TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Toimintaohje – Pilviympäristöjen poikkeamanhallinta

Traficomin julkaisuja
18/2023

Sisällysluettelo

Johdon yhteenveto

Pilvipalveluiden käyttö on monissa organisaatioissa osa normaalia toimintaa. Pilvipalveluita hyödynnetään liiketoiminnalle tärkeissä ja jopa liiketoimintakriittisissä prosesseissa. Näiden pilvipalveluiden luotettava ja tietoturvallinen toiminta on monissa organisaatioissa edellytys päivittäiselle liiketoiminnalle ja sen sujuvalle jatkumiselle.

Tietoturvan ylläpito vaatii kuitenkin jatkuvaa tekemistä ja toiminnan kehittämistä. Tässä ohjeessa kerrotaan, miten organisaatiot voivat varautua pilvipalveluita koskeviin tietoturvapoikkeamiin, sekä toimimaan tilanteissa, jossa epäillään pilviympäristöön kohdistunutta tietoturvapoikkeamaa.

Keskeisiä asioita ovat erityisesti seuraavat:

1. Tietoturva palveluita hankittaessa

Mikäli olette hankkimassa uusia pilvipalveluita, varmistakaa, että palvelun tietoturvallisuuteen kiinnitetään riittävästi huomiota jo hankintavaiheessa. Pilvipalveluita hyödynnettäessä on mahdollisuus tehdä tietoturvaltaan hyvätasoisia ratkaisuja helpommin ja usein edullisemmin kuin konesalissa. Tämä edellyttää riittävää osaamista myös asiakkaalta.

2. Jaetun vastuun malli eri palvelutyypeissä

Erityisesti IaaS- ja PaaS-mallisissa pilvipalveluissa iso osa palvelun tietoturvavastuusta on sitä käyttävän organisaation vastuulla. Näiden palveluiden ylläpidon osalta on hyvin tärkeä varmistaa, että organisaation käytössä olevat ylläpidon resurssit ovat riittävät ja että heidän osaamiseensa tietoturvan osalta on riittävällä tasolla. Pilvipalveluiden tietoturvassa vaaditaan nimenomaan näiden palveluiden erityisosaamista. Moni tietoturvapoikkeama saa alkunsa virheellisesti konfiguroidusta palvelusta, tai muutoksesta, jolla konfiguraatio muuttuu vähemmän tietoturvalliseksi. Virheiden mahdollisuus pienenee, kun varmistetaan, että konfiguraatioista vastaavilla henkilöillä on asiaan tarvittava osaaminen.

3. Monivaiheinen tunnistautuminen

Pilvipalveluiden suojaamiseen kannattaa panostaa. Perusasioihin kuuluu, että palveluihin ei ole mahdollista kirjautua pelkällä käyttäjätunnuksen ja salasanan yhdistelmällä. Varmistakaa, että monivaiheinen tunnistautuminen on käytössä kaikissa pilvipalveluissanne, kaikille käyttäjäryhmille.

4. Poikkeamatilanteiden harjoittelu

Poikkeamatilanteisiin tulee varautua. Vaikka tietoturvaan panostettaisiin huomattavasti, on poikkeamatilanne aina mahdollinen. Poikkeamatilanteisiin liittyvien suunnitelmien tekeminen ja poikkeamatilanteiden harjoittelu antavat varmuutta, mikäli oikea tilanne joskus tapahtuu.

5. Varautumisen toimenpiteet

Poikkeamatilanteilla on pääsääntöisesti tietynlainen elinkaari, joka sisältää erilaisia vaiheita. Vaiheet ja niihin liittyvät keskeiset tehtävät kuvataan tässä ohjeessa. Varmistakaa organisaatiossanne, että teillä on riittävät kyvykkyydet poikkeamanhallintatoimenpiteiden suorittamiseen. Usein nämä toimenpiteet vaativat etukäteen tehtyjä valmisteluja, kuten esimerkiksi riittävän lokituksen käyttöönottoa ja varmuuskopiointiprosessia, jonka toiminta on varmistettu testaamalla.

6. Poikkeamatilanteiden asiantuntija-avun hankkiminen

Mikäli organisaatiossa tapahtuu tietoturvan poikkeamatilanne, sen selvittämisessä saatetaan tarvita asiantuntija-apua. Tällaiseen asiantuntija-apuun liittyvät sopimukset kannattaa tehdä jo etukäteen kaiken varalta.

1 Johdanto

1.1 Ohjeen tarkoitus

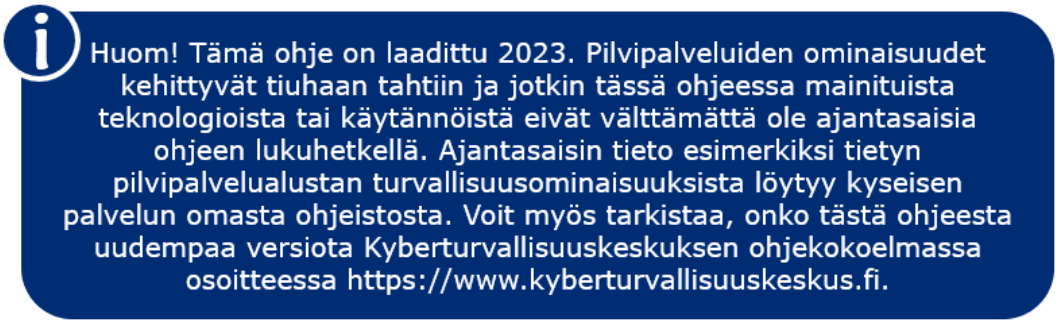
Tämän Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen laatiman ohjeen tavoitteena on neuvoa organisaatioita varautumaan pilvipalveluita koskeviin tietoturvapoikkeamiin, sekä toimimaan tilanteissa, jossa epäillään pilviympäristöön kohdistunutta tietoturvapoikkeamaa. Ohje on tarkoitettu kaikille organisaatioille koosta tai toimialasta riippumatta.

Tämä ohje kattaa tietoturvapoikkeaman elinkaaren seuraavat vaiheet:

- Tietoturvapoikkeaman havainnointi – ohje kertoo, miten pilviympäristöjen tietoturvapoikkeamia voidaan havaita.
- Poikkeamatilanteessa toimiminen – ohje kattaa keskeiset toimet, joita organisaation tulisi tehdä poikkeamatilanteessa.
- Poikkeamasta palautuminen – ohje kuvaa, miten pilven tietoturvapoikkeamasta voidaan palautua takaisin liiketoimintaan.

Ohje on osa Kyberturvallisuuskeskuksen ohjesarjaa, joka kuvaa erityyppisistä tietoturvapoikkeamatilanteista toipumista. Muista kuin pilviympäristöihin liittyvistä poikkeamista palautumisesta kerrotaan ohjesarjan muissa osissa, jotka löytyvät Kyberturvallisuuskeskuksen verkkosivuilta.

Pilvipalvelujen turvallisuudesta yleisesti kerrotaan julkaisussa Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille[1]. Huoltovarmuuskeskus on julkaissut oppaan yrityspäättäjille, jotka harkitsevat pilvipalveluiden käyttöönottoa tai käytön laajentamista kriittisiin toimintoihin[2].



1.2 Mitä tarkoittaa pilviympäristön tietoturvapoikkeama?

Tietoturvapoikkeamat ovat odottamattomia tai ei-toivottuja tapahtumia tai tapahtumasarjoja, joissa suojattavien tietojen tai palveluiden turvallisuus vaarantuu. Tässä ohjeessa määrittelemme pilviympäristön tietoturvapoikkeaman turvallisuuspoikkeamaksi, jossa vaarantunut tieto on tallennettu pilvipalveluun tai turvallisuustapahtuman kohteena oleva palvelu on pilvipalvelu.

Pilvipalveluilla tarkoitetaan sellaisia asiakkaan käyttämiä tietotekniikkasovelluksia tai alustapalveluita, jotka tuotetaan palveluntarjoajan laiteympäristöstä, käytetään tietoliikenneverkon yli, ja joiden tekniset yksityiskohdat ovat joiltakin osin

[1] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohjeita-pilvipalvelujen-turvallisuudesta-yksityishenkiloille-pienyhteisoille-ja
[2] https://www.huoltovarmuuskeskus.fi/files/dfd001d3135a6a37876a5afe88ba2a816156e8ae/huoltovarmuutta-pilvipalveluilla-230306.pdf

palveluntarjoajan vastuulla ja peitetty asiakkaalta. Asiakkaan näkökulmasta pilviresurssit ovat aina saatavilla, niitä on helppo skaalata kulloiseenkin tarpeeseen sopiviksi ja hinnoittelu perustuu yleensä käyttöön. Pilvipalvelut eivät edellytä asiakkaalta investointeja laitteisiin tai pitkäaikaista sitoutumista tilaukseen.

Pilviympäristöissä esiintyy erilaisia tietoturvapoikkeamia, joiden tyypillisiä juurisyitä ovat:

- Heikot tai vuotaneet käyttäjätunnus- ja salasanatiedot, tai muut salaisuudet, joiden avulla luvaton taho voi saada pääsyn pilvessä sijaitseviin tietoihin ja palveluihin. Erityisesti tähän on riski silloin, kun käytössä ei ole monivaiheista tunnistamista (MFA) tai kun salaisuuksia kuten pääsyavaimia (engl. access key) on käsitelty huolimattomasti, vaikkapa osana ohjelmiston lähdekoodeja.
- Pilviympäristön oletuskonfiguraatioiden käyttö, joka johtaa tietojen, toimintojen tai sovellusten ajateltua laajempaan näkyvyyteen julkisessa verkossa.
- Aiemmin käytössä olleiden hyvien tietoturva-asetusten höllentäminen, jolloin palveluissa avautuu odottamaton mahdollisuus verkkorikolliselle.
- Asiakkaan työkuormassa, kuten virtuaalikoneessa tai kontissa oleva haavoittuvuus.

Edellä kuvatut tilanteet ovat vältettävissä hyvällä pilven käytön asiantuntemuksella, toimivalla konfiguraatio- ja muutoshallinnalla, sekä tietoturvahaavoittuvuuksien aktiivisella seurannalla.

Euroopan unionin kyberturvallisuusvirasto ENISA[3] on arvioinut, että hyökkääjät kohdistavat hyökkäyksiä pilviympäristöihin muun muassa seuraavilla tavoilla:

- käyttämällä hyväkseen pilviympäristön haavoittuvuuksia
- pyrkimällä sosiaalisen hakkeroinnin keinoin saamaan tietoonsa pilviympäristöjen valtuustietoja (eng. credentials)
- käyttämällä hyväkseen virheellisesti konfiguroituja konttimäärittelyitä
- pyrkimällä saamaan jalansijan pilvi-infrastruktuurista, rajapinnoista tai pilvessä sijaitsevista varmuuskopioista.

1.3 Pilviympäristöjen erityispiirteet poikkeamanhallinnan kannalta

Pilviympäristöjen tietoturvapoikkeamilla on muutamia erityispiirteitä. Pilvipalveluiden asiakkaiden on hyvä huomioida nämä erityispiirteet, jotta he voivat poikkeamatilanteessa toimia mahdollisimman tehokkaasti.

1.3.1 Näkyvyys palveluntarjoajan prosesseihin

Pilvipalvelun käyttö on ulkoistus, jossa asiakas antaa palveluntoimittajan hoidettavaksi hankittavan palvelun kehittämisen ja ylläpidon kokonaan tai osittain. On hyvä tiedostaa, että päätös pilvipalvelun käyttöönotosta on samalla päätös luottaa pilvipalveluntarjoajaan ja sen tarjoamien palveluiden tietoturvan tasoon.

Pilvipalveluihin liittyy vastuunjakoa koskevia sopimusehtoja, jotka asettavat rajoja näkyvyydelle palveluntarjoajan prosesseihin tai mahdollisuutta aktiiviseen yhteistyöhön. Tietoturvanäkökulmasta katsottuna tämä tarkoittaa, että kun asiakasorganisaatio on valitsemassa käyttöönsä pilvipalveluntarjoajaa, organisaation tulisi ennen palvelun hankkimista arvioida tarkkaan palveluntarjoajan

[3] ENISA:n englanninkielinen raportti: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

dokumentaatio, jossa kuvataan käytössä olevat tietoturvaprosessit ja -hallintakeinot, mukaan lukien tietoturvapoikkeamiin liittyvät toimintamallit ja poikkeamatilanteessa saatavilla olevan tuen taso.

On hyvä huomioida, että jotkin pilvipalveluiden tietoturvaominaisuudet voivat olla lisämaksullisia tuotteita, joiden käyttöönotto vaatii sekä investointeja että erityisasiantuntemusta.

1.3.2 Jaetun vastuun malli

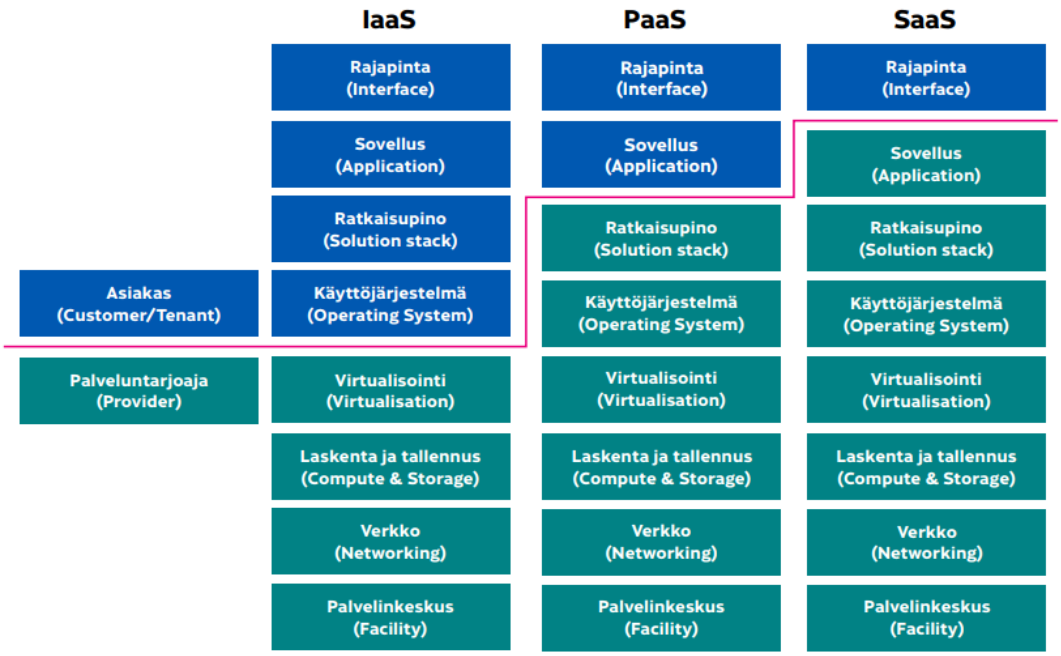
Pilvipalveluntarjoaja ja pilvipalvelun asiakas jakavat aina vastuun palvelun tietoturvallisuudesta. Pilvipalvelun tyyppi (SaaS, PaaS, IaaS) ja palveluntarjoajan kanssa tehty sopimus sekä käytössä olevat palvelut määrittävät, miten vastuut jakautuvat osapuolien välille. Vastuut heijastuvat myös poikkeamatilanteisiin:

Infrastructure-as-a-Service (IaaS): IaaS-mallissa pilvipalveluntarjoaja tarjoaa skaalautuvan IT-infrastruktuurin, josta asiakas ottaa käyttöönsä haluamansa palvelut, esimerkiksi virtuaalikoneita, verkkoyhteyksiä ja tallennuskapasiteettia. Käytännössä palvelut sijaitsevat fyysisesti palveluntarjoajan konesaleissa ja palveluntarjoaja vastaa laitteiston fyysisestä turvallisuudesta. Asiakkaan vastuulla on varmistaa käyttämiensä palveluiden ja tallentamiensa tietojen turvallisuus, mukaan lukien esimerkiksi käyttäjien ja käyttövaltuuksien määrittäminen, pilviresurssien tietoturvan konfigurointi, konttien ja käyttöjärjestelmien haavoituksien hallinta, hyökkäysten havainnointi ja torjunta, palveluiden kahdentaminen sekä riittävä varmuuskopiointi. Tietoturvapoikkeamatilanteessa asiakas on hyvin laajasti vastuussa poikkeaman selvittämisestä ja korjaustoimista, mikäli poikkeama ei koske palveluntarjoajan vastuulla olevia tilaus- ja ylläpitojärjestelmiä tai tuotannon infrastruktuuria.

Platform-as-a-Service (PaaS): PaaS-mallissa pilvipalveluntarjoaja tarjoaa sovellusten kehittämiseen ja julkaisuun tarkoitetun alustan. Asiakas ottaa alustalta käyttöönsä haluamansa palvelut, jotka yleensä sisältävät kehitystyökalujen ja koodin ajoalustan lisäksi tallennus- ja käsittelypalveluita tiedostoille ja datalle. PaaS-mallissa asiakkaan vastuulla on varmistaa kehitysympäristönsä, sovellustensa ja tallentamiensa tietojen turvallisuus sekä palveluiden pääsynhallinta. Tietoturvapoikkeamatilanteessa asiakas on päävastuussa poikkeaman selvittämisestä, mutta pilvipalveluntarjoaja saattaa toimia yhteistyökumppanina.

Software-as-a-Service (SaaS): SaaS-mallissa pilvipalveluntarjoaja tarjoaa asiakkailleen valmiin sovelluksen, jota käytetään yleensä julkisen verkon kautta eli internetyhteydellä. SaaS-mallissa palveluntarjoaja vastaa sovellukseen liittyvän infrastruktuurin ja varsinaisen sovelluksen turvallisuudesta. Asiakas kuitenkin vastaa jossakin määrin sovelluksen käytön aikaisesta turvallisuudesta, esimerkiksi käyttäjien, käyttövaltuuksien ja tunnistusvälineiden hallinnoinnista. Tietoturvapoikkeamatilanteen selvittäminen tapahtuu yhteistyössä pilvipalveluntarjoajan kanssa, sillä asiakkaalle ei todennäköisesti ole pääsyä sovelluksen loki- ja muihin tietoihin, joita tarvitaan poikkeaman selvittämisessä. SaaS-palveluissa voi olla tietoturvaan liittyviä maksullisia lisäominaisuuksia, liittyen esimerkiksi tunnistusvälineisiin, tietojen salaamiseen ja käyttölokien saatavuuteen.

Pilvipalveluiden asiakkaan tulisi aina perehtyä hankittavan palvelun vastuunjakomalliin, jotta vältytään väärinkäsityksiltä ja ikäviltä yllätyksiltä turvallisuuteen ja poikkeamanhallintaan liittyen.



Kuva 1 Tyypillinen vastuunjakomalli. Lähde: Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

1.3.3 Poikkeamanselvitykseen tarvittava erityisosaaminen

Pilviympäristöt saattavat olla monimutkaisia ja sisältää paljon dataa. Lisäksi niihin voi kohdistua jatkuvia muutoksia, mikä tekee poikkeamien selvittämisestä tehtävän, joka vaatii erityisosaamista.

Pilvipalveluiden toimittajat voivat tarjota eritasoisia palvelusopimuksia, jotka vaikuttavat siihen, millaista tukea heiltä on saatavissa poikkeamatilanteissa. Lisäksi asiantuntijapalvelumarkkinalla on erikoistuneita toimittajia, jotka voivat auttaa poikkeamien selvittämisessä ja palautumisessa.

Monissa tapauksissa on hyödyllistä, että organisaatio solmii etukäteen sopimukset sellaisten palveluntarjoajien kanssa, jotka voisivat auttaa poikkeamatilanteessa. Sopimusten solmiminen etukäteen kannattaa, jotta poikkeamatilanteen ollessa päällä aikaa ei tarvitse käyttää sopimusneuvotteluihin.

Organisaation tulee myös varmistaa, että sen oman IT-henkilöstön tiedot ja taidot pilvipalveluiden ja niiden turvallisen käytön suhteen ovat riittävät. Pilviosaamista voidaan kehittää koulutuksilla ja hankkimalla pilvipalveluihin liittyviä ammattisertifikaatteja.

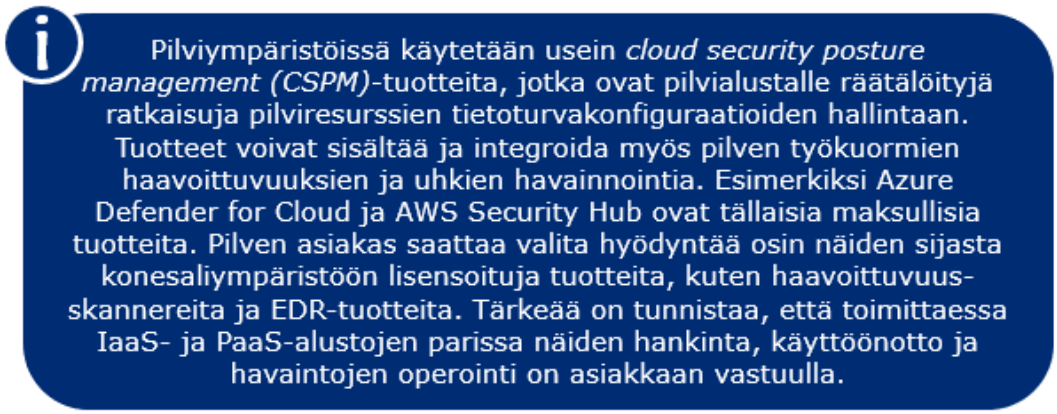
Poikkeamatilanteisiin liittyvää osaamista voi kehittää harjoittelemalla, josta kerrotaan lisää kappaleessa 2.3 Pilviympäristöön liittyvien tietoturvapoikkeamien harjoittelu.

1.3.4 Palvelun tietoturvaominaisuudet voivat riippua sopimuksesta tai lisenssistä

Joissakin pilvipalveluissa voi olla tietoturvaan liittyviä maksullisia lisäominaisuuksia, liittyen esimerkiksi tunnistusvälineisiin, tietojen salaamiseen ja käyttölokien saatavuuteen. Toisaalta pilvipalveluiden käytössä olevat tietoturvaominaisuudet saattavat myös olla sidoksissa siihen, minkälainen lisenssi palveluun on hankittu.

IaaS- ja PaaS-malleissa monet tietoturvateknologiat, joilla saadaan lisätehoja esimerkiksi ympäristön ja tietoturvatapahtumien valvontaan, ovat usein lisämaksullisia.

Pilvipalveluita hankkivan tai käyttävän organisaation tulisi perehtyä palvelun ominaisuuksiin, lisensseihin ja palvelumalleihin voidakseen varmistua siitä, että kokonaisuus täyttää organisaation tietoturvavaatimukset.



1.3.5 Tiedonkeruu poikkeamatilanteessa

Poikkeamatilanteen selvittäminen pilviympäristössä riippuu pitkälti käytössä olevista lokitiedoista. Se, tuottavatko ja keräävätkö palvelut lokitietoja, riippuu palvelusta ja sen konfiguroinnista. Mikäli asiakkaan keräämiä lokeja ei ole, voi tietoturvapoikkeaman osoittaminen toteen olla vaikeaa tai mahdotonta.

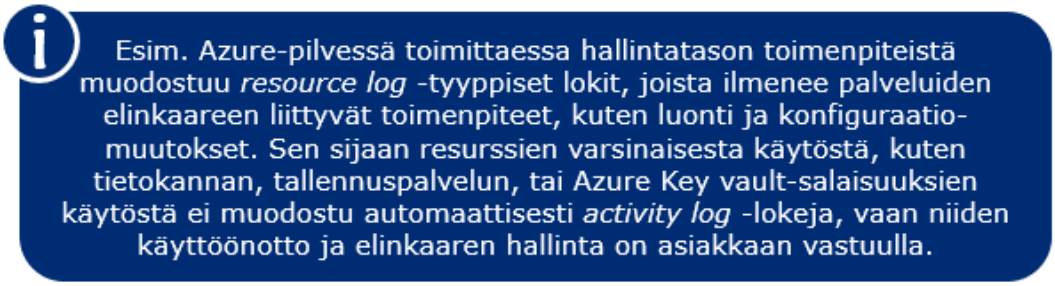
Monet pilvipalvelualustat keräävät lokitietoja IaaS- ja PaaS- palveluista automaattisesti niin sanotulla **hallintatasolla** (engl. ”control plane”, joskus myös ”management plane”). Hallintataso tarkoittaa niitä käyttöliittymiä, työkaluja ja rajapintoja, joita asiakkaan ylläpitohenkilöstö käyttää pilvipalveluiden tilaamiseen ja konfigurointiin. Esimerkiksi uusien palveluiden käyttöönotto ja uusien ylläpitohenkilöiden valtuuttaminen alustalla tallentuu tyypillisesti hallintatason lokiin ilman, että asiakas on huomannut kytkeä tällaista audit-lokia käyttöön.

Lokin tallennusaika vaihtelee, ja sen riittävyys tulee tarkistaa alustapalvelusta. Tallennusaika voi olla esimerkiksi muutamia kuukausia, jolloin pidempään jatkuneen epäillyn väärinkäytöksen tutkinta voi olla hankalaa. Tyypillisesti lokeja on mahdollista säilyttää lisämaksusta oletusta pidempään.

Pilvipalveluita käytetään niin kutsutulla **tieto- tai sovellustasolla** (engl. ”data plane” tai ”application plane”). Tämän tason käyttötapahtumia ovat esimerkiksi kirjautuminen virtuaalikoneeseen, tiedoston lataaminen pilvitallennustilasta, ja tietokantapalvelun dataan liittyvät operaatiot. Tämän tason käyttölokien saatavuus riippuu usein asiakkaan käyttöön ottamista menettelyistä, joita palvelualustat tarjoavat lisämaksua vastaan. Voi olla, että pilvipalvelu ei tuota automaattisesti lokeja näistä tapahtumista lainkaan, vaan niiden käyttöönotto ja lokien hallinnan elinkaari kuuluu asiakkaalle.

SaaS-palveluissa lokitiedot kerätään palveluntarjoajan toimesta. SaaS-palveluita käyttöönottaessa tulee varmistaa, että palveluntarjoajan lokittamiskäytännöt vastaavat organisaation lokittamiselle asettamia vaatimuksia. Esimerkiksi käyttötapahtumien ja epäiltyjen väärinkäytösten tutkinta tulisi olla mahdollista.

Joissakin palveluissa tällaiset lokit voivat olla asiakkaan saatavilla, joissakin muissa ne edellyttävät palveluntarjoajan hakutoimia, ja joskus lokeja ei muodostu lainkaan.



Lokien lisäksi pilvipalvelut saattavat mahdollistaa verkkoliikenteen seurannan (engl. network flow logs), jolloin pilven työkuormien kuten virtuaalikoneiden, konttien ja sovellusten tietoliikenteen analysointi on mahdollista.

1.3.6 DevOps-käytänteet

Nykyaikainen sovelluskehitys perustuu DevOps-käytänteisiin, joissa keskiössä ovat koodi, automaatio ja toistettavuus. Erityisen yleisiä tällaiset automaatiot ovat pilviympäristössä.

Käytännössä tämä tarkoittaa sitä, että asiakkaan osuus pilvipalveluiden käyttöönotosta, konfiguroinnista, tuotantoon otosta ja tuotannon seurannasta on mahdollista automatisoida ja luoda toistettavaksi malliksi. Tämä tekee poikkeamatilanteista palautumisen joustavammaksi. Asiakkaalla voi olla mahdollisuus palauttaa sovellus ja sen tukipalvelut lähdekoodeista ja datan varmuuskopioista joko samaan sijaintipaikkaan, saman pilvipalvelutoimittajan toiseen sijaintipaikkaan tai joskus vähäisillä muutoksilla toisen palvelutoimittajan ympäristöön. Hyvien käytäntöjen mukaan lähdekoodi ei sisällä mitään valtuutustietoja (esim. tunnuksia, avaimia, varmenteita) vaan niitä hallitaan erikseen.

Poikkeamatilanteiden kannalta keskeisiä huomioitavia asioita DevOps-käytänteiden osalta ovat, että lähdekoodin ja data varmuuskopioiden saatavuus on varmistettu. Parhaiten tämä toteutuu siten, että varmuuskopioita on tallennettu erilaisiin palveluihin (esim. tietokanta vs. objektitallennus), ne on suojattu eritasoisilla pääsyoikeuksilla, ja mahdollisuuksien mukaan myös hajautettu omaan konesaliin, saman pilvipalvelun maantieteellisesti eri tallennuspaikkaan, tai kokonaan toiseen pilvipalveluun. Lisää tietoa varmuuskopioinnista on luvussa 2.2.7 Varmista riittävät varmuuskopiointi- ja toipumismenettelyt.

2 Varautuminen

Varautuminen poikkeamiin on keskeinen tapa vähentää poikkeamien vakavuutta ja mahdollistaa nopea toipuminen ja liiketoiminnan jatkuminen. Organisaatio voi arvioida omaa valmiuttaan käyttämällä hyväksi esimerkiksi Kyberturvallisuuskeskuksen Kybermittaria[4]. Etukäteen laadittu poikkeamanhallintasuunnitelma antaa hyvät lähtökohdat toimia, kun poikkeamatilanne tapahtuu. Organisaation tulee myös varmistaa, että toimet kuten käyttäjätunnusten lukitseminen, palvelinten ja päätelaitteiden eristäminen verkosta, sekä verkkoliikenteen rajoittaminen haitallisiin IP-osoitteisiin tai verkkotunnuksiin on teknisesti mahdollista ja henkilöstöltä löytyy tähän myös osaaminen sekä toimintaohjeet.

Lokitietojen kerääminen, kokoaminen ja monitorointi on tärkeää poikkeaman havaitsemiseksi ajoissa. Lokitiedot mahdollistavat myös poikkeaman perusteellisen tutkimisen ja täten nopeuttavat mahdollista ympäristön siivousta sekä palauttamista. Kyberturvallisuuskeskus on laatinut lokitietojen keräämisestä ja käyttämisestä oppaan[5]. Riippuen organisaation käyttämistä järjestelmistä, kattavaan havainnointiin vaaditaan tyypillisesti lisäksi verkko- ja järjestelmätason ratkaisuja.

2.1 Hallinnolliset toimet

Poikkeamatilanteet ovat lähes aina hektisiä tilanteita, jolloin organisaatiossa ollaan kovilla. Tilannetta voi pyrkiä etukäteen helpottamaan tekemällä suunnitelmia ja harjoittelemalla poikkeamatilanteen toimintamalleja. Nämä toimenpiteet varmistavat, että tilanteen ollessa käynnissä poikkeamanhallintaryhmä pystyy keskittymään poikkeaman selvittämiseen, kun tilanteessa tarvittavat keskeiset toimintatavat, vastuut, roolit ja menettelyt ovat jo tuttuja.

2.1.1 Tunne pilvipalvelusi

Ensimmäinen askel varautumisessa on tunnistaa, mitä pilvipalveluita organisaatiolla on käytössään: tyypillinen nykyajan IT-ympäristö koostuu esimerkiksi useista SaaS-palveluista sekä yhdestä tai useammasta pilvialustasta (esim. Azure, AWS tai Google Cloud). Organisaatiolla voi myös olla käytössä niin sanottu monen pilven strategia (engl. multi-cloud), jossa hyödynnetään useamman pilvipalvelualustan palveluita.

Organisaation on hyvä muodostaa käsitys omasta pilvipalvelukokonaisuudestaan ja sen turvallisuudesta selvittämällä esimerkiksi:

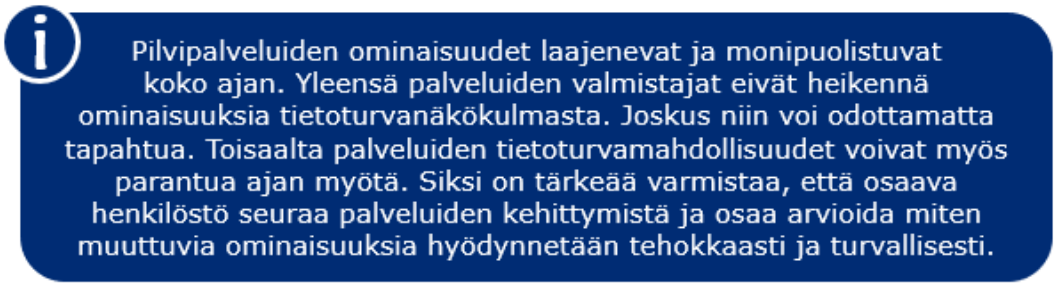
- Mitä pilvipalveluita ja pilvipalveluntarjoajia sillä on käytössä.
- Mitä sopimuksissa ja palveluehdoissa sanotaan turvallisuusvastuiden jakautumisesta palvelua käyttävän organisaation ja pilvipalveluntarjoajan välille (ns. jaetun vastuun malli, kts. luku 1.3.2).
- Mitä tietoja ja tietotyyppejä (esim. asiakastieto, luottamuksellinen tieto) kussakin palvelussa käsitellään. Erityisesti tulee tietää, missä pilvipalveluissa käsitellään tietosuoja-asetuksen piiriin kuuluvaa henkilötietoa.
- Miten pilvipalveluiden käyttöoikeudet on määritelty ja miten varmistetaan, että pääsy on ns. vähimpien oikeuksien periaatteen mukainen.
- Onko erityyppiset ympäristöt (esim. testi ja tuotanto) eroteltu.

[4] https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari
[5] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

- Miten pilven palvelun on segmentoitu verkkotasolla.
- Onko pilvestä avattu yhteyksiä konesaliin.
- Mitä identiteettejä sovellukset ja automaatiot käyttävät, ja millaisia oikeuksia niillä on.
- Millaisia erilaisia pilvipalveluita ja -resursseja on käytössä, ja millaisia ominaisuuksia niillä on tietoturvanäkökulmasta.
- Missä palvelut ja tiedot sijaitsevat (geolokaatio). Onko palvelut kahdennettu useampaan sijaintiin yksittäiseen maantieteelliseen sijaintiin perustuvan riskin pienentämiseksi?
- Miten palveluita ja tietoja suojataan tällä hetkellä kyberuhilta.
- Minkälaisia lokeja palvelut tuottavat, minne ne tallentuvat, ja kuinka pitkään ne ovat saatavilla.
- Miten lokitietojen ja turvallisuustuotteiden poikkeamia ja hälytyksiä monitoroidaan.
- Minkälaiset varmuuskopiointi- ja palautumiskäytännöt on otettu käyttöön kussakin palvelussa.

On hyvä tunnistaa, millaisia riippuvuuksia ja vaikutuksia pilvipalveluilla on muihin palveluihin ja organisaation liiketoimintaan, esimerkiksi:

- Miten tiettyyn pilvipalveluun kohdistuva tietoturvapoikkeama vaikuttaisi organisaation muihin IT-järjestelmiin?
- Miten tiettyyn pilvipalveluun kohdistuva tietoturvapoikkeama vaikuttaisi organisaation liiketoimintaprosesseihin?



2.1.2 Suunnittele ja dokumentoi poikkeamanhallintatoimet

Poikkeamanhallintasuunnitelma: Poikkeamanhallintasuunnitelman laatiminen on hyvä harjoitus, jossa organisaatio pystyy arvioimaan esimerkiksi poikkeamatilanteissa tarvittavia rooleja, viestintäkanavia ja ulkoisia toimijoita (esim. lakipalvelut, kriisiviestintäpalvelut, poikkeaman laajuuden ja vakavuuden selvittäminen) sekä määrittelemään, minkälainen tapahtuma organisaatiossa määritellään poikkeamaksi, joka käynnistää poikkeamanhallintaprosessin. Poikkeamanhallintasuunnitelmassa kuvataan myös päätöksentekoketju, jonka mukaisesti poikkeamatilanteissa toimitaan. Valmis poikkeamanhallintasuunnitelma toimii poikkeamanhallinnan tukirankana ja sen noudattamista on mahdollista harjoitella etukäteen. Poikkeamanhallintasuunnitelman avulla pystytään myös organisaation sisällä avaamaan ja kouluttamaan toimintamallia, jonka mukaan poikkeamatilanteissa toimitaan.

Poikkeamanhallintasuunnitelman lisäksi esimerkiksi seuraava dokumentaatio voi olla hyödyllistä:

Yhteystiedot: Niiden tahojen yhteystiedot, joita tarvitaan poikkeamanhallinnassa (esim. organisaation päätöksentekijät, tekninen tuki, palveluntarjoajien yhteystiedot).

Arkkitehtuuri ja tekninen dokumentaatio: Kuvaukset organisaation pilviympäristöjen arkkitehtuurista ja tekninen dokumentaatio, kuten pilviresurssien konfiguraatiot. Kun käytössä on modernit DevOps-käytänteet, yleensä pilviresurssien konfiguraatiot ovat saatavilla koodina. Automaattinen tekninen dokumentaatio on yleensä mahdollista muodostaa myös lataamalla SaaS- ja PaaS-komponenttien konfiguraatio pilvestä. Näin kannattaa toimia aina muutosten jälkeen, mikäli muutoksia ei toteuteta koodilla ja DevOps-automaatiolla.

Tietoinventaari: Tietoinventaarin tai vastaava dokumentaation avulla voidaan selvittää, missä järjestelmissä tai tallennuspaikoissa on henkilötietoa. Tätä tietoa tarvitaan poikkeaman vaikutusten selvittämisessä ja tietoturvaloukkauksen tunnistamisessa.

Poikkeamanhallintaan liittyvät toimintaohjeet: ohjeistus esimerkiksi siitä, miten poikkeamanhallinnassa voidaan toteuttaa teknisiä toimenpiteitä, kuten eristää laitteita, kerätä todistusaineistoa tai palauttaa tiedot varmuuskopioilta. Teknisiin selvitys- ja palauttamistoimenpiteisiin sisältyy usein muun muassa rooleihin, vastuisiin ja velvollisuuksiin liittyviä hallinnollisia elementtejä, mikä on yksi tärkeä syy suunnitella ja dokumentoida nämä menettelyt etukäteen. Esimerkiksi lokitietojen keräämiseen ja käsittelyyn liittyy lainsäädännöllisiä velvoitteita. Jotta tällaiset velvollisuudet pystytään huomioimaan riittävällä tasolla poikkeamatilanteessa toimittaessa, toimet tulee suunnitella ja dokumentoida etukäteen. Huomioi myös, että toimintaohjeiden tulee olla linjassa poikkeamanhallintasuunnitelman kanssa, niin että esimerkiksi päätöksentekoketju vastaa sitä, mitä poikkeamanhallintasuunnitelmassa on määritelty.

Poikkeamanhallintalokin mallipohja: pohja, johon kirjataan poikkeaman tapahtumaloki. Vähintään tulee etukäteen sopia, mitä järjestelmää tai tallennuspaikkaa poikkeamatilanteessa käytetään tapahtumalokin kirjaamiseen ja ylläpitoon ja varmistaa, että tiedon suojaamiseen on käytössä riittävät menettelyt.

Poikkeamanhallinnan ja pilviympäristöjen turvallisuuden vuosikellot: Sekä poikkeamanhallintatoimet että tietoturvallisuus kokonaisuudessaan ovat prosesseja, joita on ylläpidettävä ja kehitettävä säännöllisesti. Varmista, että esimerkiksi poikkeamanhallintasuunnitelman päivittäminen, poikkeamatilanteiden harjoittelu ja pilvialustojen parhaiden turvallisuuskäytäntöjen katselmointi ovat mukana organisaation vuosikellossa.

2.1.3 Määrittele poikkeamanhallinnan roolit ja vastuut

Varmista, että organisaatiollasi on ajantasainen poikkeamanhallintasuunnitelma, jossa on sovittu poikkeamatilanteisiin liittyvät roolit ja vastuut.

Poikkeamatilanne vaatii yhteistyötä organisaation eri tahojen välillä. Poikkeamatilanteessa muodostetaan niin sanottu poikkeamanhallintaryhmä, jossa tulisi olla vähintään yksi johtoa edustava henkilö ja yksi tekninen osaaja. Mikäli mahdollista, ryhmässä tulisi myös olla viestinnän ja lainsäädännön osaajia sekä poikkeamanselvityksen vaatimaa teknistä asiantuntijuutta. Tietoturvapoikkeamiin liittyviä tehtävärooleja ja niiden vastuita kuvataan esimerkiksi Valtiovarainministeriön ohjeessa Tietoturvapoikkeamatilanteiden hallinnasta[6]. Mikäli organisaatiolla ei ole käytössään em. resursseja, organisaatio voi harkintansa mukaisesti hankkia ulkopuolisia asiantuntijoita avuksi tilanteen hallintaan ja selvittämiseen. Poikkeamatilanteessa mahdollisesti tarvittavaa lisäosaamista on hyvä suunnitella etukäteen.

Roolituksen ja vastuiden määrittelyssä on oleellista huomioida myös palveluntoimittajien rooli poikkeamatilanteissa. Poikkeamatilanteiden toimintamallista on hyvä sopia palveluntarjoajien kanssa kirjallisesti. Pilvipalveluntarjoajien kohdalta on hyvä tarkistaa sopimusehdoista tai muusta dokumentaatiosta, miten pilvipalveluntarjoaja avustaa poikkeamatilanteissa. Varmista myös, että palveluntarjoajien yhteystiedot ovat hätätilanteessa nopeasti löydettävissä.

Tilanteissa, joissa poikkeamaan liittyy henkilötietojen tietoturvaloukkaus, pilvipalveluntarjoajalla voi henkilötietojen käsittelijänä olla velvollisuus avustaa asiaan liittyvässä tutkinnassa.

2.2 Tekniset toimet

Tässä luvussa kuvataan keskeisiä teknisiä toimia, joilla parannetaan varautumista poikkeamatilanteisiin.

> Luku käsittelee teknisiä toimenpiteitä ylätasolla. Koska eri pilvipalvelut ovat erilaisia, kaikkien teknisten toimien osalta on tärkeää, että tutustut pilvipalveluntarjoajan omiin aiheeseen liittyviin ohjeisiin, joista löytyy ajantasainen tieto.

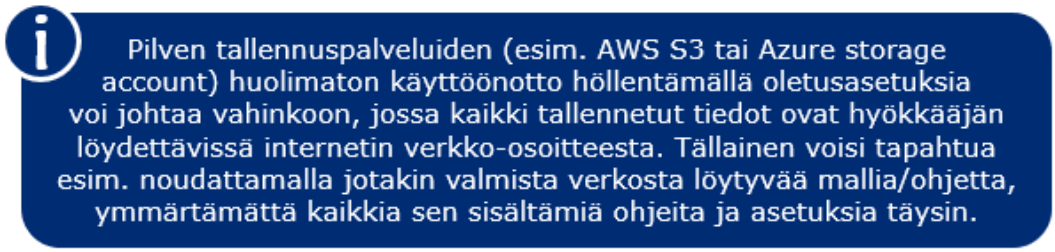
2.2.1 Suunnittele pilviympäristö huolella

Hyökkääjät voivat saada pääsyn pilviympäristöön esimerkiksi hyödyntämällä jotakin haavoittuvuutta tai saamalla käyttöönsä luvitetun käyttäjän käyttäjätunnukset ja tunnisteet. Palvelu tulisi suunnitella siten, että vaikka hyökkääjä onnistuisi pääsemään sisälle palveluun, pääsy yhteen kohteeseen ei tarjoaisi pääsyä kaikkialle. Voidaan puhua niin sanotusta vaikutusalueesta (engl. blast radius) eli siitä, kuinka laajalle hyökkäyksen aiheuttamat toimet voivat vaikuttaa.

Pilvipalveluissa on tyypillistä, että jos väärin konfiguroidusta tallennuspalvelusta vuotaa tietoja, ne yleensä vuotavat kaikki kerralla. Tämän takia on erityisen tärkeää huolehtia resurssien pääsynhallinnasta ja rajapintojen näkyvyyden

[6] https://julkaisut.valtioneuvosto.fi/handle/10024/79258

rajoittamisesta siten, että ne eivät olisi tavoitettavissa verkkotasolla koko internetistä, kuten yleensä oletuksena pilvessä on.



Mahdollisten hyökkäysten vaikutusta pyritään minimoimaan niin kutsuttua Zero Trust -suunnittelumallilla, esimerkiksi minimoimalla käyttäjien ja palveluiden pääsyt eri palveluihin:

- Anna käyttäjille mahdollisimman suppeat käyttöoikeudet: luvita oikeudet vain niihin resursseihin/palveluihin, joita he tarvitsevat.
- Todenna käyttäjä ja laite usealla eri valtuustiedolla käytön hetkellä.
- Luvita korotetut käyttöoikeudet vain sellaisiksi ajankohdiksi, jolloin niitä tarvitaan (niin sanottu Just-In-Time -luvitus).

Pyri myös erottelemaan pilvialustalla käyttämäsi palvelut loogisiin kokonaisuuksiin, esimerkiksi:

- Jakamalla loogiset kokonaisuudet – kuten kukin sovellus, sen tiedot ja tukipalvelut – erillisten tilien tai tilausten alle.
- Jakamalla erityyppiset ympäristöt käyttötarkoituksen mukaan (esim. kehitys, testaus ja tuotanto) eri infrastruktuurikokonaisuuksiin.

Huolehdi, että pääsy näiden osakokonaisuuksien välillä on rajoitettu tai estetty.

Käyttäjätunnuksien, joilla on pääsy useisiin kokonaisuuksiin tai ympäristöihin tulisi olla vain hallintakäytössä. Tällaisten oikeuksien käyttö tulisi toteuttaa esimerkiksi Just-In-Time-mallilla ja valvoa niiden käyttöä.

Odottamattomien muutosten tekemistä on yleensä mahdollista rajoittaa pilvessä. Esimerkiksi salaisuuksien hallintaan käytettävät pilvipalvelut, datapalvelut, ja konttirekisterit kannattaa mahdollisuuksien mukaan määritellä siten, ettei niiden sisällön tuhoaminen ole mahdollista ilman pakotettuja viipeitä.

2.2.2 Noudata palveluntarjoajien ohjeistamia käytäntöjä

Pilviympäristöjen luonteeseen kuuluu, että ne uudistuvat ja muuntautuvat tiuhaan tahtiin. Monet pilvipalveluntarjoajat pyrkivät tiedottamaan käyttäjiään muutoksista sekä ylläpitämään ajantasaista ohjeistusta siitä, mitkä ovat parhaat käytännöt palveluiden käyttöön ja ylläpitoon, tietoturvallisuus mukaan lukien. Varmistaaksesi palvelun tietoturvallisuus, huomioi ainakin seuraavat seikat:

- Seuraa käytössä olevien pilvipalveluiden tiedotteita (esim. sähköpostitiedotteet, verkkosivut). Tiedotteissa voi olla tietoa esim. uusista turvallisuusominaisuuksista tai tiedossa olevista haavoittuvuuksista.

- Noudata sekä pilvipalveluiden käyttöönotossa että käytön aikana palveluntarjoajien suosituksia turvallisuudesta. Kansainvälisten palveluntarjoajien osalta ohjeita löytää hakusanoilla ”security best practices”. Turvallisuussuosituksien noudattamatta jättämisen tulisi aina olla organisaatiolta tietoinen ja perusteltu päätös. Jossakin pilvipalveluissa on tietoturvaa tukevia automaatioita (engl. esim. security defaults tai guardrails), joiden avulla pilven konfiguraatioita ja muutoksia voi lukita tai ohjata turvallisemmaksi. Nämä mahdollisuudet vaihtelevat palvelutoimittajittain.

- Kovenna palvelut palveluntarjoajan koventamisohjeiden mukaan (esim. turvallinen konfiguraatio, oletussalasanojen ja -tilien yms. poistaminen käytöstä). Kansainvälisten palveluntarjoajien osalta ohjeita löytää hakusanoilla ”hardening guide”.

- Varmista, että pilviympäristöön luodut uudet palvelut ja resurssit noudattavat vaatimuksia ottamalla käyttöön vakioidut määritykset (engl. policy) ja mallit (engl. templates). Vakioidut määritykset ja mallit luovat kohteilleen määrityksen mukaiset vakioasetukset. Määritykset voi luoda itse vastaamaan oman organisaation vaatimuksia ja arkkitehtuuria. Pilvialustoilla voi olla tarjolla myös valmiita vaatimuspohjia, esimerkiksi hyviin käytäntöihin perustuen (esim. AWS Well-Architected Framework, Azure Architecture Center).

- Hyödynnä pilvipalveluiden hallinnoinnissa palveluntarjoajan tukemia koodiautomaatioita (Infrastructure-as-Code, IaC), jolloin konfiguraatioiden elinkaari ja muutosten hallinta on selkeämpää. IaC:n hyödyntäminen liittyy hyviin DevOps-käytänteisiin, ja nopeuttaa uusien resurssien luontia ja palveluiden palauttamista vakavissa häiriötilanteissa.

- Valvo, onko pilviympäristösi hyvien käytäntöjen mukainen. Tähän tarkoitukseen voit käyttää sekä automatisoituja arviointeja (esim. Azure Security Score ja Defender for Cloud, AWS Security Hub) tai ulkoista tarkastusta.

- Tutustu palveluntarjoajien poikkeamanhallintadokumentaatioon. Pilvipalvelualustoilla on palveluntarjoajakohtaisia ohjeita poikkeamanhallintaan liittyen. Ota käyttöön ne ohjeiden mukaiset tekniset ratkaisut, jotka sopivat organisaatiosi ratkaisuun.

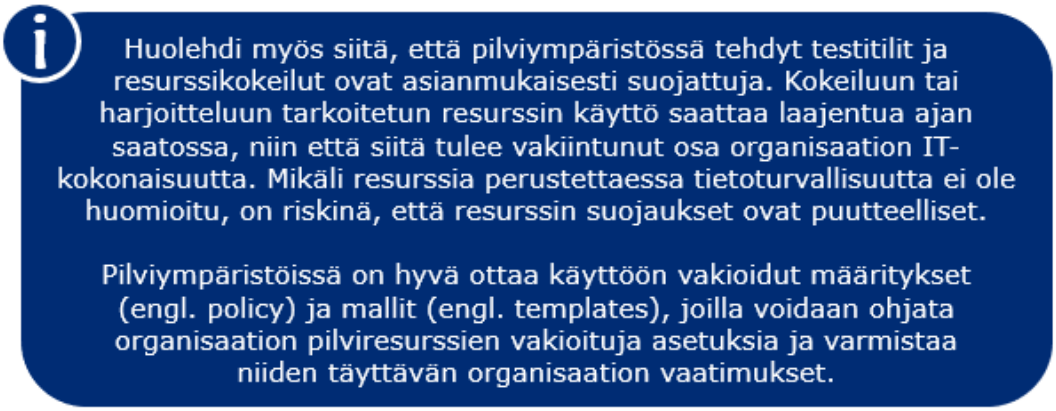
2.2.3 Varmista kehitys- ja tuotantoympäristöjen turvallisuus

Huomiota tulee kiinnittää myös pilviympäristöissä tapahtuvan sovelluskehityksen tietoturvallisuuteen. Siinä missä turvallisen sovelluskehityksen prosessimallista on paljon ohjeita[7], on syytä kiinnittää huomiota myös itse kehitys- ja tuotantoympäristöjen turvallisuuteen, esimerkiksi:

- Suunnittele kehitys- ja tuotantoympäristöt tavalla, jossa eri käyttötarkoituksen mukaiset ympäristöt ovat eri infrastruktuurikokonaisuuksissa.
- CI/CD-automaatiot ovat yleinen tapa murtautua pilven tuotantoympäristöihin. Muista huolehtia myös näiden järjestelmien tietoturvasta.

[7] Eräs esimerkkiohje: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/turvallinen-tuotekehitys-kohti-hyvaksyntaa

- Ajoita kehityksen aikainen tietoturvatekeminen mahdollisimman aikaiseen vaiheeseen (usein käytetään termiä “vasemmalle siirtämisestä” viittauksena sijoittumisessa projektin aikajanakaavioon, eng. "shift left"). Huomioi tietoturvallisuus kehityksen yhteydessä erilaisten tietoturvaa varmistavien työkalujen ja teknologioiden avulla. Kun tietoturva integroidaan oikealla tavalla kehitysputkeen, vältytään siltä, että käytössä olisi tietoturvattomia konfiguraatiota tai haavoittuneita komponentteja.
- Suunnittele CI/CD-automaatio, jossa sovellukseen tehtävät asennukset ja päivitykset on luvitettu vain tietylle tunnukselle. Tämän tunnuksen käyttö tulee saattaa tietoturvavalvonnan piiriin ja valvoa, mikäli sen käytössä ilmenee poikkeamia.



2.2.4 Pienennä hyökkäyspinta-alaa

Organisaation hyökkäyspinta-alalla tarkoitetaan sen tietojärjestelmiä, palveluita ja tietoliikenneportteja, jotka ovat auki julkiverkkoon ja joita kohtaan hyökkääjä voisi – ainakin teoriassa – hyökätä. Hyökkäyspinta-alan käsite konkretisoi sitä, että mitä enemmän tietojärjestelmiä ja -palveluja verkkoon on auki, sitä enemmän organisaation tulee myös pystyä havainnoimaan mahdollisia hyökkäyksiä ja pystyä estämään niitä. Hyökkäyspinta-alan pienentämiseksi:

- Varmista, että käytössä on vain sellaisia pilvipalveluja ja -resursseja, joita organisaatio tarvitsee.
- Kovenna käytössä olevat palvelut koventamisohjeiden mukaan (katso luku 2.2.2 Noudata palveluntarjoajien ohjeistamia käytäntöjä).
- Huomioi, että hyökkäyspinta-alaa kasvattavat myös käyttäjille annetut, työtehtäviin nähden liian laajat käyttöoikeudet. Varmista käyttäjien käyttöoikeuksien noudattavan vähimpien oikeuksien periaatetta ja että erityisiin työtehtäviin tarkoitettuja admin-tunnuksia ja muita korotettuja käyttöoikeuksia ei käytetä päivittäisessä työssä.
- Luo prosessi, jonka avulla turhat palvelut ja -resurssit sekä käyttäjät ja käyttöoikeudet poistetaan käytöstä säännöllisesti.

2.2.5 Aseta resurssien käytölle kulubudjetti

Joskus hyökkääjän toimenpiteisiin voi kuulua pilven resurssien aktivointi siten, että asiakkaalle aiheutuu merkittävä rahallinen vahinko pilven käytöstä. Tällaisen vaikutuksen rajaamiseksi pilven tilauksiin ja tileille tulisi asettaa sääntöjä, jotka

rajoittavat kalliiden resurssien aktivointia sekä kulubudjetti, jota ei ole mahdollista ohittaa ilman omistajan hyväksyntää. Pilvialustojen ominaisuudet näiden ominaisuuksien suhteen vaihtelevat, ja niihin tulisi tutustua käyttöön otettaessa.

2.2.6 Varmista pääsy palveluihin hätätilanteessa

Varmista pilvipalvelualustojen osalta, että organisaatio on konfiguroinut niihin niin sanotut hätätilanteiden pääsymenettelyt (engl. emergency access). Näiden menettelyiden tarkoitus on varmistaa, että asiakas pääsee kaikissa tilanteissa hallinnoimaan pilvipalveluitaan.

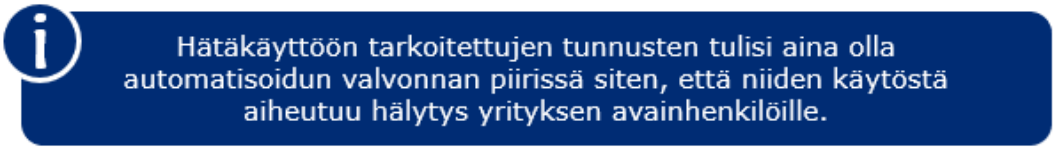
Näitä pääsymenettelyjä voidaan tarvita poikkeustilanteissa, joissa esimerkiksi organisaation normaalisti käyttämä monen tekijän todennustapa (esim. todennussovellus) ei ole käytettävissä. Pääkäyttäjien on hätätilanteessa mahdollisuus tunnistautua palveluun erilaisella menettelyllä. Näitä tunnuksia käytetään vain poikkeustilanteissa ja niiden luomiseen ja säilyttämiseen täytyy luoda menettelyt. Tunnusten tulisi olla yksinomaan organisaation hätäkäyttöön tarkoitettuja, eikä siten kytkeytyä työntekijöiden tunnuksiin tai tunnistusvälineisiin.

Hätätilannetta varten luoduille tunnuksille on suositeltavaa käyttää vahvinta mahdollista tunnistautumistapaa, esimerkiksi FIDO2-tunnisteavainta. FIDO2-avain on fyysinen, joten se on mahdollista säilöä lukitussa paikassa kuten yrityksen kassakaapissa.

Hätätilanteiden pääsymenettelyjen käytön on hyvä olla tietoturvavalvonnan piirissä siten, että tunnusten käytöstä syntyy hälytys. Tällöin tunnusten mahdollisiin väärinkäytöksiin on mahdollista reagoida.

Hätäkäyttöön luotuja tunnuksia tulisi testata suunnitelluin aikavälein sen varmistamiseksi, että tarvittavat henkilöt tuntevat niiden käyttöön liittyvät vaiheet, ja että tunnukset edelleen ovat toimivia.

Huolehdi lisäksi siitä, etteivät tunnusten tai käyttöoikeuksien siivoamiseen ja poistoon liittyvät automatiikat tai riskipohjaiset pääsynhallinnan käytänteet (esim. Conditional Access) vahingossa estä hätätunnusten toimintaa.



2.2.7 Varmista riittävät varmuuskopiointi- ja toipumismenettelyt

Varmista, että pilvipalveluille on luotu riittävät varmuuskopiointi- ja palautumismenettelyt[8]. Pilvipalvelualustalla voi olla automaattisesti käytössä joitakin palautumismenettelyjä, esimerkiksi palveluiden kahdentaminen useampaan kuin yhteen konesaliin. On kuitenkin hyvä huomioida, että pilvialustoilla asiakas saa niitä palveluita, joista hän maksaa: käytännössä kehittyneemmät ja vankemmat varmuuskopiointi- ja palautumismenettelyt ovat yleensä lisämaksullisia palveluita,

[8] Suunnittelun on hyvä pohjautua palveluille määriteltyihin toipumisaikoihin ja toipumispisteisiin (engl. Recovery Time Objective (RTO) ja Recovery Point Objective (RPO)). Lisätietoa toiminnan jatkuvuuden hallinnasta ja sen suunnittelusta löydät esimerkiksi VAHTI 2/2016 ohjeesta Toiminnan jatkuvuuden hallinta verkko-osoitteesta: https://julkaisut.valtioneuvosto.fi/handle/10024/75168.

jotka ovat käytössä vain, jos organisaatio on ne ostanut käyttöönsä ja integroinut palveluihinsa.

Mikäli organisaatiosi ei ole ottanut käyttöönsä pilvipalveluiden varmuuskopiointipalveluja tai varmistanut palveluiden kahdentamista useampaan maantieteelliseen sijaintiin[9], näitä toimenpiteitä ei todennäköisesti ole tehty automaattisesti pilvipalveluntarjoajan toimesta. Ilman riittäviä varmuuskopiointi- ja toipumismenettelyjä organisaatio voi poikkeamatilanteen seurauksena pahimmillaan menettää kaikki pilveen rakentamansa resurssit ja tallentamansa tiedot.

Konttipohjaisia työkuormia käytettäessä (esim. Docker) palvelut ja sovellukset on yleensä palautettavissa käyttöjärjestelmäpohjaisia palveluita nopeammin. Palautumisessa keskeistä on, että konttien jakeluun käytettävä rekisteri on edelleen saatavilla, tai sellainen voidaan pystyttää ja kontit koota uudelleen lähdekoodeista.

Varmista riittävät varmuuskopiointimenettelyt suunnittelemalla, mistä pilvipalveluresursseista on oltava varmuuskopiot ja miten usein kopiot otetaan. Pilvialustoilla on olemassa omat palvelunsa ja arkkitehtuurisuosituksensa varmuuskopioinnin toteuttamiseen. Suunnitellessasi varmuuskopioinnin toteuttamista huomioi, että mikäli tallennat varmuuskopiot samaan pilviympäristöön kuin niiden lähdeaineistot, varmuuskopiot voivat altistua samoille tietoturvahyökkäyksille. Pahimmillaan hyökkäys pilviympäristöön voisi siis tuhota sekä alkuperäiset palvelut ja niiden sisältämän datan, sekä näiden varmuuskopiot. Varmuuskopiot voi hajauttaa lähdejärjestelmistä eriytetyille tileille (esim. engl. AWS account) tai tilauksille (esim. engl. Azure subscription).

Varmuuskopioiden palauttamista on suositeltavaa testata säännöllisesti sekä teknisenä toimenpiteenä, että osana kriisiharjoitusta. Katso myös luku 2.3 Pilviympäristöön liittyvien tietoturvapoikkeamien harjoittelu.

2.2.8 Määrittele ja toteuta lokitus

Riittävällä lokituksella on keskeinen rooli tietoturvapoikkeamien havaitsemisessa ja selvittämisessä. Asiakkaan keräämät lokit voivat olla ainoa tapa näyttää toteen tietoturvapoikkeama.

Lokittamista suunniteltaessa on hyvä huomioida, että lokit voivat sisältää henkilötietoa ja että lainsäädäntö asettaa vaatimuksia lokien käsittelylle[10].

Varmista, että organisaatiosi on ottanut käyttöönsä riittävät lokitusmenettelyt pilvipalveluissa. Lokittamiselle voidaan pilvialustoilla asettaa sääntöjä (engl. data collection rules), jotka määrittelevät lokin keräämistä. Mikäli lokitietojen keräämistä eri palveluista ei ole määritelty, lokitietojen kerääminen poikkeamatilanteen selvittämiseksi voi osoittautua todella haastavaksi.

Lokien osalta voit miettiä esimerkiksi seuraavia asioita:

- Onko lokeista mahdollista nähdä muutoksia liittyen pilvipalveluiden konfiguraatioita ja pääkäyttäjiä koskevia muutoksia?

[9] On hyvä huomioida, että vain yhteen maantieteelliseen sijaintiin sijoitetut pilvipalveluresurssit voivat altistua häiriöille, mikäli palveluntarjoajan kyseisessä sijainnissa olevaan infrastruktuuriin kohdistuu häiriö.
[10] Lisää tietoa lokitietojen käsittelystä löytyy esimerkiksi Kyberturvallisuuskeskuksen ohjeesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

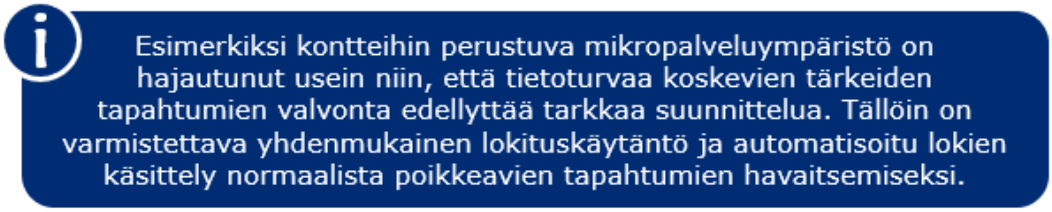
- Onko lokeista mahdollista nähdä, kuka palvelua/resurssia on käyttänyt, koska, mistä ja milloin?
- Kuinka pitkään eri lokit ovat saatavilla?
- Kenellä on pääsy lokeihin? Pääsy tulee rajata tiukasti ja lokien käsittelyä tulee valvoa.
- Ovatko lokit ja niiden tallentamiseen käytetyt palvelut suojattu muutoksilta? Lokien eheys eli muuttumattomuus tulee varmistaa, jotta lokitiedot ovat luotettavia. Pilviympäristön tietoturvapoikkeaman tutkinta vaikeutuu selvästi, jos hyökkääjällä on mahdollisuus tuhota lokeja.
- Miten verkkolokit (engl. network flow logs) voidaan ottaa käyttöön ja tarvitaanko niiden analysointiin erityisosaamista tai -työkaluja?

Asiaa käsitellään myös edellä luvussa 1.3.5 Tiedonkeruu poikkeamatilanteessa.

2.2.9 *Monitoroi ympäristöjä ja havaitse poikkeamat*

Poikkeamien havainnointi pilvipalvelun normaalista toiminnasta ja tietoliikenteestä vaatii sen seurantaa. Pilvialustoilla on mahdollista ottaa käyttöön erilaisia, yleensä lisämaksullisia, valvontatyökaluja. SaaS-palveluissa, jotka sijaitsevat palveluntarjoajan ylläpitämässä IT-ympäristössä, poikkeamien havainnointi on yleensä palveluntarjoajan vastuulla.

Keskeistä palvelussa esiintyvien poikkeamien havainnoinnille on ymmärtää palvelun normaali toiminta ja tietoliikenne (engl. baseline). Kun normaalit käyttötavat, -määrät ja liikenne tunnetaan, pystytään havainnoimaan tästä poikkeavaa toimintaa ja liikennettä.



Lisää tietoa poikkeamien havainnoinnista on luvussa 4 Tietoturvapoikkeaman havaitseminen.

2.2.10 *Suunnittele poikkeamatilanteen selvityksen tekninen toteutus*

Osana teknisiä varautumistoimia suunnittele, miten poikkeamatilanteen tekninen selvitys käytännössä voitaisiin toteuttaa:

- Ovatko riittävät lokit saatavilla ja kuka niihin pääsee käsiksi poikkeamatilanteessa? Miten lokitiedot säilytetään tavalla, joka mahdollistaa myöhemmän tutkimuksen ja niiden käytön todisteena?
- Onko käytössä ympäristö, jossa poikkeamaa voidaan tutkia? Ideaalitilanteessa poikkeaman tutkinta ei tapahdu samassa ympäristössä, johon hyökkääjällä on pääsy. Pilvialustoilla voi esimerkiksi olla mahdollisuuksia luoda erillinen tutkintaympäristö (engl. forensic investigation environment).
- Osataanko lokitietoon kohdistaa oikeanlaisia hakuja tapahtuneen selvittämiseksi? Lokitietoa kertyy paljon ja tarvittavien tietojen löytäminen saattaa olla haastavaa. Lokituksen formaattiin ja lokihakujen tekemiseen on hyvä tutustua hetkellä, jolloin poikkeamatilanne ei ole päällä.

- Varmista, että poikkeamatilanteen tekniseen selvitykseen on olemassa kirjallisia menetelmäohjeita ja että teknistä selvitystä tekevillä henkilöillä on tähän tehtävään riittävä osaaminen.

2.3 Pilviympäristöön liittyvien tietoturvapoikkeamien harjoittelu

Hallinnollisen ja teknisen varautumisen lisäksi yksi tehokkaista keinoista varautua poikkeamatilanteisiin on harjoitella niissä toimimista. Poikkeamatilanteessa organisaatiolla on normaalin liiketoimintansa ylläpitämisen lisäksi selvitettävänään poikkeama, jossa vaaditaan sekä ripeää päätöksentekoa että toimenpiteitä. Poikkeamatilanteiden harjoittelu tekee organisaatiolle tutuksi poikkeamatilanteessa noudatettavat käytännöt, päätöksentekomallin, roolit ja vastuut sekä keskeiset toimenpiteet. Harjoittelun avulla varsinaisessa poikkeamatilanteessa osallistujilla on jo hyvä käsitys edellä mainituista asioista, mikä auttaa toimimaan sovitusti.

Poikkeamaharjoituksia on monenlaisia ja niiden kirjo kattaa sekä niin sanotut työpöytäharjoitukset että simuloidut hyökkäykset (engl. red teaming, purple teaming) ja harjoitustyypit näiden väliltä. Organisaatiot, joissa poikkeamanhallinta ei vielä ole vakiintunutta voivat hyötyä työpöytäharjoituksesta, joka havainnollistaa esimerkiksi eri rooleihin poikkeamatilanteessa kohdistuvia vastuita ja vaatimuksia. Pöytäharjoituksen avulla voidaan myös käydä läpi poikkeamasuunnitelmaan kirjattuja toimenpiteitä ja keskustella niiden tehokkuudesta ja löytää näin suunnitelmista kehittämiskohteita.

Harjoittelun avulla pystytään myös havaitsemaan poikkeamanhallintakyvykkyyksien mahdollisia puutteita. Harjoitusten avulla voidaan testata esimerkiksi sitä, onko organisaatio huomioinut suunnitelmissaan ja toiminnassaan Luvussa 1.3 kuvatut pilviympäristöjen poikkeamanhallintaan liittyvät erityispiirteet sekä sitä, onnistuuko luvussa 5 Toimintaohjeet lueteltujen toimenpiteiden suorittaminen poikkeamanhallintaryhmältä.

Tietoturvapoikkeamien harjoitukseen tulee harjoitustyypistä riippumatta valita organisaatiolle relevantti harjoitusskenaario. Pilviympäristöjen osalta näitä voivat olla esimerkiksi seuraavan tyyppiset aloitusskenaariot, joiden kautta poikkeamanhallintatoimenpiteitä lähdetään suorittamaan:

- Pimeästä verkosta löytyy organisaation luottamuksellista dataa sisältävä ”data dump”. Miten se on päätynyt sinne?
- Hyökkääjä on kryptannut eli salannut jotkin pilvipalveluresurssit ja vaatii nyt lunnaita. Miten tilanteesta voidaan palautua?
- Pilviympäristön monitorointityökalu ilmoittaa admin-tilillä tapahtuvasta epäilyttävästä käytöksestä. Miten tilanteessa toimitaan?

Poikkeamaharjoituksia voi järjestää myös yhdessä organisaation IT-palveluntarjoajien kanssa, mikäli nämä toimivat poikkeamatilanteessa keskeisessä roolissa.

Lisää ohjeita kyberharjoitteluun ja lukuisia harjoitteluskenaarioita on Kyberturvallisuuskeskuksen sivustolla[11].

[11] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

3 Tietoturvapoikkeaman elinkaari

Tietoturvapoikkeamien elinkaari koostuu tyypillisesti seuraavista vaiheista:

- Havainnointi
- Poikkeaman selvitys
- Palautuminen
- Poikkeaman jälkiselvitys.

Kaikki tietoturvapoikkeamat noudattavat karkeasti tätä elinkaarta, riippumatta siitä, mihin palveluihin tai tietoihin poikkeama vaikuttaa. Poikkeaman kohteeksi joutuneen organisaation rooli elinkaaren eri vaiheissa riippuu kuitenkin siitä, minkä tyyppinen pilvipalvelumalli on kyseessä ja mitä sopimuksellisesti on sovittu toiminnasta poikkeamatilanteissa. Taulukko alla kattaa keskeiset eroavaisuudet.

Taulukko 1 Tietoturvapoikkeaman elinkaareen liittyvät tyypilliset asiakkaan vastuut eri pilvipalvelutyypeillä

Vaihe	IaaS	PaaS	SaaS
Havainnointi	Asiakas on vastuussa käytössään olevien pilviresurssien tietoturvapoikkeamien havainnoinnista. Tyypillisiä tapoja tähän ovat lokilähteiden seuranta, tietoturvan valvontatyökalujen käyttö, tietoliikenteen poikkeamien valvonta, sekä konfiguraatioiden muutosten valvonta.	Asiakas on vastuussa sovellustensa tietoturvan havainnoinnista. Tyypillisiä tapoja ovat sovellusten ja sovellusrajapintojen (API) tapahtumalokien valvonta, konfiguraatioiden muutosten valvonta, sekä sovelluskohtaisesti toteutetut mahdollisia väärinkäytöksiä kuvaavat valvonnan logiikat.	Asiakkaan vastuu tietoturvapoikkeamien havainnoinnista on rajallinen. Yleensä asiakas voi havaita sellaisen esimerkiksi, jos palvelun sisältö muuttuu odottamattomasti, palvelussa näkyy outoja käyttäjiä, tai palvelun käyttö estyy.
Poikkeaman selvitys	Asiakas käyttää käytössään olevia työkaluja, kuten tietoturva-, konfiguraatio- ja lokianalyysityökaluja, havaintojen tekoon ja tilanteen selvittämiseen. Palvelutuottaja avustaa poikkeaman selvityksessä yleensä ainakin silloin, kun poikkeamalla voi olla vaikutuksia myös heidän operaatioihinsa tai muiden asiakkaiden tietoihin ja palveluihin.		Selvitysvaiheessa pilvipalveluntarjoajalla on keskeinen rooli. Asiakkaan on raportoitava havainnoistaan palveluntarjoajalle tarvittaessa.
Palautuminen	Asiakas aktivoi palautumissuunnitelmansa mukaiset toimenpiteet ja palauttaa tiedot ja pilviresurssit. Yleensä palautuminen pilvessä tapahtuu perustamalla uudet palveluinstanssit. Palvelutuottaja saattaa avustaa palautumistoimenpiteissä. Palvelusopimusten laajuus ja sisältö voivat vaikuttaa saatavilla olevaan apuun.		Palautumiskyky riippuu pitkälti palveluntarjoajan ratkaisuista.
Poikkeaman jälkiselvitys	Asiakas selvittää poikkeaman juurisyyt ja analysoi poikkeaman hallinnan onnistumisen. Havaintojen perusteella toimintaa pyritään parantamaan, jotta vastaava tilanne ei toistuisi.		Jälkiselvitys tapahtuu organisaation ja palveluntarjoajan yhteistyössä.

Keskeistä on, että SaaS-palveluissa niitä käyttävän organisaation kyky selvittää poikkeamaa ja palautua siitä on usein rajallinen: SaaS-mallissa näitä kyvykkyyksiä on usein vain palveluntarjoajalla. Tämän takia luvuissa 4–6 luetelluista toimenpiteistä vain osa soveltuu SaaS-palvelujen käyttäjille. SaaS-mallissa organisaatiot keskittyvät poikkeamanhallinnassa tilanteen selvittämiseen yhdessä palveluntarjoajan kanssa sekä tilanteesta viestimiseen organisaation sisä- ja tarvittaessa ulkopuolelle, esimerkiksi viranomaisille.

4 Tietoturvapoikkeaman havaitseminen

Tietoturvapoikkeamat, mukaan lukien pilviympäristöjen turvallisuuspoikkeamat, voidaan havaita useilla eri tavoilla. Organisaatio voi itse havaita poikkeaman esimerkiksi monitoroinnin avulla tai havaitsemalla palvelussa häiriöitä. Organisaatio voi myös saada tiedon poikkeamasta ulkoisilta tahoilta, esimerkiksi asiakkailta, medialta, valkohattuhakkereilta tai palveluntarjoajalta.

Tässä luvussa kerrotaan, miten pilviympäristöt voivat edesauttaa tietoturvatapahtumien ja -poikkeamien havainnointia.

Hälytykset ja turvallisuusnäkymät

Isoilla pilvialustoilla on usein organisaation nimetyille käyttäjille näkyviä, käytössä olevien palveluiden turvallisuuden tilaa kuvaavia näkymiä tai sivustoja, joista ylläpitäjät voivat nähdä sekä palveluihinsa liittyviä turvallisuussuosituksia että hälytyksiä tietoturvatapahtumista ja -poikkeamista.

Pilvialustoilla käytössä olevilla erilaisilla palveluilla voi olla omia turvallisuusnäkymiään (engl. security dashboard) ja ne voivat tuottaa hälytyksiä epäilyttävästä toiminnasta. Esimerkiksi pilvipohjainen keskitetty identiteetinhallintateknologia (esim. Azure AD, Google Cloud Identity, Okta) voi tarjota käyttäjäorganisaatiolle hälytyksiä epäilyttävästä toiminnasta. Tällaiset ominaisuudet saattavat kuitenkin vaatia tietyn tasoisia käyttölisenssejä ja automaatioiden käyttöönottoa.

SaaS-palveluissa hälytykset epäilyttävästä toiminnasta voivat tulla tietoon palveluntarjoajalta tai palvelun käyttäjiltä.

Pilvipohjaiset tietoturvaratkaisut

Isoilla pilvialustoilla on usein tarjolla erillisiä turvallisuusratkaisuja, jotka voivat suojata pilvessä sijaitsevia teknologioita (esim. Microsoft Defender for Cloud, AWS GuardDuty). Näiden ratkaisujen avulla voidaan suojata ja monitoroida pilviympäristöjen ja -resurssien turvallisuutta. Tällaisilla ratkaisuilla voidaan myös toteuttaa automatisoituja työnkulkuja, jotka reagoivat epäilyttävään toimintaan. Ratkaisuilla voidaan esimerkiksi automaattisesti eristää laite, jolla on havaittu epäilyttävää toimintaa. Näihin ratkaisuihin liittyvien sääntöjen luominen, kehittäminen ja ylläpitäminen vaatii organisaatiolta riittävää resursointia.

Tietoturvan monitorointijärjestelmä

Organisaatio voi lisätä havaintokykyään investoimalla edellä kuvattujen pilviratkaisujen lisäksi erilliseen tietoturvatiedon ja -tapahtumien hallintajärjestelmään (engl. Security Information and Event Management, SIEM). Tällaiset keskitetyt lokijärjestelmät voivat analysoida lokitietoja ja tehdä niistä havaintoja tietoturvatapahtumista. Myös näihin ratkaisuihin liittyvien sääntöjen luominen, kehittäminen ja ylläpitäminen vaatii organisaatiolta riittävää resursointia.

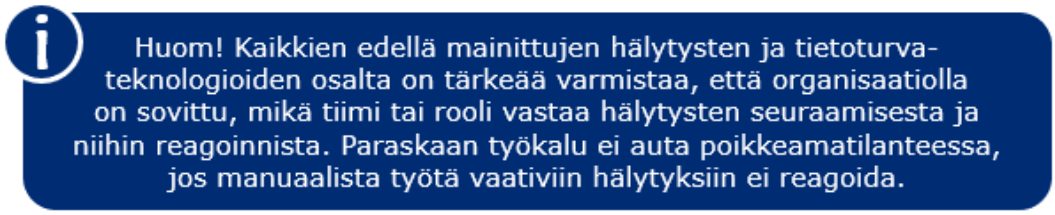
Palveluntoimittajien ilmoitukset

Joskus ensimmäinen havainto tietoturvapoikkeamasta tulee pilvipalveluntarjoajalta. Näissä tapauksissa on tärkeää toimia pilvipalveluntarjoajan ohjeiden mukaisesti, esimerkiksi vaihtaa salasanat ja muut pääsytiedot.

Ole kuitenkin tarkkana, että havainto tulee oikeasti pilvipalveluntarjoajalta – verkkorikolliset nimittäin käyttävät usein tunnettujen ja yleisten toimijoiden, kuten Microsoftin ja Amazonin nimiä huijausviesteissä, jotka helposti näyttävät aidoilta viesteiltä.

Asiakkaiden ja muiden tahojen ilmoitukset

Joskus tietoturvapoikkeamaa koskevat ensimmäiset havainnot tulevat asiakkailta, valkohattuhakkereilta, riippumattomilta tietoturvatutkijoilta, tai muilta odottamattomilta tahoilta. Organisaatiolla tulisi olla tavat käsitellä näitä ilmoituksia, ja tarkoituksenmukaiset ohjeet esimerkiksi asiakaspalvelun käyttöön. Sopivien yhteystietojen julkaiseminen on hyödyllistä prosessin järjestämisessä[12].



[12] Organisaatio voi esimerkiksi määrittää verkkosivuilleen security.txt-tiedoston, jossa kertoo toiveistaan vastaanottaa tietoturvaan liittyviä havaintoja ja toivotusta ilmoituskanavasta. Lisätietoja esimerkiksi osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuuksien-ilmoittamista-helpottavaa-kaytantoa-ei-viela-taysin-hyodynneta.

5 Toimintaohjeet

Voitte käyttää tämän luvun sisältämiä toimenpiteiden tarkistuslistoja apunanne, kun epäilette joutuneenne pilviympäristön tietoturvapoikkeamatilanteeseen.

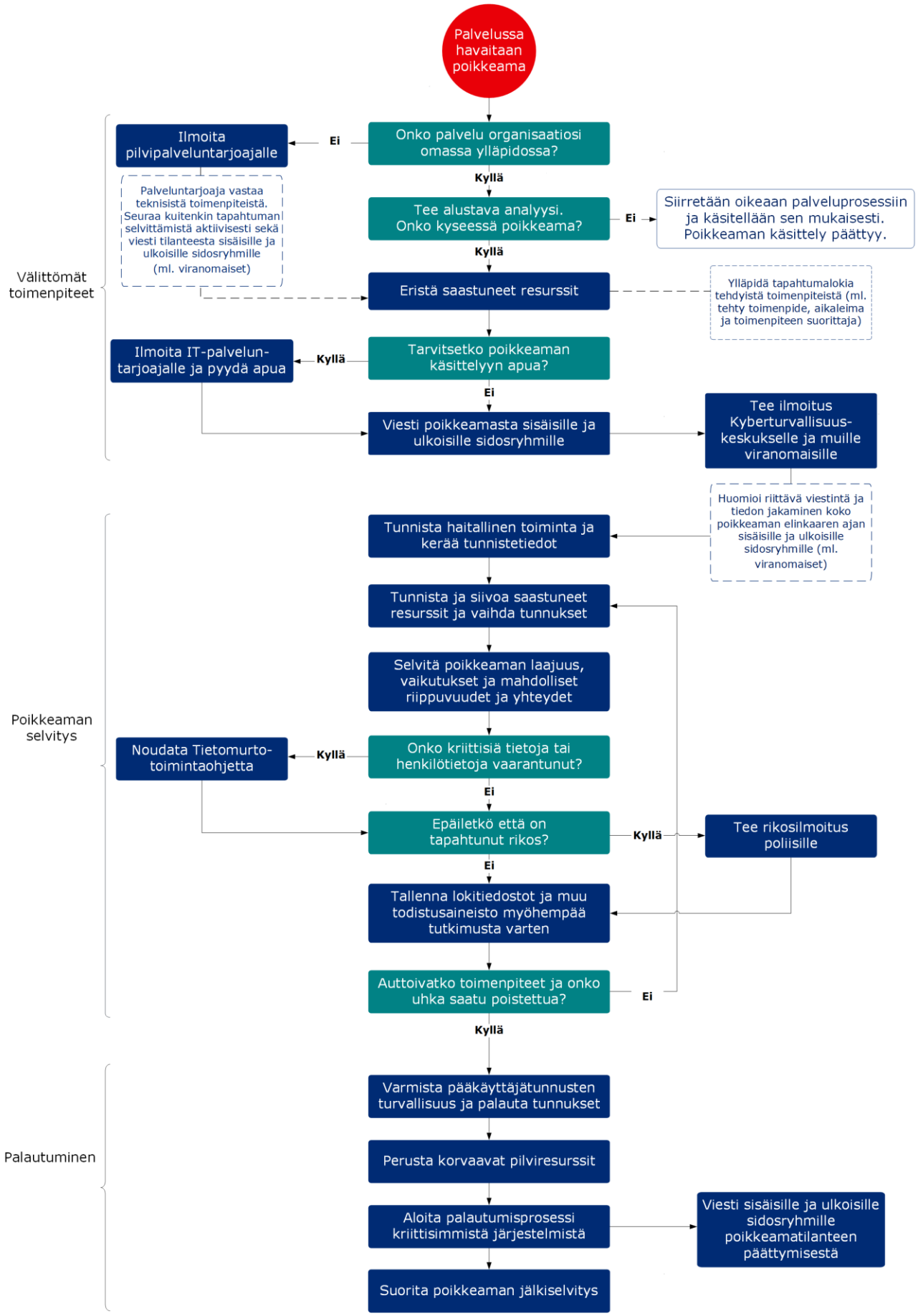
Tarkistuslista auttaa organisaatiota priorisoimaan ja vaiheistamaan toimintaa tietoturvapoikkeaman selvittämisessä.

5.1 Pilviympäristön tietoturvapoikkeaman selvityksen työnkulku

Seuraavalla sivulla oleva kaavio kuvaa keskeisiä poikkeamanhallintaan liittyviä toimia. Kaavio tukee taulukkomuodossa olevan tarkistuslistan käyttöä. Organisaation on hyödyllistä tehdä omaan poikkeamanhallintaprosessiinsa sopiva vuo- tai uimaratakaavio, joka vastaa poikkeamanhallintasuunnitelmaan kirjattuja menettelyitä.

Poikkeamanhallintaprosessin aikana on myös tärkeää ylläpitää tarkkaa tapahtumalokia tehdyistä toimenpiteistä. Lokista tulisi käydä ilmi tehty toimenpide, aikaleima ja toimenpiteen suorittaja.

Myös mahdollinen todistusaineiston kerääminen on syytä dokumentoida huolellisesti. Ylös tulisi kirjata kuka keräsi, mitä aineistoa sekä mistä ja milloin se kerättiin. Huolellisesti laadittu tapahtumaloki helpottaa tutkintaa sekä yhteistyötä poliisin ja tietoturvatutkijoiden kanssa merkittävästi.



Kuva 2 Pilviympäristön poikkeamanselvityksen työnkulku, yksinkertaistettu kaavio

5.2 Välittömät toimenpiteet

Vaiheen tavoitteet	Välittömien toimenpiteiden tarkoitus on suojata ympäristön kriittiset tiedot, estää hyökkääjän jalansija ympäristössä sekä alustaa palautumisprosessin aloittaminen.

Vaihe	Tarkoitus	Toimenpiteet
Palvelussa havaitaan poikkeama		
Onko palvelu organisaatioisi omassa ylläpidossa? **Ilmoita pilvipalveluntarjoajalle**	Tilanteen selvittämisessä voidaan tarvita pilvipalveluntarjoajan tai IT-kumppanin apua. Saatavilla olevat tukipalvelut vaihtelevat sen mukaan mihin teknologia-alueeseen poikkeama kohdistuu, ja onko se asiakkaan vai palvelutarjoajan vastuulla. IaaS, PaaS: Ole yhteydessä mahdollisiin IT-kumppaneihin tai pilvipalveluntarjoajaan, mikäli poikkeama on heidän vastuualueellaan. SaaS: Pilvipalvelun tuottajaorganisaatio on välttämätön tilanteen selvittämisessä. Huomioi, että palvelusopimus voi määrittää, että organisaatiolla on velvollisuus ilmoittaa poikkeamasta palveluntarjoajalle.	Paikallista poikkeaman esiintyminen: tunnista palvelu tai palvelut, joissa mahdollinen poikkeama esiintyy ja selvitä ovatko ne oman organisaatiosi ylläpidossa vai vastaako niistä pilvipalveluntarjoajasi tai IT-kumppanisi. Jos palvelu on pilvipalveluntarjoajan tai IT-kumppanin ylläpidossa, **ota yhteyttä palveluntarjoajan tukikanavaan**. Palveluntarjoaja vastaa teknisistä toimenpiteistä, mutta seuraa kuitenkin tapahtuman selvittämistä ja huolehdi mm. viestinnästä sisäisille ja ulkoisille sidosryhmille (ml. viranomaiset). Siirry kohtaan "Eristä saastuneet resurssit". Jos palvelu on organisaatiosi omassa ylläpidossa, jatka poikkeamanhallintaprosessia (siirry kohtaan "Tee alustava analyysi").
Tee alustava analyysi. Onko kyseessä poikkeama?	Kaikki tietoturvahälytykset ja -havainnot eivät johda poikkeamanhallintatoimiin. Jotkut hälytykset ovat ns. vääriä hälytyksiä. Jotkut hälytykset ja häiriöt hoidetaan osana organisaation normaalia operatiivista toimintaa. Organisaation tulisi määritellä, minkälainen tietoturvatapahtuma tai -tapahtumaketju on vakavuudeltaan sellainen, että se käynnistää poikkeamanhallintaprosessin. <u>Käynnistä tarvittaessa jatkuvuudenhallinnan toimenpiteet</u> Poikkeaman vakavuudesta riippuen ja liiketoiminnan jatkuvuuden turvaamiseksi voi olla tarpeen käynnistää poikkeusmenettelyjä, siirtyä käyttämään väistösivuja, yms. jatkuvuudenhallinnan toimenpiteitä. Myös osittaisia palautumistoimenpiteitä voidaan joutua käynnistämään tapauskohtaisesti liiketoiminnan jatkuvuuden varmistamiseksi. Ideaalitilanteessa järjestelmien palauttaminen aloitetaan vasta, kun on varmistuttu poikkeaman juurisyyanalyysin kautta, ettei hyökkääjällä ole enää pääsyä ympäristöihin. Liiketoiminnan jatkuvuuden kannalta ei kuitenkaan välttämättä voida odottaa tutkinnan valmistumista vaan jatkuvuuden varmistamiseksi osittainen palautuminen voidaan joutua aloittamaan jo aiemmin. Tällöin on riski siitä, että järjestelmä on palautumisen jälkeen edelleen haavoittuva ja tapahtuu uusi poikkeama.	Tee alustava analyysi: tutki hälytyksen tai muun saamasi indikaation tiedot ja käytä tarvittavia lisälähteitä arvioimaan, vaikuttaako siltä, että kyseessä on tietoturvapoikkeama. Jos arvelet, että kyseessä on tai saattaa olla tietoturvapoikkeama, jatka poikkeamanhallintaprosessia. Muille tapauksille tulee noudattaa niille määriteltyä työnkulkua. Poikkeaman käsittely päättyy. Tee arvio tilanteen vakavuudesta ja käynnistä tarvittaessa jatkuvuudenhallinnan toimenpiteet (poikkeusmenettelyt, väistösivut, yms.). Liiketoiminnan jatkuvuuden varmistamiseksi voidaan tapauskohtaisesti joutua käynnistämään osittaisia palautumistoimenpiteitä jo ennen tutkinnan valmistumista. Hyökkäysriskin pienentämiseksi väliaikainen palauttaminen tulisi mahdollisuuksien mukaan toteuttaa erilliseen infrastruktuuriin käyttäen eriytettyjä ylläpitomenettelyjä (tunnukset, laitteet yms.). Seuraa ja arvioi tilannetta ja päivitä toimenpiteitä koko poikkeamanhallintaprosessin ajan.

Eristä saastuneet resurssit	Eristämällä uhka pyritään estämään hyökkäyksen eteneminen sekä suojelemaan järjestelmän tietoja.	Pyri eristämään saastunut resurssi käyttämällä pilviympäristön hallintatyökaluja. Eristämisen toimenpiteet voivat tarkoittaa pilviympäristössä esimerkiksi seuraavia: • Tunnuksen tai käyttöoikeustietueen (access token) sulkeminen. • Sovelluksen toiminnan pysäyttäminen. • Sovelluksen rajapintojen ja verkkoliikenteen toiminnan rajoittaminen. • Integraatiorajapinnan sulkeminen. • Virtuaalikoneen tai konttipohjaisen palvelun toiminnan pysäyttäminen. Ylläpidä tapahtumalokia tehdyistä toimenpiteistä. Lokista tulisi käydä ilmi tehty toimenpide, aikaleima ja toimenpiteen suorittaja.
Tarvitsetko poikkeaman käsittelyyn apua? **Ilmoita IT-palveluntarjoajalle ja pyydä apua**	Poikkeaman selvittämisessä voidaan tarvita ulkopuolista apua esim. teknisissä toimenpiteissä, poikkeaman hallinnassa tai toimenpiteiden organisoinnissa. Mikäli sisäisesti tai suoraan IT-palveluntarjoajilta ei löydy riittävää osaamista, tulee harkita ulkopuolisen avun tarvetta. Ulkopuolista osaamista voivat vaatia esimerkiksi tunnistetietojen kerääminen ja uhan selvittäminen niiden perusteella. Ulkopuolinen apu voi myös esimerkiksi auttaa tarkastamaan, onko hyökkääjä saanut käsiinsä liiketoiminnan kannalta tärkeää dataa, ja jos on, niin mitä.	Jos arvioit tarvitsevasi poikkeaman käsittelyyn ulkopuolista apua, **ota yhteyttä poikkeamien käsittelyyn erikoistuneeseen palveluntarjoajaan**. Alaviitteessä listatuista resursseista löydät suomalaisia palveluntarjoajia[13].
Viesti poikkeamasta sisäisille ja ulkoisille sidosryhmille	Poikkeamatilanteessa on tärkeää, että keskeiset päätöksentekijät tietävät, missä mennään. Tietoturvapoikkeama voi aiheuttaa yhteistyökumppaneille, asiakkaille ja palveluntarjoajille riskejä tai ongelmia palveluiden saatavuudessa.	Toimi organisaatiosi poikkeamanhallintasuunnitelman mukaisesti ja varmista, että poikkeamanhallintaryhmä on perustettu ja tieto kulkee ryhmän kesken. Tarvittava viestinnän määrä riippuu pitkälti tilanteesta: etenkin vakavaa tilannetta epäiltäessä on syytä ilmoittaa tilanteesta johdolle heti. Ilmoita eri sidosryhmien kriisiyhteyshenkilöille tapauksesta, mikäli uskotte sen voivan vaikuttaa heidän palveluidensa saatavuuteen tai vaarantaa niiden turvallisuutta. Mikäli palvelimella on ollut käytössä yhteyksiä muihin organisaatioihin, ilmoita myös heille. Näin he voivat mitätöidä tunnukset, avaimet tai varmenteet, joita on ollut käytössä saastuneella palvelimella. On myös tärkeää, että he tarkastavat omien tietojensa eheyden.

[13] Suomalaisia palveluntarjoajia löytyy seuraavilta verkkosivuilta: https://dfir.fi/; https://www.fisc.fi/fi; https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija

Tee ilmoitus Kyberturvallisuuskeskukselle ja muille viranomaisille	EU:n verkko- ja tietoturvadirektiivin (ns. NIS-direktiivi) alaisten huoltovarmuuskriittisten toimijoiden ja palveluntarjoajien tulee ilmoittaa verkko- ja tietojärjestelmässä olevista tietoturvapoikkeamista viranomaisille[14]. Lisäksi tietoturvapoikkeamista kannattaa aina ilmoittaa Kyberturvallisuuskeskukselle, joka tukee ja neuvoo organisaatioita poikkeamatilanteissa. Huomioi, että Kyberturvallisuuskeskukselle tekemäsi ilmoitus on lähtökohtaisesti luottamuksellinen eikä siitä mene tietoa esimerkiksi Poliisille. Mikäli epäilet rikosta, rikosilmoituksen tekeminen Poliisille on erillinen prosessi. <u>Huomioi riittävä viestintä ja tiedon jakaminen koko poikkeaman elinkaaren ajan</u> Poikkeamanhallinta vaatii koordinoitua viestintää sekä organisaation sisällä että ulkoisille sidosryhmille ja viranomaisille. Nämä viestintävastuut tulisi olla sovittuna etukäteen ja löytyä poikkeamanhallintasuunnitelmasta.	Mikäli organisaatiosi on keskeinen huoltovarmuuskriittinen toimija, ilmoita tietoturvapoikkeamasta oman toimialasi valvovalle viranomaiselle. Lisäksi tietoturvapoikkeamasta kannattaa aina ilmoittaa Kyberturvallisuuskeskukselle mahdollisimman varhaisessa vaiheessa.[15] Kyberturvallisuuskeskus voi auttaa organisaatioita erityisesti tapauksen ensivasteessa ja tarjoamalla lisätietoja vastaavista tapauksista Suomessa ja kansainvälisesti. Nimeä rooli(t) tai henkilö(t), joiden tehtävä on jakaa tilannetietoa sisäisille ja ulkoisille sidosryhmille (ml. viranomaiset) ja pitää nämä ajan tasalla koko poikkeaman elinkaaren ajan.

[14] https://www.kyberturvallisuuskeskus.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus
[15] Tee ilmoitus Kyberturvallisuuskeskukselle verkkolomakkeella https://www.kyberturvallisuuskeskus.fi/fi/ilmoita, sähköpostitse (cert@traficom.fi) tai puhelimella numeroon 0295 345 630 (pvm/mpm) numero palvelee arkisin klo 9-15

5.3 Poikkeaman selvitys		
Vaiheen tavoitteet	Tietoturvapoikkeaman selvityksen tavoitteena on selvittää hyökkäyksen laajuus ja vaikutus organisaatiossa. Perinpohjaisella tutkinnalla varmistetaan, että haittaohjelmat ja mahdolliset takaovet ovat siivottu ympäristöstä.	
Vaihe	**Tarkoitus**	**Toimenpiteet**
Tunnista haitallinen toiminta ja kerää tunnistetiedot	Tunnistetietoja kerätään, jotta voidaan kartoittaa miten laajasti laitteet ovat saastuneet ja miten varastettuja käyttöoikeuksia on hyödynnetty. Jalansijan saatuaan hyökkääjä voi käyttää eri hyökkäysmenetelmiä. Tunnistetietoja tuleekin kerätä laajasti ja niiden käytön merkkejä tutkia huolellisesti, jotta ympäristön puhdistaminen voidaan tehdä luotettavasti. Vasta kun hyökkääjä on karkotettu ympäristöistä, voidaan palautuminen aloittaa turvallisesti.	Tunnista haitallinen toiminta ja kerää tunnistetietoja mahdollisimman kattavasti. Kerättäviä tunnistetietoja ovat muun muassa tapahtuma-aika, kuten milloin palvelimelle on kirjauduttu, tai milloin tietty komento on ajettu palvelimella. Haittaohjelma kommunikoi usein hyökkääjän komentopalvelimen kanssa. Tarkastelemalla saastuneiden laitteiden verkkoliikennettä tai verkkotunnusten selvitystä (DNS-lokit), voidaan tunnistaa lähde-IP-osoitteet tai verkkotunnukset, joita hyökkääjä käyttää. Kun haitallisia tiedostoja tunnistetaan, voidaan niistä ottaa tiivisteet (MD5/SHA256), joiden avulla voidaan tunnistaa haitalliset tiedostot myös muilta laitteilta. Saastuneisiin laitteisiin kohdistuneista tunnistautumistapahtumista ja näihin liittyvillä käyttäjätileillä suoritetuista toimenpiteistä voidaan päätellä tunnukset, joilla haittaohjelmaa on levitetty. Keskitetystä päätelaitteiden valvonnasta löytyy usein ominaisuudet edellä mainittujen tunnistetietojen keräämiseen ja niiden käyttämiseen. Muussa tapauksessa toimet tulee tehdä käsin käyttämällä keskitettyä lokipalvelinta. Mikäli tätäkään ei ole saatavilla, tulee tutkia yksittäisten palvelinten ja päätelaitteiden lokeja.
Tunnista ja siivoa saastuneet resurssit ja vaihda tunnukset	Kerättyjen tunnistetietojen avulla voidaan selvittää, kuinka laajalle hyökkääjä on päässyt tunkeutumaan organisaatiossa. Keräämällä tunnistetietoja ja hakemalla niitä kohdejärjestelmistä voidaan varmentaa, että kaikki saastuneet laitteet, tunnukset, avaimet ja varmenteet löydetään ja siivotaan. Tunnistetietojen avulla voidaan etsiä saastuneita laitteita, esimerkiksi käyttämällä keskitetyn päätelaitteiden valvonnan ominaisuuksia, jotka usein tarjoavat mahdollisuuden hakea laitteilta tapahtumia eri tunnisteilla. Mikäli organisaatiolla on käytössään myös keskitetty lokienhallinta, voidaan sen avulla tehokkaasti etsiä tunnisteiden perusteella tapahtumia useilta eri koneilta samanaikaisesti. On olemassa riski, että hyökkääjä laitteelle päästyään on yrittänyt peittää jälkiään kytkemällä lokien keräämisen pois päältä. Tällöin laitteen lokeista ei välttämättä voida löytää kaikkia kerättyjä tunnistetietoja. Tämän vuoksi on tärkeää pyrkiä käyttämään laajaa kirjoa erilaisia tunnistetietoja ja tapahtumalähteitä.	Käytä tunnistetietoja avuksi tunnistamaan kaikki saastuneet järjestelmät ja hyökkääjän tiedossa olevat tunnukset, avaimet ja varmenteet. Käytä esimerkiksi tietoja päätelaitteiden valvonnasta tai lokienhallinnasta. Mikäli kumpikaan edellä mainituista ratkaisusta ei ole käytettävissä, tulee tunnisteita hakea erikseen kaikilta laitteilta. Tässä voidaan kuitenkin käyttää hyväksi vielä erilaisia etähallintaratkaisuja, jotka usein mahdollistavat esimerkiksi PowerShell-komentojen ajamisen yhtäaikaisesti useammalla palvelimella. Siivoa saastuneet järjestelmät. Vaihda hyökkääjän tiedossa olevat tunnukset, avaimet ja varmenteet.

Selvitä poikkeaman laajuus, vaikutukset ja mahdolliset riippuvuudet ja yhteydet	Usein pilviresursseilla on käytössä yhteyksiä muihin järjestelmiin. Näitä voivat olla esimerkiksi tietokantayhteys tai erilaiset API-kutsut, avaimet ja varmenteet. Yhdistettyjen järjestelmien eheys sekä poikkeaman vaikutus liiketoimintaan tulee varmistaa ensi tilassa, jotta voidaan ymmärtää tilanteen vakavuus.	Mikäli palvelulla on käytössä yhteyksiä muihin järjestelmiin, varmista tietojen eheys tarkastelemalla yhdistettyjen järjestelmien lokeja. Selvityksessä tulisi keskittyä niihin tunnuksiin, varmenteisiin tai käyttöoikeustietueisiin (access token), joilla integraatiot on tehty.
Onko kriittisiä tietoja tai henkilötietoja vaarantunut? **Noudata Tietomurto-toimintaohjetta**	Osana tutkimusta tulee selvittää, onko hyökkääjä päässyt käsiksi organisaation tärkeisiin tietoihin, tai mahdollisesti asiakkaiden tai työntekijöiden henkilötietoihin. Huomaa, että vaikka hyökkääjä ei olisi tuhonnut tai varastanut tietoja, hän on saattanut muokata niitä. Hyökkääjä on saattanut myös varastaa kooltaan pientä, mutta merkityksellistä dataa, kuten tunnuksia. Tilanteissa, joissa pilvipalveluntarjoaja toimii henkilötietojen käsittelijänä, ja poikkeama voi olla myös tietosuojaloukkaus, tällä on velvollisuus auttaa tilanteen selvittämisessä ja ilmoituksen täyttämisessä.	Selvitä onko yhteyksissä käytetyillä tunnuksilla, varmenteilla tai avaimilla kirjauduttu muualta kuin palvelimelta, jolla niitä kuuluu käyttää. Selvitä onko hyökkääjä päässyt käsiksi tietoihin ja varastanut niitä tarkastelemalla tietopalveluiden ja rajapintojen lokeja. Tehdyistä hauista tai kuormituksesta voit päätellä, onko hyökkääjä pyrkinyt noutamaan tai muokkaamaan tietoja. Mikäli kriittisiä tietoja tai henkilötietoja on vaarantunut, **noudata Kyberturvallisuuskeskuksen Tietomurto-toimintaohjetta[16].**
Epäiletkö että on tapahtunut rikos? **Tee rikosilmoitus Poliisille**	Raportoi poikkeamasta viranomaistahoille. Organisaatiolla voi olla vastuu ilmoittaa poikkeamasta säädösten tai kybervakuutuksen ehtojen velvoittamana. Huomioi, että Kyberturvallisuuskeskukselle tekemäsi ilmoitus on lähtökohtaisesti luottamuksellinen eikä siitä mene tietoa esimerkiksi Poliisille. Rikosilmoitus on aina tehtävä erikseen.	Jos epäilet rikosta, **tee tapauksesta rikosilmoitus Poliisille[17].**
Tallenna lokitiedostot ja muu todistusaineisto myöhempää tutkimusta varten	Todisteiden keräämisellä ja säilömisellä pyritään takaamaan laadukas tapauksen jälkitutkinta, jotta tapauksen juurisyyt saadaan selvitettyä. Todisteita voidaan tarvita rikosilmoituksen yhteydessä ja oikeuskäsittelyä varten. Jos organisaatiolla on kybervakuutus, voi myös vakuutusyhtiö vaatia poikkeamasta tarkempia tietoja ja todisteita tutkintaa varten.	Tallenna lokitiedostot, joista löytyy poikkeaman tutkinnan kannalta oleellista tietoa, verkosta eristetylle kovalevylle. Kerää myös talteen mahdolliset haitalliset sähköpostit ja muut viestit. Pyri säilyttämään todisteet, kuten kokonaiset levykuvat ja muistinäytteet, mahdollisimman eheinä. Ota niistä eheystiivisteet tämän varmistamiseksi. Pyri säilömään näytteet havaituista haittaohjelmista. Käsittelyssä tulee noudattaa suurta varovaisuutta. Turvallinen toteuttaminen vaatii usein ammattiosaamista. Lähetä näytteet Kyberturvallisuuskeskukselle[18].
Auttoivatko toimenpiteet ja onko uhka saatu poistettua?	Ennen palautumisen aloittamista, varmista että tehdyt toimenpiteet ovat auttaneet.	Mikäli toimenpiteet auttoivat, aloita palautumisprosessi kriittisimmistä järjestelmistä ja palveluista.

[16] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TietomurtoToimintaohje.pdf
[17] https://poliisi.fi/tee-rikosilmoitus
[18] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sahkopostin-valittaminen-ja-naytteiden-lahettaminen-kyberturvallisuuskeskukselle

5.4 Palautuminen

Vaiheen tavoitteet	Palautumisvaiheessa organisaatio pyrkii palauttamaan liiketoiminnan takaisin normaaliksi mahdollisimman pian sen jälkeen, kun palautuminen voidaan toteuttaa turvallisesti. Palautuminen kannattaa aloittaa liiketoiminnan kannalta kriittisimmistä järjestelmistä.

Vaihe	Tarkoitus	Toimenpiteet
Varmista pääkäyttäjätunnusten turvallisuus ja palauta tunnukset	Varmistetaan, että kaikkien mahdollisesti saastuneiden tunnusten kirjautumistiedot vaihdetaan, jotta hyökkääjällä ei olisi enää pääsyä tunnusten avulla organisaation järjestelmiin. Kovennetaan käyttäjien kirjautumisvaatimuksia, mikäli mahdollista.	Vaihda saastuneiden tunnusten salasanat ja ota tunnukset takaisin käyttöön. Samoin avaimet ja varmenteet. Vaihda varmuuden vuoksi ylläpitotunnusten ja palvelutunnusten salasanat siltä varalta, että osa niistä on joutunut hyökkääjien käsiin. Toimita uudet salasanat käyttäjille joko suullisesti, tekstiviestillä tai soittamalla. Älä käytä organisaation sähköpostia tai pikaviestimiä, sillä hyökkääjällä saattaa edelleen olla niihin pääsy. Varmista, että kaikilla tunnuksilla on käytössä monivaiheinen tunnistautuminen. Valvo kuitenkin hyökkäyksessä käytettyjä tunnuksia palauttamisen jälkeen siltä varalta, että hyökkääjä saa ne uudelleen käsiinsä. Mikäli organisaatiolle jää epäselväksi, miten hyökkääjä oli saanut tietyt tunnukset käsiinsä, harkitse täysin uusien tunnusten luomista.
Perusta korvaavat pilviresurssit	Luo uudet pilviresurssit asentamalla palvelut ja sovellukset uudelleen. Älä pyri puhdistamaan saastunutta järjestelmää automaattisilla työkaluilla tai haittaohjelman torjuntaohjelmistoilla, sillä ne eivät välttämättä kykene puhdistamaan järjestelmää täydellisesti.	Pilviympäristössä toimimisen etuihin kuuluu, että resurssit ovat yleensä asennettavissa täysin tai lähes automatisoidusti uudelleen. Lisäksi DevOps-käytänteitä noudatettaessa myös sovellukset ja kontit on jaeltavissa automaattisesti. Tämä tekee työkuormien palauttamisesta huomattavasti nopeampaa, sillä tarve puhdistaa ja verifioida palvelimia uudelleenkäytettäväksi ei ole. Toki palautuminen tulee toteuttaa siten, että riski hyökkäyksen aktivoinnista uudelleen on hallittu. Tämä tarkoittaa esimerkiksi sen varmistamista, ettei hyökkääjä ole esimerkiksi muuttanut konttirekisterin tai lähdekoodien sisältöä siten, että uudet resurssit sisältävät vaikkapa takaportin.
Aloita palautumisprosessi kriittisimmistä järjestelmistä	Pyritään palauttamaan tiedot ja järjestelmät ja palaamaan normaalin toimintaan. Palautus pyritään suorittamaan mahdollisimman turvallisesti, jotta hyökkääjä ei pääsisi tunkeutumaan takaisin järjestelmiin. Jos hyökkääjän epäillään muokanneen tietokannan sisältöä, tulee tietokanta palauttaa varmuuskopiosta hyökkääjän muutosten mitätöimiseksi, mikäli tietoja ei ole mahdollista puhdistaa.	Pilviympäristössä toimiessa on usein niin, että tietojen palauttaminen riittää ja infrastruktuuripalvelut, ajoalustat, kontit, ja pilvessä ajettavat sovelluskoodit voidaan asentaa uudelleen automaatiolla. Tämä on suositeltava palautustapa. Palauta tarvittaessa myös järjestelmät kuten virtuaalipalvelimet varmuuskopioista. Ota huomioon myös riski, että aikaisemmat päiväkohtaiset (inkrementaaliset) varmuuskopiot voivat olla jo saastuneita. Palauttaessasi vanhoja varmuuskopioita ota huomioon, että varmuuskopio voi sisältää haavoittuvuuksia, joita hyökkääjä on hyväksikäyttänyt hyökkäyksessä.

	<u>Viesti sisäisille ja ulkoisille sidosryhmille poikkeamatilanteen päättymisestä</u> Ilmoita sisäisille ja ulkoisille sidosryhmille (ml. viranomaisille) poikkeamatilanteen päättymisestä. Ilmoita sidosryhmille (esim. asiakkaille), jos tietoja on jouduttu palauttamaan vanhempaan versioon tietystä päivämäärästä alkaen, jotta asianomaiset voivat päivittää tietonsa ajan tasalle.	Palautumisen aikaista riskiä uudesta murrosta voi yrittää välttää palauttamalla pilvipalvelut ja työkuormat siten, että niiden rajapinnat ja verkkoyhteydet avataan rajoitetummin. Esimerkiksi aiemmin internetiin avoinna ollut rajapinta voitaisiin avata uudelleen vain tarvittavien osoitteiden tai verkkojen tavoitettavaksi. Käytä hyväksesi lokeja selvittääksesi, onko hyökkääjä muokannut tietueita. Jos lokien tarkkuus ei riitä muokkausten siivoamiseen, palauta tietokannan tiedot viimeisimpään turvalliseen varmuuskopioon. Mikäli hyökkääjä on varastanut tietoja, tulee kaikki varastetuissa tiedoissa olleet salasanat vaihtaa. Näin tulee myös toimia, vaikka salasanat olisikin säilötty vain tiivisteinä.
Suorita poikkeaman jälkiselvitys	Kriisin päätyttyä ja liiketoimintojen normalisoiduttua on tärkeää käynnistää poikkeaman jälkiselvitys ja oppia tapahtuneesta tulevaisuutta varten.	Suorita poikkeaman jälkiselvitys, tunnista tarvittavat toimenpiteet ja päivitä poikkeamanhallintasuunnitelmaa.

6 Poikkeaman jälkiselvitys

Kriisin päätyttyä ja liiketoimintojen normalisoiduttua on tärkeää käynnistää hyökkäyksen jälkiselvitys ja oppia tapahtuneesta tulevaisuutta varten. Samalla kriisinhallintasuunnitelmat on syytä päivittää tehtyjen havaintojen mukaan. On mahdollista, että organisaatio joutuu uudelleen vastaavan hyökkäyksen uhriksi, mikäli tapahtuneen juurisyyt eivät selviä eikä tapauksesta oteta opiksi.

Jälkiselvityksessä (engl. Post Incident Review) tarkastellaan toimintaa kriisitilanteessa: mitkä toimet tehtiin hyvin, missä oli parantamisen varaa ja kuinka voidaan parantaa turvallisuustasoa ja -suunnitelmia. Jälkiselvityksestä on syytä laatia raportti, joka tarkastelee tapahtumien kulun lisäksi ainakin seuraavia kysymyksiä:

- Tapahtuman juurisyyt:
  - Mitkä tekniset tai toiminnalliset heikkoudet johtivat tilanteeseen?
- Oman suojauksen tehokkuus:
  - Olivatko hyökkäyksien havaitsemista varten käytetyt kontrollit riittäviä?
  - Aiheuttivatko hyökkääjän toimet hälytyksiä?
  - Miten hälytyksiin reagoitiin? Välittyikö tieto hälytyksistä oikeille vastuuhenkilöille?
- Toiminta kriisitilanteessa:
  - Noudatettiinko kriisisuunnitelmaa? Miten käyttökelpoinen se oli?
  - Jaettiinko kriisiryhmän vastuut oikeille henkilöille?
  - Miten hyökkäyksen rajaamisessa ja hyökkääjän karkottamisessa onnistuttiin?
  - Kuinka kriisiryhmän viestintä onnistui? Miten sidosryhmät huomioitiin?
- Palautuminen:
  - Miten kriittisten tietojen ja palveluiden palautuminen onnistui?
- Jälkiselvitys:
  - Onko tapahtumien kulku ja selvitystyö dokumentoitu?
  - Oliko tapauksen tekninen tutkinta riittävää? Onko esim. viranomaisten käyttöön voitu toimittaa riittävät aineistot hyökkäyksestä?
  - Arvioi palvelutoimittajien toimintaa. Oliko vasteaika ja sovitut palvelut riittäviä tapauksen selvittämistyötä varten?

Organisaation tulee päivittää omaa poikkeamanhallintasuunnitelmaansa ja tarkempia erilaisten poikkeamien torjuntaan suunniteltuja pelikirjoja tapahtuneen jälkeen. On myös suositeltavaa harjoitella eri skenaarioita säännöllisin väliajoin, jotta niiden hyöty kriisitilanteissa voidaan varmistaa.

Kyberturvallisuuskeskus toivoo, että yritykset ja organisaatiot jakaisivat sillekin tärkeimmät poikkeamasta saamansa opit. Tapausraporttien avulla Kyberturvallisuuskeskus voi auttaa muita organisaatioita Suomessa ja kansainvälisesti vastaavien tapauksen selvittämisessä. Palautumisesta saadut opit auttavat kehittämään kaikkien organisaatioiden varautumista.

Liitetiedostot

Liite 1

Kuvan 1 (Tyypillinen vastuunjakomalli, jonka lähteenä on Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)) tietosisältö taulukkomuodossa (saavutettava versio).

Taulukko 2 Tyypillinen vastuunjakomalli esitettynä taulukkomuodossa

Pilvipalvelutyyppi	Vastuunjakomalli
IaaS (Infrastructure-as-a-Service)	Asiakkaan (engl. Customer / Tenant) vastuulla tyypillisesti ovat: Rajapinta (Interface), Sovellus (Application), Ratkaisupino (Stack) ja Käyttöjärjestelmä (Operating System) Palveluntarjoajan (engl. Provider) vastuulla tyypillisesti ovat: Virtualisointi (Virtualisation), Laskenta ja tallennus (Compute & Storage), Verkko (Networking) ja Palvelinkeskus (Facility)
PaaS (Platform-as-a-Service)	Asiakkaan (engl. Customer / Tenant) vastuulla tyypillisesti ovat: Rajapinta (Interface) ja Sovellus (Application) Palveluntarjoajan (engl. Provider) vastuulla tyypillisesti ovat: Ratkaisupino (Stack), Käyttöjärjestelmä (Operating System), Virtualisointi (Virtualisation), Laskenta ja tallennus (Compute & Storage), Verkko (Networking) ja Palvelinkeskus (Facility)
SaaS (Software-as-a-Service)	Asiakkaan (engl. Customer / Tenant) vastuulla tyypillisesti on: Rajapinta (Interface) Palveluntarjoajan (engl. Provider) vastuulla tyypillisesti ovat: Sovellus (Application), Ratkaisupino (Stack), Käyttöjärjestelmä (Operating System), Virtualisointi (Virtualisation), Laskenta ja tallennus (Compute & Storage), Verkko (Networking) ja Palvelinkeskus (Facility)

Liite 2

Kuvassa 2 olevan kaavion tietosisältö taulukkomuodossa (saavutettava versio).

Taulukko 23 Pilviympäristön poikkeamanselvityksen työnkulku esitettynä taulukkomuodossa

Vaihe	Lisätiedot tai vaihtoehtoinen prosessikulku
Välittömät toimenpiteet	
Palvelussa havaitaan poikkeama	
Onko palvelu organisaatiosi omassa ylläpidossa?	Jos ei, ilmoita pilvipalveluntarjoajalle. Palveluntarjoaja vastaa teknisistä toimenpiteistä. Seuraa kuitenkin tapahtuman selvittämistä aktiivisesti sekä viesti tilanteesta sisäisille ja ulkoisille sidosryhmille (ml. viranomaiset). Siirry kohtaan "Eristä saastuneet resurssit". Jos kyllä, siirry kohtaan "Tee alustava analyysi".
Tee alustava analyysi. Onko kyseessä poikkeama?	Jos ei, havainto siirretään oikeaan palveluprosessiin ja käsitellään sen mukaisesti. Poikkeaman käsittely päättyy. Jos kyllä, siirry kohtaan "Eristä saastuneet resurssit".
Eristä saastuneet resurssit	Ylläpidä tapahtumalokia tehdyistä toimenpiteistä (ml. tehty toimenpide, aikaleima ja toimenpiteen suorittaja).
Tarvitsetko poikkeaman käsittelyyn apua?	Jos kyllä, ilmoita IT-palveluntarjoajalle ja pyydä apua. Jos ei, siirry kohtaan "Viesti poikkeamasta…".
Viesti poikkeamasta sisäisille ja ulkoisille sidosryhmille	
Tee ilmoitus Kyberturvallisuuskeskukselle ja muille viranomaisille.	Huomioi riittävä viestintä ja tiedon jakaminen koko poikkeaman elinkaaren ajan sisäisille ja ulkoisille sidosryhmille (ml. viranomaiset).
Poikkeaman selvitys	
Tunnista haitallinen toiminta ja kerää tunnistetiedot	
Tunnista ja siivoa saastuneet resurssit ja vaihda tunnukset	
Selvitä poikkeaman laajuus, vaikutukset ja mahdolliset riippuvuudet ja yhteydet	
Onko kriittisiä tietoja tai henkilötietoja vaarantunut?	Jos kyllä, noudata Tietomurto-toimintaohjetta. Jos ei, siirry kohtaan "Epäiletkö että on tapahtunut rikos?"
Epäiletkö että on tapahtunut rikos?	Jos kyllä, tee rikosilmoitus Poliisille. Jos ei, siirry kohtaan "Tallenna lokitiedostot…".
Tallenna lokitiedostot ja muu todistusaineisto myöhempää tutkimusta varten	
Auttoivatko toimenpiteet ja onko uhka saatu poistettua?	Jos ei, siirry takaisin kohtaan "Tunnista ja siivoa saastuneet resurssit ja vaihda tunnukset". Jos kyllä, jatka kohtaan "Varmista pääkäyttäjätunnusten turvallisuus ja palauta tunnukset".
Palautuminen	
Varmista pääkäyttäjätunnusten turvallisuus ja palauta tunnukset	
Perusta korvaavat pilviresurssit	
Aloita palautumisprosessi kriittisimmistä järjestelmistä	Viesti sisäisille ja ulkoisille sidosryhmille poikkeamatilanteen päättymisestä.
Suorita poikkeaman jälkiselvitys	
(Prosessi päättyy)	

Liite 3

Ohjeen infolaatikoiden tietosisältö taulukkomuodossa (saavutettava versio).

Taulukko 4 Ohjeessa esiintyvien infolaatikoiden tietosisältö taulukkomuodossa

Sivu	Infolaatikko
Sivu 3	Huom! Tämä ohje on laadittu 2023. Pilvipalveluiden ominaisuudet kehittyvät tiuhaan tahtiin ja jotkin tässä ohjeessa mainituista teknologioista tai käytännöistä eivät välttämättä ole ajantasaisia ohjeen lukuhetkellä. Ajantasaisin tieto esimerkiksi tietyn pilvipalvelualustan turvallisuusominaisuuksista löytyy kyseisen palvelun omasta ohjeistosta. Voit myös tarkistaa, onko tästä ohjeesta uudempaa versiota Kyberturvallisuuskeskuksen ohjekokoelmassa osoitteessa https://www.kyberturvallisuuskeskus.fi.
Sivu 7	Pilviympäristöissä käytetään usein cloud security posture management (CSPM)-tuotteita, jotka ovat pilvialustalle räätälöityjä ratkaisuja pilviresurssien tietoturvakonfiguraatioiden hallintaan. Tuotteet voivat sisältää ja integroida myös pilven työkuormien haavoittuvuuksien ja uhkien havainnointia. Esimerkiksi Azure Defender for Cloud ja AWS Security Hub ovat tällaisia maksullisia tuotteita. Pilven asiakas saattaa valita hyödyntää osin näiden sijasta konesaliympäristöön lisensoituja tuotteita, kuten haavoittuvuusskannereita ja EDR-tuotteita. Tärkeää on tunnistaa, että toimittaessa IaaS- ja PaaS-alustojen parissa näiden hankinta, käyttöönotto ja havaintojen operointi on asiakkaan vastuulla.
Sivu 8	Esim. Azure-pilvessä toimittaessa hallintatason toimenpiteistä muodostuu resource log -tyyppiset lokit, joista ilmenee palveluiden elinkaareen liittyvät toimenpiteet, kuten luonti ja konfiguraatiomuutokset. Sen sijaan resurssien varsinaisesta käytöstä, kuten tietokannan, tallennuspalvelun, tai Azure Key vault-salaisuuksien käytöstä ei muodostu automaattisesti activity log -lokeja, vaan niiden käyttöönotto ja elinkaaren hallinta on asiakkaan vastuulla.
Sivu 10	Pilvipalveluiden ominaisuudet laajenevat ja monipuolistuvat koko ajan. Yleensä palveluiden valmistajat eivät heikennä ominaisuuksia tietoturvanäkökulmasta. Joskus niin voi odottamatta tapahtua. Toisaalta palveluiden tietoturvamahdollisuudet voivat myös parantua ajan myötä. Siksi on tärkeää varmistaa, että osaava henkilöstö seuraa palveluiden kehittymistä ja osaa arvioida miten muuttuvia ominaisuuksia hyödynnetään tehokkaasti ja turvallisesti.
Sivu 11	Varmista, että poikkeamatilanteessa tarvittava dokumentaatio on saatavissa myös sellaisissa tilanteissa, joissa ensisijainen dokumentaation säilytyspaikka kuten verkkopalvelu ei ole käytettävissä.
Sivu 12	Luku käsittelee teknisiä toimenpiteitä ylätasolla. Koska eri pilvipalvelut ovat erilaisia, kaikkien teknisten toimien osalta on tärkeää, että tutustut pilvipalveluntarjoajan omiin aiheeseen liittyviin ohjeisiin, joista löytyy ajantasainen tieto.
Sivu 13	Pilven tallennuspalveluiden (esim. AWS S3 tai Azure storage account) huolimaton käyttöönotto höllentämällä oletusasetuksia voi johtaa vahinkoon, jossa kaikki tallennetut tiedot ovat hyökkääjän löydettävissä internetin verkko-osoitteesta. Tällainen voisi tapahtua esim. noudattamalla jotakin valmista verkosta löytyvää mallia/ohjetta, ymmärtämättä kaikkia sen sisältämiä ohjeita ja asetuksia täysin.
Sivu 15	Huolehdi myös siitä, että pilviympäristössä tehdyt testitilit ja resurssikokeilut ovat asianmukaisesti suojattuja. Kokeiluun tai harjoitteluun tarkoitetun resurssin käyttö saattaa laajentua ajan saatossa, niin että siitä tulee vakiintunut osa organisaation IT-kokonaisuutta. Mikäli resurssia perustettaessa tietoturvallisuutta ei ole huomioitu, on riskinä, että resurssin suojaukset ovat puutteelliset. Pilviympäristöissä on hyvä ottaa käyttöön vakioidut määritykset (engl. policy) ja mallit (engl. templates), joilla voidaan ohjata organisaation pilviresurssien vakioituja asetuksia ja varmistaa niiden täyttävän organisaation vaatimukset.
Sivu 16	Hätäkäyttöön tarkoitettujen tunnusten tulisi aina olla automatisoidun valvonnan piirissä siten, että niiden käytöstä aiheutuu hälytys yrityksen avainhenkilöille.
Sivu 18	Esimerkiksi kontteihin perustuva mikropalveluympäristö on hajautunut usein niin, että tietoturvaa koskevien tärkeiden tapahtumien valvonta edellyttää tarkkaa suunnittelua. Tällöin on varmistettava yhdenmukainen lokituskäytäntö ja automatisoitu lokien käsittely normaalista poikkeavien tapahtumien havaitsemiseksi.
Sivu 22	Huom! Kaikkien edellä mainittujen hälytysten ja tietoturva-teknologioiden osalta on tärkeää varmistaa, että organisaatiolla on sovittu, mikä tiimi tai rooli vastaa hälytysten seuraamisesta ja niihin reagoinnista. Paraskaan työkalu ei auta poikkeamatilanteessa, jos manuaalista työtä vaativiin hälytyksiin ei reagoida.

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-879-9
ISSN 2669-8757 (verkkojulkaisu)

Huoltovarmuuskeskus

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus