jamk.fi

Pilvipalvelun käyttöönoton tietoturva

Office365-pilvipalvelun tietoturvan arviointi julkisen sektorin vaatimusten pohjalta

Ville Halminen

Opinnäytetyö
Toukokuu 2019
Tekniikan ja liikenteen ala
Insinööri (AMK), tieto- ja viestintätekniikan tutkinto-ohjelma
Kyberturvallisuus

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Halminen, Ville	Opinnäytetyö, AMK	05/2019
	Sivumäärä 40	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: X

Työn nimi

Pilvipalvelun käyttöönoton tietoturva

Office365-pilvipalvelun tietoturvan arviointi julkisen sektorin vaatimusten pohjalta

Tutkinto-ohjelma

Tieto- ja viestintätekniikka

Työn ohjaaja(t)

Sampo Kotikoski, Juha Saarisilta

Toimeksiantaja(t)

Istekki Oy

Tiivistelmä

Istekki Oy:lle tehdyn opinnäytetyön tarkoituksena oli selvittää minkälaisia vaatimuksia eri viranomaistahoista, säädöksistä tai laeista kohdistuu julkishallinnon toimijoiden pilvipalveluiden tietoturvalle sekä kuinka näitä vaatimuksia pystytään toteuttamaan Office365-palvelun tarjoamilla kontrolleilla. Lisäksi haluttiin muodostaa Istekin asiantuntijoille tehtävälista, jota he pystyvät käyttämään työssään avuksi ottaessaan käyttöön Office365-palvelua eri julkisen sektorin toimijoille.

Teoriaosuudessa selvitettiin vaatimuksia valtiovarainministeriön julkisen hallinnon pilvipalvelulinjauksista, EU:n tietosuoja-asetuksesta sekä terveyden- ja hyvinvoinnin laitoksen määräyksistä sekä kuvattiin tietyt oleelliset Microsoftin Office365-palvelun tietoturvakontrollit ja niiden mahdollisuudet sekä toteutustavat.

Tarkkojen teknisten vaatimusten löytäminen julkisen hallinnon pilvipalveluiden tietoturvalle oli haastavaa löytää, mutta etenkin valtiovarainministeriön linjaukset antoivat hyvät lähtökohdat tietoturvan arvioinnille. Office365-palvelusta löydettiin useita hyviä tietoturvakontrolleja, joilla vaatimusten asettamia määreitä pystyttiin toteuttamaan.

Viranomaislähteiden vaatimuksista ei saatu riittävän laajaa kuvaa siihen, että olisi voitu sanoa Office365-palvelun täyttävän kaikki julkisen sektorin pilvipalvelun tietoturvan vaatimukset, mutta Office365-palvelussa olevilla tietoturvakontrolleilla pystytään toteuttamaan valtiovarainministeriön julkisen hallinnon pilvipalvelulinjauksien kuvaamat linjaukset.

Avainsanat (asiasanat)

Office365, pilvipalvelu, julkinen sektori, tietoturva, tietosuoja

Muut tiedot (salassa pidettävät liitteet)

Liite 2 on salassa pidettävä ja poistettu julkisesta työstä. Salassapidon peruste Julkisuuslain 621/1999 24§, kohta 17, yrityksen liike- tai ammattisalaisuus. Salassa pitoaika kymmenen (10) vuotta, salassapito päättyy 15.5.2029.

jamk.fi

Description

Author(s)	Type of publication	Date
Halminen, VIlle	Bachelor's thesis	May 2019
		Language of publication: Finnish
	Number of pages: 40	Permission for web publication: x

Title of publication

Information security in deployment of cloud service

Examination of the information security of Office365 cloud service in the public sector

Degree programme

Information and communications technology

Supervisor(s)

Kotikoski Sampo, Saarisilta Juha

Assigned by

Istekki Oy

Abstract

The goal of the thesis was to examine the recommendations, requirements and laws regarding information security of the cloud services of the public sector and how these requirements can be satisfied with the security measures offered in the Office365 service. Secondary goal was to produce a list of tasks that the specialists of Istekki can use when implementing the Office365 service for the organization of the public sector.

The Ministry of Finance's policies regarding the cloud services of the public sector, the European Union's general data protection regulation and the specifications of the National Institute for Health and Welfare were used to build a foundation of the required information security and data protection regulations and rules to comply with. The essential security measures and controls made possible by Office365 were also described.

Finding precise and exact requirements for the information security of the public sector's cloud services was challenging, but especially the policies of the Finnish Ministry of Finance proved to be useful for this purpose. Multitude of useful security measures in Office365 were identified to be useful in complying with the requirements set to the public sector.

The extent of the requirements set to the information security of the public sector could have been wider and because of this it couldn't be determined if the controls available in the Office365 service were enough to meet the given criteria. Most of the given requirements were acceptably met with the information security controls and measures that Office365 offers.

Keywords/tags (subjects)

Office365, cloud service, public sector, information security, data protection

Miscellaneous (Confidential information)

Annex 2 is confidential and is removed from the published thesis. Confidentiality is based on the Act on the Openness of Government Activities 621/1999 24§, subsection 17, commercial and trade secrets of a business. This document is classified as confidential until May 15th, 2029.

Sisältö

Kuviot

Taulukot

Sanasto

AAD	Azure Active Directory
AD	Active Directory
ADFS	Active Directory Federation Services
ADFS claim	ADFS:n myöntämä autentikaatiopoletti
Iaas	Infrastructure as a Service, pilvipalvelumalli
ICMT	Information, Communications and Medical Technology
IMAP	Internet Message Access Protocol, sähköpostiprotokolla
IPv4	Internet Protocol versio 4, tietoliikenneprotokolla
Katakri	Tietoturvallisuuden auditointityökalu viranomaisille
MFA	Multi-Factor Authentication, monivaiheinen varmennus
NIST	National Institute of Standards and Technology
O365	Office365, Microsoftin tarjoama pilvipalvelu
PaaS	Platform as a Service, pilvipalvelumalli
POP	Post Office Protocol, sähköpostiprotokolla
RBAC	Role-Based Access Control, roolipohjainen pääsynhallinta
SaaS	Software as a Service, pilvipalvelumalli
SMTP	Simple Mail Transfer Protocol, sähköpostiprotokolla
VAHTI	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

1 Lähtökohdat

1.1 Toimeksiantaja

Istekki Oy tarjoaa ICMT-ratkaisuja asiakasomistajilleen, joita ovat

- Pohjois-Savon, Etelä-Pohjanmaan, Etelä-Savon, Itä-Savon, Kanta-Hämeen, Keski-Suomen ja Pirkanmaan sairaanhoitopiirien kuntayhtymät
- Kiuruveden, Kuopion, Suonenjoen ja Varkauden kaupungit
- Kaavin, Keiteleen, Lapinlahden, Leppävirran, Pielaveden, Rautalammin, Rautavaaran, Siilinjärven, Tervon, Tuusniemen ja Vesannon kunnat
- Sansia Oy, ISLAB, Kuhilas Oy, KuntaPro Oy, LapIT Oy, Nordlab, Pohjois-Karjalan tietotekniikkakeskus, Pohjois-Savon liitto, Servica, Savon ICT-palvelut Oy ja Ylä-Savon SOTE kuntayhtymä

Istekki tarjoaa asiakasomistajilleen Microsoftin Office365-pilvipalvelun (jatkossa O365 tai O365-palvelu) käyttöönottoa palvelunaan. Osana O365-palvelua Istekki tarjoaa tietoturvan määrittelyjä, suosituksia ja asetuksia. Tämän opinnäytetyön tarkoituksena on luoda kattava näkemys mahdollisista tietoturvakontrolleista, joita voidaan ottaa käyttöön eri lisenssitasoille osana O365-pilvipalvelun käyttöönottoa. Näiden kontrollien kuvaamisen lisäksi tarkoitus on pohtia ja selvittää täyttävätkö O365:n mahdollistamat tietoturvakontrollit ja -prosessit julkishallinnon toimijoille asetetut vaatimukset, säädökset ja linjaukset. Työn tuloksena on tarkoitus saada Istekin käyttöön tehtävälistaus, joita käyttöönoton eri osapuolien täytyy huomioida, määritellä ja päättää.

Istekin asiakasomistajien julkishallinnollisesta luonteesta johtuen on pilvipalveluiden käyttöönoton yhteydessä tietoturvan ja tietosuojan osalta huomioitava Suomen lain sekä EU:n tietosuoja-asetuksen asettamat vaatimukset julkishallinnon toimijoille. Näiden tavoitteiden saavuttamiseksi Office365-palvelun tarjoamia tietoturvakontrolleja arvioidaan käyttämällä kriteeristönä Valtiovarainministeriön julkaisemia julkisen hallinnon pilvipalvelulinjauksia, Terveyden ja hyvinvoinnin laitoksen määräyksiä sekä VAHTI-ohjeistuksia.

Microsoft tarjoaa O365-palveluun monia eri tason lisenssiratkaisuja. Tässä työssä sivutaan E5-lisenssitason ominaisuuksia ja sen mahdollistamia toimintoja, mutta pääasiallinen tietoturvakontrollien huomiointi ja selvitys tehdään E3-lisenssitasolle, joka

tarjoaa käytetyimmät O365-palveluun kuuluvat komponentit. (The Most Popular Office 365 Products Revealed, N.d.)

1.2 Tutkimusmenetelmät ja tutkimuskysymys

Opinnäytetyön tarkoituksena on tutkia millaisia vaatimuksia, linjauksia, säädöksiä, asetuksia tai lakeja julkisen hallinnon toimijoiden pilvipalveluiden tietoturvalle on asetettu ja kuinka Microsoftin Office365-palvelun tarjoamilla menetelmillä ja tietoturvakontrolleilla pystytään niitä toteuttamaan. Lisäksi työn tuloksena on tarkoitus muodostaa muistilista Office365-käyttöönoton yhteydessä suoritettavista tehtävistä.

Opinnäytetyön tutkimuskysymyksenä on: Voidaanko julkisen hallinnon pilvipalveluiden tietoturvalle asetetut vaatimukset, linjaukset, säädökset, asetukset ja lait toteuttaa riittävällä tasolla Office365-palvelun tarjoamilla ominaisuuksilla?

Tämän opinnäytetyön tuloksia voivat hyödyntää pilvipalveluiden kanssa työskentelevät tietoturva- ja järjestelmäasiantuntijat, jotka konfiguroivat pilvipalveluiden asetuksia julkisen hallinnon toimijoille.

2 Vaatimukset pilvipalvelun tietoturvalle

2.1 Valtiovarainministeriön pilvipalvelulinjaukset

Valtiovarainministeriön vuonna 2018 julkaisemassa dokumentissa ”Julkisen hallinnon pilvipalvelulinjaukset” määritetään seitsemän linjausta, joilla annetaan julkishallinnon toimijoille ohjeistus siitä, kuinka pilvipalvelut tulisi toteuttaa. Linjaukset ovat seuraavat:

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta
2. Pilvipalveluissa on kiinnitettävä erityistä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen
3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset
4. Mikäli pilvipalvelu tai pilvipalveluteknologia tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita
5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti sekä oleellisten sopimusehtojen muuttuessa
6. Julkisen tiedon käsittelyä ei rajoiteta
7. Ei-julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu

(Julkisen hallinnon pilvipalvelulinjaukset 2018, 9.)

Näiden linjausten taustamateriaalina on käytetty muun muassa Norjan, Skotlannin ja Kanadan vastaavia linjauksia. Osana linjausten tekoa valtiovarainministeriö on myös selvittänyt linjausten edellyttämiä muutoksia VAHTI- sekä muihin tietoturvaohjeistuksiin. (Julkisen hallinnon pilvipalvelulinjaukset 2018, 11.)

Valtiovarainministeriö on todennut pilvipalveluiden toteutusmalleja olevan kolme erilaista: yksityinen pilvi (private cloud), julkinen pilvi (public cloud) sekä hybridipilvi (hybrid cloud). Näiden lisäksi valtiovarainministeriö toteaa olevan perinteinen toteutusmalli eli oma konesali. (Julkisen hallinnon pilvipalvelulinjaukset 2018, 13.)

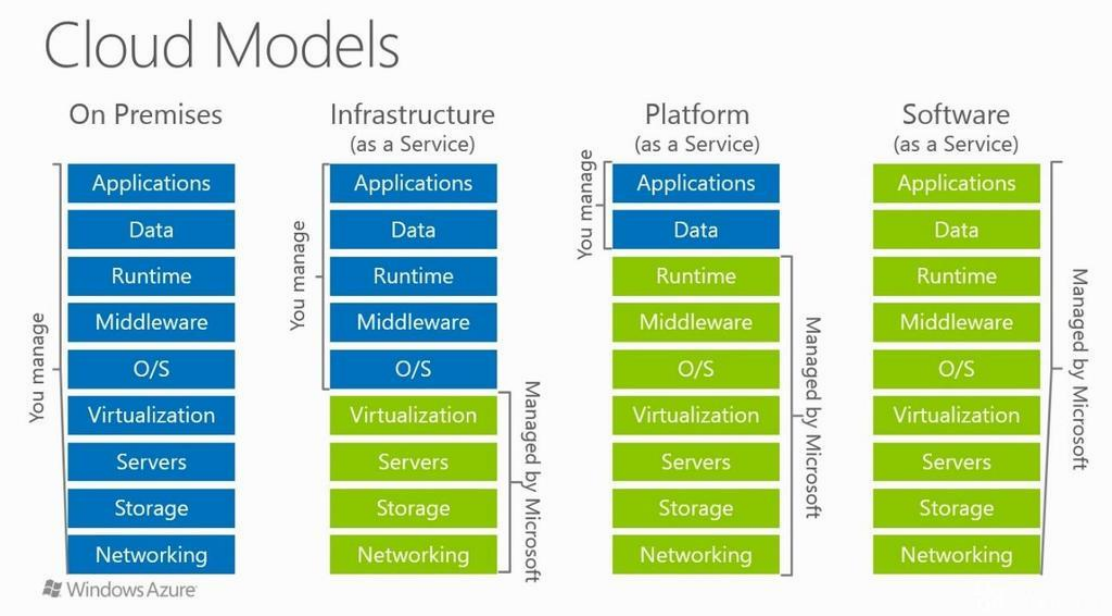
Yksityisellä pilvellä tarkoitetaan palvelua, joka tuotetaan vain palvelua käyttävälle organisaatiolle. Palveluiden tuotteistus- ja vakiointiaste voidaan tyypillisesti sovittaa käyttäjäorganisaation mukaisesti. Palveluiden käyttäjän neuvotteluasema tarjoajaan nähden riippuu palveluiden tuottajasta, mutta on parhaimmillaan suuri. Palveluhyöty ja -takuu sekä käyttösopimukset ovat tyypillisesti neuvoteltavissa. (Julkisen hallinnon pilvipalvelulinjaukset 2018, 14.)

Julkisella pilvellä tarkoitetaan palvelua, joka on julkisesti tarjolla ja hankittavissa kenen tahansa toimesta. Palvelut ovat tyypillisesti erittäin pitkälle tuotteistettuja ja kustannustehokkaita. Palvelun käyttäjän neuvotteluasema tarjoajaan nähden on pieni, jolloin tarjottavan palvelun palveluhyöty ja -takuu voivat muuttua. Käyttösopimukset ovat myös tyypillisesti standardoituja, jotka täytyy hyväksyä sellaisenaan. (Julkisen hallinnon pilvipalvelulinjaukset 2018, 14.)

Hybridipilvellä tarkoittaa palvelua, jossa yhdistetään oma konesali tai yksityinen pilvi sekä julkinen pilvi yhdeksi palvelukokonaisuudeksi. Tällöin julkista pilveä voidaan käyttää oman konesalin tai yksityisen pilven ”jatkeena” esimerkiksi tilanteessa, jossa tarvitaan nopeasti lisäkapasiteettia. Hybridipilvi mahdollistaa myös tietojen hajasijoittamisen eri pilvien välillä. Palveluhyöty ja -takuu sekä käyttösopimukset ovat tyypillisesti neuvoteltavissa. (Julkisen hallinnon pilvipalvelulinjaukset 2018, 14-15.)

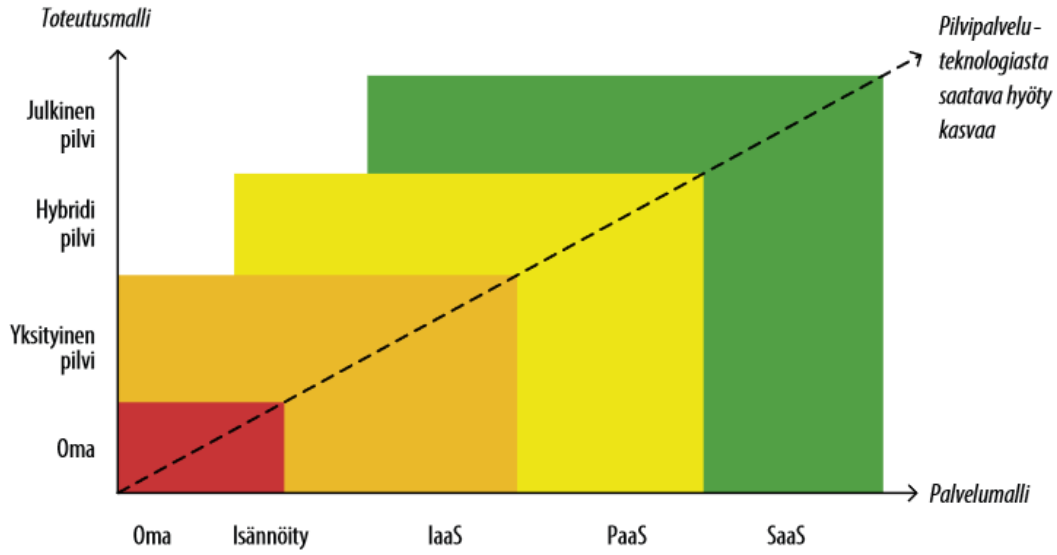
Valtiovarainministeriö on määritellyt kolme eri pilvipalveluiden pääpalvelumallia: infrastruktuuri palveluna (IaaS), ohjelmistoalusta palveluna (PaaS) sekä ohjelmisto pal-

veluna (SaaS) (Julkisen hallinnon pilvipalvelulinjaukset 2018, 13). Kuviossa 1 on esitetty, kuinka eri palvelumalli vaikuttaa asiakkaan ja toimittajan väliseen vastuunjakoon.



Kuvio 1. Pilvipalvelumallien vaikutus asiakas- ja toimittajavastuisiin (Nugara 2017).

Valtiovarainministeriön linjauksissa on esitetty, että pilvipalvelun edut kasvavat yleisellä tasolla, kun palvelu- ja toteutusmallin laajuutta kasvatetaan (Julkisen hallinnon pilvipalvelulinjaukset 2018, 15). Tämä on havainnollistettu kuviossa 2.



Kuvio 2. Pilvipalveluista saatava etu palvelu- ja toteutusmallien muuttuessa (Julkisen hallinnon pilvipalvelulinjaukset 2018, 15).

Julkisen hallinnon pilvipalvelulinjauksissa (2019) valtiovarainministeriö on todennut, että pilvipalveluiden tuottajilla on tyypillisesti palveluun liittyen parempi kyvykkyys ja paremmat resurssit toteuttaa tietoturvaa kuin palvelun käyttäjillä, jolloin palvelun käyttäjän näkökulmasta tarvittava tietoturvaosaamisen määrä pienenee. (Julkisen hallinnon pilvipalvelulinjaukset 2018, 16.)

2.2 Terveyden ja hyvinvoinnin laitoksen (THL) määräykset

Terveyden ja hyvinvoinnin laitoksen (THL) laitoksen määräyksen 1/2015 kuvaamat vaatimukset koskevat Kanta-palveluihin liittyviä järjestelmiä ja Kanta-välityspalveluita, jotka kuuluvat käyttötarkoituksensa ja ominaisuuksiensa perusteella 19 b § mukaiseen luokkaan A (Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset, 3). Office365-palvelu ei ole tämän määräyksen soveltamisalan piirissä, mutta Istekin asiakasomistajilla voi tulevaisuudessa olla tarvetta rakentaa ratkaisuja, joissa O365-palvelu tai sen osat olisivat tämän määräyksen vaatimusten piirissä.

Terveyden ja hyvinvoinnin laitoksen määräyksessä 1/2015: ”A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset” mainitaan, että määräyksessä luetellut tietoturvavaatimuksien täyttyminen tulee auditoida hyväksytyn tietoturvallisuuden arviointilaitoksen toimesta. Määräys 1/2015 koskee kaikkia Kanta-palveluihin liittyviä järjestelmiä ja Kanta-välityspalveluita, jotka kuuluvat käyttötarkoituksensa ja ominaisuuksiensa perusteella asiakastietolain 19 b § mukaiseen luokkaan A. Määräyksen 1/2015 liitteessä 1 (Tietoturvavaatimukset A-luokkaan kuuluville järjestelmille ja järjestelmien käyttöympäristöille) kohdassa 2 kriteeriksi on määritelty ”Asiakirjan muuttumattomuus tulee pystyä varmistamaan.” Kriteerin tarkemmaksi kontrolliksi on määritetty, että asiakirjojen muuttumattomuus tulee varmistaa sähköisellä allekirjoituksella sekä paikallisessa tallennuksessa että tiedonsiirrossa. Asiakirjan muodostamisesta tulee muodostua lokimerkintä. Lisäksi sähköiset potilasasiakirjat tulee allekirjoittaa organisaation tai tietoteknisen laitteen tekemällä kehittynyttä sähköistä allekirjoitusta luotettavuudeltaan vastaavalla allekirjoituksella, niin sanotulla järjestelmäallekirjoituksella. (Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset: Liite 1.)

THL:n määräyksen 1/2015 kriteerin 4 mukaan tietojärjestelmän käyttäjä tulee pystyä tunnistamaan ja todentamaan yksiselitteisesti ja tunnistamisessa tulee käyttää terveydenhuollon varmennepalvelua ja varmenteita, mutta erityistilanteissa voi käyttää käyttäjätunnusta ja vahvaa salasanaa. Kontrollissa mainitaan myös, että järjestelmässä ei saa olla yleisiä ylläpito- tai muita vastaavia oikeuksia ja toiminnallisuuksia, joiden avulla järjestelmän käyttö ilman käyttäjän yksiselitteistä tunnistamista olisi mahdollista. (Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset: Liite 1, kriteeri 4.)

Tietojärjestelmien tuotantoympäristöihin kirjautuessa tulee käyttää ainoastaan varmennekorttia tai vahvaa salasanaa. Muuta kuin varmennekorttia käytettäessä voi käyttää ainoastaan organisaation omassa potilastietojärjestelmässä olevia tietoja. Käyttäjien mahdolliset salasanat tulevat olla vahvat ja ne tulee vaihtaa säännöllisesti. Vanhenemisvaatimukset eivät koske järjestelmän teknisten ylläpitäjien salasanoja. Järjestelmä ei saa välittää vahvaa salasanaa muille järjestelmille. Vahvan salasanan määritelmät ovat määritelty Vahti-ohjeistuksen Sisäverkko-ohjeessa. (Määräys

1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset: Liite 1, kriteeri 5.)

Tietojärjestelmän tulee mahdollistaa eri tasoisten käyttöoikeuksien myöntäminen käyttäjäryhmittäin ja työrooleittain järjestelmän käyttötarkoituksen mukaisesti. Järjestelmässä tulee olla poikkeustilanteiden hallinnan edellyttämät toiminnot, joilla käyttöoikeus voidaan tilapäisesti ohittaa. Tämä tarkoittaa sitä, että jokin toimenpide voidaan tehdä esimerkiksi järjestelmän pääkäyttäjän oikeuksilla, vaikka kyseinen toimenpide ei kuuluisikaan pääkäyttäjän tehtäviin. Toimenpide ja sen tekijä tulee lokittaa selkeästi ja yksilöivästi. (Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset: Liite 1, kriteeri 8.)

THL:n määräyksen 1/2015 liitteen 1 kriteerissä 11 määritetään, että järjestelmissä ei saa olla aktiivisia oletustunnuksia tai -asetuksia, jotka ovat tietoturvallisuuden kannalta huonoja asetuksia.

2.3 Viestintäviraston suositukset liittyen Office365-palveluun

Viestintävirasto on julkaissut useita varoituksia ja tiedotteita liittyen Office365-palveluun kohdistettuihin hyökkäyksiin vuoden 2018 aikana. Viestintävirasto suositellee tiedotteissaan suojautumiskeinoiksi monivaiheisen varmennuksen (MFA) käyttämistä huolellisesti määriteltynä siten, että kaikki sallitut yhteystavat ja protokollat kuten EWS, ActiveSync ja POP/IMAP vaativat monivaiheista varmennusta. Lisäksi ylläpitäjien tulisi viestintäviraston mukaan varmistaa, että modern authentication -menetelmä on käytössä ja että vain kyseistä menetelmää tukevia sovelluksia saa käyttää. (Tietojenkalastelijat pyrkivät ohittamaan Office365 -palvelun monivaiheisen todentamisen, 2018.)

Viestintävirasto mainitsee 11.06.2018 julkaistussa tiedotteessaan, että useiden suomalaisten yritysten työntekijöiden käyttäjätunnuksilla on tehty useita petoksia ja petoksen yrityksiä. Tarvittaviksi suojatoimiksi viestintävirasto suosittelee, että tietojenkalastelun estämiseksi tulisi ottaa käyttöön lähettäjän osoitteen väärentämisen estäviä menetelmiä, joita Office365-palvelussa on tarjolla. Lisäksi sähköpostilaatikoiden edelleenohjaussäännöt tulee tarkistaa ja uusien sääntöjen tekemistä tulee rajoittaa

Microsoftin ohjeiden ja suositusten mukaisesti sekä havaituista huijausyrityksistä tulee ilmoittaa viranomaisille. Onnistuneista huijauksista pitäisi tehdä rikosilmoitus. (Suojaustoimia Office365 -tunnusten tietojenkalastelua vastaan, 2018.)

2.4 EU:n tietosuoja-asetuksen vaatimukset

Euroopan unionin tietosuoja-asetuksen luvun 5 artiklan 45 kohdassa 1 mainitaan seuraavaa: ”Henkilötietojen siirto johonkin kolmanteen maahan tai kansainväliselle järjestölle voidaan toteuttaa, jos komissio on päättänyt, että kyseinen kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kyseinen kansainvälinen järjestö varmistaa riittävän tietosuojan tason. Tällaiselle siirrolle ei tarvita erityistä lupaa.” Kolmas maa tarkoittaa tässä yhteydessä komission erikseen hyväksymää Euroopan unionin ulkopuolista maata. Komissio arvioi hyväksyttäväksi ehdotettuja maita artiklan 45 kohdan 2 perusteella. Komissio julkaisee Euroopan unionin virallisessa lehdessä ja verkkosivustollaan luettelon niistä kolmansista maista ja maiden alueista sekä kansainvälisistä järjestöistä, joiden tietosuojan tason se on todennut riittämättömäksi. (Euroopan parlamentin ja neuvoston asetus 2016/679.)

Henkilötietojen siirto voidaan suorittaa Euroopan unionin ulkopuolisiin maihin myös sellaisessa tilanteessa, jossa komissio ei ole kohdemaata tai -järjestöä erikseen hyväksynyt. Tällaisessa tapauksessa tietojensiirron tulee noudattaa artiklan 46 kuvaamia asianmukaisia suojatoimia soveltaen. Artiklassa 46 lueteltuja suojatoimia ovat:

- viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline
- 47 artiklan mukaiset yritystä koskevat sitovat säännöt
- komission artiklan 93 kohdassa 2 tarkoitettua tarkastelumenettelyä noudattaen antamat tietosuojaa koskevat vakiolausekkeet
- tietosuojaa koskevat vakiolausekkeet, jotka tietosuojaviranomainen vahvistaa ja jotka komissio hyväksyy artiklan 93 kohdassa 2 tarkoitettua tarkastelumenettelyä noudattaen
- artiklassa 40 tarkoitetut hyväksytyt käytännesäännöt yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi, myös rekisteröityjen oikeuksiin
- artiklassa 42 tarkoitettu hyväksytty sertifiointimekanismi yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa asianmukaisten suojatoimien soveltamiseksi, myös rekisteröityjen oikeuksiin. (Euroopan parlamentin ja neuvoston asetus 2016/679.)

Euroopan unionin tietosuoja-asetuksen luvun 5 artiklassa 47 kuvataan yritystä koskevat sitovat säännöt, joiden täyttyessä henkilötietojen siirto kolmanteen maahan, jota Euroopan komissio ei ole hyväksynyt, voidaan sallia. Artiklan 47 kohdan 1 perusteella mainitaan seuraavaa:

1. Toimivaltainen valvontaviranomainen vahvistaa yrityksiä koskevat sitovat säännöt 63 artiklassa säädetyn yhdenmukaisuusmekanismin mukaisesti, jos
    a. säännöt ovat oikeudellisesti sitovat ja niitä sovelletaan kaikkiin asianomaisiin konsernin tai yritysryhmän jäseniin, jotka harjoittavat yhteistä taloudellista toimintaa, työntekijät mukaan luettuna, ja kaikki nämä yksiköt myös panevat säännöt täytäntöön
    b. säännöissä nimenomaisesti annetaan rekisteröidyille täytäntöönpanokelpoisia heidän henkilötietojensa käsittelyä koskevia oikeuksia
    c. säännöt täyttävät 2 kohdassa säädetyt vaatimukset.

Artiklan 47 kohdan 2 vaatimukset kuvataan liitteessä 1. (Euroopan parlamentin ja neuvoston asetus 2016/679.)

3 Office365-palvelun kuvaus

O365 on Microsoft Corporationin tarjoama SaaS-mallin pilvipohjainen tilauspalvelu, joka on osa Microsoft Office -tuoteperhettä. O365-palvelusta on tarjolla useita erilaisia tilausmalleja. Tässä työssä kuvataan Microsoftin Enterprise E3 -tason tilaukseen sisältyvät palvelut, applikaatiot ja tietoturvakontrollit. Enterprise E3 -tason lisenssiin sisältyvät applikaatiot ja palvelut on kuvattu taulukossa 1.

Taulukko 1. Enterprise E3-lisenssin palvelut

Nimi	Applikaatio/Palvelu
Access	Applikaatio (vain PC)
Excel	Applikaatio
OneNote	Applikaatio
Outlook	Applikaatio
PowerPoint	Applikaatio
Publisher	Applikaatio (vain PC)
Word	Applikaatio
Exchange	Palvelu
Microsoft Teams	Palvelu
OneDrive	Palvelu
SharePoint	Palvelu
Stream	Palvelu
Yammer	Palvelu

Tämän työn laajuudessa käsitellään käytetyimpiä Office365-palvelun E3-lisenssiin kuuluvia palveluita: Exchangea, Microsoft Teamsia, OneDrivea sekä SharePointia. Valittavissa olevat sovellukset riippuvat organisaatiolla olevasta lisenssistä sekä organisaation omista valinnoista. (Discover the Microsoft 365 Enterprise solution that's right for you, n.d.)

4 Palveluiden pääsynhallinta

Office365-ympäristön kirjautuminen hybrid-toteutuksissa on toteutettu siten, että kirjautumisen tunnistetiedot synkronoidaan Active Directoryn kanssa käyttämällä Active Directory Federation Services (ADFS) -palvelua. Loppukäyttäjän näkökulmasta tämä tarkoittaa sitä, että O365-palveluihin voi kirjautua samalla tunnuksella, kuin omaan, organisaation toimialueeseen liitettyyn työasemaan.

Office365-palvelu voidaan toteuttaa myös cloud-only -mallilla, jolloin palvelua käyttävän organisaation ei tarvitse itse omistaa tai hankkia perinteistä konesalia, jossa palvelut toimisivat niille erikseen järjestetyillä palvelimilla. Tällaisessa ratkaisussa käyttäjien autentikointi tapahtuu suoraan pilvessä toimivaa tietokantaa vasten.

O365-palvelun pääsynhallinta voidaan normaalin tunnus-salasana -yhdistelmän lisäksi suojata myös monivaiheisen varmenteen Multi-Factor Authentication (MFA) keinoin.

4.1 Monivaiheisen varmennuksen toteuttaminen hallintaportaalista

O365-hallintaportaalin kautta monivaiheiselle varmennukselle voidaan määrittää käyttöön lisäkontrolleja. Kyseiset kontrollit ovat

1. Sovellussalasanat
2. Luotetut verkot
3. Sallitut varmennusmenetelmät
4. Monivaiheisen varmennuksen muistaminen.

Sovellussalasanat voidaan joko sallia tai estää. Sovellusalasanoilla käyttäjä pystyy käyttämään modernia autentikaatiota tukemattomia Office-sovelluksia silloinkin, kun monivaiheinen varmennus vaaditaan. Tällaisia sovelluksia ovat kaikki Office 2010:n -paketin versiot ja sitä vanhemmat Office-sovellukset. (App passwords 2018.)

Luotetuilla verkoilla tarkoitetaan IPv4-verkkoavaruuksia, joista kirjautuminen ilman monivaiheista varmennusta sallitaan. Federoiduissa ympäristöissä voidaan myös sallia organisaation intranetista kirjautuminen ilman monivaiheista varmennusta. Tällöin käyttäjän kirjautuminen sallitaan ADFS-palvelusta saadun claimin avulla. (Trusted IPs 2018.)

Sallituissa varmennusmenetelmissä voidaan määrittää, mitkä varmennustavat käyttäjälle sallitaan käytettäviksi. Mahdollisia vaihtoehtoja ovat tekstiviestivarmennus, puheluvarmennus, suojakoodi Authenticator-mobiilisovelluksesta tai ilmoitus Authenticator-mobiilisovelluksesta. (Verification methods 2018.) NIST ei suosittele tekstiviesti- tai puheluvarmennuksen käyttöä kaksi- tai monivaiheisen varmennuksen autentikointitapana johtuen siitä, että kyseisistä varmennustavoista on löydetty haavoittuvuuksia (SP 800-63-3:2017, 29).

Monivaiheisen varmennuksen muistamisella tarkoitetaan sitä määrää päiviä, jonka käyttäjän sallitaan kirjautua ensimmäisen varmennuksen suoritettuaan ilman uuden varmennuksen kysymistä. Tämä asetus voidaan sallia aikavälillä 1-60 päivää. Mikäli asetus on määritetty käyttöön, myönnetään käyttäjälle ensimmäisen monivaiheisen varmenteen suorittamisen yhteydessä päivitystunniste (refresh token), joka myöntää sallitun ajan verran käyttäjälle uusia pääsytunnisteita (access token) tunnin välein. (Remember multi-factor authentication 2018.)

4.2 Monivaiheisen varmennuksen toteuttaminen Azure AD:sta

Azure Active Directorysta (AAD) voidaan määritellä ehdollisen pääsyn sääntöjä, joiden osana monivaiheinen varmennus voidaan toteuttaa. Ehdollisen pääsyn sääntö voidaan osoittaa koskevaksi joko yksittäistä käyttäjää, käyttäjäryhmää tai kaikkia käyttäjiä. Tämä mahdollistaa monivaiheisen varmennuksen kohdistamisen käyttöoikeusryhmien perusteella, eli esimerkiksi hallintatunnuksille voidaan määrittää tiukemmat MFA-säännöt kuin perustason käyttäjille. Tätä menettelytapaa kutsutaan roolipohjaiseksi pääsynhallinnaksi (RBAC). Tässä kohdassa sääntöä voidaan myös määritellä, että sääntö ei koske joitain tiettyjä yksittäisiä käyttäjiä tai käyttäjäryhmiä. (Users and groups 2018.)

Ehdollisen pääsyn säännöt voidaan kohdistaa koskemaan ainoastaan yhtä, useaa tai kaikkia palveluita. Tämän ominaisuuden perusteella saadaan lisää mahdollisuuksia rajata tai sallia käyttäjien pääsyä tiettyihin palveluihin, sillä se mahdollistaa MFA:n vaatimisen joihinkin, mutta ei kaikkiin, palveluihin. (Cloud apps 2018.)

AAD:n ehdollisen pääsyn sääntö on mahdollista konfiguroida koskemaan vain tietyn, Microsoftin muiden kontrollien määrittämän, riskiluokan käyttäjiä. Tällöin on mahdollista määrittää, että käyttäjät, joiden tili saattaa olla uhan alla, määritetään tiukempien pääsynhallinnan politiikan piiriin. (Sign-in risk 2018.)

Ehdollisen pääsyn sääntö voidaan kohdistaa myös tietyille käyttöjärjestelmille tai alustoille. Tämä tarkoittaa sitä, että esimerkiksi Android-laitteelta kirjautuessa käyttäjän tulee tehdä joitain toimenpiteitä suorittaakseen kirjautumisen onnistuneesti, mutta vaikkapa Windows-laitteelta kirjautuessa kyseisiä toimenpiteitä ei tarvitse

tehdä. Mahdolliset alustarajaukset voidaan tehdä viiden eri alustan perusteella: Windows, Windows-puhelin, iOS, Android ja macOS. (Device platforms 2018.)

AAD:n säännössä voidaan määrittää luotettuja IPv4- tai IPv6-verkkoja samaan tapaan kuin O365-hallintaportaalin määrityksissä, mutta AAD mahdollistaa sen, että nämä verkot voidaan nimetä. Yhden nimetyn verkon alle voidaan määrittää useita verkkopeitteitä, joista kirjautumisen yhteydessä monivaiheista varmennusta joko vaaditaan tai päinvastoin, ei vaadita. (Locations 2018.)

Alkuasetuksilla ehdollisen pääsyn sääntö koskee selainsovelluksia sekä mobiili- ja työpöytäsovelluksia, jotka tukevat modernia autentikointia. Lisäksi säännön asetuksilla voidaan joko sallia tai estää Exchange ActiveSync-sovellukset (vain silloin, kun sääntö on asetettu koskemaan ainoastaan Exchange Onlinea) sekä vanhentuneita autentikointitapoja käyttävät protokollat IMAP, POP ja SMTP. (Client apps 2018.)

4.3 Käyttötapaus monivaiheiselle varmennukselle

MFA on kannattavaa konfiguroida käyttöön Azure Active Directoryn Conditional Access -säännön kautta, koska se mahdollistaa MFA:lle huomattavasti monipuolisemmat konfiguraatiomahdollisuudet kuin Office365:n hallintaportaali. Tässä kappaleessa kuvatun käyttötapauksen lähtökohdat ovat seuraavat:

- Organisaatio X haluaa käyttöönsä monivaiheisen varmennuksen kaikkiin Office365:n tarjoamiin palveluihin
- Organisaation kaikilla jäsenillä ei ole käytettävissään älypuhelinta, johon Authenticator-sovelluksen voi asentaa
- Organisaation omasta IP-verkosta tulee pystyä kirjautumaan Office365-palveluihin ilman MFA-varmennusta, jotta sen käyttö ei aiheuta tarpeettoman paljon haittaa työnteolle
- MFA-säännön tulee koskea kaikkia organisaation käyttäjiä

Näiden kuvattujen lähtökohtien perusteelta organisaatiolle voitaisiin luoda Conditional Access -sääntö, jonka määrityksiksi asetetaan seuraavat ominaisuudet:

- **Users and groups:** Ryhmä, johon kuuluvat kaikki organisaation käyttäjät
- **Cloud apps:** All cloud apps
- **Conditions:** Location: any, except exclude a named location
- **Grant:** Require multi-factor authentication

Kun Conditional Access -sääntö kohdistetaan käyttäjäryhmään, johon kuuluvat kaikki organisaation käyttäjät, tulevat uudet organisaation palvelukseen työsuhteeseen astuvat henkilöt automaattisesti säännön vaikutuksen piiriin, kunhan käyttäjät lisätään uuden työntekijän prosessissa kyseiseen käyttäjäryhmään. Sääntö kohdistetaan koskemaan kaikkia mahdollisia applikaatioita (all cloud apps) ja se vaaditaan kaikista sijainneista (locations), paitsi nimetystä verkkoalueesta, joka on organisaation julkinen IP-verkkoavaruus, joka näkyy Microsoftin palvelimille käyttäjien kirjautuessa organisaation (sisä)verkosta O365-palveluihin. Grant-määrityksellä sallitaan käyttäjien pääsy palveluihin, kunhan he suorittavat MFA-varmennuksen.

Lisäksi sallitaan O365-hallintaportaalista MFA:n vaihtoehdoiksi Authenticator-sovelluksen vahvistuskoodi ja vahvistusilmoitus sekä lisäksi tekstiviestivarmennus, jotta sellaisetkin käyttäjät, joilla ei ole älypuhelinta, voivat suorittaa ja rekisteröidä monivaiheisen varmennuksen käyttöönsä.

5 Tiedon säilytyksen ja luokittelun tietoturvakontrollit

5.1 Yleistä tiedon menetyksen estosta

Data Loss Prevention (DLP) -säännöillä tarkoitetaan sellaisia työkaluja, tietoturvakontrolleja tai prosesseja, joiden tarkoitus on estää arkaluontoisen tiedon jakaminen sellaisille tahoille, joille tiedon ei tahdota päätyvän. Organisaatiot määrittelevät kriteerit, politiikat tai säännöstöt, joiden perusteella DLP-ohjelmistot estävät, hälyttävät tai suojaavat tietoja. (Zhang 2019.)

5.2 Data Loss Prevention O365:ssä

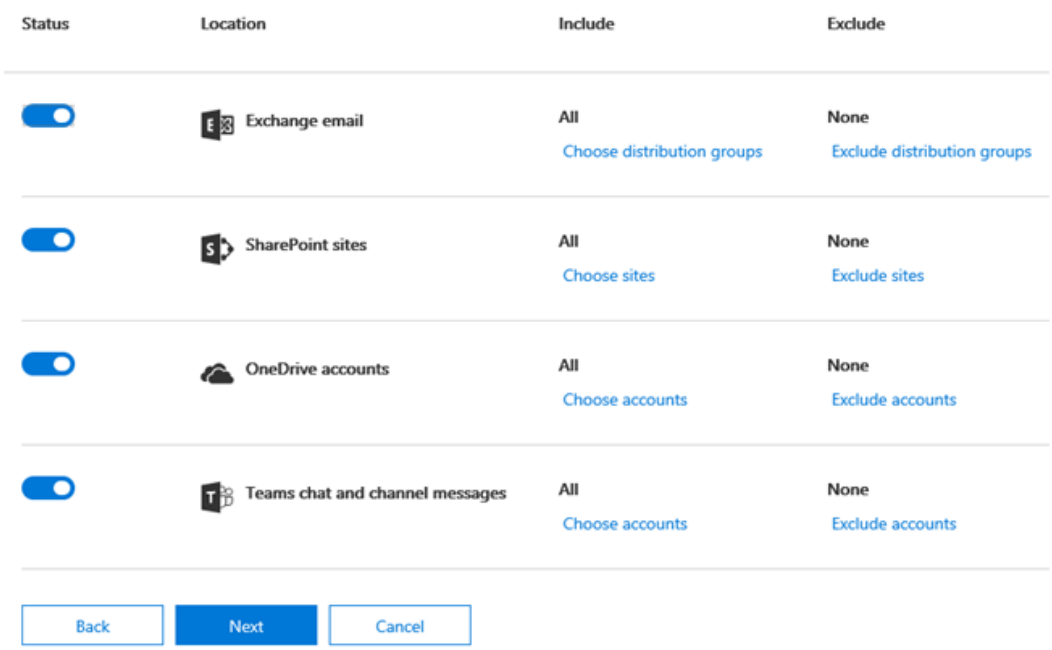
Tiedon menetyksen eston (DLP) säännöillä voidaan saavuttaa seuraavia tavoitteita:

- Arkaluontoisen tiedon tunnistaminen eri palveluissa kuten OneDrivessa, SharePointissa tai Exchange Onlinessa
- Arkaluontoisen tiedon tahallisen tai tahattoman jakamisen estäminen
- Käyttäjien kouluttaminen tietoturvalliseen toimimiseen käytäntövihjeiden tai sähköposti-ilmoitusten kautta
- DLP-sääntöjen osumien raportointi ja tarkastelu

Data Loss Prevention -sääntöjen toiminta yleisellä tasolla on kuvattu kuviossa 3.

Kuvio 3. DLP-säännön toiminta (Overview of data loss prevention policies 2018).

Data Loss Prevention -sääntöön voidaan konfiguroida monia eri ehtoja. Ensimmäisenä ehtona tulee määrittää, missä kohteessa sijaitsevaa tietoa halutaan suojata: Exchange Onlinessa, SharePoint Onlinessa, OneDrivessa vai Microsoft Teamsissa. Näistä vaihtoehdoista voidaan valita niin monta palvelua, kuin tarpeelliseksi nähdään. Lisäksi jokaisesta palvelusta voidaan rajata säännön laajuuden ulkopuolelle joitain ryhmiä, sivustoja tai tilejä. Tämän ominaisuuden vaihtoehtojen konfigurointi on havainnollistettu kuviossa 4. (Overview of data loss prevention policies 2019.)



Kuvio 4. DLP-säännön sijaintikohdisteet (Overview of data loss prevention policies 2018).

5.3 Käyttötapaus Data Loss Prevention -säännölle

Tässä kappaleessa kuvatun käyttötapauksen perusteella organisaatiolla on tiedon menetyksen estolle seuraavat vaatimukset:

- (Suomen) henkilötunnuksia ei saa organisaation tietoturvapolitiikan mukaisesti lähettää salaamattomalla sähköpostilla
- (Suomen) henkilötunnuksia ei saa organisaation tietoturvapolitiikan mukaisesti jakaa SharePointissa ja Teams-työtiloissa
- Yritetyistä jakamisista tulee lähettää hälytykset valvontapostilaatikkoon

Näiden vaatimusten perusteella organisaatiolle voidaan luoda Security&Compliance Centeristä kaksi erillistä Data Loss Prevention -sääntöä. Ensimmäisen säännön määritykset tulee tehdä seuraavasti:

- **Locations:** All distribution groups
- **Conditions:**
  - **Content contains**: Sensitive info type “Finland National ID”, instance count 1 to any, match accuracy min 90% max 100%
  - **Content is shared**: with people outside my organization
- **Actions**: Encrypt email messages
- **User notification**: Notify the user who sent the document
  - **Customize policy tip**: Organisaation tietohallinnon tai vastaavan edustajan kirjoittama käytäntövihje, joka käyttäjälle tulee näkyviin ennen viestin lähettämistä

    - **Customize the email text**: Organisaation tietohallinnon tai vastaavan edustajan kirjoittama sähköposti-ilmoitus, jonka käyttäjä saa lähetettyään sensitiivistä informaatiota sisältävän sähköpostin
- **Incident reports**: Use email incident reports to notify you when a policy match occurs (halytyslaatikko@organisaatio.fi)

Tämä ensimmäinen sääntö koskee ainoastaan sähköpostia ja sen lähettämistä. Mikäli käyttäjä kirjoittaa sähköpostin, joka sisältää suomalaisia henkilötunnuksia, näkyy käyttäjälle sähköpostin ylätunnisteessa kustomoitu käytäntövihje, joka samalla varoittaa käyttäjää että myös kouluttaa häntä tietoturvallisempaan käyttäytymiseen. Mikäli käyttäjä tästä huolimatta lähettää sähköpostin, tulee hänelle sähköposti-ilmoitus, joka kertoo hänen lähettäneen sensitiivistä tietoa. Lähetetty sähköposti salataan automaattisesti ja sähköpostin lähettämisestä tulee halytyslaatikko-nimiseen postilaatikkoon ilmoitus, jonka perusteella ympäristön ylläpitäjät voivat tutkia ja seurata sähköpostien lähettämistä sekä tehdä muita tarvittavia toimenpiteitä.

Toiseen sääntöön asetetaan seuraavat asetukset:

- **Locations:** All SharePoint sites, all OneDrive accounts
- **Conditions:**
    - **Content contains:** Sensitive information type “Finland National ID”, instance count 1 to any, match accuracy min 90%, max 100%
    - **Content is shared:** with people outside my organization
- **Actions:** Block people from sharing and restrict access to shared content (Only people outside your organization, people inside your organization will continue to have access)
- **User notification:** Notify the user who shared or last modified the document
    - **Customize policy tip:** Organisaation tietohallinnon tai vastaavan edustajan kirjoittama käytäntövihje, joka käyttäjälle tulee näkyviin ennen dokumentin jakamista
    - **Customize the email text**: Organisaation tietohallinnon tai vastaavan edustajan kirjoittama sähköposti-ilmoitus, jonka käyttäjä saa jaettuaan sensitiivistä informaatiota sisältävän dokumentin
- **Incident reports**: Use email incident reports to notify you when a policy match occurs (halytyslaatikko@organisaatio.fi)

Toisen säännön tarkoitus on estää suomalaisia henkilötunnuksia sisältävien dokumenttien jakaminen SharePointista ja OneDrivesta organisaation ulkopuolisille käyttäjille. Käyttäjille näytetään käytäntövihjeet ”Jaa” -painikkeen vieressä. Mikäli käyttäjä yrittää jakaa dokumentin, estetään jakaminen kaikille muille, paitsi organisaation omille käyttäjille. Jakamisyrityksestä lähetetään sähköposti-ilmoitus käyttäjälle, joka yritti luoda jakoa, sekä halytyslaatikko-sähköpostilaatikkoon, jotta järjestelmän ylläpitäjät voivat tehdä tarvittavat toimenpiteet tai pohtia henkilöstön

lisäkoulutuksen tarvetta, jotta käyttäjät eivät yrittäisi jakaa kriittistä tietoa sisältäviä dokumentteja organisaation tietoturvapolitiikan vastaisella tavalla.

5.4 Säilytyskäytännöt

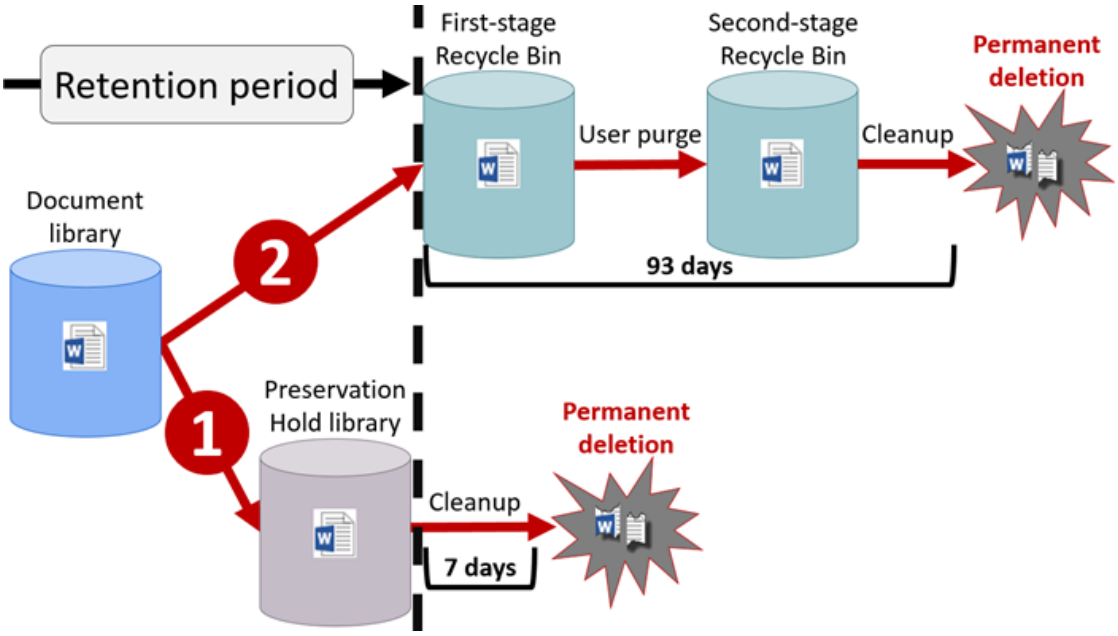
Säilytyskäytännöillä (retention policies) tarkoitetaan organisaation politiikkaa tai protokollaa, jossa määritellään datan vaatimusten tai määräysten mukaisen säilyttämisen tai sen poistamisen sitten, kun sitä ei enää tarvita. Politiikka määrittelee missä muodossa data tulee säilyttää ja millaisia laitteita datan säilytykseen tulee käyttää sekä kuinka kauan sen säilytysajan tulee olla. Säilytyspolitiikka tai -käytäntö perustuu usein jonkin valvovan elimen määräyksiin. (Data-Retention Policy 2018.)

O365-palvelussa säilytyskäytännöt mahdollistavat datan säilyttämisen määrätyn ajan verran sekä sen poistamisen tietyn ajan kuluttua. Säilytyskäytännöllä voidaan myös varmistaa, että mahdollisia tietomurtotapauksia pystytään tutkimaan tehokkaasti vielä senkin jälkeen, kun tietomurtoon liittyvä data on käyttäjän tai pahantekijän toimesta poistettu. Politiikka voidaan osoittaa koskemaan ainoastaan tiettyjä tiedon säilytyssijainteja tai käyttäjiä. O365 mahdollistaa myös säilytyskäytäntöjen asettamisen ainoastaan tiettyjä kriteereitä täyttävälle tiedolle. Organisaation ylläpitäjä voi itse määritellä kriteerit tai vaihtoehtoisesti käyttää Microsoftin valmiiksi tarjoamia kriteeristöjä. (Overview of retention policies 2019.)

Olemassa oleva data säilytetään siinä sijainnissa, jossa se on sillä ajanhetkellä, kun säilytyskäytäntö astuu voimaan. Tämä tarkoittaa sitä, että vaikka käyttäjä näennäisesti poistaisi sisältöä esimerkiksi omasta OneDrivestaan, vie poistettu tieto edelleen saman verran tallennustilaa käyttäjän OneDrivesta, vaikka käyttäjä itse ei voi tiedostoa enää nähdä. (Overview of retention policies 2019.)

Säilytyskäytännön astuessa voimaan SharePoint-sivustokokoelmalle luodaan kyseiselle sivustokokoelmalle Preservation Hold Library, johon käyttäjien poistamat tai muokkaamat tiedostot siirtyvät, vaikkeivat kyseiset tiedot olisikaan minkään voimassaolevan säilytyskäytännön vaikutuksen alaisina. Ajastettu prosessi siivoaa Preservation Hold Librarysta sellaiset tiedostot, jotka eivät ole minkään säilytyskäytännön alaisina, jolloin tiedostot poistuvat pysyvästi. (Overview of retention policies 2019.)

Kuviossa 5 on kuvattu säilytyskäytännön toiminta SharePointin ja OneDriven osalta. Nuolen 1 osoittama reitti kuvaa sen, että jokainen poistettu tai muokattu dokumentti siirtyy Preservation Hold Libraryyn, josta se siivotaan seitsemän päivän välein, mikäli kyseinen dokumentti ei ole säilytyskäytännön piirissä. Nuolen 2 osoittamassa tapauksessa dokumenttia ei poisteta tai muokata, jolloin se säilytyskäytännön määräämän ajan kuluttua siirtyy ensimmäisen tason roskakoriin (first-stage recycle bin), josta käyttäjä itse voi sen poistaa ja siten siirtää toisen tason roskakoriin (second-stage recycle bin). Molempien tasojen roskakorit kuuluvat saman, 93:n päivän pituiseen säilytysaikaan, jonka jälkeen dokumentti poistetaan lopullisesti riippumatta siitä, kummanko tason roskakorissa se sijaitsee säilytysajan loputtua. (Overview of retention policies 2019.)

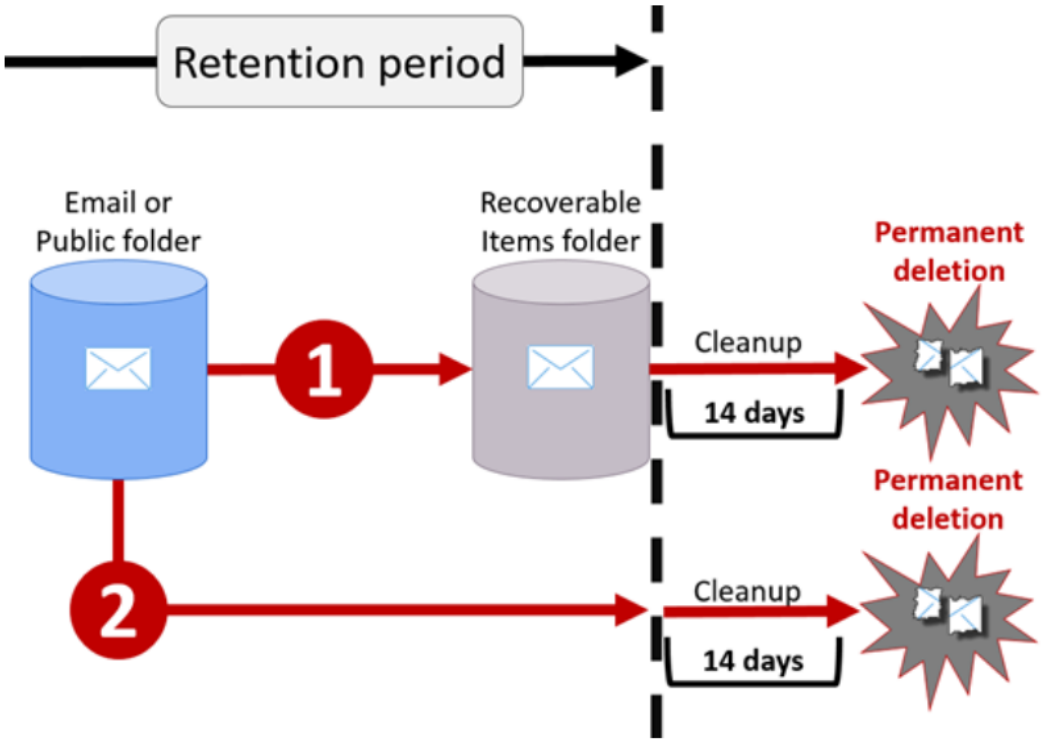


Kuvio 5. Säilytyskäytäntö SharePointissa ja OneDrivessa (Overview of retention policies 2018.)

Säilytyskäytännöt pätevät eri tavalla sähköpostilaatikoissa ja julkisissa kansioissa säilytettävään tietoon. Poistettaessa kohteita sähköpostilaatikosta ne siirtyvät aluksi Poistetut-kansioon, josta käyttäjä voi poistaa ne itselleen näennäisen lopullisesti. Todellisuudessa kohteet tällöin siirtyvät ”Palautettavat” (Recoverable Items) -kansioon,

jonka voi nähdä ainoastaan ylläpitäjä, jolle on määritetty eDiscovery-oikeudet. Käyttäjä voi myös ohittaa Poistetut-kansion tekemällä kohteelle suoraan ”kevyen poiston” (soft delete) painamalla *shift+delete,* jolloin kohde siirtyy suoraan Palautettavat-kansioon. Määritetty prosessi skannaa kaikki Palautettavat-kansion sisältämät dokumentit säännöllisesti ja poistaa kansiosta sellaiset tiedostot, jotka eivät ole minkään säilytyskäytännön piirissä. (Overview of retention policies 2019.)

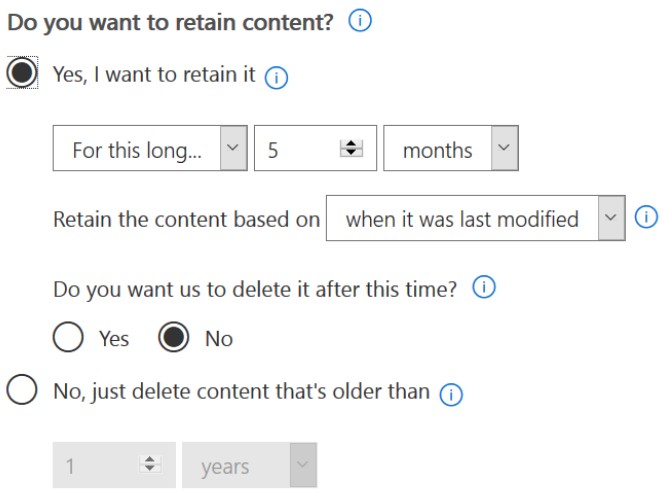
Kuviossa 6 on kuvattu, kuinka säilytyskäytäntö toimii sähköpostilaatikoissa ja julkisissa kansioissa. Nuolen 1 osoittamalla reitillä dokumenttia ei poisteta tai muokata, jolloin se säilyy sijainnissaan säilytyskäytännön määrittämän ajan, jonka jälkeen automaattinen siivousprosessi poistaa sen pysyvästi 14 päivän jälkeen. Nuolen 2 osoittama reitti kuvaa sen, kuinka dokumentti siirtyy Poistetut- tai Palautettavat kansioon käyttäjän poistettua tai muokattua dokumenttia. Siivousprosessi on oletusasetuksella määritetty 14 päivän pituiseksi, mutta sen voi konfiguroida pisimmillään 30 päivän pituiseksi. (Overview of retention policies 2019.)



Kuvio 6. Säilytyskäytäntö sähköpostilaatikoissa ja julkisissa kansioissa (Overview of retention policies 2018.)

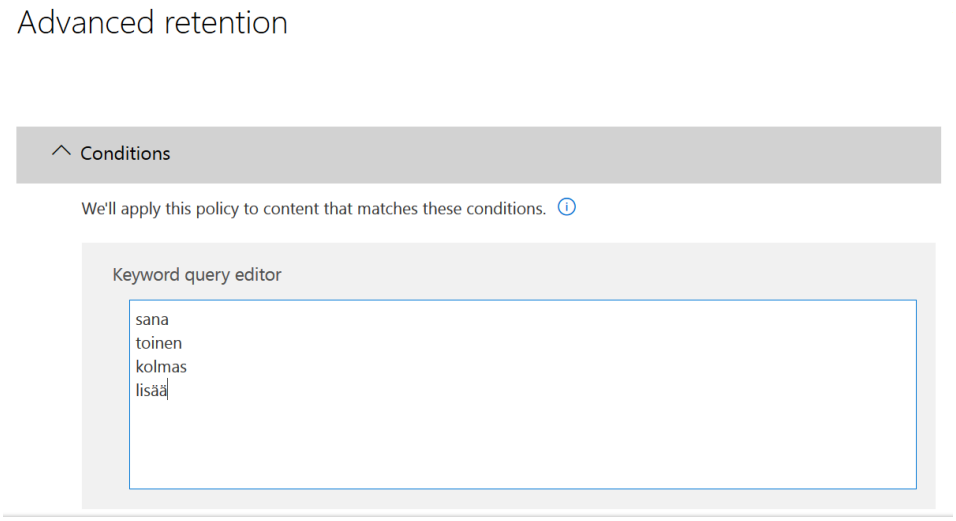
Dokumenttien säilytyskäytäntö voidaan määrittää alkamaan dokumentin luontihetkestä tai viimeisimmästä muokkauksesta. Jos säilytyskäytäntö konfiguroidaan alkamaan luontihetkestä, dokumentista ja sen eri versioista säilytetään 500 viimeisintä versiota ja kaikkien versioiden säilytyskäytäntö loppuu saman ajanhetkenä. Mikäli säilytyskäytäntö määritetään siten, että se alkaa dokumentin muokkaushetkestä, säilytetään tällöin jokaisesta dokumentin eri versiosta kopio, jolla on oma säilytyskäytännön päättymisajankohta. (Overview of retention policies 2019.)

Säilytyskäytäntö voidaan määrittää joko ikuiseksi tai tietyn määrän päiviä, kuukausia tai vuosia pituiseksi. Käytäntöön voidaan myös määrittää tiedoston poistaminen säilytyskäytännön loputtua tai että säilytyskäytäntöä ei käytetä tiedon säilyttämiseen ollenkaan, vain tietyn iän saavuttaneiden tiedostojen poistamiseen. Näiden ominaisuuksien määrittäminen on havainnollistettu kuviossa 7. (Overview of retention policies 2019.)



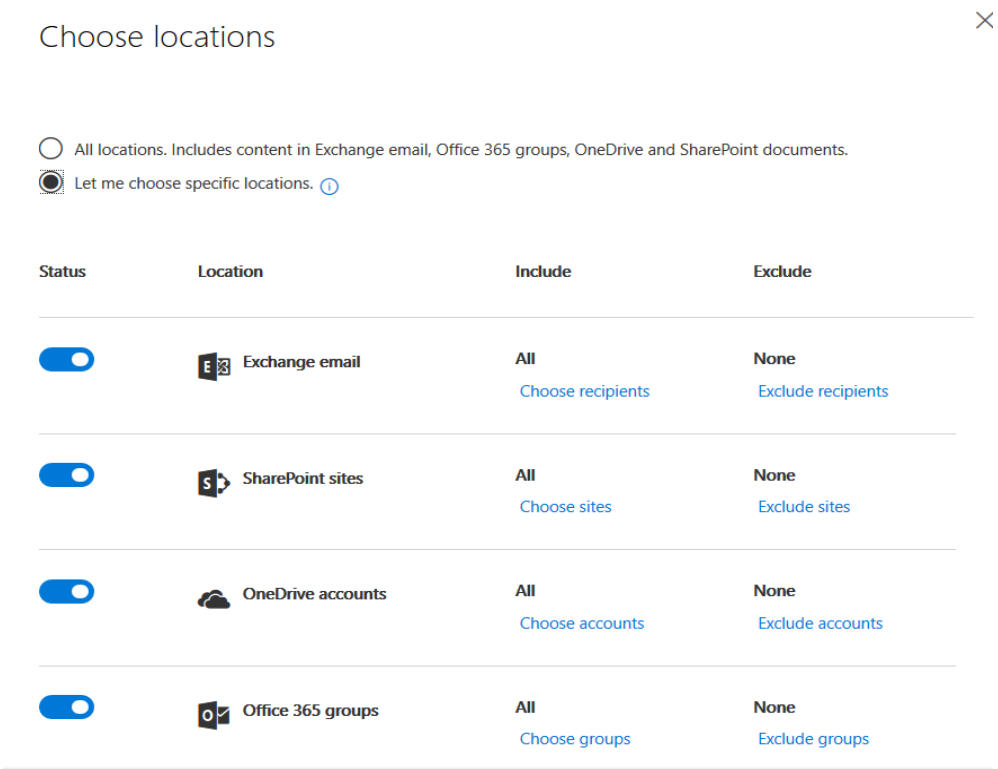
Kuvio 7. Säilytyskäytännön ajan määrittäminen (Overview of retention policies 2018.)

Säilytyskäytäntö voidaan asettaa koskemaan ainoastaan sellaisia dokumentteja, jotka sisältävät jonkin avainsanan tai lauseen. Tällöin ainoastaan kyseisiä sanoja tai lauserakenteita sisältävät dokumentit kuuluvat kyseisen säilytyskäytännön piiriin. Esimerkki avainsanojen määrittämisestä on kuviossa 8. (Overview of retention policies 2019.)



Kuvio 8. Säilytyskäytännön avainsanat (Overview of retention policies 2018.)

Säilytyskäytäntö voidaan asettaa koskemaan kaikkien mahdollisten palveluiden kaikkia sijainteja tai sitten se voidaan asettaa koskemaan vain esimerkiksi tietyn palvelun tiettyjä käyttäjiä, käyttäjäryhmiä tai sivustoja. Mahdolliset sisällytykset ja poikkeukset on havainnollistettu kuviossa 7. (Overview of retention policies 2019.)



Kuvio 9. Säilytyskäytännön sisältämät sijainnit (Overview of retention policies 2018.)

5.5 Käyttötapaus säilytyskäytännölle

Tässä kappaleessa kuvatun käyttötapauksen lähtökohtina ovat seuraavat organisaation asettamat vaatimukset:

- Dokumentit, joiden sisällössä tai nimessä mainitaan ”säilytettävä” täytyy saada säilytettyä vähintään 5 vuotta
- Dokumenttien kaikki versiot pitää säilyttää
- Säilytyksen täytyy päteä jokaisessa mahdollisessa säilytyssijainnissa (palvelussa)
- Organisaatiolla ei ole käytössä tietojenluokittelun periaatteita tai muuta dokumentteja lajittelevaa teknistä ominaisuutta

Näiden vaatimusten perusteelta organisaatiolle luodaan Security&Compliance Centeristä säilytyskäytäntö, joka määritellään seuraavin ehdoin:

- **Locations applied:** All Exchange recipients, all SharePoint sites, all OneDrive accounts, all Office365 Groups, all Exchange public folders
- **Advanced retention:** Detect content that contains specific words or phrases
    - **Conditions:** Keyword: “säilytettävä”
    - **Action:** Retain content: 5 years, no deletion after retention

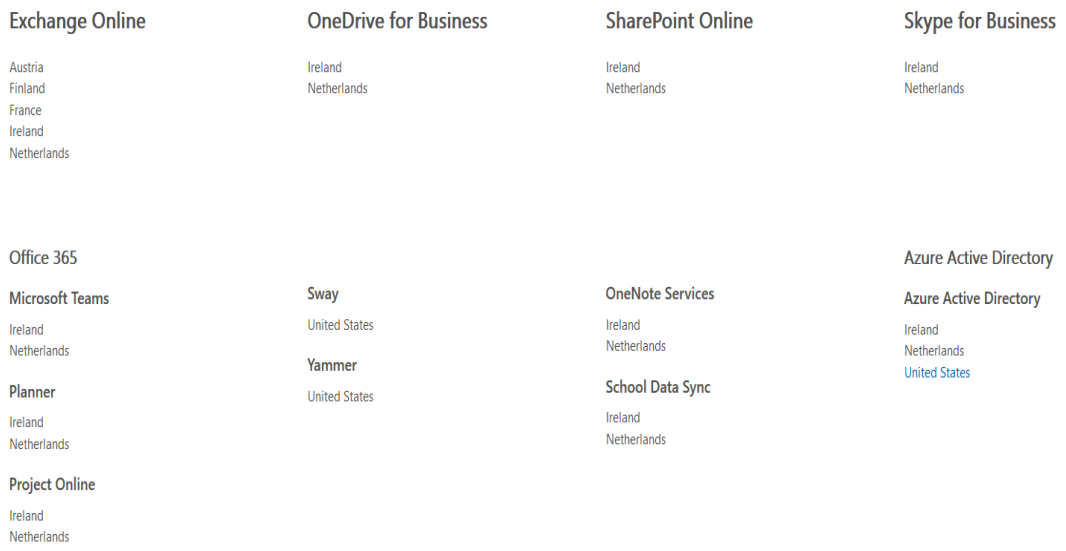
Tällaisella säännöllä kaikki dokumentit, jotka sisältävät sanan ”säilytettävä” säilytetään vähintään viisi vuotta, jonka jälkeen käyttäjä pystyy itse poistamaan dokumentit lopullisesti. Jos organisaatiolla olisi käytössä tietojenluokittelun periaatteet, he voisivat luoda Security&Compliance Centeristä labelin, jonka käyttäjä pystyisi itse asettamaan dokumenteilleen tai sähköposteilleen, jolloin automaattista luokittelua ei tehtäisi kaikille dokumenteille, jotka sisältävä avainsanan ”säilytettävä.”

Microsoft Enterprise E3 -lisenssissä tulee mukana lisäksi mahdollisuus käyttää Azure Information Protection -palvelua, joka tarjoaa datan luokittelua käyttäjille. Automaattinen datan luokittelu AIP-palvelussa on kuitenkin E5-tason ominaisuus, joten organisaatiolla täytyisi olla jokaiselle käyttäjälle E5-lisenssi, mikäli he haluaisivat käyttää automaattista datan luokittelua kaikkien käyttäjiensä dokumentteihin AIP:n kautta.

5.6 Tiedon sijainti Office365:ssä

Microsoft tarjoaa kaikille julkisesti saatavilla olevaa palvelua, jonka avulla pystyy tarkistamaan missä datakeskuksessa tietyn maantieteellisen alueen tietoja säilytetään. Työkalulla pystyy tarkistamaan tiedon sijainnin organisaation kotimaan tai Microsoftin maantieteellisen Geo-luokittelun perusteella. Suomi kuuluu tässä luokittelussa

”European Union” -alueeseen. Tiedon sijaintimaat suomalaiselle organisaatiolle palveluittain on kuvattu kuviossa 10. (Where is your data located? N.d.)



Kuvio 10. Tietojen sijainti palveluittain (Where is your data located? N.d.)

Microsoft ei paljasta datakeskuksiensa tarkkoja sijainteja, mutta kertoo, että heidän datakeskuksensa Euroopan alueella sijaitsevat Suomessa, Irlannissa, Itävallassa, Ranskassa ja Alankomaissa. (Where is your data located? N.d.)

Valtiovarainministeriön kommentoimassa Microsoftin Online Services Terms -dokumentissa huomautetaan kommenteissa A38-A42, että vaikka asiakas valitsee asiakastiedon sijaitsevan vain Euroopan Unionin alueella, ei kaikki tieto siitä huolimatta sijaitse EU:n alueella. Samassa dokumentissa Microsoft kertoo myös, että vain Core Services’ien osalta tiedonsiirrot tapahtuvat mallisopimusehtojen mukaisesti. Microsoft kertoo myös, että he saattavat käsitellä asiakkaidensa tietoja alikäsittelijöidensä toimesta ympäri maailmaa. (Online Services Terms, 2018, 11.)

Microsoftin online-palveluiden käyttöehdoissa mainitaan myös, että Microsoft saattaa käyttää joidenkin palveluidensa tuottamiseen kolmannen osapuolen toimijoita ja että asiakas suostuu tällaiseen menettelyyn hyväksyessään käyttöehdot. Jos asiakas

ei halua hyväksyä uutta alikäsittelijää, voi asiakas irtisanoa online-palvelun tilauksensa ilman rangaistusta, kunhan antaa siitä kirjallisen huomautuksen syineen. (Online Services Terms, 2018, 12.)

6 Johtopäätökset

6.1 Tietoturvalle asetetut vaatimukset ja niiden täyttyminen

Tässä työssä käytetyistä lähteistä ei saanut selkeitä teknisiä ja konkreettisia vaatimuksia tietoturvan tasolle. Tällaisia vaatimuksia olisivat voineet olla esimerkiksi tietojen säilytysajat, pääsynhallinnan vaatimukset, salasanakäytännöt tai salasanan minimivahvuusvaatimukset, hallintatunnusten myöntämisprosessin määrittely tai tietoturvan valvontaan liittyvät asiat kuten security operations center (SOC) -toiminta, lokitietojen säännöllinen katselmointi ja erilaiset poikkeamien ja uhkien reagointiprosessit ja vastuut.

Microsoftin tarjoaman palvelumallin periaatteena on tarjota laajempia mahdollisuuksia eri lisenssitasoille. E5-lisenssi mahdollistaa lähes kaikkien tarjolla olevien kontrollien käytön ja konfiguroinnin, kun taas E3-tason lisenssistä jää ulkopuolelle monia oleellisia seuranta- ja hallintakeinoja sekä tietoturvaa lisääviä ominaisuuksia, kuten esimerkiksi MFA Registration policy, joka mahdollistaa MFA rekisteröinnin pakottamisen jokaiselle käyttäjälle ensimmäisellä kirjautumiskerralla. Asiantuntija pystyy kuitenkin simuloimaan erilaisia skriptejä ja ryhmäperusteisia sääntöjä hyväksikäyttäen saman toiminnan, jonka E5-tason lisenssi tarjoaa käyttöliittymällisenä toimintona. Tämä pätee useisiin korkeamman lisenssitason vaativiin ominaisuuksiin, mutta aiheuttaa sen, että asiantuntijan on oltava erittäin hyvin perehtynyt järjestelmään ja sen mahdollisuuksiin.

O365:n useat hallintaportaalit ja niiden ristiriidat ja epäselvyydet toistensa suhteen aiheuttavat myös asiantuntijan konfiguraatiomuutoksille korkean kynnyksen, jos asiantuntija ei ole täysin varma siitä, mihin kaikkeen hänen suunnittelemansa tai tekemänsä muutos vaikuttaa. Esimerkkinä tällaisesta voidaan mainita esimerkiksi Office365:n Security&Compliance Centerin (S&C) Data Loss Prevention -säännöt, joita pystyy konfiguroimaan käyttöön myös Exchange Admin Centerin (EAC) puolelta.

EAC:n DLP-säännöt vaikuttavat ainoastaan sähköpostin kulkuun, mutta eivät ota kantaa esimerkiksi OneDrivesta jaettaviin dokumentteihin, kun taas S&C centerin DLP-säännöt voivat koskea useita muitakin O365-palvelun sovelluksia kuin sähköpostia.

Säilytyskäytäntöjä käytettäessä tulee harkita tarkasti, mitkä ovat hyödyt ja haitat siitä, jos säilytyskäytäntö määritetään koskemaan kaikkia tiedon sijainteja pitkällä aikavälillä. Esimerkiksi OneDrive mahdollistaa suuretkin säilytystilat (vakiona 1TB), mutta mikäli käyttäjällä on paljon sellaista dataa, joka aiheuttaa versiointia, voi yhden teratavun säilytystila joissakin käyttötapauksissa osoittautua riittämättömäksi. Säilytystilan loppuessa käyttäjä alkaa kokea työtään haittaavia tai peräti estäviä haittoja eivätkä käyttäjän muokkaamat tai poistamat dokumentit enää tallennu, vaikka säilytyskäytäntö niin määrittelisi tapahtuvan. Ihanteellisessa tilanteessa asiakkaalla olisi selkeä tietämys siitä, millaista tietoa heidän täytyy tai he haluavat säilyttää ja kuinka pitkän ajan verran.

Viestintäviraston suositusten mukaisesti O365-käyttöönotossa tulisi kiinnittää erityistä huomiota monivaiheisen varmennuksen käyttöön asettamiseen. Monivaiheinen varmennus estää tehokkaasti käyttäjätunnusten menettämisen vaikutuksia, kun palveluihin ei pystykään kirjautumaan ainoastaan käyttäjätunnuksella ja salasanalla. MFA:ta asiakkaille esitellessä ja sitä konfiguroitaessa tulee ottaa kuitenkin huomioon, että useat merkittävät organisaatiot kuten NIST ja Microsoft itse eivät suosittele tekstiviesti- tai puheluvarmennuksen käyttöä, koska ne on pystytty toteamaan tietoturvaltaan heikommiksi vaihtoehdoiksi. MFA:han liittyvien määritysten teossa on myös pyrittävä löytämään sopivasti tietoturvaa lisäävät asetukset siten, etteivät ne aiheuta asiakkaan henkilöstölle liiallisia vaikeuksia tai hankaluuksia työtehtäviensä suorittamiseen. Tällainen konfiguraatio on yksinkertaisimmillaan esimerkiksi kirjautumisen salliminen organisaation omasta IP-verkosta ilman, että MFA:ta vaaditaan.

Eri palveluiden, kuten OneDriven ja SharePointin, hallintaportaaleista voidaan lisäksi määritellä ulkoisen jakamisen sääntöjä eri tavalla. Office365-palvelua käyttöönottavan organisaation tulisi etukäteen määritellä, mihin käyttötarkoitukseen he aikovat mitäkin palvelua käyttää. Näiden organisaation määritysten perusteella ulkoista jakamista voidaan rajata eri palveluista eri tasolle. OneDrivea on käytännöllistä ja luontevaa käyttää korvaamaan ”on-premises maailman” levyjakoja tai muita henkilökohtaisia tiedon säilytyssijainteja, kun taas SharePoint ja Microsoft Teams mahdollistavat

hyvin organisaatiorajat ylittävän yhteistyön toteuttamisen esimerkiksi erilaisia projekteissa tai yhteistyöhankkeissa. Tällöin tulisi määritellä, että tiettyihin SharePoint-sivustoihin, joissa on myös muiden organisaatioiden edustajia, ei saa viedä yhtä arkaluontoista tietoa, kuin esimerkiksi omaan, henkilökohtaiseen OneDriveen.

Office365:n voidaan sanoa täyttävän tässä työssä kuvatut vaatimukset vähintään riittävällä tasolla, mutta siihen osakseen vaikuttaa edellä mainittu vaatimusten tarkkuuden vajavaisuus. Office365 tarjoaa jokaiselle NIST:in määrittelemälle tietoturvan osa-alueelle (identify, protect, detect, respond, recover) kontrolleja, joista suurin osa on erittäin hyvin konfiguroitavissa erilaisten asiakkuuksien erilaisiin tarpeisiin.

Tämän opinnäytetyön eräänä tavoitteena oli muodostaa Istekin asiantuntijoiden käyttöön tehtävien tarkistuslista, jota asiantuntija voi käyttää apunaan suorittaessa Office365-käyttöönoton tietoturvan tehtäviä. Tehtävälistaus löytyy liitteestä 2.

6.2 Tietosuojalle asetetut vaatimukset ja niiden täyttyminen

Tietosuojan vaatimukset johdettiin tässä työssä suurilta osin Euroopan Unionin tietosuoja-asetuksesta. Valtiovarainministeriön kommentoiman ”Online Services Terms” -dokumentin kommenteista käy selkeästi ilmi, että vaikka Microsoft suurilta osin mahdollistaa GDPR:n mukaisen toiminnan toteuttamisen Office365-palvelussa, on heidän käyttöehdoissaan kuitenkin jätetty joitakin arveluttavia kohtia. Microsoft ei yksiselitteisesti lupaa, että O365-palveluun tallennetun datan käsittely tapahtuisi ainoastaan tietosuoja-asetuksen määrittelemillä tavoilla. Eritoten kyseisen dokumentin kommentti [A13] kertoo, kuinka Microsoft käyttöehdoissaan mainitsee, että Microsoft saattaa siirtää mitä tahansa asiakastietoja mille tahansa alihankkijoilleen ympäri maailman. Tällainen maininta ei täytä GDPR:n asettamia vaatimuksia siitä, mihin ja miten EU:n jäsenvaltioiden kansalaisten tietoja saa käsitellä.

Euroopan unionin tietosuoja-asetuksessa annetaan vaatimuksia henkilötietojen siirtämiselle Euroopan unionin ulkopuolisiin maihin. Tärkein ja Microsoftin Office365-palvelun tapauksessa oleellisin ehto on se, että Euroopan komission hyväksymiin (kolmansiin) maihin ja kansainvälisiin järjestöihin saa siirtää henkilötietoja, kunhan tietosuoja-asetuksessa kuvatut tarkastustoimenpiteet suoritetaan tai vaatimukset

täyttyvät. Epäselväksi jää, täyttävätkö Microsoftin Office365-palvelun käyttöehdot tietosuoja-asetuksen asettamat vaatimukset.

7 Pohdinta

Tietoturvan toteuttaminen pilvipalveluissa tulisi tehdä kuten missä tahansa muussakin palvelussa tai järjestelmässä. Tietoturvakontrollien ja -prosessien esittäjän tai muun vastaavan asiantuntijan tulisi tietää eri säädösten, lakien ja määrittelyiden asettamat vaatimukset ja sen lisäksi olla tietoinen kaikista (tai mahdollisimman monista) mahdollisuuksista, jotka kyseessä oleva järjestelmä tai palvelu mahdollistaa. Asiakkaan tarpeiden, käytänteiden, prosessien ja omien tietoturvamääritysten tietäminen on myös hyvin oleellista sen kannalta, että asiakkaalle saadaan muodostettua juuri asiakkaan tarpeita vastaava kokonaispalvelu. Näiden pohjatietojen perusteella asiantuntijan tulee pystyä esittämään asiakkaalle juuri hänen tarpeisiinsa sopivat ja tarvittavat kontrollit ja keinot tietoturvan tason nostamiseksi tarvittavalle tasolle.

Virallisia lähteitä julkisen hallinnon pilvipalveluiden tietoturvan vaatimuksille on hankala löytää ja niiden suhteet toisiinsa ovat epäselviä. Suomen lainsäädäntö ei suoranaisesti anna määräyksiä teknisistä vaatimuksista tai kontrolleista, joita tulisi käyttää tai noudattaa toteutettaessa tietoturvaa pilvipalveluille. Valtiovarainministeriön julkaisemat julkisen hallinnon pilvipalvelulinjaukset ovat hyvä ohjenuora tietoturvatyön tekemiselle, mutta eivät ole lakiin kirjattuja tai ehdottomia määräyksiä, joita palveluntarjoajan tulee noudattaa. Terveyden ja hyvinvoinnin laitoksen määräykset antavat tarkkoja vaatimuksia teknisistä kontrolleistakin, mutta koskevat enimmäkseen vain suoraan potilas- tai henkilötietojen käsittelyä ja Kanta-palveluihin liitettyjä järjestelmiä, jollainen Office365-palvelu ei itseisarvoltaan ole, mutta johon sitä voitaisiin käyttää. (Tietoturva)asiantuntijan on hyvä kuitenkin tiedostaa, millaisia vaatimuksia potilas- ja henkilötietojen pilveen viemiselle on olemassa, vaikka ne eivät olisikaan lakiin kirjattuja asioita.

Tässä työssä olisi voinut käyttää hyväksi myös eri tietosuoja- ja tietoturva-asiantuntijoiden, Istekin asiakkaiden sekä Microsoftin asiantuntijoiden haastatteluja

tai lausuntoja, jotta työn pohjalle olisi saatu konkreettisempi perusta siitä, mihin Istekin toiminta pilvipalveluiden osalta tulee tulevaisuudessa suuntautumaan.

Lähteet

2018 Cost of a Data Breach Study: Global Overview. 2018. Ponemon Institute LLC:n tekemä tutkimus. https://www.ibm.com/security/data-breach

App Passwords. 2018. Microsoftin dokumentaatio MFA:sta. Viitattu 15.3.2019. https://docs.microsoft.com/fi-fi/azure/active-directory/authentication/howto-mfa-mfasettings#app-passwords

Arlan Nugara. 2017. Transitioning from On-Premise Virtual Machines to More Cost Effective Azure Cloud Models. Blogikirjoitus. Viitattu 1.5.2019. https://blogs.partner.microsoft.com/mpn-canada/transitioning-premise-virtual-machines-cost-effective-azure-cloud-models/

Client apps. 2018. Microsoftin dokumentaatio Azure AD:n ehdollisen pääsyn säännöstä. Viitattu 15.3.2019. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#client-apps

Cloud apps. 2018. Microsoftin dokumentaatio Azure AD:n ehdollisen pääsyn säännöstä. Viitattu 15.3.2019. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#cloud-apps

Data-Retention Policy. N.d. Techopedia-verkkosivuston termimääritelmä. Viitattu 18.4. 2019. https://www.techopedia.com/definition/31812/data-retention-policy

Device platforms. 2018. Microsoftin dokumentaatio Azure AD:n ehdollisen pääsyn säännöstä. Viitattu 15.3.2019. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#device-platforms

Discover the Microsoft 365 Enterprise solution that’s right for you. N.d. Microsoftin verkkojulkaisu eri Enterprise lisenssien mahdollistamista palveluista. Viitattu 8.5.2019. https://www.microsoft.com/en-us/microsoft-365/compare-all-microsoft-365-plans

Euroopan parlamentin ja neuvoston asetus 2016/679. 2016. Euroopan parlamentin tietosuoja-asetus. Viitattu 5.5.2019. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e40-1-1

Julkisen hallinnon pilvipalvelulinjaukset 2018. Valtiovarainministeriön julkaisu 35/2018. Viitattu 16.04.2019. http://urn.fi/URN:ISBN:978-952-251-982-5

Locations. 14.12.2018. Microsoftin dokumentaatio Azure AD:n ehdollisen pääsyn säännöstä. Viitattu 15.3.2019. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#locations

Määräys 1/2015: A-luokkaan kuuluvien sosiaali- ja terveydenhuollon tietojärjestelmien olennaiset tietoturvavaatimukset. 2015. Terveyden ja hyvinvoinnin laitoksen määräys. Viitattu 23.4.2019. https://thl.fi/documents/920442/1449818/Allekirjoitettu_THL_M%c3%a4%c3%a4r%c3%a4ys_1_2015_Tietoturvavaatimukset_20150130-b.pdf/bcbc0d70-1749-488d-8e09-54f1ebd46484

Online Services Terms. 2018. Microsoftin online-palveluiden käyttöehdot, valtiovarainministeriön kommentoima versio. Viitattu 6.5.2019. https://vm.fi/documents/10623/9602398/MicrosoftOnlineServicesTerms%28English%29%28August2018%29_180820_1C.pdf/3a9d6caa-6f20-4e36-9a6a-0ac14a0a11bf/MicrosoftOnlineServicesTerms%28English%29%28August2018%29_180820_1C.pdf.pdf

Overview of Data Loss Prevention policies. 2018. Microsoftin dokumentaatio Data Loss Prevention -säännöistä. Viitattu 12.4.2019. https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

Overview of retention policies. 2019. Microsoftin dokumentaatio säilytyskäytännöistä. Viitattu 18.4.2019. https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

Remember multi-factor authentication. 2018. Microsoftin dokumentaatio MFA:sta. Viitattu 15.3.2019. https://docs.microsoft.com/fi-fi/azure/active-directory/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication

Sign-in risk. 2018. Microsoftin dokumentaatio Azure AD:n ehdollisen pääsyn säännöstä. Viitattu 15.3.2019. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#sign-in-risk

Suojaustoimia Office365 -tunnusten tietojenkalastelua vastaan. 2018. Viestintäviraston tiedote O365-tietojenkalastelun estämisestä ja mitigointitoimista. Viitattu 7.5.2019. https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/06/ttn201806111418.html

SP 800-63-3. NIST Digital Identity Guidelines. Viim. muutos 22.7.2017. Viitattu 22.3.2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

The Most Popular Office 365 Products Revealed. N.d. Compete 366:n verkkoartikkeli. Viitattu 8.5.2019. https://www.compete366.com/blog-posts/popular-office-365-products/

Tietojenkalastelijat pyrkivät ohittamaan Office 365 -palvelun monivaiheisen todentamisen. 2018. Viestintäviraston tiedote. Viitattu 25.3.2019. https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/09/ttn201809261243.html

Trusted IPs. 2018. Microsoftin dokumentaatio MFA:sta. Viitattu 15.3.2019. https://docs.microsoft.com/fi-fi/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips

Users and groups. 2018. Microsoftin dokumentaatio Azure AD:n ehdollisen pääsyn säännöstä. Viitattu 15.3.2019. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#users-and-groups

Verification methods. 2018. Microsoftin dokumentaatio MFA:sta. Viitattu 15.3.2019. https://docs.microsoft.com/fi-fi/azure/active-directory/authentication/howto-mfa-mfasettings#verification-methods

Where is your data located? N.d. Microsoftin työkalu tiedon sijainnin tarkkailemiseksi. Viitattu 6.5.2019. https://products.office.com/en-us/where-is-your-data-located?geo=All

Zhang, E. 2019. What is Data Loss Prevention (DLP)? Digital Guardianin verkkoblogi 3.1.2019. Viitattu 3.4.2019. https://digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention

Liitteet

Liite 1. Euroopan unionin tietosuoja-asetuksen artiklan 47 kohta 2

Liite 2. Tehtävien tarkistuslista (salassa pidettävä)

Liite 1. Euroopan unionin tietosuoja-asetuksen artiklan 47 kohta 2

2. Näissä 1 kohdassa tarkoitetuissa yritystä koskevissa sitovissa säännöissä on määritettävä vähintään

a) konsernin tai yritysryhmän, joka harjoittaa yhteistä taloudellista toimintaa, ja sen kaikkien jäsenten rakenne ja yhteystiedot;

b) tiedonsiirrot tai tiedonsiirtojen sarjat, henkilötietoryhmät mukaan lukien, käsittelytoimien tyyppi ja käsittelyn tarkoitukset, käsittelyn kohteena olevien rekisteröityjen ryhmä sekä tieto siitä, mistä kolmannesta maasta tai kolmansista maista on kyse;

c) sääntöjen oikeudellinen sitovuus sekä unionin sisällä että sen ulkopuolella;

d) yleisten tietosuojaperiaatteiden soveltaminen, erityisesti käyttötarkoitussidonnaisuus, tietojen minimointi, rajoitetut säilytysajat, tietojen laatu, sisäänrakennettu ja oletusarvoinen tietosuoja, käsittelyn oikeusperuste, erityisten henkilötietoryhmien käsittely, tietoturvallisuuden takaavat toimenpiteet ja vaatimukset, jotka koskevat henkilötietojen siirtämistä edelleen elimille, joita nämä yrityksiä koskevat sitovat säännöt eivät sido;

e) rekisteröityjen henkilötietojen käsittelyä koskevat oikeudet ja keinot käyttää niitä, mukaan lukien oikeus olla joutumatta sellaisten 22 artiklassa tarkoitettujen päätösten kohteeksi, jotka perustuvat pelkästään automaattiseen käsittelyyn, mukaan lukien profilointi, oikeus tehdä valitus toimivaltaiselle valvontaviranomaiselle ja oikeus oikeussuojakeinoihin jäsenvaltioiden toimivaltaisissa tuomioistuimissa 79 artiklan mukaisesti sekä oikeus muutoksenhakuun ja tarvittaessa korvauksen saamiseen yritystä koskevien sitovien sääntöjen rikkomisen vuoksi;

f) jäsenvaltion alueelle sijoittautuneen rekisterinpitäjän tai henkilötietojen käsittelijän suostumus kantaa vastuu siitä, että asianomainen yritysryhmän jäsen, joka ei ole sijoittautunut unionin alueelle, rikkoo yritystä koskevia sitovia sääntöjä; rekisterinpitäjä tai henkilötietojen käsittelijä voidaan vapauttaa tästä vastuusta osittain tai kokonaan vain edellä mainitun rekisterinpitäjän tai henkilötietojen käsittelijän osoitettua, ettei kyseinen jäsen ole vastuussa vahingon aiheuttaneesta tapahtumasta;

g) se, miten yritystä koskevista sitovista säännöistä ja erityisesti tämän kohdan d–f alakohdassa tarkoitetuista säännöksistä ilmoitetaan rekisteröidyille 13 ja 14 artiklan vaatimusten lisäksi;

h) kaikkien 37 artiklan mukaisesti nimitettyjen tietosuojavastaavien taikka konsernissa tai yritysryhmässä, joka harjoittaa yhteistä taloudellista toimintaa, yritystä koskevien sitovien sääntöjen noudattamisen valvonnasta sekä koulutuksen ja valitusten käsittelyn seurannasta vastaavan minkä tahansa muun henkilön tai yksikön tehtävät;

i) valitusmenettelyt;

j) mekanismit, joiden avulla konsernissa tai yritysryhmässä, joka harjoittaa yhteistä taloudellista toimintaa, pyritään varmistamaan, että yritystä koskevien sitovien sääntöjen noudattaminen varmistetaan. Tällaisia mekanismeja ovat tietosuojaa koskevat tarkastukset ja menetelmät, joilla varmistetaan korjaavat toimenpiteet rekisteröidyn oikeuksien suojaamiseksi. Tällaisten varmistusten tulokset olisi ilmoitettava h alakohdassa tarkoitetulle henkilölle tai yksikölle sekä konsernissa määräysvaltaa käyttävän yrityksen tai yhteistä taloudellista toimintaa harjoittavan yritysryhmän hallitukselle, ja niiden olisi oltava pyynnöstä toimivaltaisen valvontaviranomaisen saatavilla;

k) mekanismit sääntöihin tehtävistä muutoksista ilmoittamista ja niiden kirjaamista varten sekä niistä valvontaviranomaiselle ilmoittamista varten;

l) yhteistyömenettely valvontaviranomaisen kanssa sen varmistamiseksi, että kaikki konsernin tai yritysryhmän, joka harjoittaa yhteistä taloudellista toimintaa, jäsenet noudattavat sääntöjä, erityisesti toimittamalla valvontaviranomaisen käyttöön j alakohdassa tarkoitettujen toimenpiteiden varmistamisen tulokset;

m) mekanismit, joilla ilmoitetaan toimivaltaiselle valvontaviranomaiselle kolmannessa maassa konsernin tai yhteistä taloudellista toimintaa harjoittavan yritysryhmän jäseneen mahdollisesta sovellettavista oikeudellisista vaatimuksista, jotka todennäköisesti merkittävästi haittaavat yritystä koskeviin sitoviin sääntöihin sisältyviä takeita; ja

n) asianmukainen tietosuojakoulutus henkilöstölle, jolla on pysyvä tai säännöllinen pääsy henkilötietoihin.