoturva-arkkitehtuureissa on?

Tässä luvussa kuvataan toimittajien pilvialustojen tietoturva-arkkitehtuurin erityispiirteet. Luvussa ei ole tarkoitus mennä teknisten ratkaisujen yksityiskohtiin, vaan kuvata kunkin toimittajan arkkitehtuurillinen lähestymistapa pilvipalvelun tietoturvallisuuteen.

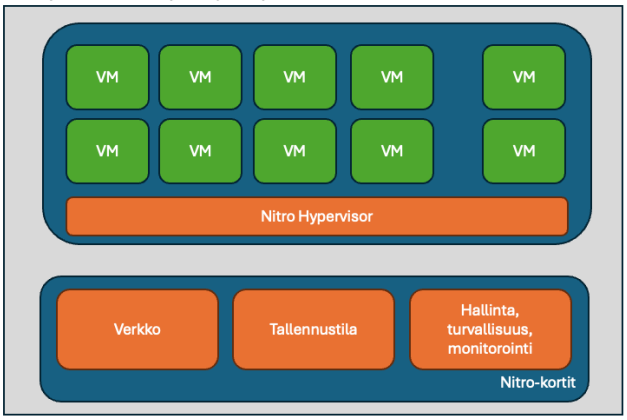
Lukijaa kehotetaankin tutustumaan toimittajien kattavampiin tietoturvakuvauksiin näiden www-sivuilla (kts. linkit tämän luvun lopussa).

4.1 Amazon Web Services (AWS)

Amazon Web Services (AWS) on Yhdysvaltoihin rekisteröidyn Amazon.com, Inc. –yrityksen pilvipalvelualusta. Se on nykyään kokoelma erilaisia pilvipalvelua, jotka tarjoavat työvälineitä verkkopalvelujen rakentamiseen ja pilvipalveluympäristöjen luomiseen.

AWS:n EC2-palvelin koostuu pääemolevystä ja yhdestä tai useammasta Nitro-kortista. Nitro-kortit ovat erityisiä laitteistokomponentteja, jotka mahdollistavat vahvan eristyksen virtuaalikoneiden välillä. Fyysinen eriyttäminen varmistaa, että ulkoisen ympäristön kanssa vuorovaikutuksessa olevat komponentit ovat fyysisesti erillään pääjärjestelmästä, mikä auttaa estämään mahdollisia tietovuotoja ja hyökkäyksiä. Järjestelmän rutiinipäivitykset on suunniteltu siten, että päivitettäessä järjestelmän suojausprotokollia ei tarvitse pudottaa tai lieventää päivitysten vuoksi.

Nitro-järjestelmään integroitu turvallisuussiru valvoo ajon aikana kaikkia toimintoja ja laiteohjelmistoja mahdollistaen turvalliset käynnistysoperaatiot.



Nitro-järjestelmän suunnittelussa on evätty operaattorien pääsy asiakastietoihin. Mikään järjestelmä tai henkilö ei voi kirjautua sisään EC2 Nitro -isäntäpalvelimelle (host) tai käyttää EC2 instanssien muistia. Mikäli AWS-operaattorin on tehtävä huoltotöitä EC2-palvelimelle, heillä on mahdollisuus käyttää vain rajoitettua liittymiä. API-liittymät eivät tarjoa operaattorille pääsyä asiakastietoihin EC2-palvelimella.

AWS-operaattorilla ei ole mahdollista ohittaa kontrolleja tai suojauksia. Korkean suojaustason haittapuolena on, että operaattoreilla ei ole mahdollisuutta jäljittää virheitä tuotantopalvelimilla. Kyseisissä tapauksissa asiakkaan on annettava lupa AWS:n henkilöstölle virheen jäljittämiseen asiakasympäristössä.

Nitro-järjestelmä noudattaa passiivisen viestinnän suunnitteluperiaatetta. Se tarkoittaa, että tuotantotoiminnan aikana järjestelmän komponentit eivät koskaan aloita lähtevää viestintää toiseen palveluun. Sen sijaan järjestelmäverkossa on yksi kovetettu luotettu palvelu, joka kuuntelee verkon tai järjestelmäväylän komentoja ja toimii näiden komentojen perusteella. Viestintäpolkujen molemmat puolet suorittavat parametrien validoinnin, jotta voidaan varmistaa lähetettyjen ja vastaanotettavien parametrien luotettavuus. Koska normaaliin toimintaan kuuluu vain määriteltyjen, parametreilla varmennettujen viestien kuunteleminen ja niihin vastaaminen käyttämällä parametrivalidoituja vastauksia, järjestelmä on suunniteltu tunnistamaan ja varoittamaan mahdollisesta poikkeavasta toiminnasta.

Siitä huolimatta, että Nitro-järjestelmä tarjoaa tiettyjä tietoturvahyötyjä, se ei takaa kokonaisuutena alustapalveluiden tietoturvallisuutta. Palveluiden tietoturvallinen käyttö vaatii huolellista suunnittelua, konfigurointia ja hallintaa kaikilla tasoilla, myös loppukäyttäjäorganisaation vastuulla olevilla alueilla. AWS:n palveluvalikoima sisältää työkaluja ja palveluita, jotka auttavat loppukäyttäjäorganisaatioita parantamaan tietoturvan ja tietosuojan tasoja AWS-infrastruktuurissa, kun ne konfiguroidaan käyttöön parhaiden käytäntöjen ja suositusten mukaisesti. Suositeltavien työkalujen ja palveluiden käyttö ja käyttöönotettava laajuus riippuu käyttötapauksesta.

Lisätietoja:

Nitro-järjestelmä | Amazon Web Services
https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/the-components-of-the-nitro-system.html

4.2 Google Cloud Platform (GCP)

Yhdysvaltalaisen Google LLC:n julkipilvialusta on nimeltään Google Cloud Platform (GCP).

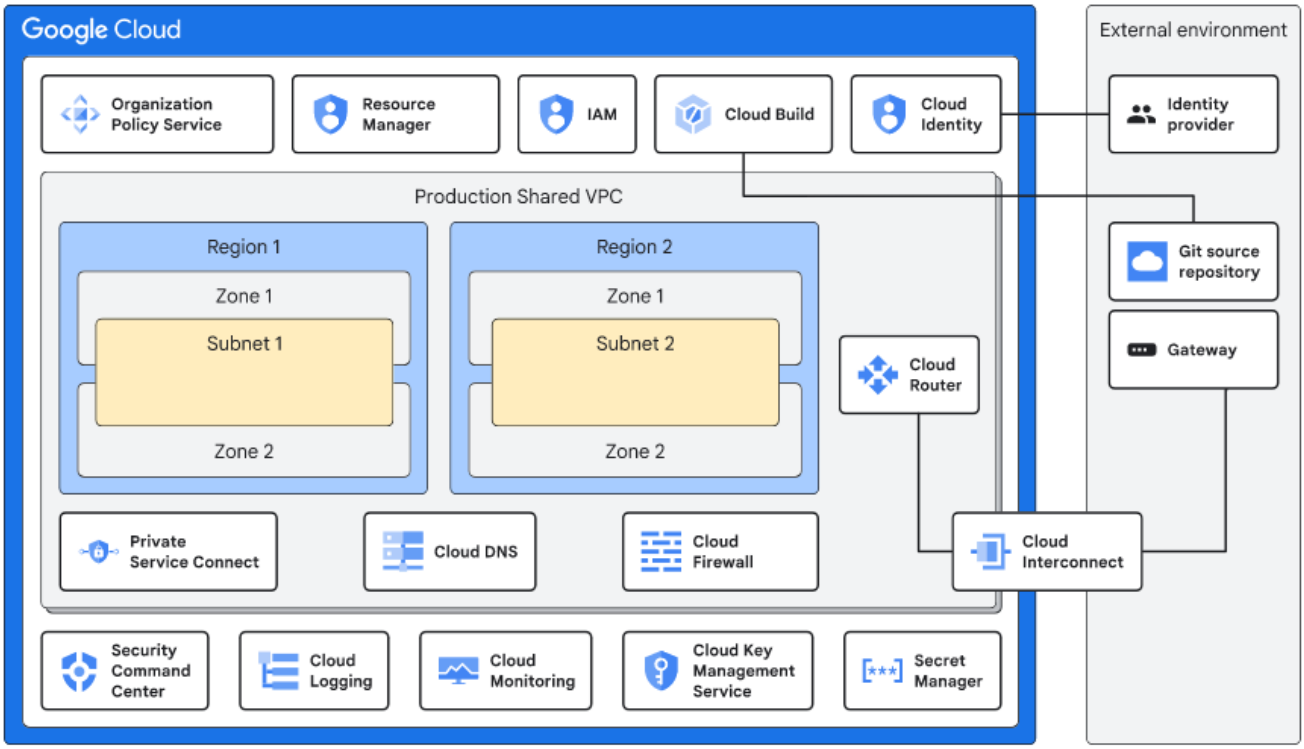
Google Cloud panostaa tietojen suojaamiseen käyttäen Zero Trust- ja pienimmän käyttöoikeuden periaatteisiin perustuvaa arkkitehtuuria. Googlella ei ole oletusarvoisesti pääsyä asiakkaiden tietoihin ja sitä valvotaan tiukasti rajoitettujen pääsyoikeuksien avulla. Asiakkaat voivat hallita salausavaimiaan ja käyttää end-to-end-suojausta varmistaakseen tietojen suojauksen. Google käyttää jatkuvaa seurantaa (24/7) ja analytiikkaa rajoittaakseen valtuutettujen tunnusten väärinkäyttöä, havaitakseen epätavallista työntekijätoimintaa ja reagoimaan automaattisesti uusiin tai kehittyviin uhkiin. Google Cloud:ssa säilytettävää ja hallinnoitavaa asiakasdataa käsitellään asiakkaan ohjeiden mukaisesti, eikä sitä käytetä mainontaan tai muihin tarkoituksiin. Google tarjoaa myös erinäisiä tekniikoita arkaluontoisen tiedon luokitteluun ja suojaamiseen.

Asiakkaiden työkuormat hajautetaan turvallisesti useisiin alueisiin, saatavuusalueisiin, läsnäolopisteisiin ja verkkoyhteyksiin, mikä mahdollistaa sisäänrakennetun vikasietoisuuden ja sovellusten käytettävyyden. Google suorittaa vuosittain koko yritystä koskevia palautustestejä (DiRT) varmistaakseen, että Googlen palvelut ovat käytettävissä ja jatkavat toimintaansa katastrofin aikana. Asiakkaat, jotka haluavat pitää tietonsa tietyssä maantieteellisessä sijainnissa, voivat hyödyntää Google Cloud:n residenssipalveluja.

Google Cloud:n residenssipalvelut mahdollistavat asiakastietojen tallentamisen valitsemissaan maantieteellisissä sijainneissa. Esimerkiksi Euroopan unionissa tietoresidenssipalveluja käyttävät asiakkaat voivat säilyttää asiakastietoja yksinomaan Euroopan alueilla Belgiassa, Saksassa, Suomessa, Puolassa, Ranskassa, Italiassa, Espanjassa ja Alankomaissa. Google Cloud:n asiakkaat voivat käyttää VPC-palvelun hallintatoimintoja rajoittaakseen verkkojen sijainteja, joista heidän käyttäjänsä voivat käyttää tietoja. Palveluperimetrin määritys estää tietojen käyttämisen konfiguraatioasetusten ulkopuolelta.

Google Cloud on toteuttanut erilaisia pääsynhallintatoimenpiteitä, joiden avulla tiedonsaantireitit toimivat tarkoituksenmukaisesti. Palvelut suorittavat valtuutustarkistukset varmistaakseen, että tietoja pyytävällä taholla on asianmukaiset käyttöoikeudet ennen jatkamista. Pyyntöjä arvioidaan koko kontekstin (käyttäjän identiteetti, sijainti, laitteen omistus ja konfiguraatio, sekä hienojakoiset käyttöoikeuspolitiikat) perusteella sen pätevyyden määrittämiseksi. Läpinäkyvyyttä edistetään käyttöhallinnan lokien avulla. Tarkastuslokit tallentavat toimet, joita asiakasorganisaation henkilöt ovat suorittaneet Google Cloud -resursseissa. Access Transparency -lokit taas tarjoavat läpinäkyvyyden niihin toimiin, joita Google-henkilökunta on suorittanut asiakasympäristöissä. Google Cloud mahdollistaa pääsyn hyväksynnän, jonka avulla asiakkaat voivat nimenomaisesti hyväksyä pääsyn asiakastietoihin tai -kokoonpanoihin Google Cloud:ssa. Työntekijän pääsyoikeuksien virheellisen määrittelyn tai hyökkääjien hyödyntäessä vaarantuneita tilejä, VPC-palvelun hallintatoiminnot mahdollistavat erilaisten suojausrajojen määrityksen tietojen vuotamisen estämiseksi.

Tietoturva- ja yksityisyysvalvontatoimien ollessa käytössä Google tarjoaa keskitetyn paikan, jossa asiakasorganisaatio voi estää, havaita ja reagoida uhkiin. Security Command Center (SCC) antaa asiakkaille keskitetyn näkyvyyden pilvivarantoihinsa. Se sisältää myös sisäänrakennetun tietoturva-analytiikan kokonaisturvallisuustilanteen arvioimiseksi.



Kuvan lähde: Google

Lisätietoja:

Trusting your data with Google Cloud | Google
https://services.google.com/fh/files/misc/072022_google_cloud_trust_whitepaper.pdf

Google security overview | Google
https://cloud.google.com/docs/security/overview/whitepaper

Enterprise foundations blueprint | Google
https://cloud.google.com/architecture/security-foundations

Take charge of your data: using Cloud DLP to de-identify and obfuscate sensitive information | Google
https://cloud.google.com/blog/products/identity-security/taking-charge-of-your-data-using-cloud-dlp-to-de-identify-and-obfuscate-sensitive-information

4.3 Microsoft Azure (Azure)

Microsoft Azure on yhdysvaltalaisen Microsoft Corporationin julkipilvipalvelu.

Azuren turvallisuusarkkitehtuuri pohjautuu pitkälti laajaan tarjoamaan erilaisia yksittäisiä palveluita, jotka nivoutuvat yhteen käyttötapauksesta riippuen.

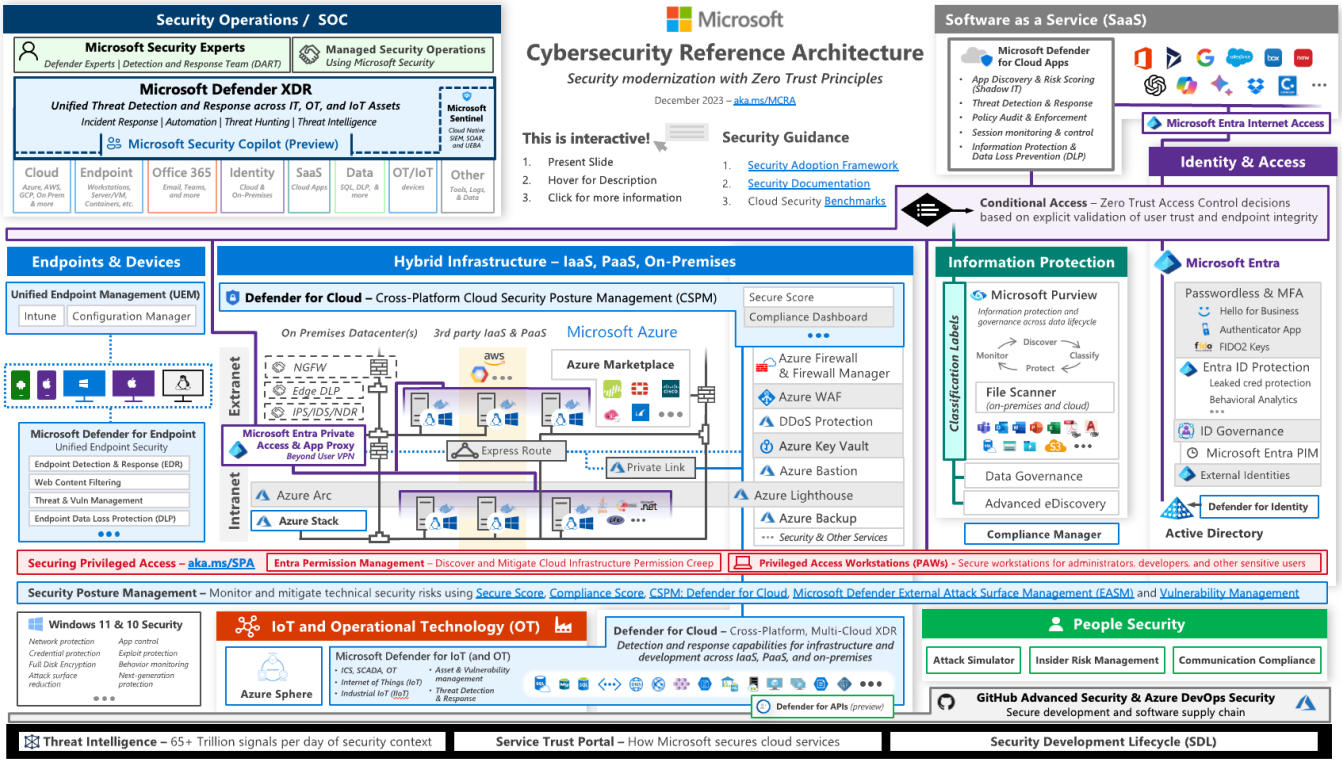
Yksittäisistä tietoturvapalveluista esimerkkeinä ovat Purview sekä Defender-tuoteperhe. Ensin mainittu tarjoaa työkaluja tietojen suojauksen hallintaan, ympäristön tietoturvaan sekä riski- ja vaatimustenmukaisuus-ratkaisuihin. Defender taas auttaa poikkeamien havaitsemisessa sekä loki- ja uhkatietojen keräämisessä. Palvelut mahdollistavat monikerroksellisen tietoturvan- ja -suojan rakentamisen, mutta ne vaativat palveluita käyttöönottavalta taholta asiantuntijuutta kokonaisturvallisuusratkaisun rakentamiseen ja konfigurointiin.

Toimintaprosessit, jotka ohjaavat pääsyä asiakastietoihin Azure-pilvipalveluissa, on suojattu vahvoilla kontrolleilla ja todennuksella, jotka jakautuvat kahteen luokkaan: fyysiseen ja loogiseen. Microsoftin henkilöstön virtuaalista pääsyä asiakastietoihin rajoitetaan roolipohjaisella kulunvalvonnalla, monitekijätodennuksella, tuotantotietojen pysyvän käytön minimoimisella ja muilla kontrolleilla. Microsoftin ja sen alihankkijoiden pääsy asiakastietoihin kirjataan lokiin. Sekä Microsoft että kolmannet osapuolet suorittavat säännöllisiä tarkastuksia (ja näytetarkastuksia) varmistaakseen, että pääsy on asianmukainen.

Suurin osa Microsoftin suorittamista korjaustoimenpiteistä, asiakkaan tukitikettien ongelmien selvittämisestä ja vianetsinnästä eivät vaadi pääsyä asiakkaiden omiin ympäristöihin. Asiakkaiden omien tikettien yhteydessä Microsoft ei siirrä tai kopioi fyysisesti asiakasdataa pois asiakkaan määrittelemästä ympäristöstä. Niissä tapauksissa, joissa tällaista käyttöoikeutta vaaditaan, Customer Lockbox tarjoaa asiakkaille käyttöliittymän, jolla nämä voivat tarkastella ja hyväksyä tai hylätä tietojen käyttöpyyntöjä. Sitä käytetään tapauksissa, joissa Microsoftin insinöörin on päästävä käsiksi asiakastietoihin. Syynä voi silloin olla asiakkaan tekemä tukipyyntö tai Microsoftin havaitsema ongelma.

Microsoftin rakentama automaatio tarkkailee palvelulokeja tietoturvapoikkeamien varalta, ilmoittaa ongelmat tutkintaa varten sekä suorittaa joissakin tapauksissa automaattisia toimia (esim. palvelunestohyökkäykset Azurea vastaan). Poikkeamienhallinnan ilmoitusprosessit ovat riippumattoman kolmannen osapuolen suorittaman pilvipalveluiden vuotuisen auditoinnin piirissä ja niillä varmistetaan, että oikeat toiminnalliset ja tekniset prosessit ovat käytössä. Jokainen palveluelementti käy läpi tietosuojatarkastuksen suunnittelun aikana ja sen jälkeen uudelleen, jos palveluun tai palvelussa käsiteltäviin tietoihin tulee muutoksia. Microsoft dokumentoi palvelunsa, jotta asiakas tietää, miten niitä käytetään ja mitä tietoja haluttuun palveluiden toimintaan tarvitaan.

Pääasiallisia Azure-sovellusten työkuormien suojaamisen toimenpiteitä ovat todennus ja salaus itse sovelluksissa. Suojauskerroksia voi lisätä myös sovellusten käyttämiin virtuaaliverkkoihin. Julkisen sektorin asiakkaiden luotettavuus- ja saatavuusvaatimuksiin Azure tarjoaa kyvykkyyksiä mm. vikojen ennakointiin, automaatioita, palvelinkeskusten varajärjestelmiä sekä palvelinkeskusten saatavuusalueiden ryhmittelymahdollisuuksia. Loppukäyttäjäorganisaatiot voivat määrittää palvelut replikoimaan tietoja muihin alueisiin ja lieventää näin alueellisten häiriöiden vaikutuksia.



Kuvan lähde: Microsoft

Lisätietoja:

Safeguard individual privacy with cloud services from Microsoft | Microsoft https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview

Access your data on your terms | Microsoft https://www.microsoft.com/en-us/trust-center/privacy/data-access

Security architecture design | Microsoft https://learn.microsoft.com/en-us/azure/architecture/guide/security/security-start-here

Security considerations for highly sensitive IaaS apps in Azure | Microsoft https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/high-security-iaas

Security tradeoffs | Microsoft https://learn.microsoft.com/en-us/azure/well-architected/security/tradeoffs

Microsoft Cybersecurity Reference Architectures | Microsoft https://learn.microsoft.com/en-us/security/adoption/mcra

4.4 Oracle Cloud Infrastructure (OCI)

Oracle Corporation on yhdysvaltalainen tietotekniikkayhtiö, joka tarjoaa nykyään yritysohjelmistojen ja laitteistojen lisäksi myös pilvipalveluita.

Oraclen suvereenin pilven tietoturva-arkkitehtuuri perustuu vahvaan fyysiseen ja loogiseen erotteluun muista pilvistä tai pilvialueista. Suvereenilla pilvellä on Euroopassa omat palvelinkeskuksensa ja sitä ylläpitää EU-asukkaista koostuva henkilökunta. Lisäksi palvelua ylläpidetään ja hallinnoidaan sitä varten perustettujen EU-perusteisten oikeushenkilöiden avulla.

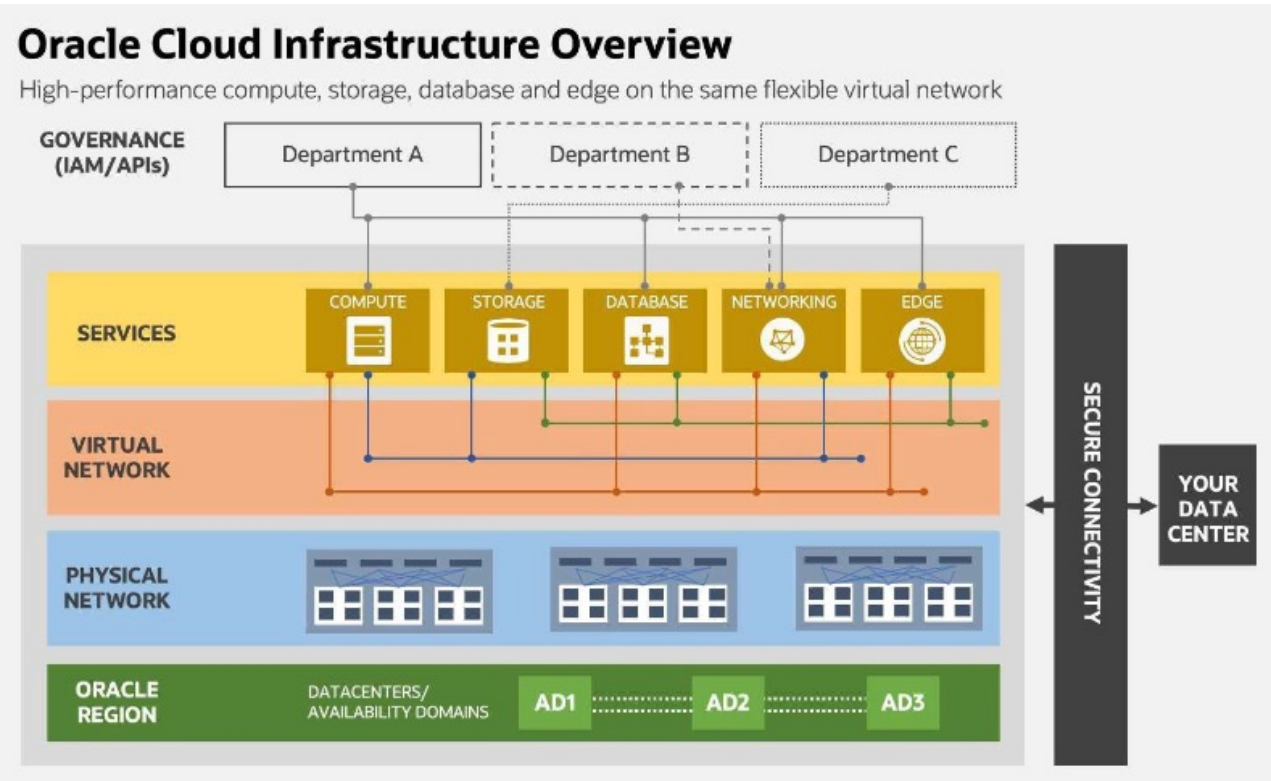
Suvereenin pilvi sisältää kaikki samat palvelut kuin Oraclen julkinen pilvi, mutta se on erotettu fyysisen sijainnin,

palvelinkeskusten, henkilökunnan ja laitteiston tasolla. Suvereenista pilvestä ei ole yhteyttä muihin pilviin, joten asiakkaan on huomioitava suunnittelussaan mahdolliset rajoitteet mm. multipilvi-ratkaisujen osalta. Oraclen suvereenin pilven palvelukeskukset sijaitsevat Saksassa ja Espanjassa.

Eristetty ratkaisu mahdollistaa tuki- ja ylläpidosta vastaavan henkilöstön rajoittamisen EU:n asukkaisiin, joilla on fyysinen ja looginen pääsy vain suvereenin pilven alueeseen (realm). Jokaisella alueella (realm) on erilliset tilat (tenancy) ja pääsynhallinnan säännöt, jotka mahdollistavat EU:n suvereenin pilven erillisen hallinnoinnin ja tukitiimin käytön. Pääsynhallinnan (IAM) verkkotunnuksia ei kopioida suvereenin pilven ulkopuolelle, eikä Oracle voi kirjautua sisään asiakkaan OCI IAM -verkkotunnukseen.

Suvereeni pilvi mahdollistaa monia tietoturvakontrolleja. Autentikointilokit lähetetään SIEM-työkaluun, jossa ne säilytetään vähintään 90 päivää. Pääsy lokivarantoon on rajoitettu hyväksytyille henkilöille. Lisäksi Oracle pilvi-infrastruktuuri käyttää järjestelmä- ja verkon tunkeutumisen havainnointi-järjestelmiä (HIDS, NIDS), virustorjuntaa ja tiedostojen eheyden valvontaa (FIM) pyrkiessään seuraamaan ja havaitsemaan tietoturvauhkia.

Kaikki Oracle-tietokannat on salattu yksittäisellä salausavaimella, jota asiakas hallinnoi (Bring your own key) tai vaihtoehtoisesti Oracle hallinnoi avaimia. Kummassakin tapauksessa maskausavain (masker key) on tallennettu laitteiston suojausmoduuliin (HSM).



Kuvan lähde: Oracle

Oracle OCI:n tietoturva-arkkitehtuuri noudattaa Zero Trust ja Always-on-security -malleja. Konesaliympäristön verkot on segmentoitu mm. virtualisointialustan sekä asiakkaiden tenantien osalta.

Lisätietoja:

Kryptograafiset ratkaisut | Oracle Sovereign Cloud
https://blogs.oracle.com/cloud-infrastructure/post/oracle-sovereign-cloud-solutions-data-encryption

Pääsynhallinta | Oracle Sovereign Cloud
https://blogs.oracle.com/cloud-infrastructure/post/oracle-sovereign-cloud-control-data-access-mgmt

Tietoturva-arkkitehtuuri | Oracle Cloud IaaS
https://blogs.oracle.com/cloud-infrastructure/post/oracle-sovereign-cloud-control-data-access-mgmt

Toimittajien yleisiä tietoturvakuvauksia:

AWS Security Documentation | AWS
https://docs.aws.amazon.com/security/

Protect your organization with Google Cloud security solutions | Google
https://cloud.google.com/solutions/security

Strengthen your security posture with Azure | Microsoft
https://azure.microsoft.com/en-us/explore/security

Oracle Security, Identity, and Compliance | Oracle
https://www.oracle.com/security/

5

Keskeiset tekniset ratkaisut ja prosessit

Miten erilaisilla teknisillä ratkaisuilla sekä toimintatavoilla voidaan hallita tietosuojariskejä julkipilvipalveluissa?

Tässä luvussa analysoidaan keskeiset pilvipalvelun tietoturvallisuuteen vaikuttavat tekniset ratkaisut ja prosessit.

Analyyseissa tarkastellaan ratkaisun toimintaa, sen vaikutusta tietoturva- ja tietosuojauhkiin, jäännösriskejä ja muita seikkoja, joihin tulee kiinnittää huomiota. Analysoitava tekninen ratkaisu käsitellään ensin toimittajariippumattomasti, jonka jälkeen kuvataan toimittajakohtaiset erityispiirteet.

5.1 Tietojen salaus

Tiedon salauksella varmistetaan, että tieto on luettavissa ja käytettävissä vain sovituille henkilöille. Tiedon salaus toteutetaan käyttäen salausteknisiä menetelmiä, joissa ”työkaluna” toimii salausavain. Avaimen avulla tietoa voidaan salata ja salaus voidaan purkaa. Natiivit pilvipalvelut tarjoavat hyvät edellytykset tiedon suojaamiselle.

Kaikki palveluntarjoajat kuitenkin perustavat toimintansa ja turvallisen arkkitehtuurin jaetun vastuun mallille (Shared Responsibility Model). Se tarkoittaa, että pilvipalvelun infrastruktuurin turvallisuus on palveluntarjoajan vastuulla, mutta asiakas on vastuussa pilvipalvelun sisällä olevan tiedon suojaamisesta.

Lisätietoja:

Shared Responsibility Model | AWS
https://aws.amazon.com/compliance/shared-responsibility-model/

Shared Responsibility in the Cloud | Azure
https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Demystifying the Cloud Shared Responsibility Security Model | Oracle
https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf

Shared responsibilities and shared fate on Google Cloud | GCP
https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

Tiedon salaus jaetaan kahteen kokonaisuuteen:

- Data-in-transit viittaa liikkeessä olevaan tietoon.
- Data-at-rest viittaa digitaalisessa muodossa fyysiselle koneelle tallennettuun tietoon.

Data-in-transit salaus toteutetaan yleensä TLS-protokollan avulla. Suojaus puretaan yleensä kuormantasaajassa, minkä jälkeen asiakkaan oman virtuaaliverkon sisällä olevaa tietoa ei ole salattu (poikkeuksena GCP). Myöskään konesalien sisällä olevaa liikennettä ei ole salattu verkkotasolla. Virtuaaliverkon sisällä liikenteen salaamiseen voidaan käyttää TLS-protokollaa ja/tai service mesh -teknologiaa.

Data-at-rest salaus on yleensä toteutettu valmiiksi pilvipalveluntarjoajan omissa palveluissa (esim. tietokanta). Käytössä on ns. envelope encryption -menetelmä. Envelope encryption, eli kirjekuorisalaus, on menetelmä, jossa tieto salataan ensin yhdellä avaimella (Data key, DEK), minkä jälkeen avain salataan vielä toisella avaimella (KMS Key, KEK).

Toimittajakohtaiset täsmennykset

Google Cloud:

Google Cloud tarjoaa oman ALTS-protokollan (Application Layer Transport Security) sovellustason data-in-transit salaukselle. Se tarjoaa myös vakiona kirjekuorisalausta data-at-rest suojaukseen. Muista palveluntarjoajista poiketen, jotkut Googlen palveluista käyttävät AES-128-algoritmia. Muutoin käytössä on alan standardina pidetty AES-256.

Lisätietoja:
Encryption in Transit | GCP
https://aws.amazon.com/compliance/shared-responsibility-model/

Ratkaisun analyysi

Keskeinen tekijä tietojen salauksessa on luottamus palveluntarjoajan organisatorisiin ja teknisiin keinoihin rajoittaa ja estää omien työntekijöiden pääsy sisältödataan. Riski perustuu siihen, ettei palveluntarjoaja noudattaisi omia käytäntöjään ja siten palveluntarjoajan sisäiseen uhkatekijään. Näissä tapauksissa riskiarvioinnin kannalta merkityksellisintä ovat palveluntarjoajan sertifikaatit, sillä palveluntarjoajan tietoturvaprosessit ovat harvoin julkisia. Prosesseihin liittyvää dokumentaatiota saattaa olla tarjolla enemmän salassapitosopimuksen kanssa.

Itse tiedon salaukseen löytyy kattavasti dokumentaatiota kaikilta palveluntarjoajilta. Vuonna 2023 käytettävissä olevan tiedon valossa AES-256- ja AES-128-algoritmeja voidaan pitää riittävän turvallisena tähän käyttötarkoitukseen. Algoritmeissa ei ole tiedossa olevia haavoittuvuuksia. Ne kestävät myös väsytyshyökkäyksiä (brute force attack) sekä ovat symmetrisinä algoritmeina immuuneja kvanttiuhalle. Näillä algoritmeilla salattujen avaimien turvallisuuteen ei näin ollen liity riskejä. On kuitenkin otettava huomioon, että tiedon salaaminen on rekisterinpitäjän vastuulla.

5.2 Salausavainten hallinta

Kaikilla pilvipalveluntarjoajilla on omat natiivit salaisuuksienhallinta-järjestelmät (Secret Management Systems). Sen lisäksi järjestelmiä voi toteuttaa myös integroimalla asiakkaan oman salaisuuksienhallintajärjestelmän palveluntarjoajan järjestelmään (esim. Bring Your Own Key, BYOK). Integroinnin voi toteuttaa vaihtelevissa määrin. Yleensä pilvipalveluntarjoajilla on integroinnille muutamia eri keinoja, joissa asiakkaan oman hallinnoinnin määrä vaihtelee. Omien järjestelmien integroiminen on pääsääntöisesti monimutkaisempaa ja siten myös kalliimpaa. Salaisuuksienhallinnan voi toteuttaa myös “hybridinä” siten, että osa pilvipalveluista käyttää natiivia ratkaisua ja osa asiakkaan omaa.

Salausavaimet jaetaan karkeasti palveluntarjoajan hallinnoimiin avaimiin ja asiakkaan hallinnoimiin avaimiin (customer managed keys, CMK). CMK:t ovat asiakkaan itse luomia ja täysin asiakkaan hallinnassa. Palveluntarjoajan hallinnoimat avaimet ovat pilvipalveluiden luomia avaimia tietyn palvelun käyttötarkoitukseen. Asiakkaalla on täysi näkyvyys näihin avaimiin, muttei hallintaoikeuksia niihin. Useat pilvipalvelut mahdollistavat CMK:n käytön palveluntarjoajan hallinnoiman avaimen sijaan.

Salausavaimien hallintaan suositellaan laitteiston suojausmoduulin (Hardware Security Module, HSM) käyttämistä. Pilvipalveluntarjoajilla on HSM-ratkaisut, jotka ovat FIPS 140-2 sertifioituja1.

Pilvipalvelun tarjoajat eivät ota erikseen varmuuskopioita asiakkaiden hallinnoimista avaimista. Asiakkaan mahdollisuus ottaa varmuuskopio omasta avaimestaan vaihtelee. Esimerkiksi AWS ei salli varmuuskopioita natiiveista asiakkaan hallinnoimista avaimista, kun taas Azure sallii.

Pilvipalveluiden tarjoajilla on sekä organisatorisia että teknisiä keinoja estää palveluntarjoajan työntekijöiden pääsy asiakkaan salausavaimiin.

Toimittajakohtaiset täsmennykset

Azure:

Azurella on neljä eri avaintenhallintaratkaisua: Azure Key Vault (AKV) Standard, AKV Premium, Managed HSM ja Dedicated HSM. Azuren mukaan AKV Premium tarjoaa riittävän suojan suurimmalle osalle asiakkaista. Managed HSM:ää käytetään ratkaisuna, jos asiakkaalta edellytetään juridisesti omaa avaintenhallintaa. Managed HSM tukee vain salausavaimia, ei muita salaisuuksia tai sertifikaatteja. Sen lisäksi asiakas itse rakentaa järjestelmän ”turvallisuusmaailman”. AKV:ssa Azure vastaa järjestelmän turvallisuudesta ja näkee järjestelmän turvallisuuskonfiguraatiot, muttei järjestelmän sisältöä.

AWS:

AWS:n avaintenhallintajärjestelmä on nimeltään AWS Key Management Service (KMS). KMS on vain yksi versio, mutta se voidaan konfiguroida vastaamaan erilaisia käyttötarkoituksia. Palvelua voidaan käyttää täysin pilvinatiivisti sellaisenaan tai siihen voidaan yhdistää AWS:n oma CloudHSM-holvi, jossa on laitteiston suojausmoduuli. Äärimmäisin ratkaisu on asiakkaan oman hallintajärjestelmän integroiminen AWS:ään.

Google Cloud:

Muilla toimittajilla pääsy asiakkaan ympäristöön tapahtuu asiakkaan IAM:n kautta. Poikkeuksen tähän tekee Google Cloud, jossa toimittajalla on mahdollisuus päästä asiakkaan avaimiin käsiksi, joskin se on suunniteltu hankalaksi prosessiksi, eikä tapahdu ilman asiakkaan tietämystä. Googlen avaintenhallintapalvelu on nimeltään Cloud Key Management. Myös Googlella on mahdollisuus käyttää HSM:ää. Jotkut Googlen pilvipalveluista mahdollistavat myös asiakkaan omien avainten käyttämisen.

Oracle:

Oracle tarjoaa erilaisia ratkaisuja avaintenhallintaan.

OCI Vault on asiakkaan hallinnoima salauksenhallintapalvelu, joka mahdollistaa avainten hallinnan OCI:n turvamoduuleissa (HSM), ja Oracle ylläpitää HSM-laitteistoja.

OCI Dedicated KMS on yksittäisen asiakkaan HSM palveluna, joka tarjoaa täysin eristetyn ympäristön salausavainten tallentamiseen ja hallintaan.

OCI External KMS mahdollistaa oman kolmannen osapuolen avainhallintajärjestelmän käytön tietojen suojaamiseksi OCI-palveluissa. Avaintenhallinta ja HSM ovat OCI:n ulkopuolella.

Lisätietoja:

Key Management Service | AWS
https://aws.amazon.com/kms/

Key Vault | Azure
https://azure.microsoft.com/en-us/products/key-vault

Key Management | Oracle
https://www.oracle.com/security/cloud-security/key-management/

Cloud Key Management | Google
https://cloud.google.com/security/products/security-key-management

FIPS PUB 140-2 | NIST
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

Privileged Access | Google
https://cloud.google.com/assured-workloads/access-transparency/docs/privileged-access

Ratkaisun analyysi

Pilvipalvelut mahdollistavat standardoidun salausavainten hallinnan melko helposti. Kaikilla palveluntarjoajilla on tarjolla lisäksi mahdollisuus lisätä asiakkaan omaa hallinnointia avaimiin. Pilvinatiivit avaintenhallintajärjestelmät ovat pääosin edullisempia ja yleensä takaavat riittävän suojaustason henkilötiedolle, kun HSM on implementoituna.

Salausavainten hallinnan riski on asiattomat salauksen purkuoperaatiot. Tätä voidaan asiakkaan osalta lieventää vain hallinnoimalla avaimia itse ja integroimalla ulkopuolinen avaintenhallintajärjestelmä (External Key Manager, EKM) pilvipalveluun. EKM on monimutkaisempi ja kalliimpi toteuttaa kuin pilvinatiivi järjestelmä. Siinä tietoturvan vastuu siirtyy pitkälti asiakkaalle. Tätä ei suositella toimijoille, joilla ei ole kattavaa kokemusta salaisuuksienhallinnasta. Toisaalta se takaa, ettei palveluntarjoaja pysty tekemään purkuoperaatioita tai tiedonluovutuksia. Palveluntarjoajat ehkäisevät asiattomia purkuoperaatioita teknisin ja organisatorisin keinoin.

5.3 Pääsyoikeuksien hallinta

Pilvipalveluntarjoajilla on palveluita käyttäjäoikeuksien hallintaan (identity and access management, IAM). IAM on keskitetty palvelu, jossa asiakas voi hallita käyttöoikeuksia. Käyttöoikeuksia jaetaan kahden tyyppisille toimijoille (principal): ihmisille ja (muille pilven) palveluille. Toimijoille määritetään resurssit, joihin niillä on käyttöoikeus (scope), sekä käyttöoikeuksien laajuus (permissions). IAM toimii myös autentikaatiojärjestelmänä ja sillä voidaan esimerkiksi edellyttää käyttäjiltä monivaiheista tunnistautumista (multifactor authentication, MFA) käyttöä. Googlea lukuun ottamatta palveluntarjoajien IAM-palveluita voidaan laajentaa myös asiakkaan omaan palvelinympäristöön.

Hyvä käytäntö pääsyoikeuksien hallinnassa on antaa käyttäjille ja palveluille minimioikeudet, jotka resurssi tarvitsee toimiakseen odotetusti. Tästä puhutaan vähimpien oikeuksien periaatteena (principle of least privileges). Periaate voidaan toteuttaa helposti IAM:n avulla esimerkiksi ryhmien kautta. Ryhmille voidaan asettaa valmiita tai räätälöityjä rooleja. Kaikilla samaan ryhmään kuuluvilla käyttäjillä/palveluilla on samat oikeudet. Tästä käytetään termiä role-based access control (RBAC). Se tekee käyttäjänhallinnasta skaalautuvampaa. IAM-palveluita voi käyttää myös APIn kautta.

IAM-palveluun kuuluu olennaisena osana myös lokitus. Lokien kattavuus vaihtelee palveluntarjoajien kesken. Lokit voidaan valjastaa automatisoituihin toimenpiteisiin. Toisin sanoen, tietyn lokimerkinnän sattuessa, voidaan automaattisesti ajaa komento esimerkiksi tapahtuman tarkasteluun. Nämä lokit ovat asiakkaalle näkyvissä ja niitä ei voi muokata tai poistaa säilytysaikana.

IAM:n kohdalla on otettava huomioon, että osa IAM-tiedoista näkyy myös palveluntarjoajalle. Asiakkaille on saatavilla ohjeet henkilötiedon minimoimiseksi IAM-tiedoissa.

Toimittajakohtaiset täsmennykset

Azure:

Azuren IAM-palvelu on nimeltään Azure Entra ID (ent. Azure AD). Se poikkeaa muista palveluista pääsyoikeuksien hallinnassa, sillä se on tiiviisti liitetty Active Directory -palveluun. Entra ID:ssä käyttöoikeuksien laajuus ja resurssit, joihin ne pätevät, ovat tallennettuna eri paikoissa ja Entra ID mahdollistaa käyttöoikeuksien periytymisen.

Ihmisten käyttöoikeuksien hallinta tapahtuu Entra ID:ssa roolien ja ryhmien kautta. Palveluiden käyttöoikeuksien hallinta on monimutkaisempaa. Se voidaan toteuttaa Managed Identities -konseptin avulla. Managed Identities mahdollistaa palveluiden todentamisen ja tunnistetietojen hankkimisen automaattisesti. Siten se poistaa palveluiden tunnistetietojen manuaalisen käsittelyn. Toisaalta palveluiden käyttäjänhallinta voidaan toteuttaa myös käyttäen Service Principal -konseptia. Service Principal sopii tapauksiin, joissa palvelulle tai sovellukselle halutaan antaa tietyt oikeudet, kun taas Managed identity sopii tapauksiin, joissa palvelun todentaminen halutaan automatisoida.

AWS:

AWS poikkeaa muista pilvipalveluista attribuutteihin perustuvan pääsynhallinnan (attribute-based access control, ABAC) vuoksi. Tämä johtuu pitkälti AWS:n tietorakenteesta, joka ei tarjoa yhtä rakenteellista pääsynhallintaa kuin RBAC. Käyttäjänhallinta toteutetaan IAM Policyn avulla. IAM Policy on dokumentti, jossa määritellään sekä resursseja käyttävät henkilöt että heidän käyttöoikeutensa laajuudet. Siten käyttöoikeudet ja niitä koskevat resurssit (permissions ja scope) löytyvät samasta paikasta.

AWS suosittelee käyttämään väliaikaisia käyttäjäoikeuksia ihmisille. Silloin henkilöllä ei varsinaisesti ole roolia kirjautuessaan, vaan kirjautumisen jälkeen käyttäjä omaksuu jonkin roolin (esimerkiksi admin tai developer). Roolista käytetään termiä IAM role. Käyttäjiä hallinnoidaan siis AWS:ssä samaan tapaan kuin palveluita Googlessa. Myös palvelut ja sovellukset omaksuvat tietyn roolin.

GCP:

Googlen IAM on samankaltainen lähestymistapa käyttäjänhallintaan kuin Azurella. Se myös toimii ryhmien ja roolien kautta. Myös Googlen IAM:ssä käyttöoikeuksien laajuus ja resurssit, joihin ne pätevät, ovat tallennettuna eri paikoissa. Googlen IAM on tiiviisti liitettävä muihinkin Googlen palveluihin, kuten Google Workspaceen. Google IAM mahdollistaa käyttöoikeuksien periytymisen.

Ihmisten käyttäjänhallinta tapahtuu Google Cloud Identityn tai Google Workspacen avulla. Azuren tapaan myös Google käyttää ryhmiä ja rooleja. Ryhmien lisäksi käyttöoikeuksia voidaan antaa myös muille kokonaisuuksille, kuten ”kaikille tunnistautuneille henkilöille” ja

”palveluille”. Ne ovat hieman kuin ennalta määriteltyjä ryhmiä. Palveluiden käyttäjänhallinta voidaan toteuttaa esimerkiksi Service Account -konseptin avulla. Tällöin todennettu palvelu ”omaksuu” tietyn Service accountin roolin ja saa sen käyttöoikeudet. Se toteutetaan lyhytaikaisten tunnuksien (short term credentials) avulla.

Googlella on myös palvelu nimeltä Identity-Aware Proxy, jonka avulla voidaan rajata pääsyä sovelluksiin identiteetin perusteella. Tätä voidaan pitää yksinkertaisempana kuin verkkokonfiguraatioiden ja VPN:n avulla saman tekeminen.

OCI:

Oraclen IAM toimii myös ryhmien ja roolien perusteella, ja on siten toiminnallisuudeltaan RBAC. Toisaalta OCI:ssa käyttöoikeudet määritellään IAM politiikoissa, kuten AWS:ssä. Myös Oraclen järjestelmässä toimijoiden käyttöoikeudet ja resurssit (permissions ja scope) ovat siis samassa paikassa. Myös Oracle tukee väliaikaisia käyttöoikeuksia. Silloin käyttäjät voivat kirjautua käyttäen muitakin järjestelmiä kuin Oraclen omaa ja sen jälkeen saada Oracle-ympäristön roolin.

Ratkaisun analyysi

Pilvipalvelut tarjoavat kattavat pääsyoikeuksien hallintapalvelut, jotka voidaan konfiguroida noudattamaan vähimpien oikeuksien periaatetta. IAM-palvelut ovat hyvin mukautuvia erilaisiin käyttötarkoituksiin, eikä niiden käytön tulisi rajoittaa asiakkaan omaa toimintaa.

IAM-palveluiden lokitus on kattavaa ja sen ja toimittajien kuvausten perusteella niiden eheys on varmistettu. Lokituksen valjastaminen tietoturvatoimintoihin automatisoi tietoturvakäytäntöjä.

Lisätietoja:

What is IAM | AWS
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

Entra ID | Microsoft
https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

Identity and Access Management (IAM) | Oracle
https://www.oracle.com/security/identity-management/

IAM Overview | Google
https://cloud.google.com/iam/docs/overview

5.4 Eri asiakkaiden tietojen erottelu

Julkiset pilvipalvelut perustuvat ratkaisuun, joissa useat eri asiakasorganisaatiot jakavat saman fyysisen infrastruktuurin, kuten palvelimet, tallennustilan ja verkkoresurssit (eng. multitenant architecture). Tämä mahdollistaa resurssien tehokkaan käytön ja kapasiteetin joustavan skaalautuvuuden, mutta aiheuttaa samalla palveluntarjoajille arkkitehtuurisen vaatimuksen asiakasympäristöjen loogiselle erottelulle. Monitasoiseen infrastruktuuriin, jossa asiakasympäristöt on eriytetty virtuaalisilla rajapinnoilla, liittyy riski eri organisaatioiden asiakastietojen sekoittumiselle.

Jaettujen resurssien hyödyntämiseen liittyy tietosuojariski tietojen luvattomaan käyttöön, etenkin jos käyttöoikeuksien valvonta on puutteellista. Riskiä voidaan ehkäistä vahvoilla identiteetin- ja pääsynhallinnan keinoilla sekä erilaisilla salausratkaisuilla, joita on käyty tarkemmin läpi salaukseen liittyvissä kappaleissa. Toinen tietoturva- ja tietosuojariski liittyy tietojen virheelliseen tai puutteelliseen loogiseen eristämiseen (eng. data segregation), mikä johtaisi eri asiakasympäristöjen tietojen sekoittumiseen. Pilvitoimittajan tulee käyttää vahvoja virtualisointi- ja eristystekniikoita varmistaakseen, että eri asiakkuuksilta tulevat tiedot pysyvät erillään. Säännölliset turvallisuusarvioinnit ja -auditoinnit ovat myös tärkeitä.

Toimittajakohtaiset täsmennykset

AWS:

AWS käyttää Xen-pohjaista hypervisor-tekniikkaa virtualisoinnissa ja luottaa vahvaan eristystekniikkaan hypervisor-tasolla tietojen erottelun varmistamiseksi. AWS tarjoaa Virtual Private Cloud (VPC) -palvelun verkon eristämiseen ja antaa asiakkaille mahdollisuuden luoda yksityisiä aliverkkoja. AWS IAM-palvelu mahdollistaa käyttöoikeuksien tarkan hallinnan, mikä edistää tietojen erottelua, joskin IAM on globaali palvelu, jolloin tiedonsiirtojen riskienarviointiin tulee kiinnittää erityistä huomiota. AWS:n avulla asiakkaat voivat luoda yksityisiä aliverkkoja VPC:ssä, mikä varmistaa, että näiden aliverkkojen resursseja ei voida käyttää suoraan Internetistä.

Google:

Google käyttää GCP-alustallaan KVM-hypervisoria virtualisoinnissa ja käyttää ohjelmiston määrittämän verkkoyhteyden ja hypervisor-tason eristyksen yhdistelmää ylläpitääkseen tietojen erottelua. Kuten Azure ja AWS, GCP tarjoaa virtuaalisen yksityisen pilven (VPC) verkon eristämiseen ja identiteetin ja käyttöoikeuksien hallinnan (IAM) yksityiskohtaiseen kulunvalvontaan. GCP mahdollistaa VPC peeringin, joka mahdollistaa kahden VPC-verkon yhdistämisen, jolloin ne voivat

kommunikoida turvallisesti paljastamatta tietoja julkiseen Internetiin.

Microsoft:

Microsoft käyttää Azure-ympäristössään hypervisor-tason eristämisen ja ohjelmiston määrittämän verkkoyhteyden yhdistelmää tietojen erottelun varmistamiseksi. Azure tarjoaa virtuaaliverkkoja (VNet), joiden avulla asiakkaat voivat eristää resurssinsa virtuaaliverkossa. Pääsyn hallinta ja verkon suojausryhmät (NSG) parantavat edelleen tietojen eristämistä. Verkkosuojausryhmät (NSG) toimivat virtuaalisina palomuureina, jotka sallivat tai estävät liikenteen verkkoliitäntöihin, virtuaalikoneisiin tai aliverkkoihin. NSG:t tarjoavat saapuvan ja lähtevän liikenteen kontrolloinnin.

Oracle:

Oraclen suvereeni pilvi on suunniteltu täyttämään säänneltyjen toimialojen erityistarpeet. Se korostaa tietojen sijaintia ja vaatimustenmukaisuutta varmistaen, että tiedot säilytetään tiettyjen maantieteellisten rajojen sisällä. Oracle käyttää omaa Oracle Cloud Infrastructure (OCI) -arkkitehtuuriaan, joka yhdistää laitteiston ja ohjelmiston määrittämän verkkoyhteyden tietojen eristämiseen. Oracle tarjoaa virtuaalisia pilviverkkoja (Virtual Cloud Networks) verkon eristämiseen, jolloin asiakkaat voivat luoda yksityisiä verkkoja Oraclen pilviympäristössä.

Ratkaisun analyysi

Jokainen palveluntoimittaja tarjoaa verkon eristysominaisuuksia, pääsynvalvontaa ja identiteetinhallintamekanismeja varmistaakseen, että vain valtuutetut henkilöt pääsevät käsiksi asiakastietoihin. Lisäksi palvelutoimittajat tarjoavat hallintatyökaluja (compliance services), joiden avulla asiakkaat pystyvät tunnistamaan tietoturva- ja tietosuojariskejä ja luokittelemaan ja suojaamaan arkaluontoisia tietoja.

Palvelutoimittajat tarjoavat tietoa ja läpinäkyvyyttä ratkaisuidensa arkkitehtuuriin ja teknisiin suojausmenetelmiin. Teknisten ratkaisujen luotettavuutta ja toimintaa palvelutoimittajat todentavat sertifikaatein. Poikkeamien ja häiriötilanteiden osalta loppukäyttäjäorganisaation on luotettava palvelutoimittajien prosessien toimivuuteen. Jaetun ympäristön jäännösriskiä julkipilvipalvelussa on mahdotonta poissulkea täysin.

On mahdollista, että jaetun ympäristön käyttö aiheuttaa organisaation vaikutustenarvioinnissa sellaisin riskin, jota ei voida hyväksyä. Silloin loppukäyttäjäorganisaation on turvauduttava teknisen ratkaisun osalta yksityiseen pilveen tai on-premise-ympäristöön.

Lisätietoja:

Logical Separation on AWS | AWS
https://docs.aws.amazon.com/whitepapers/latest/logical-separation/welcome.html

Google infrastructure security design overview | Google
https://cloud.google.com/docs/security/infrastructure/design

Azure customer data protection | Microsoft
https://learn.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data

Isolate Resources and Control Access | Oracle
https://docs.oracle.com/en/solutions/oci-best-practices/isolate-resources-and-control-access1.html - GUID-86C12BF6-48CE-405A-989E-A83DD3A62E60

5.5 Toimittajan pääsy asiakkaan tietoihin

Asiakkaan tiedoilla tarkoitetaan asiakkaan omistamia sisältötietoja pilvipalvelun sisällä. Kun sisältötietoja tallennetaan pilvialustalle, asiakas antaa palveluntarjoajalle vastuun tietojen asianmukaisesta käsittelystä. Siksi on arvioitava, ovatko palveluntarjoajan kontrollit asiakastiedon eristämiseksi riittävän hyvät. Lisää siitä, mikä tieto on asiakkaan sisältötietoa, löytyy kohdasta ”**5.7 Sisältötietojen siirrot**”.

Pääsääntöisesti palveluntarjoajat estävät työntekijöidensä pääsyn sisältötietoon teknisin ja organisatorisin keinoin. Tyypillinen poikkeustilanne on asiakkaan tekemä tukipyyntö, jolloin tukihenkilön tekemisistä jää lokitiedot.

Lokitietojen kattavuus ja näkyvyys asiakkaalle vaihtelevat. On huomattava, että palveluntarjoajalla on pääsy konfiguraatio- ja metriikkatietoihin.

Toimittajakohtaiset täsmennykset

AWS:

AWS kieltää työntekijöiltään pääsyn asiakkaan sisältöön ja myös tekniset ratkaisut pyrkivät estämään tämän. Poikkeus tähän linjaan voidaan tehdä kolmesta syystä:

1. Asiakas itse pyytää AWS:n työntekijän pääsyä omaan ympäristöönsä. Tämä tarkoittaa yleensä tukipyyntöjä.
2. Pääsy tarvitaan petoksen tai väärinkäytöksen ehkäisemiseksi.
3. AWS tarvitsee pääsyn asiakkaan dataan noudattaakseen lakia. Tämä liittyy yleensä tietopyyntöihin.

Mikäli AWS:n työntekijälle myönnetään pääsy asiakkaan sisältötietoon, siitä ilmoitetaan asiakkaalle. Kaikki AWS:n tukikomennot toteutetaan julkaisuputken (pipeline) avulla, eli AWS:n tukihenkilölle annetaan tarkkaan rajatut käyttöoikeudet. AWS vahvistaa tätä prosessia lokitiedoilla ja organisatorisilla prosesseilla. Jokainen työntekijän pääsy asiakasympäristöön nauhoitetaan ja lokitietoihin kirjataan kaikki työntekijän ajamat komennot. Sen lisäksi johtoasemassa oleva insinööri (principal engineer) käy läpi jokaisen tapauksen.

Google:

Google ei varsinaisesti erittele tapauksia, joissa sen työntekijöillä on pääsy asiakkaan sisältötietoon. Sen sijaan, se opastaa asiakasta konfiguroimaan ympäristön siten, että pääsy selkokieliseen dataan ei ole mahdollista. Tämä tapahtuu yhdistämällä EKM (asiakkaan ulkoinen avaintenhallintajärjestelmä) ja Key Access Justifications -palvelu. Key Access Justifications luo järjestelmän, joka ilmoittaa asiakkaalle kaikki pyynnöt, jotka kohdistuvat salausavaimiin. Se antaa jokaisen pyynnön kohdalla myös selityksen kyseiselle pyynnölle ja mahdollisuuden hyväksyä tai hylätä se.

Microsoft:

Azuren tukihenkilöille annetaan käyttöoikeudet ”least privileges” -periaatteen mukaisesti. Silloin tukihenkilöillä on kyvykkyydet tehdä vain tukitehtävään liittyviä toimenpiteitä. Azuren tukihenkilöt eivät pääse yliajamaan asiakkaan omaa IAM-järjestelmää. Sen sijaan Azuren Customer Lockbox -palvelu tarjoaa rajapinnan, jossa asiakas voi tarkastella, hyväksyä ja evätä tukihenkilöiden pääsyn asiakkaan sisältöön3. Jos tukitiketti ei ratkea palveludatalla, tukihenkilö pyytää tunnuksia Just in Time -järjestelmältä (JIT). JIT arvioi pyynnön, ja se lähetetään eteenpäin Customer Lockboxille. Asiakas voi itse määrittää, ketkä asiakasorganisaatiossa voivat luoda tukipyyntöjä ja hyväksyä tukihenkilöiden pyyntöjä päästä asiakkaan ympäristöön.

Tukitiketissä voidaan myös sallia tai evätä Azuren tukihenkilöiltä oikeus kerätä lokidataa asiakkaan sisältötiedoista.

Oracle:

Oracle käyttää tukiprosesseissa asiakkaan omaa käyttäjänhallintaa, eli sillä ei ole itsenäistä keinoa asiakkaan sisältötietoihin. Oracle myös kieltää omissa prosesseissaan ”takaovien” (backdoors) rakentamisen omiin palveluihinsa5. Tämä tarkoittaa, että palveluissa ei tulisi olla toiminnallisuuksia, jotka mahdollistaisivat tunnistautumisen tai muun turvallisuustoiminnon ohittamisen. Oracle, muiden palveluntarjoajien tapaan, painottaa, että asiakas voi salata tietonsa siten, että palveluntarjoajalla ei ole keinoa nähdä sisältöä selkokielisenä.

Lisätietoja:

Privacy Features of AWS Services | AWS
https://aws.amazon.com/compliance/privacy-features/

Trusting your data with Google Cloud | Google
https://services.google.com/fh/files/misc/072022_google_cloud_trust_whitepaper.pdf

Customer Lockbox for Microsoft Azure | Microsoft
https://learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

Create an Azure support request | Microsoft
https://learn.microsoft.com/en-us/azure/azure-portal/supportability/how-to-create-azure-support-request

Data Flows and Oracle Services | Oracle
https://www.oracle.com/fr/a/ocom/docs/corporate/privacy-shield-statement-071720.pdf

Ratkaisun analyysi

Yleisesti ottaen pilvipalvelut tarjoavat keinoja, joilla asiakas voi minimoida toimittajan pääsyä asiakkaan sisältötietoihin. Palveluntarjoajien on hankala julkisesti todentaa, ettei pääsyä asiakkaan sisältötietoihin ole. Siksi asiakkaalle annetut keinot luottamuksellisuuden varmistamiseksi painottuvat sisältötiedon salaamiseen ja avaintenhallintaan.

Pilvi-infrastruktuuri on myös toteutettavissa siten, että palveluntarjoajalla ei ole pääsyä asiakkaan sisältötietoon, mutta se rajoittaa pilven potentiaalia. Esimerkiksi palomuurit käsittelevät tietoliikennettä suojaamattomana, jotta ne voivat analysoida sitä tarkemmin. Jos tietoa käsitellään aina salattuna, sen analysointi ei onnistu vastaavalla tasolla ja suurin osa palomuurin yhteydessä olevista tietoturvatoiminnallisuuksista menetetään.

Palveluntarjoajien prosessit eivät ole yleensä julkisia. Toisinaan prosesseista voi saada enemmän tietoa salassapitosopimuksen kautta. Toisaalta palveluntarjoajat pyrkivät todentamaan niiden pitävyyden erilaisten sertifikaattien avulla. Jokaisella palveluntarjoajalla on julkisesti tarjolla tietoa palveluntarjoajan tietoturvasertifikaateista.

Yleisimpiä huolia ovat muiden valtioiden tekemät tietopyynnöt. Näitä varten kaikilla palveluntarjoajilla on julkisesti esillä tilastoja tehdyistä tietopyynnöistä sekä niihin vastaamisesta. Ensisijaisesti pilvipalveluntarjoajat pyrkivät hylkäämään tietopyynnöt, mutta muutoin tietopyyntöjä käsitellään tapauskohtaisesti. Palveluntarjoajat julkaisevat ylätason prosessit tietopyyntöjen käsittelylle. Tietopyyntöjen käsittelyyn vaikuttaa se, koskeeko pyyntö asiakkaan sisältötietoja vai ei. Sisältötietojen luovuttamisen kynnys on korkeampi. Palveluntarjoajat myös ilmoittavat asiakkaalle tietopyynnöstä, ellei viranomaisen tietopyyntö sitä kiellä. Palveluntarjoajat saattavat joissakin tapauksissa ohjata tietopyynnön suoraan asiakkaalle tai pyrkiä kaventamaan tietopyynnön laajuutta.

Lisätietoja:

Compliance | AWS
https://aws.amazon.com/compliance/

Law Enforcement Information Requests | AWS
https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF

Amazon Law Enforcement Guidelines | AWS
https://d1.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

Compliance resource center | Google
https://cloud.google.com/compliance

Global requests for user information | Google
https://transparencyreport.google.com/user-data/overview

How Google handles government requests for user information | Google
https://policies.google.com/terms/information-requests?sjid=4792790494153692405-EU

Lisätietoja:

Azure compliance documentation | Microsoft
https://learn.microsoft.com/en-us/azure/compliance/

Law Enforcement Requests Report | Microsoft
https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

About our practices and your data | Microsoft
https://blogs.microsoft.com/datalaw/our-practices/

Cloud Compliance | Oracle
https://www.oracle.com/corporate/cloud-compliance/

Law Enforcement Requests Report | Oracle
https://www.oracle.com/legal/law-enforcement-requests-report/

Legal Access Requests | Oracle
https://www.oracle.com/a/ocom/docs/oracle-legal-access-requests.pdf

5.6 Alikäsittelijöiden prosessit ja pääsy asiakkaan tietoihin

Alihankkijoiden sijaan palvelutoimittajat käsittelevät dokumentaatiossaan alihankkijoita alikäsittelijöinä (eng. subprocessors). Alikäsittelijöitä koskevat samat velvollisuudet ja sitoumukset kuin palvelutoimittajan omia työntekijöitä. Alikäsittelijöillä on oikeudet ainoastaan siihen osaan dataa mitä he työssään käsittelijöinä tarvitsevat. Suurimmaksi osaksi alikäsittelijöitä toimii tukipalveluissa ja fyysisen pilvipalvelualustan huoltotehtävissä ilman pääsyä asiakkaiden tietoihin.

Palvelutoimittajan (CSP) lupaamien velvoitteiden tai sitoumusten näkökulmasta, sillä ei ole asiakkaalle (CSC) merkitystä käsitteleekö dataa alikäsittelijä vai yrityksen oma työntekijä, sillä palvelutoimittajalla on asiakkailleen (CSC) täysi vastuu alikäsittelijöistään. Mikäli asiakas ei luota palvelutoimittajan prosesseihin, sillä on mahdollisuus lisätä omia suojausmenetelmiään ja säilyttää mm. omassa ympäristössään suojausavaimia.

Alikäsittelijät ovat auditointien piirissä (ISO 27018 ja SOC2), sillä auditoinnit kattavat myös ne palvelutoimittajan prosessit, joissa alikäsittelijöillä on oma roolinsa. Kaikki palvelutoimittajat (CSP) edellyttävät käyttämiltään alikäsittelijöiltä samat vaatimukset kuin omilta työntekijöiltään ja palvelutoimittajat myös hallinnoivat alikäsittelijöiden työtä ja oikeuksia. Kaikkien palvelutoimittajien alikäsittelijöitä koskee myös vähimpien oikeuksien periaate (Least Privilege). Näiltä osin alikäsittelijöitä vaaditaan siis toimimaan vaatimusten mukaisesti.

Toimittajakohtaiset täsmennykset

AWS:

AWS ilmoittaan kotisivuillaan 30 päivää ennen kuin uusi alikäsittelijä aloittaa työnsä. Asiakkaalla on mahdollisuus tilata sivujen päivityksistä tiedot automaattisesti sähköpostiin. AWS listaa sivuillaan alikäsittelijät palvelualueittain.

Google:

Google edellyttää uuden alikäsittelijän vastustamista 90 päivän sisällä siitä, kun asiakkaalle on ilmoitettu uudesta alikäsittelijästä. Google listaa dokumentaatiossaan kaikki alikäsittelijänsä palveluittain vastuualueineen (vastuutehtävä ja maantieteellinen pilvialue).

Microsoft:

Microsoft ilmoittaa sivuillaan asiakkailleen 6 kuukautta ennen kuin uusi alikäsittelijä aloittaa työnsä, jos alikäsittelijä tarvitsee työssään pääsyä sisältötietoihin. Muussa tapauksessa ilmoitusajankohta on 30 päivää ennen uuden alikäsittelijän työn aloitusta. Mikäli alikäsittelijän tehtäviin kuuluu mahdollinen pääsy asiakkaan sisältötietoihin (esim. tukipalvelut), työntekijät käyttävät tehtäviinsä työasemia, joissa pääsy ulkoiseen verkkoon on rajoitettu ja ulkoiseen mediasisältöön estetty.

Oracle:

Oracle ylläpitää alikäsittelijälistaa dokumentissa (ID 2121811.1), mutta dokumentti on luettavissa ainoastaan Oraclen portaalin kautta sopimusasiakkaille. Dokumentin kirjoitushetkellä suvereenin pilven alikäsittelijänä toimii Twilio. Se on yhdysvaltalainen yritys, mutta asiakkaalla on mahdollisuus evätä (tekstiviesti)palvelut, joihin Twiliota käytetään. Yleisesti Oracle listaa alikäsittelijöiltä vaadittavat turvallisuusstandardit omassa dokumentissaan ”Oracle Supplier Information and Physical Security Standards”.

Oracle vaatii sopimuksessaan asiakasta vastustamaan uusia alikäsittelijöitä 30 päivän sisällä tiedoksiannosta.

Lisätietoja:

Sub-processors | AWS
https://aws.amazon.com/compliance/sub-processors/

Cloud Platform Subprocessors | Google
https://cloud.google.com/terms/subprocessors

Online Services Subprocessors List | Microsoft
https://servicetrust.microsoft.com/DocumentPage/aead9e68-1190-4d90-ad93-36418de5c594

Identity and access management overview | Microsoft
https://learn.microsoft.com/en-us/compliance/assurance/assurance-identity-and-access-management

Supplier Information and Physical Security Standards | Oracle
https://www.oracle.com/assets/oracle-supplier-contractor-security-070672.pdf

Ratkaisun analyysi

EU:n yleinen tietosuoja-asetus velvoittaa, että rekisterinpitäjällä on oikeus vastustaa uusien alikäsittelijöiden hankintaa, mutta todellisuudessa yksittäisen asiakkaan vastustuksella on hyvin vähän merkitystä. Palvelutoimittajat ilmoittavat sivuillaan 1-6 kuukautta ennen kuin uusi alikäsittelijä aloittaa työnsä. Mikäli asiakas ei hyväksy uutta alikäsittelijää, ainoaksi konkreettiseksi keinoksi jää irtisanoa palvelusopimus. Asiakkaan paras keino vaikuttaa alikäsittelijöiden valintaan on tehdä laajamittaista Euroopan sisäistä yhteistyötä muiden

julkisorganisaatioiden kanssa. Tarpeeksi suuri asiakasjoukko pystynee vastustamaan alikäsittelijöiden valintaa, jos vastustukseen löytyy perusteltu syy.

Toisena kontrollikeinona on omien suojausmenetelmien käyttö, joiden avulla asiakas pystyy lisäämään suojauskerroksia omaan dataansa. Palvelutoimittajien hallinnoima sisältödata on suojattu palvelutoimittajan puolelta silloin, kun se varastoidaan kantaan tai sitä siirretään, mutta standardimenettelyssä suojausavaimia hallitsee pilvipalvelutoimittaja.

Vaikutustenarvioinnissa loppukäyttäjäorganisaation tulee myös ottaa huomioon käytettyjen alikäsittelijöiden maantieteelliset sijainnit käytettyjen palveluiden ja alikäsittelijän tehtävien mukaan. Mikäli alikäsittelijän käyttö aiheuttaa tarpeettoman tiedonsiirron, tulee kyseisen palvelun ominaisuuden käyttöä pyrkiä välttämään. Tekstiviestipalvelu, jota operoidaan Euroopan ulkopuolelta, on esimerkki tällaisesta palvelusta.

5.7 Sisältötietojen siirrot

Sisältötiedoilla tarkoitetaan kaikkea sitä asiakastietoa, jonka asiakasorganisaatio vie käsiteltäväksi tai toimitetaan asiakasorganisaation puolesta käsiteltäväksi pilvipalveluihin. Sopimuksellisesti sisältötietoja, tietojen rooleja ja vastuista käsitellään palvelutoimittajien DPA:ssa. Sisältötietojen osalta palvelutoimittajat toimivat käsittelijän roolissa. Tiedonsiirtojen näkökulmasta kiinnostuksen kohteena ovat ne sisältötiedot, jotka pitävät sisällään henkilötietoja. Sisältötietojen tiedonsiirtojen riskien arvioinnin osalta sisältötiedot voidaan jakaa kolmeen eri osa-alueeseen:

1. Tiedonsäilöntään käytettävät sijainnit (palvelinkeskukset)
2. Tukipalvelut
3. Alustan tarjoamat globaalit palvelut

Sisältötietojen osalta EU/ETA-alueen ulkopuolisiin siirtoihin ja infrastruktuuriin liittyvät riskit liittyvät:

1. tukipalveluiden sijaintiin
2. palvelutoimittajan yksittäisten palveluiden valintaan ja konfigurointiin.

Infrastruktuuripalveluiden tukipyynnöissä henkilötietojen määrä on rajoitettua palvelun luonteen vuoksi ja käyttäjäorganisaatio pystyy vaikuttamaan henkilötiedon määrään tekemällä käyttäjätunnuksista henkilötietoon perustumattomia.

Käytettävät yksittäiset palvelut vaikuttavat kuitenkin tukipyyntöjen sisältöön, joten käyttäjäorganisaation tulee arvioida riskiperusteisesti tulisiko sen turvautua ainoastaan EU-alueelta annettavaan tukeen.

Palvelutoimittajan yksittäisten palveluiden valinnan ja konfiguroinnin osalta käyttäjäorganisaation tulee varmistaa, että alustan ylläpitokumppani huomioi tietosuojariskit ottaessaan käyttöön alustalta uusia palveluita. Palvelutoimittajien tarjoama dokumentaatio ja alustalla olevat compliance-työkalut auttavat riskien arvioinnissa.

Toimittajakohtaiset täsmennykset

AWS:

AWS:n lähimmät palvelinkeskukset sijaitsevat Ruotsissa.

AWS ei takaa tukipalveluiden käsittelyä ETA-alueen sisältä, vaan toteuttaa ns. ”follow the sun” periaatetta. AWS pyrkii olemaan käsittelemättä henkilötietoja alustapalveluiden tukitiketeissään. AWS on lähtökohtaisesti puhdas tekninen ympäristö (infrastruktuuri)sovelluksille, jolloin henkilötietoriskin kannalta olennaisempaa on tarkastella niitä sijainteja, joissa sovellustoimittaja tarjoaa tukipalveluita. AWS:llä ei ole pääsyä sovellustoimittajan dataan, vaikka sovellustoimittaja hyödyntäisi palveluissaan AWS:n palveluita. AWS on julkaissut lokakuussa 2023 ottavansa käyttöön Euroopan alueelle suvereenin pilviratkaisun. Ratkaisu tulee takaamaan tuen saatavuuden EU/ETA-alueelta. Ratkaisun aikataulusuunnitelmaa ei ole dokumentin kirjoitushetkellä julkaistu.

Google:

Googlen lähin palvelinkeskus sijaitsee Haminassa.

Google tarjoaa EU:n alueellista tukea Assured Workloads ominaisuuden alla lisäpalveluna. Assured Workloads kokonaisuus tarjoaa julkisen pilvipalvelun ydinpalvelut ja niiden tuen tietyn maantieteellisen alueen sisältä. Yksi maantieteellisistä alueista on EU (Google – Assured support).

Microsoft:

Microsoft on rakentamassa palvelinkeskuksia Suomeen.

Microsoft julkaisi joulukuussa 2022 EU Data Boundary konseptinsa, jonka tarkoitus on pitää EU-alueen asiakkaiden tiedot ETA-alueen sisällä niin pitkälle kuin mahdollista. EU Data Boundary otettiin käyttöön alkuvuodesta 2023 ja sen tiekartta ulottuu vuodelle 2024 (Microsoft – EU data boundary). Vuonna 2024 Microsoftin on tarkoitus pystyä tarjoamaan tekninen tuki ydin infrastruktuuripalveluiden osalta kokonaisuudessaan ETA-alueelta. Toisaalta tälläkin hetkellä tukea on mahdollista ottaa vastaan vain ETA-alueelta. Microsoft ilmoittaa, mikäli henkilötietoa sisältävää tukitikettiä oltaisiin ratkaisemassa ETA-alueen ulkopuolella, eikä asiakkaan ole pakko hyväksyä pyyntöä. Tässä tapauksessa

tukitiketti siirtyy jonoon ETA-alueella sijaitsevaan palvelupisteeseen, mikä tarkoittaa, että tiketin ratkaisuaika myös palvelutasojen näkökulmasta pitenee.

Oracle:

Oraclen suvereeni pilvi ei siirrä sisältötietoja EU-alueen ulkopuolelle. Palvelinkeskukset sijaitsevat EU-alueella, tukipalvelut tuotetaan EU-alueelta, eikä suvereenin pilven tarjoamassa ole globaaleja palveluita. Oracle suvereenin pilven palvelinkeskukset ovat fyysisesti erillään Oraclen EU:ssa sijaitsevista julkipilven palvelinkeskuksista. Asiakasorganisaation on kuitenkin huomioitava, että mikäli se haluaa käyttää suvereenin pilven palveluita, se ei voi samanaikaisesti autentikoitua palveluihin hyödyntäen esimerkiksi Microsoftin IAM-järjestelmää (Entra ID), sillä se on luonteeltaan globaali palvelu, mikä rikkoisi EU-alueen suvereniteetin.

Oraclen suvereenin pilven tukipalvelut sijaitsevat EU-alueella. Kyseessä on olennainen suvereenin pilven ominaisuus. OCI:n suvereenin pilven palvelut ja hinnoittelu ovat samanlaisia OCI julkipilven kanssa.

Ratkaisun analyysi

Kaikkien toimittajien osalta käytettävät palvelinkeskukset voidaan rajata EU/ETA-alueelle, eivätkä palvelutoimittajat (CSP) siirrä asiakkaan (CSC) sisältötietoa tämän tietämättä EU/ETA-alueen ulkopuolelle. Tiedonsiirrot tulisivat kysymykseen, jos CSC määrittäisi sopimuksellisesti esimerkiksi ETA-alueen ulkopuolisen palvelinkeskuksen käytön varmuuskopiointiin.

Henkilötietojen käsittelyn näkökulmasta datan maantieteellisen sijainnin lisäksi tulee tarkastella niitä sijainteja, joista asiakkaalle tarjotaan teknisiä tukipalveluita. Infrastruktuuripalveluita koskevat tukitiketit eivät lähtökohtaisesti pidä sisällään henkilötietoja ja palvelutoimittajat suosittelevat, ettei tukitiketteihin liitetä henkilötietoja sisältäviä kuvakaappauksia. Palvelutoimittajat tarjoavat enenevissä määrin tukipalveluita EU-alueen sisältä, mutta se vaatii asiakasorganisaatiolta lisäpalvelun tilaamista tai sopimuksellisesta varmistusta. Lisäksi EU-alueen tuen piirissä olevia palveluita on rajattu.

Palvelutoimittajien ympäristöt pitävät sisällään satoja yksittäisiä palveluita. Jokaisella palvelulla on omat erityisehtonsa, joihin palvelukeskuksen tai vastaavan operaattorin tulee tutustua, jotta loppukäyttäjäorganisaatio voi tehdä palvelun käytöstä vaikutustenarvioinnin. Lähtökohtaisesti palvelut jakautuvat globaaleihin palveluihin (esim. IAM-palvelut, CDN, AI-palvelut) ja paikallisiin palveluihin. Paikallisten palveluiden osalta käyttäjäorganisaatio (CSC) pystyy määrittämään ne palvelukeskukset, joista palveluita tarjotaan. Globaalit palvelut ovat nimensä mukaisesti globaaleja ja henkilötietojen siirtojen näkökulmasta niiden käyttöön liittyy riskejä. Pääsääntöisesti globaalit palvelut ovat ominaisuuksiltaan lisäpalveluita. Julkipilvialustojen ominaisuuksia voidaan hyödyntää

käyttämällä pelkästään paikallisia palveluita. Poikkeuksena on IAM-palvelut, jotka ovat luonteeltaan globaaleja palveluja (lukuun ottamatta Oraclen suvereenin pilven tarjoamaa). Palvelutoimittajilla ei ole halua rajoittaa IAM -ympäristöön pääsyä sijaintiperusteisesti, jolloin organisaation tulee ottaa käyttöön kompensoivia suojausmekanismeja, mikäli se haluaa hyödyntää julkipilvitarjoajien IAM-palveluita. Yleisesti ottaen asiakas (CSC) valitsee ja on vastuussa niistä palveluista, joita se ottaa ja haluaa käyttää. Käyttöönotettavan palvelun riskiarviointi tulee tehdä käyttötapaus- ja palvelukohtaisesti. Jokainen palvelutoimittaja tarjoaa dokumentoinnissaan palvelukohtaisen läpinäkyvyyden lokaaleihin ja globaaleihin palveluihin.

5.8 Konesalien fyysinen turvallisuus

Konesalien fyysinen turvallisuus voidaan jakaa neljään osa-alueeseen:

- Rajakerros (eng. perimeter layer)
- Infrastruktuurikerros (eng. infrastructure layer)
- Datakerros (eng. data layer)
- Ympäristövalvonta (eng. environmental layer)

Palvelinkeskusten suojaus alkaa raja- tai kehäkerroksesta, mikä pitää sisällään useita suojausominaisuuksia sijainnin mukaan, kuten vartijoita, aitauksia, turvasyötteitä, tunkeutumisen havaitsemistekniikoita ja muita turvatoimia.

Infrastruktuurikerros pitää sisällään palvelinkeskusrakennuksen sekä laitteet ja järjestelmät, jotka pitävät sen toiminnassa. Komponentit, kuten varateholaitteet, LVI-järjestelmä ja palonsammutuslaitteet, ovat kaikki osa infrastruktuurikerrosta.

Tietosuojan näkökulmasta datakerros on kriittisin suojapiste, koska se on alue, jossa on asiakkaiden henkilötietoja (ja muita asiakastietoja). Suojauksen keskeisenä mekanismina on henkilökunnan pääsyn rajoittaminen datakerrokseen ja säilyttämällä eri oikeudet eri tasoille. Lisäksi teknisinä mekanismeina käytetään uhkien havaitsemislaitteita ja järjestelmäprotokollia.

Ympäristövalvonta on omistettu ympäristönäkökohtien huomioonottamiseen. Palvelinkeskussijainnit pyritään valitsemaan huolellisesti, jotta ympäristöriskit, kuten tulvat, äärimmäiset sääolosuhteet, seisminen aktiivisuus ja sähkökatkot aiheuttavat toiminnan jatkuvuudelle lähtökohtaisesti mahdollisimman matalan riskin.

Toimittajakohtaiset täsmennykset

AWS

AWS noudattaa fyysisen turvallisuuden osalta useita alan standardeja ja parhaita käytäntöjä. Näitä ovat esimerkiksi ISO/IEC 27001, SOC 2, ja NIST SP 800-53. Standardit asettavat vaatimuksia fyysisen turvallisuuden, kuten valvontajärjestelmien käytön, pääsynhallinnan ja ympäristön hallinnan suhteen. Alan standardien mukaisesti, AWS:n datakeskuksissa on korkealaatuiset paloturvallisuusratkaisut ja varajärjestelmät sähkökatkojen varalta.

Pääsy AWS:n datakeskuksiin on erittäin rajoitettua. Jokainen, joka haluaa päästä fyysisesti datakeskukseen, joutuu läpikäymään tiukan tunnistusprosessin ja saamaan asianmukaisen valtuutuksen. AWS-palvelinten Nitro-järjestelmä on suunniteltu siten, että se tarjoaa työkuorman luottamuksellisuuden eikä siinä ole operaattoripääsyä. Nitro-järjestelmässä ei ole mekanismia, jolla kukaan järjestelmä tai henkilö voisi kirjautua EC2-palvelimiin, lukea EC2-instanssien muistia tai päästä käsiksi instanssin tallennustilaan ja salattuihin EBS-tietovolyymeihin. Datakeskuksia valvotaan 24/7 valvontajärjestelmillä, mukaan lukien valvontakamerat, valvomojärjestelmät ja hälytysjärjestelmät. Lähimmät AWS:n palvelinkeskukset sijaitsevat Ruotsissa.

Google

Google Cloud noudattaa useita tietoturvasertifikaatteja, kuten ISO/IEC 27001, SOC 2 ja HIPAA. Google on panostanut omissa palvelinkeskuksissaan jatkuvuuden turvaamiseen, kuten automaattinen siirtyminen toiseen datakeskukseen häiriön tapahtuessa ja hätävarageneraattorit, jotka pitävät datakeskukset toiminnassa sähkökatkojen aikana. Googlen sitoutuminen liiketoiminnan jatkuvuuteen näkyy ISO 22301:2019 -sertifikaatissa. Google jakaa ja replikoi kaiken datan hajautetusti useisiin tietokoneisiin eri sijainneissa. Tämä estää yhden vian muodostumisen ja varmistaa, että käyttäjän kriittinen data varmuuskopioidaan automaattisesti. Google seuraa jokaisen kovalevyn sijaintia ja tilaa palvelinkeskuksissa, ja käytöstä poistetut kovalevyt tuhotaan perusteellisesti, jotta voidaan estää luvaton pääsy dataan. Googlella on 24/7 toimiva turvatiimi, joka valvoo palvelinkeskuksia usean eri turvakerroksen osalta. Google käyttää rajapuolustusjärjestelmiä, kattavaa kameravalvontaa, biometristä tunnistautumista ja vartiointihenkilöstöä. Lisäksi Google noudattaa tiukkaa pääsyn ja turvallisuuden politiikkaa palvelinkeskuksissaan ja kouluttaa henkilöstöään tietoturvalliseen toimintaan. Googlen lähimmät palvelinkeskukset sijaitsevat Haminassa.

Microsoft

Microsoftin Azure-palvelut noudattavat useita tietoturvastandardeja, kuten ISO/IEC 2700 ja NIST SP 800-53. Microsoftin fyysisen turvallisuuden eri kerroksilla on tarkat hallintaprosessit, kuten pääsyn ennakkopyyntö, hyväksyntä ja valvonta. Fyysistä turvallisuutta toteutetaan muun muassa kulunvalvontajärjestelmillä, kaksivaiheisella tunnistautumisella, biometrisillä tarkastuksilla, valvonta- ja hälytysjärjestelmillä ja metallinpaljastintarkastuksilla. Microsoft suorittaa säännöllisesti fyysisiä turvallisuuskatselmuksia varmistaakseen, että palvelinkeskukset täyttävät Azure-turvallisuusvaatimukset. Palvelinkeskuksen kunnossapidon henkilöstöllä ei ole pääsyä Azure-palveluun, ja heiltä puuttuu fyysinen pääsy Azuren palvelinhuoneisiin ja häkkeihin (eng. server rack). Microsoft on rakentamassa palvelinkeskuksia Suomeen. Toistaiseksi lähimmät palvelinkeskukset sijaitsevat Ruotsissa.

Oracle

Oracle noudattaa kattavaa tietoturvasertifiointia, kuten ISO/IEC 27001, ja sillä on omat fyysisen turvallisuuden parhaat käytännöt, jotka perustuvat alan standardeihin. Fyysinen turvallisuus sisältää pääsynvalvonnan, hälytysjärjestelmät, kameravalvonnan ja 24/7-paikalla olevat vartijat. Ympäristövalvonta varmistaa, että palvelintilojen lämpötila ja kosteusarvot noudattavat alan standardeja, ja tilat on varustettu palonsammutusjärjestelmillä. Yksityinen runkoverkko mahdollistaa luotettavan tiedonsiirron alueiden välillä. Palvelinkeskusten virransyöttö on myös varmennettu kattavasti. Kaikki sijaintipaikat käyvät läpi perusteellisen riskiarvioinnin, joka huomioi ympäristöuhkat, sähkön saatavuuden, toimittajat, naapurilaitosten toiminnot ja geopolitiikan vaikutukset. Oraclen suvereenin pilven palvelinkeskukset sijaitsevat Saksassa ja Espanjassa.

Lisätietoja:

Datacenters | AWS
https://aws.amazon.com/compliance/data-center/data-centers/

Protect your data | AWS
https://aws.amazon.com/compliance/eu-data-protection/

Data and Security | Google
https://www.google.com/about/datacenters/data-security/

Azure facilities, premises, and physical security | Microsoft
https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

Supplier Information and Physical Security Standards | Oracle
https://www.oracle.com/us/corporate/supplier/oracle-supplier-contractor-security-070672.pdf

Public Cloud Regions | Oracle
https://www.oracle.com/uk/cloud/public-cloud-regions/

Ratkaisun analyysi

Palvelutoimittajat jakavat yleisellä tasolla hyvin paljon tietoa niistä keinoista ja menetelmistä, joilla he varmistavat konesalien fyysisen turvallisuuden. Lisäksi konesalien fyysinen turvallisuus on keskeinen elementti toimittajakohtaisissa täsmennyksissä mainituissa sertifioinneissa. Tietosuojan näkökulmasta loppukäyttäjäorganisaation on arvioitava luottaako se palvelutoimittajan (zero-trust) ympäristöön ja niihin organisatorisiin menetelmiin, joilla palvelutoimittajat varmistavat, että palvelinten datakerrokseen ei kohdistu luvatonta pääsyä. Loppukäyttäjäorganisaatio voi paikata luottamusvajetta omien salausavainten käytöllä varmistaakseen tietojen suojatun säilymisen palveluntarjoajan infrastruktuurissa. Mitä tulee muihin palvelinkeskusten fyysisen turvallisuuden kerroksiin, palvelutoimittajilla on resurssit ja teknologia ylläpitää modernia suojattua turvallisuusympäristöä.

5.9 Palveludatan käsittely ja suojaaminen

Palveludatalla tarkoitetaan kaikkia niitä tietoja, joita palvelu kerää itsenäisesti tai generoi, kun sitä käytetään. Jokaisella palvelutoimittajalla on oma määritelmänsä palveludatalle ja vähintään osaan kerätystä tiedosta palvelutoimittajat määrittävät itsensä rekisterinpitäjäksi. Rekisterinpitäjän määrityksen myötä, myös EU:n yleisen tietosuoja-asetuksen alaiset rekisterinpitäjälle kuuluvat vastuut hyväksytään. Sopimuksellisesti palvelutoimittajat käsittelevät palveludataa tietosuojailmoituksissaan, erillisenä DPA:sta.

Tiedon käyttötarkoitukset määritellään palvelutoimittajien tietosuojailmoituksissa, joskin tietosuojailmoitukset on laadittu koko palveluvalikoiman ja kaiken sen tiedon osalta, johon palvelutoimittaja määrittelee itsensä rekisterinpitäjäksi. Diagnostiikka- ja telemetriatiedon lisäksi tietosuojailmoitukset pitävät sisällään palvelutilin luomiseen ja laskutukseen vaadittavat tiedot, mikä hämärtää henkilötietojen käytettävyyttä rekisteröidyn näkökulmasta.

Toimittajakohtaiset täsmennykset

AWS

AWS:n palveludata on osa ”metadataa”.

Google

Googlen terminologiassa palveludata on ”service dataa”.

Microsoft

Microsoft kutsuu palveludataa nimellä ”service generated data”.

Microsoft on palvelutoimittajista ainoa, joka pseudonymisoi palveludatan henkilötiedon. Muut toimittajat ainoastaan salaavat sen. Microsoft on ilmoittanut suorittavansa palveludatan henkilötietojen summaukset liiketoiminnallisiin tarpeisiin EU-alueen sisältä 1.1.2024 alkaen.

Oracle

Oracle ei ole selvittänyt palveludatan käsittelyä ja siirtoja kolmansiin maihin käyttötapauskohtaisesti. Oraclen suvereenin pilven kohdalla loppukäyttäjäorganisaation on vaikea arvioida palveludataan liittyviä riskejä.

Lisätietoja:

Privacy Notice | AWS
https://aws.amazon.com/privacy/

Cloud Privacy Notice | Google
https://cloud.google.com/terms/cloud-privacy-notice

Privacy Statement | Microsoft
https://privacy.microsoft.com/en-us/privacystatement

Services Privacy Policy | Oracle
https://www.oracle.com/legal/privacy/services-privacy-policy.html

Ratkaisun analyysi

Jotta riskiperusteista arviota voidaan suorittaa, tulee palvelussa liikkuvaa henkilötietoa jakaa tarkemmalla tasolla eri kategorioihin käyttötapausperusteisesti. Yleisellä tasolla palveludata on tietoa, jota alustapalvelut luovat ja keräävät, kun palvelua käytetään. Palveludatan keräämistä ei voida julkisissa pilvipalveluissa välttää, sillä palvelut vaativat dataa toimiakseen ja esimerkiksi vastatakseen tietoturvauhkiin. Minimointi periaatteen (EU:n yleinen tietosuoja-asetus art. 5) mukaisesti kerättäviä henkilötietoja tulee kuitenkin minimoida siten, että tietojen keruu on palvelun toiminnan kannalta välttämätöntä ja kerättävät tiedot poistetaan järjestelmistä heti, kun niitä ei enää tarvita.

Käyttötapausperusteisesti palveludata voidaan jakaa seuraaviin kategorioihin:

- Diagnostiikka- ja telemetrinen data
- Laskutustiedot ja palvelutilin hallintaan vaadittavat tiedot
- Metriikat
- Konfigurointidata
- Liiketoiminnallisiin tarpeisiin kerättävä data

Rekisterinpitäjinä palvelutoimittajat varaavat oikeuden siirtää palveludataa ETA-alueen ulkopuolelle. Rekisterinpitäjinä palvelutoimittajat varaavat oikeuden siirtää palveludataa ETA-alueen ulkopuolelle. Telemetriikan ja diagnostiikkatietojen osalta kyseessä on pääosin IP- ja laitetietoja, jotka EU:n yleisen tietosuoja-asetuksen mukaisesti ovat osa henkilötietoja silloin, kun ne mahdollistavat rekisteröidyn tunnistamisen. Lähtökohtaisesti palvelutoimittajat pyrkivät käsittelemään diagnostiikka- ja telemetristä tietoa lähellä käyttäjän sijaintia, sillä IP- ja laitetietoja sisältävät tietomassat ovat suuria ja niiden siirtely vaatii huomattavaa kapasiteettia. Ennen kaikkea globaalien palvelujen luonteen vuoksi palvelutoimittajat eivät ole halukkaita sitoutumaan telemetrisen tiedon prosessointiin ETA-alueen sisällä.

Lisäksi laskutus- ja organisaatioiden tilien hallinta hoidetaan kaikkien palvelutoimittajien osalta ETA-alueen ulkopuolelta.

Palveludata on aina suojattua säilöttäessä (at rest) ja siirrettäessä (in transit). Yleisesti käytetyin salausalgoritmi on AES-256, mutta myös AES-128 käyttöä esiintyy. Suojausten takia palvelutoimittajat tulkitsevat täyttävänsä GDPR:n vaatimukset riittävästä suojauksesta tiedonsiirroille. Palvelutoimittajat hyödyntävät kapasiteetti ja IP-tietoja summatussa muodossa, sisäiseen raportointiin, palveluiden kehitykseen ja kapasiteettitarpeen suunnitteluun, mutta tämä tieto ei ole identifioitavissa yksittäiseen käyttäjään.

Palveludatan osalta jäännösriskiä tietojen siirrolle ETA-alueen ulkopuolelle ei voida poistaa, sillä palvelutoimittajat (CSP) määrittelevät näiden tietojen osalta itsensä rekisterinpitäjiksi. Näin ollen ne myös vastaavat tietojen siirron turvallisuudesta ja tarpeellisuudesta. Vaikka EU:n yleisen tietosuoja-asetuksen alaiset vastuut siirtyvät palvelutoimittajalle (CSP), asiakasorganisaation (CSC) tulee riskien arvioinnissaan varmistua, että perusteet henkilötietojen keräämiselle ovat lainmukaiset. Vuoropuheluiden perusteella perusteet liittyvät palveluiden toimittamiseen ja tietoturvalliseen käyttöön, joskin sopimustekstejä tulkitsemalla käyttötarkoituksia ei ole rajattu pelkästään näihin tarkoituksiin.

Sopimustekstien tulkintaa hämärtää palvelutoimittajien tapa käsitellä kaikkia käyttötapauksia saman sopimuksen sisällä. Diagnostiikka- ja telemetriatietojen osalta se tarkoittaa, että yleisissä tietosuojasopimuksissa käsitellään kaikkia käyttötapauksia, joissa prosessoija (CSP) ottaa oikeuden toimia rekisterinpitäjänä mukaan lukien tili- ja laskutietojen käsittely, joiden osalta rekisteröidyn henkilötietoriski rajoittuu tilin hallinnasta vastaavaan. Joka tapauksessa asiakasorganisaation (CSC) tulee arvioida palveludatan tietosuojariskin tasoa ja todennäköisyyttä. Riskin arvioinnissa on huomioitava, että telemetriikka ja diagnostiikkatiedot rajoittuvat vahvasti IP- ja laitetietoihin ja laskutus- ja tilien hallintaan vaadittavat tiedot palvelusta vastaaviin henkilöihin.

5.10 Pilvipalvelun saatavuuden varmistaminen

Saatavuuden varmistaminen takaa, että palvelut ovat jatkuvasti käytettävissä, mikä on elintärkeää toiminnan jatkuvuuden ja asiakastietojen turvallisuuden kannalta. Tietosuojariskit liittyvät pääasiassa palvelun saatavuuden häiriöihin, jotka voivat johtua esimerkiksi tietoturvahyökkäyksistä, teknisistä vioista tai luonnonkatastrofeista. Palvelukatkot voivat johtaa tietojen menetykseen, mikä voi vaarantaa asiakastietoja ja aiheuttaa loppukäyttäjäorganisaatiolle ylimääräisiä selvitystöitä.

Osittain saatavuuden ja jatkuvuuden varmistaminen on loppukäyttäjäorganisaation vastuulla, sillä loppukäyttäjäorganisaatio määrittää sopimuksessaan ne palvelinkeskukset, joista haluaa palvelua tuotettavan. Loppukäyttäjäorganisaation on suunniteltava tietojen maantieteellinen hajauttaminen niin, että tietojen siirrot eivät merkittävästi lisää tietosuojariskejä (tiedot kolmansiin maihin), mutta samalla tietojen varmennusprosessissa on huomioitu huoltovarmuusnäkökulma (varmuuskopioiden maantieteellinen hajautus).

Toimittajakohtaiset täsmennykset

AWS

AWS:llä on Euroopassa 8 palvelinkeskusaluetta (regions), joista se tarjoaa infrastruktuuripalveluita. AWS:n palvelulupaus pyrkii 99,99% käytettävyyteen infrastruktuuripalveluiden osalta, joskin sopimukselliset korvausvelvoitteet eivät takaa 99,99% käytettävyyttä. AWS:llä tarjoaa erilaisia palveluita suorituskyvyn optimointiin ja automaattiseen resurssienhallintaan, kuten AWS Elastic Load Balancing ja AWS Auto Scaling. AWS:n palvelinkeskusten tarkat häiriötiedot ilmoitetaan heidän palvelunsa "Health dashboard":n kautta, jonka käyttö vaatii tunnukset palveluun.

Google

Google panostaa hajautettuun tietojenkäsittelyyn ja monikerroksiseen varmuuskopiointiin. Datan jakamiseen ja replikointiin perustuva lähestymistapa vähentää yhden pisteen vikatilanteiden riskiä, joskin hajautettu tietojenkäsittely nostaa tiedonsiirtojen tietosuojariskiä. Googlella on Euroopassa 12 palvelinkeskusaluetta (regions) ja sen käytettävyysastelupaukset vertautuvat muihin palvelintarjoajiin.

Microsoft

Microsoftilla on Euroopassa tällä hetkellä yhdeksän aluetta Azure-palveluille ja lähitulevaisuudessa se on perustamassa niitä lisää. Microsoft pyrkii siihen, että 99,99% ajasta palvelimella suoritetut asiakastoiminnot onnistuvat. Microsoftin käytettävyysvyöhykkeet (availability zones) ovat riittävän lähellä toisiaan, jotta niillä on matalaviiveiset yhteydet muihin käytettävyysvyöhykkeisiin. Käytettävyysvyöhykkeet on yhdistetty tehokkaalla verkolla, jonka edestakainen latenssi on alle 2 ms. Ne on perustettu kuitenkin riittävän kauaksi toisistaan, jotta vähennetään todennäköisyyttä, että paikalliset käyttökatkot tai sää vaikuttavat useampaan kuin yhteen vyöhykkeeseen. Saatavuusvyöhykkeillä on itsenäinen teho-, jäähdytys- ja verkkoinfrastruktuuri.

Oracle

Oraclen suvereenin pilven palvelukeskukset sijaitsevat Saksassa ja Espanjassa. Suvereeni pilvi on arkkitehtuurillisesti fyysisesti ja loogisesti eriytetty Oraclen muista pilvialueista, mikä vähentää EU-alueen ulkopuolelta tulevien hyökkäysten riskiä. Oracle antaa SLA:t OCI-palveluilleen saatavuudesta, käytettävyydestä ja suorituskyvystä. Oraclen palvelinkeskusten status ja häiriöt ilmoitetaan heidän palvelunsa konsolin kautta, jonka käyttö vaatii tunnukset palveluun.

Lisätietoja:

Service health | AWS
https://health.aws.amazon.com/health/status

Composite availability: calculating the overall availability of cloud infrastructure | Google
https://cloud.google.com/blog/products/devops-sre/composite-cloud-availability

Service Health | Google
https://status.cloud.google.com/regional/europe

Azure Status | Microsoft
https://azure.status.microsoft/en-us/status

What are availability zones? | Microsoft
https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview

System Status | Oracle
https://docs.oracle.com/en-us/iaas/Content/General/Concepts/status-service.htm

Oracle Cloud Infrastructure Service Level Agreement (SLA) | Oracle
https://www.oracle.com/cloud/sla/

5.11 Pilvipalvelun turvallisuuden seuranta

Palvelutoimittajat tarjoavat käyttäjilleen erilaisia lokituspalveluita ja SIEM-ratkaisuja, jotka auttavat ratkaisemaan valvontaan liittyviä haasteita. Kouluttamalla henkilökuntaa lokitietojen tulkintaan ja hyödyntämällä automaattisia valvontajärjestelmiä voidaan parantaa valmiutta reagoida nopeasti epäilyttäviin toimintoihin. Lokitus- ja monitorointipalveluiden lisäksi oikeaoppisen pääsyn- ja käyttöoikeuksienhallinnan avulla voidaan lisätä palvelun turvallista käyttöä. Roolipohjaisten käyttöoikeuksien hallinnan (RBAC) avulla voidaan ehkäistä pääsynhallinnan monimutkaisuuden luomaa tietosuoja- ja tietoturvariskiä.

Toimittajakohtaiset täsmennykset

AWS

AWS:n infrastruktuurissa asiakkaat voivat ottaa käyttöön CloudTrail-palvelun lokien jatkuvaan seurantaan ja tallentamiseen AWS-infrastruktuurin toimiin liittyviin tilitoimintoihin. AWS ylläpitää lokeja metatietojen käytöstä ja tarjoaa niihin läpinäkyvyyden CloudTrailin kautta. AWS soveltaa kontrolleja, jotka on validoitu ISO 27701:n ja C5:2020:n sertifikaattien mukaisesti. CloudTrailin osalta asiakas ei saa oikeuksia AWS:n generoimiin alkuperäisiin lokitietoihin, vaan asiakkaalle tarjotaan kahdennus alkuperäisistä lokitiedoista.

Google

Google kirjaa pääsyt CSC:n ympäristöön Cloud Audit -lokien ja Access Transparency -lokien kautta. Cloud Audit -lokit tarjoavat tietoja hallinnollisista toiminnoista ja käyttöoikeuksista. Tarkastuslokien käyttöönottaminen auttaa valvomaan tietoturvaa ja vaatimustenmukaisuutta. Access Transparency -lokit tarjoavat rekisteröivät tiedot toimista, joita Googlen henkilökunta on suorittanut asiakasympäristöissä. Kaikki diagnostiikkatietojen käyttö tallennetaan Access Transparency -lokien kautta. Google salaa käyttäjien laitteiden ja Google Front Endin (GFE) välisen liikenteen vahvoilla salausprotokollilla, kuten TLS:llä.

Microsoft

Microsoftin pilvipalvelut tarjoavat auditointilokin jokaisesta palvelusta. Tarkastuslokia voidaan käyttää Azure-pilvessä tai se voidaan toimittaa asiakkaan valitsemiin SIEM-ratkaisuihin (Security Information and Event Management) tai käyttää Microsoft SIEM -ratkaisuissa, kuten Sentinel. Microsoft ylläpitää tietojenkäsittelystä EU:n yleisen tietosuoja-asetuksen edellyttämiä tietueita ja toimittaa ne tietosuojaviranomaisille pyynnöstä artiklan 30 edellyttämällä tavalla.

Oracle

Oracle kirjaa tietoturvaan liittyviä tapahtumia käyttöjärjestelmissä, sovelluksissa, tietokannoissa, virtuaalikoneissa ja verkkolaitteissa. Järjestelmät on konfiguroitu lokittamaan kirjautumiset Oraclen järjestelmiin, järjestelmähälytykset, konsoliviestit ja järjestelmävirheet. Oracle tarkastaa lokit tietoteknisiä tutkimuksia ja häiriötilanteita varten, ja havaitut poikkeavuudet syötetään tietoturvahäiriöiden hallintaprosessiin. Pääsy turvallisuuslokiin sallitaan tarpeen mukaan ja vähimmäisvaltuuksin.

Lokitiedostot suojataan vahvalla salakirjoituksella ja pääsyä valvotaan. Internetiin liittyvien järjestelmien tuottamat lokitiedostot siirretään järjestelmiin, jotka eivät ole internet-yhteyden ulottuvilla. Yleisesti ottaen Oracle Cloud Operationin sisäisesti luomat diagnostiikkalokit eivät ole saatavilla asiakkaille. Asiakkaalla on mahdollisuus tehdä häiriö-/tietoturvatapauksen palvelupyyntö tukipalveluille ja pyytää juurisyyanalyysiä, mukaan lukien näkymää turvallisuuslokeihin.

Lisätietoja:

CloudTrail | AWS
https://aws.amazon.com/cloudtrail/

Cloud Audit Logs overview | Google
https://cloud.google.com/logging/docs/audit

Access Transparency | Google
https://cloud.google.com/assured-workloads/access-transparency/docs/overview

Overview of Access Approval | Google
https://cloud.google.com/assured-workloads/access-approval/docs/overview

Google security overview | Google
https://cloud.google.com/docs/security/overview/whitepaper

Trusting your data with Google Cloud | Google
https://services.google.com/fh/files/misc/072022_google_cloud_trust_whitepaper.pdf

Overview of Azure platform logs | Microsoft
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/platform-logs-overview

Azure Monitor Logs overview | Microsoft
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs

Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Applications | Oracle
https://www.oracle.com/a/ocom/docs/caiq-oracle-cloud-applications.pdf

Ratkaisun analyysi

Palvelutoimittajat operoivat poikkeuksetta zero-trust ympäristössä, jossa käytössä on vahva tunnistautuminen ja roolipohjaiset pääsynrajoitukset. Henkilöstöllä ei ole lähtökohtaisesti automaattista pääsyä asiakastietoihin, vaan päästäkseen tietoihin henkilöstön on käytettävä luotettavaa laitetta ja monivaiheista tunnistautumista.

Palvelutoimittajat kirjaavat asiakkaiden tietoihin pääsyn ja hyödyntävät lisäksi älykkäitä uhkien havaitsemisjärjestelmiä. Ne tekevät tarkastuksia sekä tuottavat hälytyksiä erilaisten indikaattoreiden perusteella. Nämä organisatoriset kontrollit vaativat asiakkaan luottamusta, sillä rekisterinpitäjällä on hyvin vähän mahdollisuuksia itse todentaa niiden toimivuus muuten kuin toimittajille annettujen sertifikaattien avulla. Asiakkaalla on tosin mahdollisuus hallita ja hyödyntää omia salausavaimia palveluissa käyttäen ulkoisia avaintenhallintajärjestelmiä.

Asiakkaalla on mahdollisuus hyödyntää myös luottamuksellista tietojenkäsittelyä (confidential computing) palvelutoimittajien ympäristössä. Se mahdollistaa loppuun asti salattujen työkuormien (workloads) käsittelyn valituissa palveluissa suojaten dataa luvattomalta pääsyltä säilytyksessä, siirrossa ja käytössä. On huomioitava, että luottamuksellisen tietojenkäsittelyn teknologia on monimutkaista ja kallista.

Lisätietoja:

What is Confidential Computing? | The Confidential Computing Consortium
https://confidentialcomputing.io/about/

5.12 Häiriötilanteiden hallinta

Poikkeamienhallinnan (Incident Management, IM) sekä niihin vastaamisen (Incident Response, IR) prosessit ovat keskiössä pilvipalveluiden häiriötilanteiden hallinnassa. Tämän selvityksen tavoitteena oli löytää pilvipalvelutoimittajien osalta ne prosessit ja kuvaukset, jotka:

- Tarjoavat ohjeistuksen häiriötilanteen toiminnalle
- Takaavat henkilötiedon luottamuksellisuuden myös poikkeustilanteissa
- Määrittelevät henkilötietoon kohdistuneen poikkeaman EU:n yleisen tietosuoja-asetuksen (art. 4) mukaisesti.
- Varmistavat asiakkaiden ajantasaisen näkymän palveluiden tilaan häiriötilanteen aikana.

Kaikkien palveluntarjoajien määritelmät henkilötietoon kohdistuneesta häiriötilanteesta ovat linjassa tietosuoja-asetuksen kanssa. Häiriötilanteiden kannalta on otettava huomioon jaetun vastuun malli

pilvipalveluissa. Tässä luvussa käsitellään palveluntarjoajan ympäristön häiriötilanteita. Palveluntarjoajat eivät ole vastuussa, mutta tarjoavat ohjeita asiakkaan omien sovellusten häiriötilanteiden varalta.

Toimittajakohtaiset täsmennykset

AWS

AWS ilmoittaa asiakkaalle viipymättä tietoturvapoikkeamasta, sekä käsittelee poikkeaman ja sen vaikutukset. AWS tekee yhteistyötä ja avustaa asiakasta poikkeaman ilmoittamisessa viranomaisille, liittämällä ilmoitukseen tiedot, jotka se saa ilmoittaa asiakkaalle. Tämä tarkoittaa, että muiden asiakkaiden tietoja ei luovuteta ilmoituksen yhteydessä. AWS:llä on viralliset IR-prosessit, jotka on auditoitu mm. ISO 22301, ISO 27001, ISO 27017, ISO 27018, SOC1, SOPC2 ja C5. AWS tarjoaa myös materiaalia asiakkaan oman häiriötilanteen hallintaan.

Google

Google priorisoi asiakkaisiin kohdistuvien tietoturvapoikkeamien selvittämisen. Googlella on viralliset prosessit tietoturvapoikkeamien hallinnoimiselle. Häiriötilanteiden hallintaohjelma on rakennettu NIST SP 800-61 mukaisesti.

Microsoft

Microsoft ilmoittaa asiakkaan sisältöön kohdistuneesta tietoturvapoikkeamasta viipymättä, sekä käsittelee poikkeaman vaikutukset. Ilmoituksen yhteydessä kerrotaan poikkeuksen syy, sekä asiakkaan tehtävät korjaavat toimenpiteet. Microsoft pyrkii auttamaan asiakasta täyttämään GDPR art. 33 mukaisen velvollisuuden ilmoittaa viranomaisille kyseisestä tietoturvapoikkeamasta. Microsoft tukee asiakasta täyttämään EU:n yleisen tietosuoja-asetuksen art.33 mukaisen velvollisuuden tietoturvapoikkeamasta ilmoittamisesta viranomaisille. Myös Azuren IR-prosessit on auditoitu.

On syytä huomata, että Azuren asiakkaat ovat velvoitettuja ilmoittamaan Azurelle mahdollisista tietoturvapoikkeamista. Poikkeamien tunnistaminen perustuu sekä ihmisten huomioihin että automatisoituihin järjestelmiin.

Azure päättää itse, mitä kanavaa pitkin asiakkaalle ilmoitetaan. On asiakkaan vastuulla ylläpitää yhteystietojaan siten, että palveluntarjoajan ilmoitukset saapuvat perille.

Oracle

Oracle ilmoittaa asiakkaalle tietoturvapoikkeamasta viipymättä, mutta kuitenkin korkeintaan 24 tunnin sisällä poikkeaman huomaamisesta. Prosessi on kuvattu hyvin niukasti.

Häiriötilanteiden statusta ja palveluiden saatavuutta voidaan seurata OCI-Support Center -konsolilta ja Oraclen sivujen kautta.

Lisätietoja:

Security Incident Response Guide | AWS
https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.html

Data incident response process | Google
https://cloud.google.com/docs/security/incident-response

Microsoft Products and Services Data Protection Addendum (DPA) | Microsoft
https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1

Support and Incident Management | Oracle
https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/support-incident-management.htm

System Status | Oracle
https://ocistatus.oraclecloud.com

DigiFinland