TRAFICOM
Kyberturvallisuuskeskus

Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta

Traficomin julkaisuja
12/2019

Sisältö

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISSN 1799-0157 (verkkojulkaisu)

Esipuhe

Erityisesti vuoden 2018 alkupuoliskolla Kyberturvallisuuskeskuksen tietoon alkoi tulla yhä useammin tapauksia, joissa organisaatioihin kohdistettiin tietojenkalastelua, jonka tarkoituksena oli saada haltuun työntekijöiden sähköpostitunnuksia. Kalastelu voi myös kohdistua niin yksityishenkilöihin kuin organisaatioihinkin, ja maailmalla puhutaankin yleisesti yritystileihin kohdistuvista tietomurroista termillä business email compromise eli BEC.

Käyttäjätunnuksia voitiin hyödyntää eri tavoin riippuen esimerkiksi tunkeutujan omista motiiveista tai murretun käyttäjätilin haltijan roolista tai tehtävistä organisaatiossa. Esimerkiksi joissain tapauksissa hyökkääjä selvästi tavoitteli merkittävää taloudellista hyötyä seuraamalla maksuliikenteeseen liittyvää viestinvaihtoa. Toisaalta varastettuja käyttäjätunnuksia on mahdollista hyödyntää myös esimerkiksi yrityssalaisuuksien vakoiluun, minkä lisäksi onnistuneeseen tietojenkalasteluun voi liittyä muun muassa erilaisia maine- ja sääntelyriskejä.

Vaikka tietojenkalastelu ilmiönä ei rajoitu vain tiettyjen palveluntarjoajien palveluihin, yhdisti näitä tapauksia se, että varastetut käyttäjätunnukset olivat nimenomaan Microsoft Office 365 -tileihin liittyviä tunnuksia. Tällaisia tapauksia tulee Kyberturvallisuuskeskuksen tietoon jatkuvasti. Kyberturvallisuuskeskus antoi aiheesta varoituksen vuoden 2018 kesäkuusta lähtien ja se on tätä opasta kirjoitettaessa yhä voimassa.

Osaltaan ilmiön sinnikkyyttä selittää se, että loppukevään ja alkukesän jälkeen kalastelukampanjoissa on nähty runsaasti erilaisia kehityskulkuja. Yksittäisiä esimerkkejä näistä ovat olleet esimerkiksi salatulta sähköpostiviestiltä näyttävät kalasteluviestit, monivaiheisen tunnistamisen kiertäminen vanhoja sähköpostiyhteystapoja käyttäen ja kalastelusivuston ulkoasun räätälöinti sen mukaan, mistä sähköpostipalvelusta käyttäjä palveluun tulee.

Uusiin kalastelukampanjoihin reagoiminen on jatkuvaa kujanjuoksua ja usein myös auttamattomasti myöhäistä siinä vaiheessa, kun aalto on jo iskenyt rantaan. Sen vuoksi palvelun tietoturvaominaisuuksien ottaminen käyttöön hyvissä ajoin on ehdottoman tärkeää. Eri keinoin voidaan pyrkiä vähentämään niin käyttäjille asti päässeiden kalasteluviestien määrää, estää kalasteltujen tunnusten helppo hyödyntäminen kuin toisaalta mahdollistaa tapausten selvittäminen tai onnistuneen kalastelun vaikutusten rajoittaminen.

Tässä oppaassa ilmiön tarkastelu on tarkoituksella rajattu Microsoftin tarjoamien tuotteiden suojaamiseen siitä syystä, että ne muodostavat kuluneen vuoden perusteella selkeän joukon kohteita, joihin liittyen Kyberturvallisuuskeskuksen tietoon on tullut erityisesti yrityksiin kohdistuvia kampanjoita. Lisäksi tuotteisiin liittyvien suojaustoimien ja -asetusten käyttöönotossa esiintyy organisaatioissa Kyberturvallisuuskeskuksen havaintojen mukaan usein puutteita.

Toivomme, että oppaasta on organisaatioille apua, kun sähköposti- ja pilvipalveluympäristöä halutaan vahvistaa erityisesti tunnuskalasteluun liittyviä uhkia vastaan. Lukijalla oletetaan olevan perusymmärrys Microsoftin pilvipalveluista.

Yhteenveto

Olemme viime vuosina saaneet monesti lukea käyttäjätunnusten ja salasanojen joutumisesta vääriin käsiin. Uutiset ovat useimmin liittyneet erilaisten palveluiden käyttäjätietokantojen vaarantumiseen. Kuluttajien eri palveluissa käyttämät samat salasanat ovat antaneet verkkorikollisille mahdollisuuden hyödyntää paljastuneita tunnuksia muissakin palveluissa.

Organisaatiokäytössä pilvipalvelut ovat yleistyneet nopeasti. Microsoftin Office 365 -palvelua käytetään Suomessa laajasti sekä yksityisellä että julkisella sektorilla. Office 365:n käyttämät identiteetit tallennetaan ja niitä ylläpidetään Azure Active Directory (AD) -palvelussa. Samoilla identiteeteillä voidaan usein käyttää myös monia muita pilvipalveluja.

Kalastelu on yksi yleisimpiä tietoturvauhkia. Kyberturvallisuuskeskuksen helmikuussa 2019 julkaistun Tietoturvan vuosi 2018 -vuosikatsauksen mukaan vuoden 2018 merkittävimmäksi tietoturvauhkaksi nousi hiljalleen levittäytyvät, käyttäjiltä tietoja kalastelevat Office 365 -huijaukset.

Office 365 ja muut Microsoftin palvelut sisältävät monia eri toimintoja, joilla riskiä kalastelun onnistu-

miselle voidaan merkittävästi pienentää. Palvelut on hankittavissa erilaisina toisistaan poikkeavina versioina ns. tilauksina. Tilaukset sisältävät halutun määrän lisenssejä, jotka organisaation ICT-hallinto allokoi käyttäjille. Organisaatio voi hankkia kaikille käyttäjille samanlaiset lisenssit tai eri rooleissa toimiville henkilöille soveltuvimmat palvelut ja niiden vaatimat lisenssit.

Kalastelun rajoittamiseen käytettävissä olevat toiminnot riippuvat käytössä olevista tilauksista. Tässä dokumentissa esitellään suojaustapoja organisaation nykyisestä tilauksesta tai lisensseistä riippumatta.

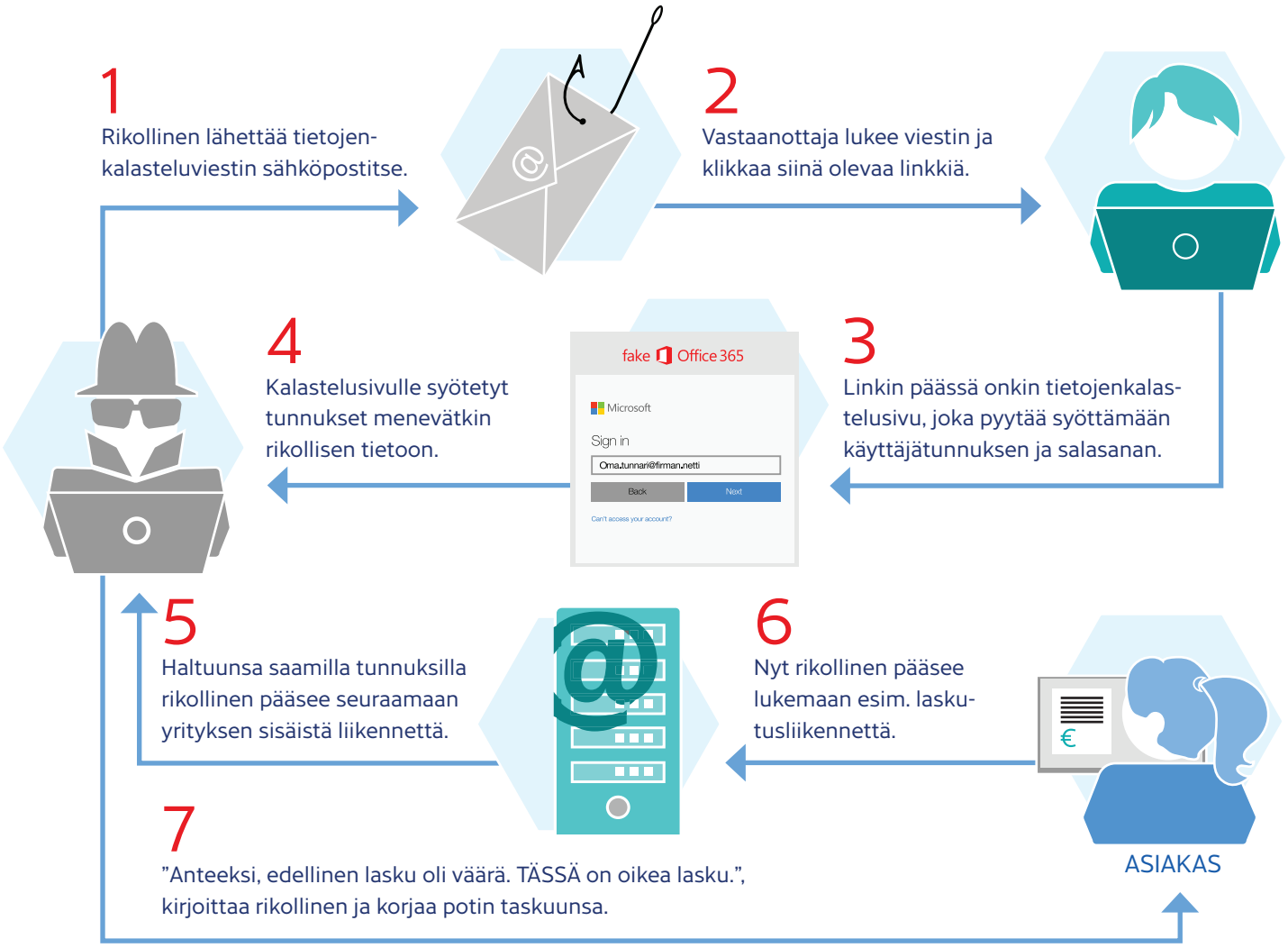
Tärkeimmät toimenpiteet kalastelun rajoittamiseksi tilauksista ja lisensseistä riippumatta ovat:

1. Modernin tunnistautumisen käyttöönotto ja pakottaminen
2. Kaksivaiheisen tunnistautumisen käyttöönotto
3. Lokituksen laadun, määrän ja säilytysajan varmistaminen.

1 Miltä pitäisi suojautua?

Tietoturva koostuu monista osa-alueista. Tässä dokumentissa keskitytään kalastelun rajoittamiseen.

Kalastelua voidaan tehdä monin eri tavoin. Laajimmillaan tietojenkalasteluun käytettyjä viestejä lähetetään suurille käyttäjäjoukoille. Kohdennetuissa huijausyrityksissä tavoitteena on saada selville esimerkiksi organisaation käyttämään pilvipalveluun tallennettuja ja/tai IT-ylläpidon tunnuksia. Hyökkäyksen kohteeksi voidaan valita myös liiketoimintajohtoa tai muuta henkilöstöä, joka käsittelee rahaliikennettä ja laskuja.



1.1 Rikollisten tavoitteena on useimmiten valelaskujen laatiminen

Kalastelua tekevät tällä hetkellä useat eri rikollisryhmät. Ryhmien osaamistaso, tyypillisesti hyödynnetyt työkalut ja toiminnan tavoite vaihtelevat jonkin verran. Pääsääntöisesti rikollisilla on nähty ainakin kahta eri toimintatapaa:

- Yleisimmässä tapauksessa rikolliset pyrkivät saamaan mahdollisimman monet sähköpostitunnukset haltuun. Tilille kirjaudutaan sisään ja etsitään laskutukseen liittyviä hakusanoja. Näitä tietoja käytetään valelaskun laatimiseen, jossa hyödynnetään oikean laskun tietoja ja kon tekstia. Jos tiliä ei koeta mielenkiintoiseksi, rikolliset hyödyntävät tiliä uusien tietojenkalastelu viestien lähettämiseen uhrin kontakteille.
- Harvinaisemmassa tapauksessa rikolliset pyrkivät seuraamaan sähköpostilaa-tikon kirjeenvaihtoa tietojen hankkimiseen. Kyberturvallisuuskeskuksen tiedossa on tapauksia, joissa keskeisessä asemassa olevien henkilöiden sähköpostitileille on murtauduttu ja viestinvaihtoa on jääty seuraamaan. Näissä tapauksissa rikolliset asettavat tilille sähköpostien uudelleenlähetyksen johonkin hallitsemaansa sähköpostilaatikkoon. Tarkkaa motiivia ei ole näissä tapauksissa pystytty osoittamaan.

1.2 Rikolliset osaavat kiertää kaksivaiheisen tunnistautumisen

Teknisesti eri rikollisryhmien kyvykkyydet vaihtelevat jonkin verran. Erot eri ryhmien välillä ovat kuitenkin kaventuneet, ja useimmat ryhmät osaavat tällä hetkellä kiertää esimerkiksi kaksivaiheisen tunnistautumisen. Kaksivaiheisen tunnistautumisen kiertoa on tehty ainakin kahdella eri tavalla:

- Tyypillisemmin rikolliset hyödyntävät Office 365:n ominaisuutta, jonka avulla laitteet ja ohjelmistot, jotka eivät tue kaksivaiheista tunnistautumista, voivat tästä huolimatta kirjautua palveluun sisään. Tämä legacy-tuen mahdollistava ominaisuus on tällä hetkellä laajasti rikollisten hyödtynnettävänä. Tässä oppaassa neuvotaankin ottamaan ns. modern authentication käyttöön ja estämään legacy-kirjautumiset palveluun.
- Rikolliset kirjautuvat kalastetulla käyttäjätunnus ja salasana -parilla heti palveluun sisään, jolloin tiedot antanut uhri saa aidon varmennuskoodin esimerkiksi SMS:llä. Rikollisten kalastelusivu pyytää uhria syöttämään myös tämän toisen vaiheen koodin, jonka avulla rikolliset pääsevät varsinaiseen palveluun sisään.

1.3 Keskusrikospoliisin esimerkkitapauksia Office 365 -tietomurroista

Poliisin silmissä tietojenkalastelu näyttäytyy hyvin huolestuttavana ilmiönä. Tietojenkalastelu on pääsääntöisesti tehty käyttäen hyvin taidokkaasti luotuja kalastelusivuja. Yritysten Office 365 -palveluun päästyään tekijät ovat saattaneet seurata yrityksen sähköpostiliikennettä hyvinkin pitkän aikaa. Toisaalta poliisille tehdään näistä suhteellisen vähän rikosilmoituksia, ja tällöin poliisille ei kerry riittävästi dataa tekijöiden tunnistamiseksi.

Finanssialan yritys A
Yrityksen Office 365 -pilvipalveluun oli murtauduttu tietojenkalastelun avulla, lähettämällä kahdelle yrityksen työntekijälle sähköpostia, jossa oli linkki tietojenkalastelusivulle. Järjestelmässä oli seurattu yrityksen sähköpostiliikennettä useamman kuukauden ajan, sekä luotu sähköpostin edelleenlähetyksen sääntömuutoksia yrityksen tietämättä. Yrityksellä A ei ollut tarkkaa käsitystä siitä, kuinka kauan sen sähköpostiliikennettä oli seurattu, eikä siitä mitä tietoa yrityksestä on saattanut vuotaa. Tämän lisäksi yrityksen maksuliikenteeseen oli yritetty lisätä laskuja, joita tekijät yrittivät saada yrityksen maksamaan heidän tililleen. Laskussa oli käytetty hyväksi sähköpostiliikenteestä saatuja tietoja ja näin yritetty saada lasku näyttämään mahdollisimman aidolta.

Teollisuusyritys B
Yrityksen Office 365 -pilvipalveluun oli murtauduttu tietojenkalastelun avulla, kuten edellisessäkin esimerkissä. Yrityksen sähköpostijärjestelmästä oli lähetetty tietojenkalastelulinkkejä eteenpäin yrityksen tytäryhtiöissä työskenteleville työntekijöille, sekä alihankkijoille että asiakkaille. Yrityksessä havaittiin, että sen sähköpostijärjestelmään oli tehty luvattomia edelleenlähetyssääntöjä. Poliisin harmiksi tietomurto yrityksen järjestelmään havaittiin niin myöhään, ettei lokitietoa murtautumisesta ollut enää saatavissa.

2 Office 365 tietojen kalastelun näkökulmasta

Microsoft Office 365 on myös Suomessa laajasti käytössä oleva pilvipalvelu. Sen tärkeimpiä osia ovat Exchange Online, Sharepoint Online ja Teams. Skype for Business Online on jäämässä pois vastaavien viestintätoimintojen löytyessä nyt Teamista. Office 365:n useimpiin lisenssivaihtoehtoihin kuuluvat myös tietotyön työpöytäsovellukset, kuten Outlook, Word, Excel ja Powerpoint.

Enterprise Mobility + Security (EMS) puolestaan kokoaa tietotyön hallinta- ja tietoturvapalvelut yhdeksi ratkaisuksi. Siihen kuuluvat Azure Active Directoryn kattavammat versiot, päätelaitteiden hallintapalvelu Intune ja tiedon suojaamisen Azure Information Protection.

Microsoft 365[1] yhdistyvät Office 365, Windows 10 ja Enterprise Mobility + Security.

Tunnusten kalastelun välineenä on yleensä sähköposti ja tavoitteena saada haltuun käyttäjän kirjautumisnimi ja salasana. Niinpä Office 365:n palveluista kalastelun kannalta keskeisessä asemassa ovat Exchange-palvelu ja kirjautumisen vastaanottava Azure Active Directory. Niiden suojausta parantamalla voidaan kalastelun onnistuminen todennäköisesti estää tai ainakin sen onnistumisen todennäköisyyttä merkittävästi pienentää.

Kalastelussa käyttäjälle voidaan näyttää esimerkiksi SharePoint-ruutuja. Ne eivät kuitenkaan ole aitoja tai organisaation omia, joten oman SharePoint-palvelun suojaaminen ei auta.

Jos kalastelu onnistuu eli rikolliset saavat haltuunsa salasanoja, voi heidän jälkiään näkyä sähköpostin ja kirjautumisten lisäksi muidenkin palveluiden lokeissa. Tätä käsitellään tarkemmin Suojaustoimet-osiossa.

[1] https://www.microsoft.com/fi-FI/microsoft-365/

2.1 Office 365 -versiot

Office 365:stä on Business-versio enintään 300 hengen organisaatioille ja Enterprise-versio sitä suuremmille. Jälkimmäisestä[2] on saatavana tasot E1, E3 ja E5. Lisäksi on myös kuluttaja- ja oppilaitosversiot (Education A1, A3 ja A5).

Office 365 on voitu hankkia erillisenä, tai sitten osana Microsoft 365:ttä. Myös Microsoft 365:stä on suppeampi taso E3 ja laajempi taso E5.

Office 365 -palveluihin kirjautuminen tapahtuu Azure Active Directoryn avulla. Sen perustaso sisältyy aina Office 365:een, mutta laajemman Premium-tason P1 tai P2 saa osana EMS:ää, siis esimerkiksi Microsoft 365:n mukana. Lisäksi Microsoft 365:sta on olemassa Microsoft 365 Firstline 1[3], jossa on mukana esim. Azure Active Directory Premium P1.

Seuraava taulukko havainnollistaa vaihtoehtoja. Siinä omana sarakkeenaan on merkitty Office 365 Business-versio, mutta kuten edellä todettiin, myös Office 365 Enterprise on mahdollista hankkia erillisenä.

Osa-alue	**Office 365 Business-versio erikseen**	**Microsoft 365 E3**	**Microsoft 365 E5**
Office 365	Business	Enterprise E3	Enterprise E5
EMS	–	EMS E3, jossa Azure AD P1 + muutakin	EMS E5, jossa Azure AD P2 + muutakin
Windows 10	–	Enterprise	Enterprise + Windows Defender Advanced Threat Protection

Tilauksia ja niiden sisältämiä lisenssejä voidaan myös yhdistellä. Yksittäisellä ylläpitäjäkäyttäjällä voisi siis olla Microsoft 365 F1 -lisenssi ja lisäksi hänelle voitaisiin hankkia Azure AD P2 -lisenssi, jotta saataisiin käyttöön esim. Privileged Identity Management -toiminto.

Microsoft 365 E3 -tilaukseen tuli 1.2.2019 saataville uudet tietoturvatoimintoja sisältävät lisäpaketit Identity & Threat Protection ja Information Protection & Compliance. Kuten nimistäkin voi päätellä, niin näistä erityisesti ensin mainittu sisältää tärkeimmät palvelut identiteettien hallintaan. Kaaviot eri palvelupaketeista ja niiden sisältämistä toiminnoista löytyy esim. sivustolta https://github.com/AaronDinnage/Licensing.

[2] https://products.office.com/fi-fi/business/compare-more-office-365-for-business-plans
[3] https://www.microsoft.com/fi-fi/microsoft-365/compare-all-microsoft-365-plans

2.2 Identiteetti (Azure Active Directory)

Azure Active Directory on identiteettien hallintapalvelu, joka on käytössä kymmenien miljoonien organisaatioiden yhteensä yli miljardilla käyttäjällä. Osa näistä on Office 365 -käyttäjiä ja osa käyttää Azure AD:ta muihin sovelluksiin. Eri organisaatiot käyttäjineen ja datoineen on jaettu loogisesti omiin tenant:eihin (vuokralaisiin) ja ne on eristetty toisistaan[4].

Azure AD:ssa on käytettävissä kaksi eri identiteettityyppiä: pilvi-identiteetti (managed) ja federoitu (federated) identiteetti. Edellisessä käyttäjä tunnistetaan aina Azure AD:n kautta. Jälkimmäisessä tunnistautuminen tapahtuu Azure AD:n ulkopuolella, ja Azure AD luottosuhteeseen perustuen luottaa ulkopuolella tehtyyn tunnistautumiseen. Identiteettityyppi on toimialuekohtainen (sähköpostin domainosa).

Azure AD:yyn on integroitu satojatuhansia sovelluksia. Niihin ei tarvitse erikseen kirjautua, vaan Azure AD-kirjautuminen riittää. Kyseisten sovellusten käytön luvituksessa voidaan hyödyntää Azure AD:n käyttäjäryhmiä.

Azure AD voidaan yhdistää organisaation omassa verkossa (On-Premises) olevaan Active Directory Domain Services -palveluun (AD DS), josta käytetään usein nimeä Active Directory tai aktiivihakemisto. Yhdistämällä voidaan käyttää samoja tunnistetietoja sekä organisaation sisäverkon palveluissa että pilvipalveluissa. Yhdistäminen tehdään useimmin oman verkon palvelimeen asennettavalla Azure Active Directory Connect -ohjelmalla.

Yhdistetyssä ympäristössä kirjautuminen tapahtuu jollakin seuraavista tavoista[5]:

1. Salasanoista johdetut merkkijonot synkronoidaan Azure Active Directoryyn.
   (Password Hash Synchronization - PHS)[6].
   Pilvipalveluja käytettäessä todennuksen tekee Microsoftin Azure Active Directory -palvelu.

2. Federoitu kirjautuminen: vain identiteetit synkronoidaan, mutta salasanoista johdettuja merkkijonoja ei.
   Käyttäjän kirjautuessa pilvipalveluun, hänet ohjataan on-premise -ympäristön Active Directory Federation Service (AD FS) -palveluun. Tämä ratkaisu vaatii useimmiten vähintään neljän palvelimen (kaksi sisäverkkoon ja kaksi DMZ-vyöhykkeelle) käyttöönoton.
   Active Directoryn domain controller (valtuuttaja) -palvelimet tekevät todennuksen.

3. On-premise -ympäristössä käytetään Passthrough Authentication (PTA) -palvelua. Tällä ratkaisulla voidaan korvata AD FS -palvelu, ellei organisaatiolla ole muita AD FS -palvelulla toteutettuja kertakirjautumista vaativia palveluita.

4. On-premise -ympäristössä käytetään PingFederate-palvelua[7], jolloin PingFederate-palvelu tekee todennuksen.

Vaikka organisaation käytössä olisi federoitu kirjautuminen (edellä olevan listan vaihtoehto 2), voidaan salasanoista johdetut merkkijonot synkronoida myös Azure AD:yyn (listan vaihtoehto 1). Tällä saavutetaan kaksi hyötyä:

a) nopeampi siirtyminen pilvi-identiteettiin federoidun sijaan on-prem federointipalvelun mahdollisesti vikaantuessa
b) vääriin käsiin joutuneiden tunnistetietojen tunnistaminen (Azure AD:n leaked credentials -raportti[8])

Azure AD sisältää myös salasanojen resetoinnin itsepalveluperiaatteella. Pilvipalvelussa resetoidun synkronoidun käyttäjän salasana voidaan synkronoida takaisin on-prem Active Directoryyn. Tähän vaaditaan Azure AD Premium -versio (P1 tai P2).

Identiteettien kokonaisvaltaisen ylläpidon ja kalastelulta suojautumisen kannalta Azure AD:n tärkeimmät toiminnot ovat:

[4] http://aka.ms/Office365TI
[5] https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn
[6] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization
[7] https://docs.pingidentity.com/bundle/O365IG20_sm_integrationGuide/page/O365IG_c_integrationGuide.html
[8] https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Azure-Active-Directory-Premium-reporting-now-detects-leaked/ba-p/249200

Monimenetelmäinen todentaminen (Multi Factor Authentication - MFA)

MFA mahdollistaa perinteisen käyttäjätunnus-salasanayhdistelmän lisäksi tehtävän lisätarkistuksen. Lisätarkistuksen vaihtoehdot ovat:

- kertakäyttöinen numerokoodi puhelulla
- kertakäyttöinen numerokoodi tekstiviestillä
- hyväksyntä mobiilisovelluksella (Microsoft Authenticator)
- kertakäyttöinen numerokoodi mobiilisovelluksella (Microsoft Authenticator).

Microsoftin pilvipohjaisesta MFA:sta on olemassa kolme eri versiota:

1. Multi-Factor Authentication for Office 365. Office 365:n mukana tuleva suppeampi versio, jonka avulla voidaan suojata ainoastaan Office 365 -sovelluksia. Tässä versiossa MFA-vaatimus täytyy kytkeä päälle käyttäjäkohtaisesti.
2. Azure Multi-Factor Authentication. Azure AD Premium (P1 tai P2) sallii MFA-vaatimuksen päälle kytkemisen Conditional Access -ehtojen avulla tai käyttäjäkohtaisesti. Tunnistautumiseen käytetään Azure MFA -palvelua tai sille voidaan asentaa erillinen palvelin omaan verkkoon.
   HUOM! 1.9.2018 saakka Azure MFA voitiin hankkia erillisellä lisenssillä, mutta nykyään se on saatavana vain Azure AD Premium -tilauksen yhteydessä.
3. MFA for Azure Active Directory Global Administrators. Alun perin MFA oli otettavissa käyttöön vain Azure AD:n kaikki oikeudet omaavan Global Administrator -roolin omaaville käyttäjille. Sittemmin palvelu on laajentunut kattamaan myös muut käyttäjät. Vuonna 2018 Microsoft toi Global Administrators -toiminnon käyttöönotettavaksi erityisen Conditional Access baseline protection-käytännön avulla. Microsoft tulee kytkemään käytännön päälle sen julkistuksen yhteydessä ts. sen saavuttaessa General Availability -vaiheen.

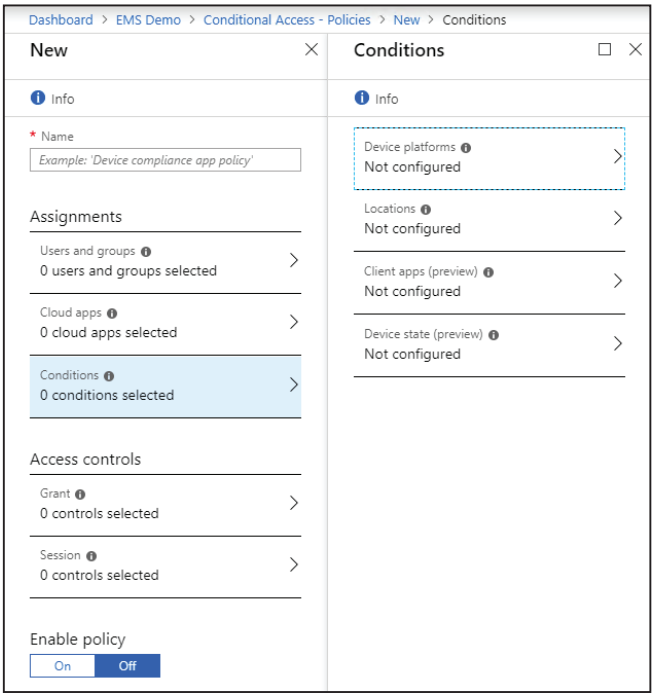
Conditional Access

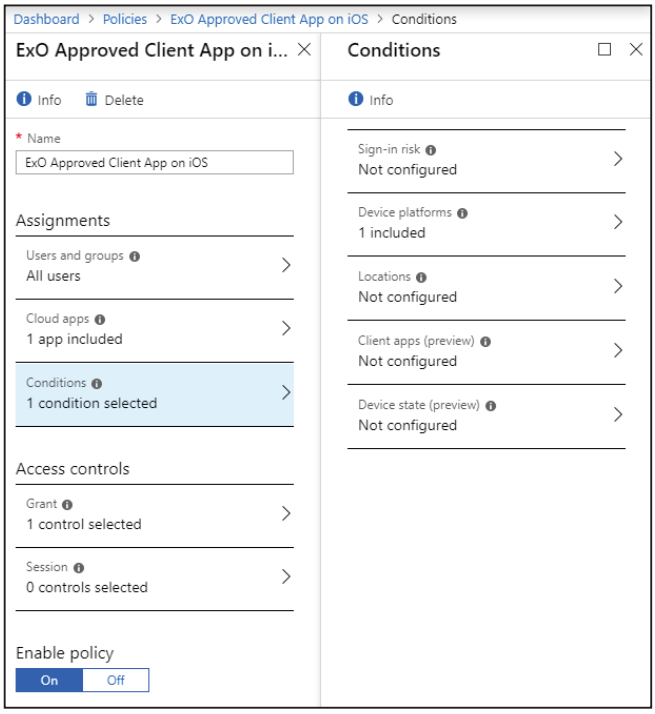
Conditional Access, eli ehdollinen pääsy, sallii tai estää määrättyjen palveluiden (esim. Office 365, Exchange Online, jne.) käytön tiettyjen ehtojen toteutuessa. Pääsy voidaan sallia esimerkiksi tietylle käyttäjän sijainnin, laitteen, palvelun ja tunnistautumismenetelmän yhdistelmälle.

Tyypillisesti esimerkiksi pelkkä käyttäjätunnus-salasana-yhdistelmä on sallittu sisäverkosta käsin, mutta julkisen verkon kautta edellytetään kaksivaiheista tunnistaumista. Toinen tyypillinen esimerkki on, että palveluita voidaan käyttää vain organisaation omilla laitteilla. Tällöin esimerkiksi kotikoneelta ei Office 365 -palveluita voi käyttää.

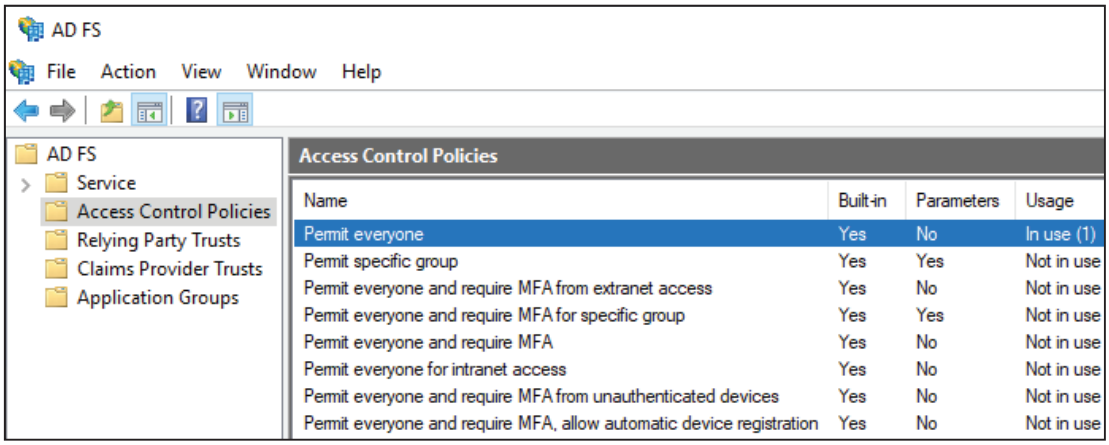
Azure Active Directory Conditional Access on käytettävissä Azure AD:n Premium-tilauksissa.

Alla olevassa kuvassa on Windows Server 2019 AD FS -palvelun oletuskäytännöt.





Mikäli käytössä ei ole Azure AD Premium -lisenssejä, voidaan saman tyyppinen toiminnallisuus toteuttaa federoidulla identiteetillä käyttämällä Microsoftin Active Directory Federation Services (AD FS) -palvelua. AD FS on Windows-palvelinkäyttöjärjestelmiin kuuluva rooli. Yllä olevassa kuvassa on Windows Server 2019 AD FS -palvelun oletuskäytännöt.



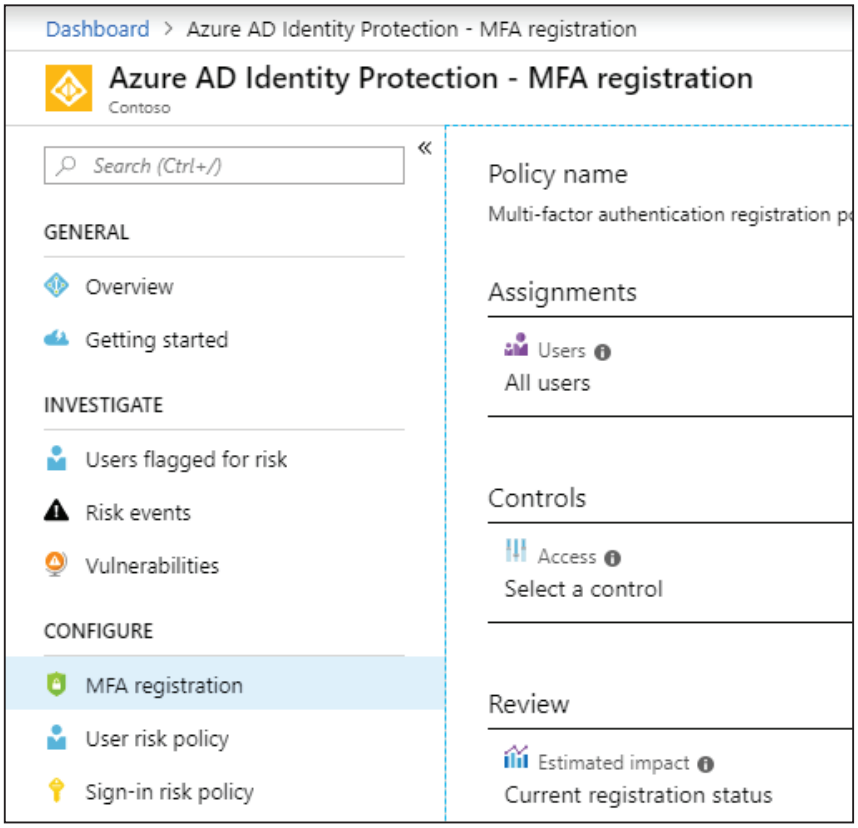
Identity Protection[9]

Identity Protection -palvelun avulla saadaan käyttöön:

1. Organisaation identiteetteihin vaikuttavien haavoittuvuuksien tunnistaminen
2. Automaattinen toiminta havaittuihin identiteetteihin liittyviin epäilyttäviin tapahtumiin liittyen
3. Epäilyttävien tapahtumien forensiikka ja ratkominen.

Identity Protection tuo mukanaan myös MFA Registration -toiminnon, jolla halutut käyttäjät voidaan pakottaa rekisteröitymään MFA:n käyttäjiksi.

Identity Protection -palveluun on tammikuussa 2019 tullut saataville uusia toimintoja[10].



[9] https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/index

[10] https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Four-major-Azure-AD-Identity-Protection-enhancements-are-now-in/ba-p/326935

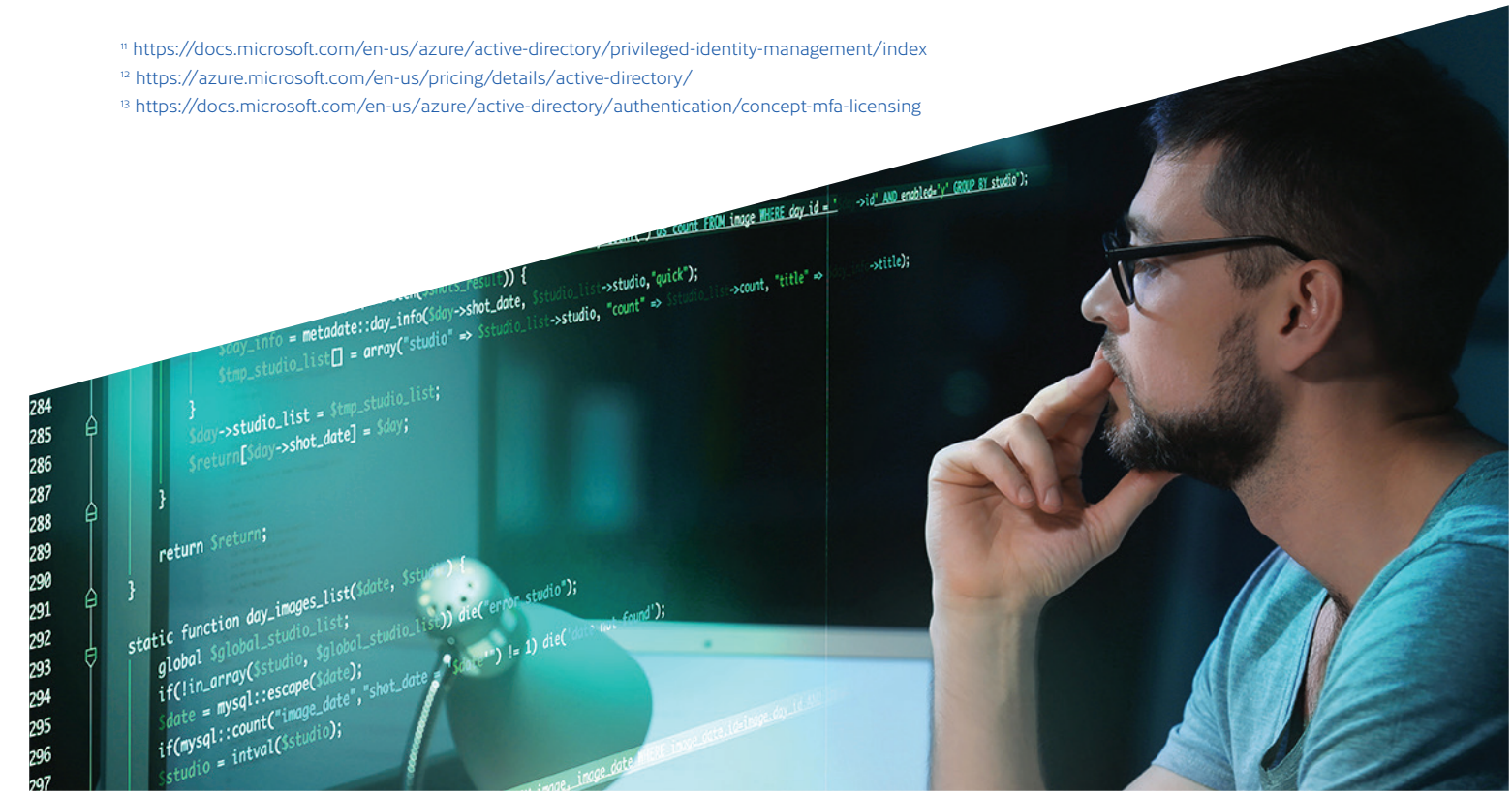
Azure Active Directory Privileged Identity Management[11]

Privileged Identity Management -palvelun avulla Azure AD:n ja Azuren hallintaroolien jäsenyys saadaan vihdoin otettua hallintaan siten, että ylläpitäjien roolit ovat joustavia. Pysyvien ylläpitäjien lukumäärää voidaan useissa tapauksissa vähentää. Käyttäjät ottavat roolit ja niiden valtuudet käyttöön tarvittaessa ja käyttöä voidaan seurata. Roolien käyttöönotossa voidaan käyttää hyväksymismenettelyä, jossa ylläpitäjäksi nosto edellyttää nimettyjen henkilöiden hyväksynnän. Nämä toiminnot on esitetty seuraavassa taulukossa:

		Azure AD-versio		
Toiminto		**Basic ja Office 365**	**Azure AD P1**	**Azure AD P2**
Multi-Factor Authentication for Office 365		X	X	X
Azure Multi-Factor Authentication			X	X
Conditional Access	Päätelaitteen käyttöjärjestelmään, sijaintiin, käytettävään sovellukseen tai laitteen tilaan perustuen		X	X
	Riskiin perustuen			X
Identity Protection				X
Privileged Identity Management				X

Eri Azure AD-versiot ja niiden toiminnot on tarkemmin esitelty Azure AD-palvelun hinnoittelusivulla[12].
MFA-palvelun eri versioiden toiminnot löytyvät omalta sivultaan[13].

[11] https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/index
[12] https://azure.microsoft.com/en-us/pricing/details/active-directory/
[13] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing



2.3 Sähköpostin suojaustekniikoita

Sähköpostia voidaan suojata erilaisin teknisin toimin. Sähköpostipalvelinten välinen liikenne voidaan pakotetusti salata TLS:n (Transport Layer Security) avulla. TLS perustuu varmenteisiin, jolloin samalla voidaan varmistua toisen osapuolen identiteetistä.

Roskapostin torjuntaan on myös käytettävissä eri tekniikoita[14]. Seuraavassa taulukossa olevien tekniikoiden avulla voidaan estää Office 365 -ympäristöstä lähetettyjen sähköpostien merkintää roskapostiksi. Sisäänpäin tulevaan sähköpostiin näillä tekniikoilla ei voi vaikuttaa, koska asetukset tekee aina lähettävä osapuoli.

	SPF	DKIM	DMARC
Mitä tarkoittaa?	Sender Policy Framework	DomainKeys Identified Email	Domain-Based Message Authentication, Reporting, and Conformance
Mikä se on?	Järjestelmä, joka julkistaa ja varmentaa kuka voi lähettää sähköpostia toimialueelta.	Sähköpostin tunnistautumisjärjestelmä, joka perustuu epäsymmetrisiin salausavaimiin.	Sähköpostin tunnistautumisjärjestelmä, joka auttaa selvittämään mitä tehdä jos viesti ei läpäise SPF tai DKIM tarkistusta.
Miten se toimii?	Vastaanottava osapuoli tarkistaa onko lähettävällä osapuolella oikeus lähettää toimialueen sähköpostia. Tieto on tallennettu toimialueen DNS järjestelmän TXT tietueeseen.	Lähettävä osapuoli allekirjoittaa sähköpostin ja/tai otsikkotiedot. Vastaanottava osapuoli tarkistaa allekirjoituksen ja varmentaa että tiedot eivät ole muuttuneet. Julkinen avain julkaistaan toimialueen DNS järjestelmän TXT tietueessa.	Vastaanottaja tekee SPF ja DKIM tarkistuksen. Jos tarkistus epäonnistuu, tarkastaa se lähettäjän DMARC käytänteet ja päättää mitä tehdä: pysäyttää viestin, laittaa sen karanteeniin, lähettää normaalisti, raportoi lähettäjälle. DMARC käytänne julkaistaan toimialueen DNS järjestelmän TXT tietueessa.
Miksi tärkeä?	Vähentää todennäköisyyttä, että ulospäin lähetetyt viestit merkitään roskapostiksi.	Vähentää merkittävästi todennäköisyyttä, että ulospäin lähetetyt viesti merkitään roskapostiksi.	Auttaa vastaanottavaa organisaatiota päättämään, mitä tehdä sähköposteille, jotka eivät läpäise tarkistuksia. Toimii myös lähettäjälle palautekanavana.

2.4 Tiedon jakaminen eri palveluissa

Office 365:ssä voidaan jakaa omia tiedostoja organisaation ulkopuolelle yhteistyön avittamiseksi.

Jakaminen tapahtuu ennen kaikkea SharePoint-dokumenttikirjastoista joko suoraan SharePoint-toiminnoilla tai sitten SharePointin varassa olevien Teams- tai OneDrive for Business -palvelujen toiminnoilla.

Vieraskäyttäjien pääsyä organisaation dokumentteihin voidaan säätää seuraavilla tasoilla:

- Azure AD. Identiteetin ja todennuksen perus-palvelu.
- SharePoint Online ja OneDrive for Business. SharePoint-dokumenttikirjastojen varassa toimii myös OneDrive for Business.
- Office 365 Groups. Näitä ryhmiä voidaan käyttää luvittamiseen ja ryhmän viestintään.
- Teams. Kunkin tiimin taustalla on Office 365 Groups -ryhmä ja SharePoint-dokumenttikirjasto.

Vieraskäyttäjien pääsyä Teams[15] -palvelun dokumentteihin on kuvattu alaviitteen linkissä.

Office 365 -palveluun tallennettavan tiedon sekä myös muiden pilvipalveluiden käytön seurantaan ja tiedon suojaamiseen Microsoftilla on CASB- (Cloud Access Security Broker) ratkaisu nimeltään Cloud App Security[16]. Sen avulla voidaan

- seurata organisaation käyttämiä pilvipalveluita ja niihin liittyvää riskiä

[14] https://blogs.technet.microsoft.com/fasttracktips/2016/07/16/spf-dkim-dmarc-and-exchange-online/

[15] https://docs.microsoft.com/en-us/microsoftteams/teams-dependencies

[16] https://docs.microsoft.com/en-us/cloud-app-security/

- suojata dataa seuraamalla ja hallitsemalla pilvipalvelujen käyttöä
- tunnistaa poikkeavaa käyttäytymistä ja tietoturvaloukkauksia ja reagoida niihin automaattisesti; tämä voisi toteutua esimerkiksi kalastelun onnistuttua, kun pilvipalvelussa jaetaan haltuun saadulla käyttäjätunnuksella tiedostoja ulkopuolisille käyttäjille.

Palvelusta on kaksi versiota[17]: Office 365 Cloud App Security ja Microsoft Cloud App Security. Näistä ensimmäinen sisältyy Office 365 E5 - ja jälkimmäinen EMS E5 -pakettiin.

2.5 Tietoturva-arkkitehtuuri

Azure Active Directory:n tietoturva-arkkitehtuuri poikkeaa merkittävästi perinteisen Active Directoryn vastaavasta. Seuraavassa taulukossa on esitelty joitakin Windows Server -käyttöjärjestelmään integroidun Active Directory Domain Service:n ja Azure Active Directoryn eroja.

	Active Directory (Domain Services)	**Azure Active Directory**
Käyttötarkoitus	On-premise verkkokäyttöjärjestelmä Windows-koneille	Identiteettipalvelu pilviaikakaudelle (Identity as a Service IDaaS)
Todennus	Kerberos ja NTLM	OpenID Connect, Security Assertion Markup Language (SAML), WS-Federation, ADAL
Valtuutus	Käyttöjärjestelmän palvelut	OAuth2
Tiedon hakeminen	LDAP	REST API:t HTTP tai HTTPS
Hallinnan rajat	Metsä, puu, toimialue	Vuokralainen (tenant)
Pääsy	Pääosin organisaation sisäverkko, jotkin toiminnot (esim. todennus) käytettävissä muiden palveluiden kautta myös ulkoverkosta	Mistä tahansa
Organisaatioiden välinen integraatio	Työlästä	Helppoa

Yhtenä Microsoftin identiteettipalveluna on saatavilla Azure Active Directory Domain Services[18]. Se on supistettu versio perinteisestä Active Directorystä. Sen pääkäyttötarkoitus on Active Directoryn palveluiden (todennus, haku ja Group Policy) tarjoaminen Azureen siirrettävien virtuaalikoneilla toimiville palveluille.

2.5.1 Azure Active Directoryn hallintamalli

Azure AD:ssa on käytössä roolipohjainen hallintamalli (Role-Based Access Control, RBAC). Käytössä on useita eri rooleja, joista suurimmat oikeudet omaa Global Administrator. Ainoastaan tähän rooliin kuuluvilla on oikeus antaa toisille käyttäjille pääkäyttäjäoikeuksia ja esimerkiksi lisätä uusia toimialueita. Pienin käyttöoikeusrooli on puolestaan käyttäjä (User), joka annetaan automaattisesti kaikille Azure AD -hakemiston käyttäjille. Päivittäiseen käyttäjien hallintaan, esimerkiksi lisenssien hallintaan ja salasanojen resetointiin, riittää ”User Account Administrator” -rooli.

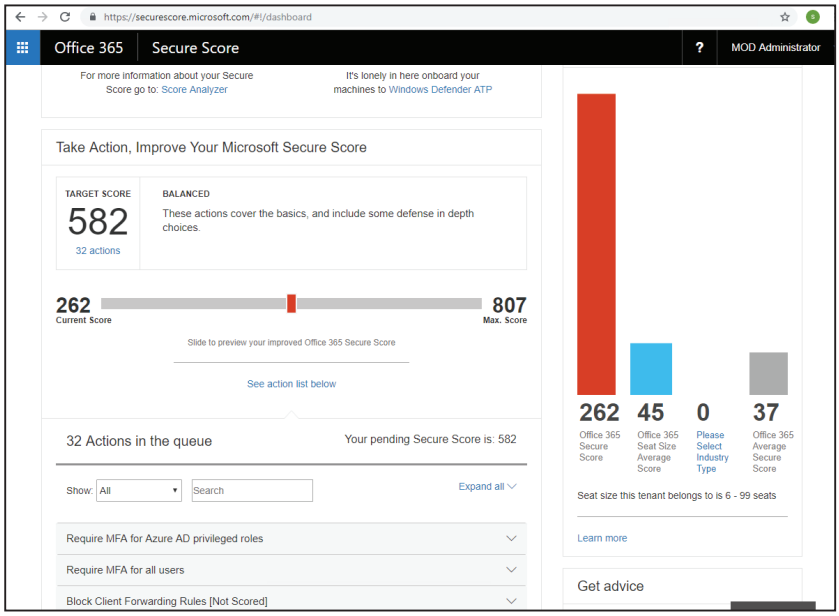
Azure AD:ssa on käytössä Active Directorystä tutut tietoturvaryhmät. Näitä ryhmiä voidaan käyttää esimerkiksi SharePoint Onlinessa pääsyoikeuksien hallintaan. Active Directory:sta poiketen Azure AD:ssa ryhmille ei voi antaa RBAC-rooleja. Jos Azure AD on yhdistetty Active Directoryyn, voidaan ryhmiä hallita Active Directoryssa.

Käytettäessä Azure AD:n suojaustoimintoja, tulee pääsy varmistaa erilaisin poikkeusjärjestelyin. Microsoft on valmistellut ohjeen[19], jonka avulla erilaisiin poikkeustilanteisiin voidaan varautua.

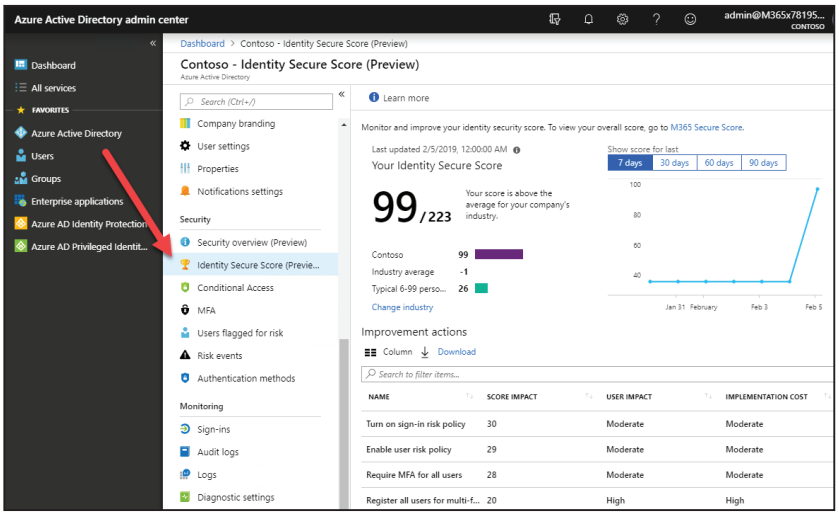
[17] https://docs.microsoft.com/en-us/cloud-app-security/editions-cloud-app-security-o365
[18] https://docs.microsoft.com/en-us/azure/active-directory-domain-services/
[19] https://aka.ms/resilientaad

2.6 Microsoft Secure Score

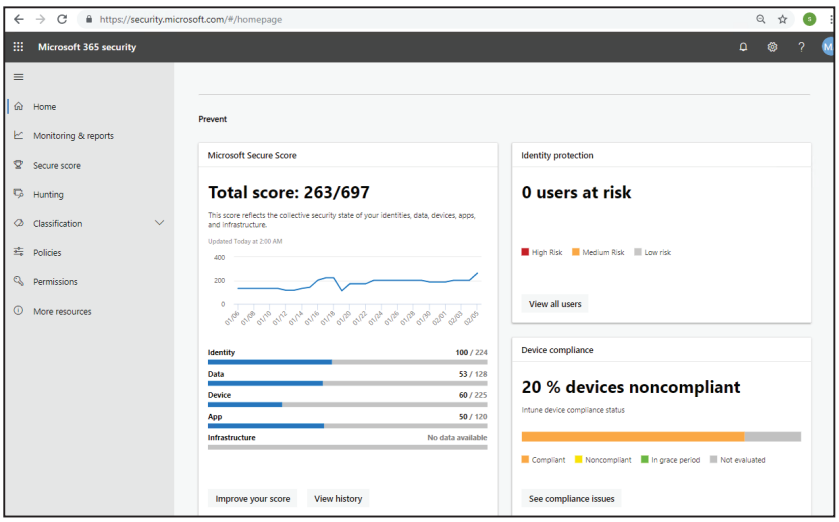
Microsoft Office 365 Secure Score[20] tuli saataville vuoden 2016 syksyllä. Sen avulla organisaation ylläpitäjä näkee analyysin organisaation kurantista Office 365 -tietoturvatilanteesta ja saa suosituksia sen parantamiseksi tehtävistä toimenpiteistä. Toimenpiteiden yhteydessä on kuvattu uhat, joiden torjumiseksi toimenpide tehdään. Toimenpiteen vaikutus käyttäjien toimintaan sekä käyttöönoton monimutkaisuus on myös kuvattu.



Identity Secure Score tuli puolestaan saataville syksyllä 2018. Se on käytettävissä Azure AD-hallintaportaalin osana.



Tammikuussa 2019 Microsoft julkisti uudet Microsoft 365 Security center ja compliance center -portaalit[21]. Ne ovat käytettävissä Microsoft 365 E3 tai E5 -tilauksilla. Security centerissä Secure Score on jaettu eri osioihin. Samaan työkaluun on yhdistetty myös esim. forensiikkatoimintoja. Security Center -portaalin avulla eri lähteistä tuleva informaatio on yhdistetty ja näin ei tarvitse avata useita eri portaaleita.



[20] https://securescore.microsoft.com/

[21] https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Introducing-the-new-Microsoft-365-security-center-and-Microsoft/ba-p/326959

3 Suojaustoimet

Organisaatioiden omissa palveluissa on vuosien varrella saattanut muodostua teknologiavelkaa, kun palveluita ei ole eri syiden takia päivitetty uusimpiin versioihin. Hyvänä esimerkkinä tästä on vieläkin laajasti käytössä oleva Windows 7 -käyttöjärjestelmä, jonka suunnittelussa ei olla aikanaan voitu ottaa huomioon nykypäivän uhkia.

Pilvipalvelut päivittyvät jopa viikoittain. Tällöin erityisesti ylläpidolle ja tukitoiminnoille tulee haasteita pysyä kehityksessä mukana.

Kun nämä kaksi todellisuutta yhdistetään, voi seurauksena olla monimutkainen käyttöönottoprojekti.

3.1 Identiteettien suojaaminen

Suojauksen kannalta tärkeintä on suojata käyttäjien identiteetit. Koska nykyään missä tahansa pilvessä sijaitsevia palveluita käytetään mistä tahansa erilaisilla päätelaitteilla, eivät perinteiset suojaustoimenpiteet ole enää riittäviä.

3.1.1 Räätälöi sisäänkirjautumissivut organisaatiosi graafisen ilmeen mukaisiksi

Office 365 -palvelun sisäänkirjautumissivut voidaan räätälöidä organisaation graafisen ilmeen mukaisiksi[22]. Samalla käyttäjät tottuvat niiden ulkonäköön ja näin kalastelun onnistuminen organisaation räätälöidystä kirjautumissivuista poikkeavalla ulkonäöllä vaikeutuu.

Toisaalta käyttäjä ei voi ulkonäköön täysin luottaa, koska kalastelija on voinut tehdä väärennetystä sivusta täysin samannäköisen. Tällaisessakin tapauksessa väärennös saattaa paljastua osoiterivin ja varmenteen (sertifikaatin) tietojen perusteella.

3.1.2 Suojaa salasanat

Salasanojen monimutkaisuudesta ja riittävästä pituudesta huolehtiminen on tärkeää. Sen avulla salasanojen murtamisen onnistumisen todennäköisyyttä voidaan pienentää. Kalastelussa monimutkaisuus ei tosin paljon auta, jos käyttäjä naputtelee fraaseista koostuvan tms. vahvan salasanan väärälle sivulle.

Yleisesti käytettyjen merkkijonojen esto on nykyään mahdollista toteuttaa sekä Azure AD:ssä että myös on-premises Active Directoryssä[23]. On-prem -ympäristön salasanojen rajoittamiseen tällä toiminnolla vaaditaan Azure AD Premium -lisenssit.

Salasanojen arvaamisen tai raa'alla laskennalla tapahtuvan murtamisen estämiseksi on olemassa monia eri tekniikoita. Microsoft on julkaissut suositeltavia toimenpiteitä arvaamisen tai murtamisen estämiseksi[24].

Jos käytössä on federoitu kirjautuminen, on syytä varmistaa, että käytössä on Extranet Lockout[25]. Toiminto tuli saataville Windows Server 2012 R2 -versiossa ja on edelleen kehittynyt uudemmissa käyttöjärjestelmissä (Windows Server 2016 ja 2019).

3.1.3 Suojaa Active Directory

Erityisesti Azure AD:yyn yhdistetyssä ympäristössä paikallisen Active Directoryn hallinta on myös tärkeää.

Active Directory julkistettiin Windows Server 2000:een integroituna vuonna 2000. Sen ylläpitoon ja suojaamiseen on muodostunut kuluneiden lähes 20 vuoden aikana paljon suositeltavia käytäntöjä. Lisäksi palvelu ei ole viimeisimmässä versioissaan enää juurikaan kehittynyt Microsoftin siirrettyä kehityspanoksiaan pilvipalveluiden ml. Azure Active Directory kehitykseen.

[22] https://docs.microsoft.com/en-us/office365/admin/setup/customize-sign-in-page?view=o365-worldwide
[23] https://aka.ms/aadpasswordprotectiondocs
[24] https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/
[25] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection

Tietoturvaan liittyviä Active Directoryn toimintoja ovat mm.

- hallinta
- käyttäjätunnusten ja -ryhmien hallinta
- asetusten keskitetty hallinta Group Policyn avulla
- havainnointi
- lokit ja hälytykset.

Tuhansien Group Policy -asetusten määritys käsin olisi työlästä. Tästä johtuen Microsoft on vuosikausien ajan julkaissut Security Baseline -dokumentteja, joissa nämä asetukset on määritetty tietoturvatasoille. Työkaluista viimeisin on nimeltään Security Compliance Toolkit (SCT)[26].

Yksi Group Policyllä hallittavista osa-alueista ovat salasanoihin liittyvät vaatimukset. Azure AD:ssa salasanalle on määritelty vaatimuksena 8-16 merkin pituus, sekä monimutkaisuusvaatimuksena sen tulee sisältää seuraavista vähintään kolme: isot kirjaimet, pienet kirjaimet, numerot ja erikoismerkit. Azure AD:yyn yhdistetyssä paikallisessa AD:ssa Azure AD:n salasanakäytännöt eivät kuitenkaan välttämättä ole voimassa. Toisin sanoen pahimmillaan on mahdollista, että Azure AD:yyn päätyy yhden merkin mittaisia salasanoja synkronoiduille käyttäjätunnuksille.

Auditointilokien määritykset tehdään yleensä myös keskitetysti Group Policyn avulla. Tässä dokumentissa ei käsitellä yksittäisiä lokeja ja niiden asetuksia. Kalasteluun liittyen esimerkiksi kirjautumistapahtumien lokitus on syytä varmistaa. Yksittäisten koneiden ja etenkin palvelinten lokit on tallennettava keskitetysti. Tämä onnistuu Windows-käyttöjärjestelmän Windows Event Forwarding -toiminnolla[27]. Konsolidoidut lokit voidaan edelleen viedä SIEM-järjestelmiin, joissa tapahtumia voidaan tarkemmin analysoida ja määrittää hälytyksiä.

3.1.4 Modern Authentication on edellytys turvalliselle kaksivaiheiselle tunnistautumiselle

Modern Authentication[28], eli moderni tunnistautuminen, on sateenvarjotermi, joka kattaa eri tunnistautumis- ja valtuutusmenetelmien yhdistelmiä. Turvallisesti toteutettu kaksivaiheinen tarkistus edellyttää modernin tunnistautumisen käyttöä.

Modernin tunnistautuminen on oletuksena käytössä 1.7.2017 jälkeen luoduissa Office 365 -tenanteissa. Sen käytön varmistaminen tai käyttöönottaminen eri palveluissa tehdään PowerShell-komennoin:

- Exchange Online[29]
- Sharepoint Online[30]
- Skype for Business Online[31]

Mikäli käytössä on hybridiympäristö, täytyy moderni tunnistautuminen kytkeä päälle myös paikalliseen Exchange[32]- ja Skype for Business[33] -ympäristöön. Federoidussa ympäristössä käyttöönoton vaiheita on enemmän.

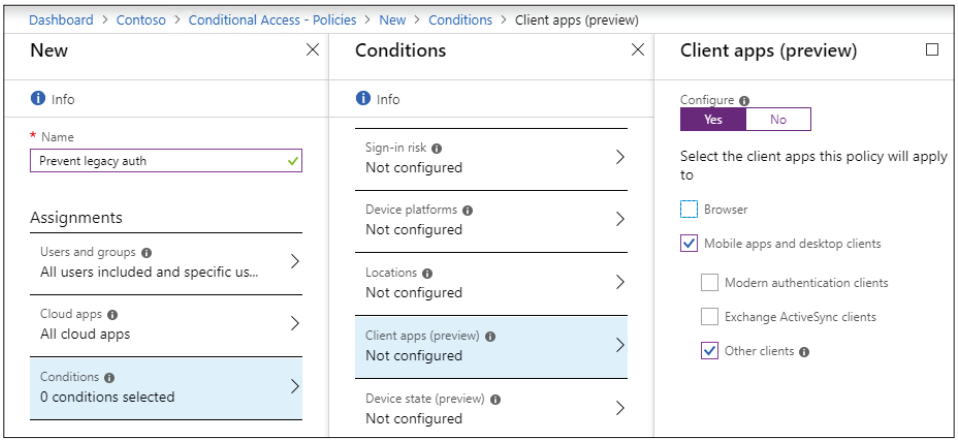
[26] https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10
[27] https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
[28] https://docs.microsoft.com/en-us/office365/enterprise/hybrid-modern-auth-overview#BKMK_WhatisModAuth
[29] https://docs.microsoft.com/en-us/Exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online
[30] https://docs.microsoft.com/ga-ie/azure/active-directory/conditional-access/conditional-access-for-exo-and-spo
[31] https://social.technet.microsoft.com/wiki/contents/articles/34339.skype-for-business-online-enable-your-tenant-for-modern-authentication.aspx
[32] https://docs.microsoft.com/en-us/office365/enterprise/configure-exchange-server-for-hybrid-modern-authentication
[33] https://docs.microsoft.com/en-gb/skypeforbusiness/manage/authentication/use-adal

3.1.5 Estä kaksivaiheista tunnistautumista tukemattomat tavat

Perinteiset sähköpostiprotokollat kuten POP, IMAP, SMTP ja ActiveSync eivät tue modernia tunnistautumista. Jos käytössä on kaksivaiheinen tunnistautuminen, voidaan näiden protokollien kautta edelleen tunnistautua käyttäjätunnus-salasana yhdistelmällä. Näiden protokollien käyttö tuleekin estää ja käyttää Office-asiakasohjelmistoa tai muita modernia tunnistautumista tukevia sovelluksia sekä tietokoneissa että mobiililaitteissa.

Kalastelun rajoittamisessa tärkeimmässä roolissa on Exchange-palvelu. Modern Authenticationin käyttö on voitu pakottaa federoidussa ympäristössä AD FS -palveluun määritetyillä säännöillä[34]. Syksyllä 2018 tuli mahdolliseksi estää Basic Authentication Exchange-palvelussa todennuskäytännöin, jotka voidaan kohdistaa jopa yksittäiseen käyttäjään[35].

Azure Active Directoryssä modernia tunnistautumista käyttämättömien sovellusten (ml. Exchange) käyttö on kesästä 2018 lähtien[36] voitu estää Conditional Access -säännöillä. Seuraavassa kuvassa Client apps -ehto määritetään siten, että ei-modernia tunnistautumista käyttävien sovellusten käyttö estetään.



Modernin tunnistamisen pakotuksen vaihtoehdot on esitetty seuraavassa taulukossa.

Toteutustapa	Edut	Haasteet
AD FS -säännöt	Käyttöjärjestelmän palvelu. Palvelun avulla voidaan estää turvattomien protokollien ja tunnistamisen käyttö sisäverkon ulkopuolelta.	Käytettävissä vain federoiduissa ympäristöissä. Monimutkaisempi määritys (oma ”ohjelmointikieli”).
Asetus palvelutasolla (Exchange Online)	Voidaan asettaa käytännöllä jopa yksittäiselle käyttäjälle.	Jos ei oletuskäytäntö, täytyy erikseen kytkeä päälle per käyttäjä.
Conditional Access	Helppo toteuttaa.	Vaatii Azure AD Premium -tilauksen.

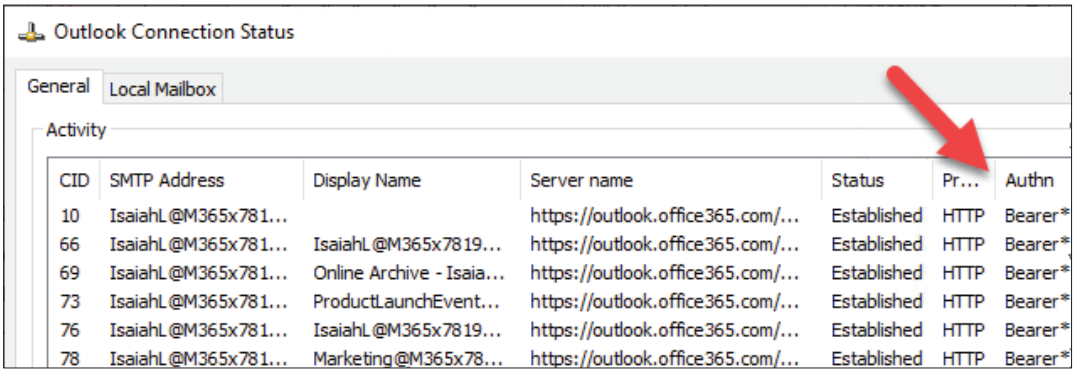
[34] https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditional-access-for-exo-and-spo
[35] https://blogs.technet.microsoft.com/exchange/2018/10/17/disabling-basic-authentication-in-exchange-online-public-preview-now-available/
[36] https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Conditional-Access-support-for-blocking-legacy-auth-is/ba-p/245417

3.1.6 Sovellusten Modern Authentication -tuki

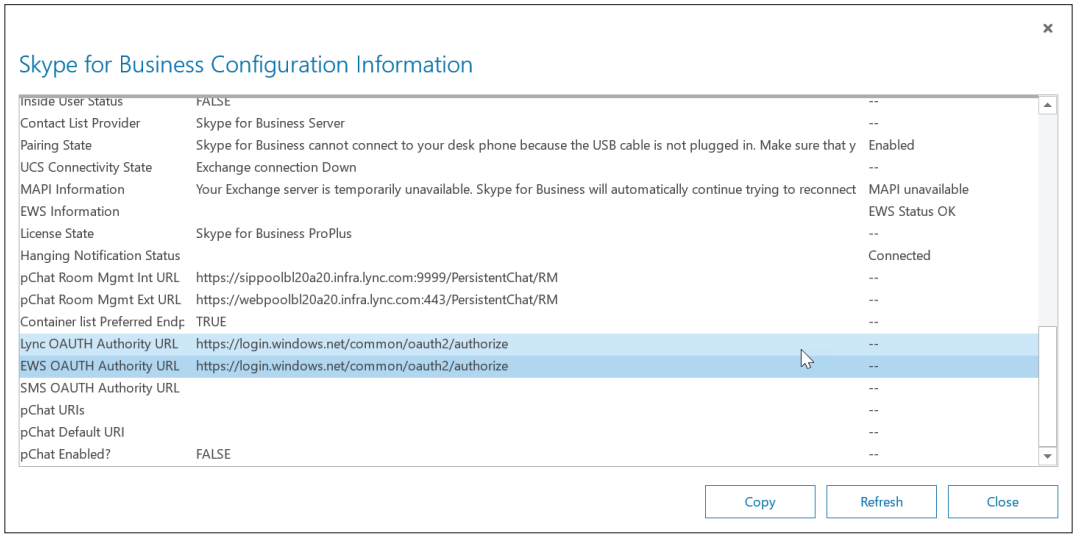
Modern Authentication vaatii tukea ja mahdollisesti toimenpiteitä myös käytössä olevissa sovelluksissa.

Kaikki Office 365:n palvelut tukevat modernia tunnistautumista. Selaimella palveluita käytettäessä moderni autentikointi onkin ainoa käytettävissä oleva tunnistautumistapa. Muut asiakasohjelmat, kuten sähköposti (Outlook) ja pikaviestintä (Skype for Business), saattavat kuitenkin edellyttää toimenpiteitä käyttäjien työasemille riippuen käytettävästä Office toimisto-ohjelmien versiosta. Office 2016 tukee oletuksena modernia tunnistautumista, Office 2013 -versiossa se täytyy kytkeä erikseen päälle[37].

Modernin tunnistautumisen käytön voi tarkistaa myös työasemasovelluksesta. Tässä on esitettynä Outlook ja Skype for Business. Molemmissa on System Trayn sovellus-kuvaketta on napsautettu <CTRL> -näppäintä samanaikaisesti painettaessa ja valittu Connection Status (Outlook) ja Configuration Information (Skype for Business).



Applen iOS-käyttöjärjestelmään modernin tunnistautumisen tuki tuli versiossa 11. Siinä on kuitenkin tiettyjä puutteita, jotka versio 12 korjasi. Apple macOS 10.14 oli ensimmäinen versio, jossa oli modernin tunnistautumisen tuki. Android-käyttöjärjestelmän natiivit sähköpostisovellukset eivät tue modernia tunnistamista. Tuki löytyy joistakin kolmansien osapuolien asiakassovelluksista, kuten esim. 9Foldersin Nine[38].



[37] https://docs.microsoft.com/en-us/office365/enterprise/modern-auth-for-office-2013-and-2016
[38] http://www.9folders.com/

3.1.7 Ota käyttöön kaksivaiheinen tunnistautuminen

Varmistathan, että Modern Authentication on aiemmin kuvattujen vaiheiden mukaisesti otettu käyttöön, jotta kaksivaiheiselle tunnistukselle ei jää takaportteja ts. se on aidosti turvallinen.

Kaksivaiheinen tunnistautuminen voidaan ottaa käyttöön joko käyttäjäkohtaisesti tai Conditional Access -toiminnon avulla. Näistä määritys käyttäjäkohtaisesti tuli saataville aiemmin, ja se on mahdollista toteuttaa ilman Azure AD Premium -lisenssejä. On myös mahdollista määrittää, että onnistuneen tunnistautumisen jälkeen tarkistusta ei tehdä seuraavaan 1-60 päivään. Tätä ei kuitenkaan suositella tehtäväksi, koska jos laite varastetaan, voitaisiin siltä kirjautua ilman kaksivaiheista tunnistautumista.

Azure MFA:n avulla on määritettävissä halutut IPv4-aliverkot, joista tarkistusta ei tehdä. Jos käytössä on federoitu identiteetti ja AD FS, voidaan tämä toteuttaa myös AD FS -säännöillä.

Haluttaessa on-prem-ympäristöön vielä monipuolisempi ratkaisu voidaan on-premises -palvelimelle asentaa MFA Server[39]. Sen avulla saadaan kaksivaiheinen tarkistus käyttöön myös muiden kuin Azure Active Directoryyn integroitujen palveluiden osalta. Tällaisia palveluita ovat esimerkiksi Remote Desktop, paikalliset IIS-websovellukset ja AD FS -palvelua kirjautumiseen käyttävät sovellukset.

Käyttäjien tulee määrittää kaksivaiheisen tarkistamisen asetukset[40]. Se tehdään käyttäjän Access Panel -portaalissa https://myapps.microsoft.com tai suoraan https://aka.ms/mfasetup. Käyttäjäkokemuksen selkeyttämiseksi salasanojen itsepalveluportaalin ja MFA:n integroitu hallintasivusto on dokumenttia kirjoitettaessa helmikuussa 2019 kokeiluvaiheessa[41]. Tämä sivusto pitää määrittää käyttöön tenatin asetuksissa.

Yhtenä kaksivaiheisen tunnistautumisen haasteena ovat ne käyttäjät, jotka eivät ole vielä rekisteröineet tarkistusta ja sen toteutustapaa. Tunnistetietojen kalastaja voi saada oman puhelimensa rekisteröityä. Kuten aiemmin kerrottiin, Azure AD Identity Protection sisältää toiminnon rekisteröinnin pakottamiseksi. Jos Identity Protection ei ole käytettävissä, niin käyttäjien MFA-tilaa voidaan seurata MFA-portaalin tai PowerShellin avulla[42].

Kaksivaiheinen tunnistautuminen aiheuttaa myös lisävaiheita ylläpitäjien PowerShell-käyttöön. Palvelusta riippuen esimerkiksi käytettävä Power-Shell-moduuli voidaan joutua vaihtamaan tai yhteyden avaaminen pilvipalveluun toteuttamaan aiemmin käytetystä käyttäjätunnus-salasana-yhdistelmästä poikkeavalla tavalla.

3.1.8 Ota Conditional Access käyttöön

Conditional Access kannattaa ottaa käyttöön luomalla useita käytäntöjä. Alkuun toiminto kannattaa testata pienemmällä kohderyhmällä. Conditional Access käyttöönotosta löytyy Microsoftin ohjeistus[43].

Tässä testaukseen ja pieneen ympäristöön soveltuvat mallikäytännöt:

1. Vaadi MFA pääkäyttäjiltä lukuun ottamatta “break-glass” -pääkäyttäjiä[44].
2. Vaadi MFA tuntemattomia laitteita käytettäessä.
3. Estä kaikilta käyttäjiltä ei-moderni tunnistautuminen.
4. Estä kaikilta käyttäjiltä ActiveSync.

Liitteessä 1 on esitetty testiympäristöön toteutettavat laajemmat esimerkkikäytännöt. Samankaltaisten käytäntöjen määrityksestä löytyy yksityiskohtaisempi ohjeistus[45].

3.1.9 On-premise Active Directoryn -todennuksen suojaaminen

Azure AD:ssa on monipuoliset suojaustoiminnot, jotka Microsoftin on mahdollista toteuttaa palvelun ison koon takia. On-premise-ympäristöissä ei välttämättä ole vastaavia resursseja käytettävissä eikä käyttöjärjestelmässä ole sisäänrakennettuina kehittyneitä

[39] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-whichversion
[40] https://support.office.com/fi-fi/article/office-365-n-kaksivaiheisen-tarkistamisen-määrittäminen-ace1d096-61e5-449b-a875-58eb3d74de14?ui=fi-FI&rs=fi-FI&ad=FI
[41] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-converged
[42] https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates
[43] https://aka.ms/deploymentplans
[44] https://aka.ms/breakglass; break-glass on analogia hätätilanteessa lasin alta löytyvään painikkeeseen tai vastaa-vaan ts. vain poikkeustilanteessa käytettäviin tunnuksiin, jotka toimivat ilman MFA:ta ja Conditional Access:iä
[45] https://bloggerz.cloud/2019/01/02/conditional-access-are-you-really-getting-the-most-out-of-it-part-2-of-2/

toimintoja hyökkäysten havaitsemiseen.

Microsoft julkisti Advanced Threat Analytics (ATA)[46] -toiminnon kesällä 2015. Sen avulla on-premise AD domain controller -palvelinten liikennettä seuraamalla voidaan havaita epänormaali identiteettien käyttäytyminen sekä useiden erilaisten haavoittuvuuksien hyödyntämisyritykset. Liikenteen seuranta voidaan toteuttaa joko port mirroring -tekniikalla tai asentamalla halutuille domain controller -palvelimille ATA Lightweight Gateway -sovellus. Toiminto kuuluu EMS E3 -lisenssipakettiin.

Azure Advanced Threat Protection (Azure ATP)[47] on ATA:n pilviversio, jossa paikallisia ATA-palvelimia ei tarvitse asentaa. Domain Controller -palvelimiin asennetaan Azure ATP sensor -sovellus. Toiminto tuli saataville maaliskuussa 2018 ja kuuluu EMS E5 -lisenssipakettiin.

3.1.10 Huolehdi ylläpitoroolien haltijoista

Active Directoryssä hallintaan käytettävien tunnusten yksi suositeltava käytäntö on ollut luoda erillinen ylläpitotunnus. Tällaisilla tunnuksilla on kuitenkin jatkuvasti kaikki ryhmäjäsenyydet ja siten kyseiset tunnukset ovat kruununjalokiviä, joihin hyökkääjä yrittää saada pääsyn.

Azure AD:ssä Privileged Identity Management -toiminnolla tällainen voidaan tehokkaasti estää. Microsoftin suositus on, että pysyviä pääkäyttäjiä olisi vain kaksi ja enintään viisi suuressakaan ympäristössä. Conditional Access ja kaksivaiheinen tunnistus pitää ottaa pois näiltä käyttäjiltä, jotta palveluun päästään kirjautumaan, vaikka näissä palveluissa olisi jotain haasteita.

Microsoft Identity Manager (MIM) 2016 mahdollistaa vastaavan toiminnallisuuden toteuttamisen myös on-premise-ympäristössä. Ratkaisun nimi on Privileged Access Management for Active Directory Domain Services[48]. Sen käyttöönotto ja ylläpito vaativat melkoisesti resursseja.

Tietoturvaa voidaan edelleen parantaa rajoittamalla ylläpitotoimenpiteiden tekeminen siihen dedikoiduilta kovennetuilta hallintatyöasemilta (engl. Privileged Access Workstation - PAW).

3.1.11 Suojaustoiminnoissa ilmenneitä haasteita

Azure AD:n federointi on toteutettu käyttäen standardeja WS-FED- ja SAML-protokollia. Azure AD:n federoinnin toteutuksesta on löydetty tietoturva-aukko[49], joka sallii Global Administrator -tasoisten pääkäyttäjien kirjautua sisään minä tahansa organisaation käyttäjänä ilman salasanaa ja ohittaen myös MFA:n. Microsoft pitää aukkoa ominaisuutena, joten sitä todennäköisesti ei korjata. Tästä syystä Global Admin -roolin omaavien pääkäyttäjien lukumäärä täytyy pitää minimissään ja aukon hyödyntämiseen liittyviä pääkäyttäjien toimia on valvottava.

Kaksivaiheisessa tunnistautumisessa on myös omat haasteensa. Etenkin suuremmissa organisaatioissa IP-aliverkkojen lukumäärä ja niiden ylläpito MFA-palvelun asetuksissa voi jo sinänsä asettaa haasteita. Maakohtaiset rajoitukset voidaan kiertää erilaisilla VPN-ratkaisuilla. Kaksivaiheisen tunnistautumisen reaaliaikainen huijaaminen on ainakin teoriassa mahdollista.

[46] https://docs.microsoft.com/en-us/advanced-threat-analytics/

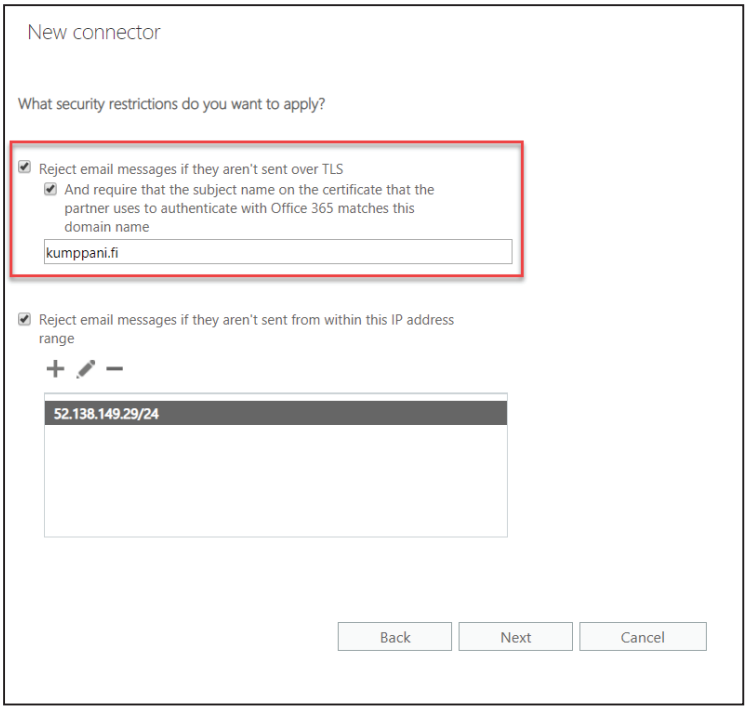
[47] https://docs.microsoft.com/en-us/azure-advanced-threat-protection/

[48] https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

[49] https://ieeexplore.ieee.org/abstract/document/8456101

3.2 Sähköpostin suojaaminen

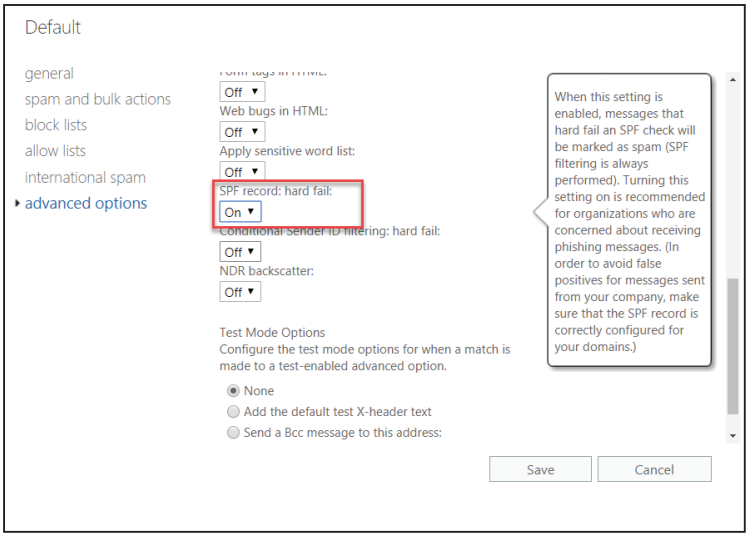
3.2.1 Suojaa sähköpostin reititys



Exchange Online mahdollistaa sähköpostiliikenteen suojaamisen esimerkiksi luotettujen kumppaneiden tai oman sisäisen sähköpostipalvelimen kanssa sähköpostiyhdistimien[50] (Connectors) asetusten avulla.

Liikenne kumppaneiden välillä tulee aina salata TLS:n avulla ja toisen osapuolen tunnistautuminen tulee tehdä varmenteen avulla. On suositeltavaa vaatia, että varmenteesta löytyy toisen puolen identifioima merkkijono, esimerkiksi yrityksen nimi tai sähköpostin domain-osa. Jos toisen osapuolen sähköpostipalvelinten ip-osoitteet ovat tiedossa, voidaan halutessa sisään tuleva posti sallia vain niistä osoitteista.

Lähettäjän määrittelemät sallitut osoitteet saa selville SPF-tietueesta seuraavalla Windows-komennolla: nslookup -q=TXT kumppani.fi



Organisaation ulkopuolelta voi tulla kalasteluun käytettävä sähköpostiviesti, jonka lähettäjäksi on väärennetty organisaation oma sähköpostiosoite. Tämä reitti voidaan tukkia SPF:n avulla. Ensin SPF-tietue tulee asettaa oikein DNS:ssä. Sitten Exchange Onlinen roskapostiasetuksista (Exchange admin center => protection => spam fil-ter) täytyy kytkeä **SPF Record: hard fail** päälle. Se määrää, että oman organisaation nimissä tulevia sähköpostiviestejä suostutaan vastaanottamaan vain SPF-tietueessa mainituita laillisista lähteistä.

[50] https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/use-connectors-to-configure-mail-flow

3.2.2 Käyttäjien suojaaminen haittaohjelmilta ja roskapostilta

Office 365 Advanced Threat Protection (Office 365 ATP)[51] on palvelu, jonka avulla suojataan käyttäjiä haittaohjelmilta, roskapostilta ja kalastelulta.

ATP Safe Attachments on toiminto nollapäivähyökkäyksiä vastaan. Viestien liitetiedostot, jotka läpäisevät tunnettujen haittaohjelmien ja virusten tarkistukset, ohjataan avattaviksi erilliseen ”tarkastuseteiseen”. Siellä liitetiedosto tutkitaan koneoppimistekniikalla ennestään tuntemattomia uhkia vastaan. Jos tiedostossa vaikuttaa olevan jotain pahantahtoista, se poistetaan, mutta muuten viesti liitteineen lasketaan eteenpäin käyttäjän postilaatikkoon.

Toinen Office 365 ATP:n ominaisuus on turvalliset linkit (ATP Safe Links). Ominaisuuden avulla epäilyttävät linkit korvataan virhesivulla, joka ilmoittaa linkin sisältävän mahdollisesti haittaohjelmia ja kalastelua.

Kalastelusuojaus (ATP Antiphishing) tutkii sisältävätkö saapuvat viestit kalasteluyrityksiä tai yritystä tekeytyä toiseksi (Impersonation). Tässäkin käytetään erilaisia koneoppimistekniikoita viestien analysointiin.

Office 365 ATP kuuluu tilauksiin Office 365 Enterprise E5, Office 365 Education A5 ja Microsoft 365 Business.

Myös ilman ATP:ta on kalastelusuojaus (Antiphishing), mutta ATP:ta suppeampana. Saapuvat viestit tarkastetaan huijausten varalta (Spoofing), mutta Impersonation -tarkastusta ei ole.

3.3 Lokitus ja integrointi SIEM-järjestelmiin

Office 365:n eri palvelut tallentavat käyttäjien tapahtumia lokeihin. Tärkeimmät lokit ovat Azure AD:n tallentamat lokit, sekä Office 365 auditloki. Office 365 audit -loki täytyy kytkeä erikseen päälle[52], muut lokit ovat automaattisesti käytössä riippuen Azure AD:n versiosta. Seuraavassa taulukossa on listattu eri lokit ja niiden tietojen säilytysajat, jotka ovat erittäin rajalliset.

Audit -lokiin tallentuu pääkäyttäjien tekemät toimenpiteet, kuten uusien käyttäjien luonti tai salasanan resetointi.

Kirjautumisaktiviteettiloki sisältää tiedon käyttäjien kirjautumisista. Tämä on käytettävissä ainoastaan Azure AD Premium -tilausten kanssa.

Office 365 audit -loki kerää tiedot sekä pääkäyttäjien, että loppukäyttäjien toimenpiteistä. Lokiin kerätään toimet kaikista palveluista, myös Azure AD:n audit ja kirjautumisaktiviteettilokeista. Muista lokeista poiketen, säilytysajat ovat pidemmät.

Azure AD:n lokien viive, eli miten nopeasti tapahtumat niihin tallennetaan, on noin 15 minuuttia. Office 365 audit -lokissa viive on pääosin 30 minuuttia, paitsi Azure AD -lokien kohdalla, joissa viive on 24 tuntia.

Lokien valvonnalla voidaan todeta kalasteluyritykset heti niiden tapahtuessa. Reaaliaikainen valvonta edellyttää käytännössä Azure AD Premium -tilausta, koska Office 365 audit -lokin viive on 24 tuntia.

On suositeltavaa viedä lokit ulkopuoliseen jär-

	Azure AD-versio ja aika vrk		
Loki	**Basic**	**Azure AD Pl**	**Azure AD P2**
Audit-loki	7	30	30
Kirjautumis-aktiviteetti	-	30	30
käyttö	30	30	30
Riskialttiit käyttäjät	7	30	30
Riskialttiit kirjautumiset	7	30	30
Office 365 audit -loki	90	365	365

[51] https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description
[52] https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

jestelmään, jossa niitä voidaan säilöä ja analysoida tarpeen mukaan pidempään. Myös Microsoftilla on Azuressa tällaisia palveluita.

Azure Monitor yhdistää sekä pilvi- että on-premise-ympäristöjen seurannan, analysoinnin ja automaattisen reagoinnin. Audit- ja kirjautumisaktiviteetti-tilokit voidaan viedä Azure Monitorista Log Analytics -palveluun jatkoanalysointia tai visualisointia varten. Ne voidaan viedä Azureen talteen (Storage Account) ja tällöin voidaan määrittää tallennusajaksi 1-365 vuorokautta tai rajaton tallennusaika. Tallennuksen aiheuttama kustannus tulee huomioida etenkin laajemmissa ympäristöissä, joissa etenkin kirjautumisaktiviteetteja on paljon ja siten myös lokitapahtumia syntyy paljon.

Lokit voidaan myös viedä Azure Event Hub -palveluun, josta ne viedään edelleen muiden valmistajien SIEM (security information and event management) -järjestelmiin. Mm. Sumologic[53], Splunk[54], IBM QRadar[55] ja Micro Focus ArcSight[56] ovat Azureen integroitavia SIEM-järjestelmiä.

Azure Monitorin palveluiden käyttö vaatii oman Azure-tilauksensa, joka ei sisälly Microsoft 365 tai Office 365 -tilauksiin.

3.4 Seuranta

Sekä Office 365 että Azure AD sisältävät monia hallintaportaaleja ja ne puolestaan erilaisia raportteja. Microsoft on tiedostanut monien portaalien haasteen ja on lähtenyt niitä yhdistämään. Syksyllä 2018 järjestetyssä Ignite-konferenssissa esiteltiin uusia palveluiden hallintaportaaleja, kuten esim. Microsoft 365 admin center https://admin.microsoft.com, joka tätä dokumenttia helmikuussa 2019 kirjoitettaessa on yhä esiversiossa.

PowerBI on nopeasti yleistymässä eri palveluiden analysoinnissa ja raportoinnissa. Helmikuussa 2019 Microsoft julkaisi tavan käyttää sitä eri palveluiden tuottamien hälytysten raportointiin[57]. Se on käytettävissä myös kirjautumislokien analysointiin Azure Active Directory Power BI content pack:in avulla[58].

3.5 Hallitse ja suojaa päätelaitteet

Office 365 -palveluita käytetään eri tyyppisillä päätelaitteilla, jotka voivat olla joko henkilön itse omistamia (Bring Your Own Device) tai organisaation omistamia.

Päätelaitteen tietoturva on olennainen osa koko järjestelmän tietoturvaa, koska jos esimerkiksi päätelaitteeseen on asennettu käyttäjän toimia seuraava haittaohjelma tai sen käyttöjärjestelmä on korvattu epävirallisella versiolla, on kaikkien käyttäjien Office 365 -palveluiden käyttö kyseiseltä päätelaitteelta vaarassa.

Laitteiden ja niillä käytettävien sovellusten hallintaan on olemassa eri vaihtoehtoja kuten:

- Office 365 Mobile Device Management[59]; Intune:a suppeampi MDM-hallinta, joka ei sisällä sovellus hallintaa (MAM) eikä sovellusten jakelua, profiilien hallintaa eikä PC- ja MacOS-laitteiden hallintaa
- Microsoft Intune (sekä laitehallinta Mobile Device Management - MDM että sovellushallinta (Mobile Application Man-agement - MAM)
- Muiden MDM-valmistajien ratkaisut, esim. Citrix Endpoint Management (ent. XenMobile), MobileIron Unified Endpoint Management, IBM MaaS360 ja VMware Workspace ONE (ent. AirWatch).

Edellä esitetyistä ratkaisuista Microsoftin omat ratkaisut integroituvat läheisimmin Azure Active Directoryyn ja niiden avulla päätelaite voidaan rekisteröidä Azure Active Directoryyn ja siten myös laitteen vaatimustenmukaisuus tallentaa laiteobjektin asetuksiin. Tätä tietoa voidaan puolestaan hyödyntää esimerkiksi Conditional Access -käytännöissä, jolloin voidaan vaatia, että tiettyä palvelua käytettävän päätelaitteen tulee olla vaatimustenmukainen.

Windows-työasemia on vuosikymmeniä hallittu Active Directoryyn määritetyillä Group Policy (suom. ryhmäkäytäntö) -asetuksilla. Microsoftin System Center Confi-guration Manager (SCCM) -järjestelmästä on puolestaan vuosien varrella muodostunut hyvin laajasti käytetty järjestelmä sovellushallintaan ja inventointiin etenkin suuremmissa ympäristöissä.

[53] https://help.sumologic.com/07Sumo-Logic-Apps/04Microsoft-and-Azure/Azure_Active_Directory/Install_the_Azure_Active_Directory_App_and_View_the_Dashboards
[54] https://splunkbase.splunk.com/app/3534/
[55] https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/t_dsm_guide_microsoft_azure_enable_event_hubs.html
[56] https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-for-Microsoft-Azure-Monitor-Event-Hub/ta-p/1671292
[57] https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Gain-rich-insights-with-the-new-Microsoft-Graph-Security-Power/ba-p/334467
[58] https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-power-bi-content-pack
[56] https://support.office.com/en-us/article/Frequently-asked-questions-about-Mobile-Device-Management-for-Office-365-3871f99c-c9db-4a23-86f9-902c1b02f58d

Windows 10:n ja kuluttajistumisen myötä tilanne on kuitenkin muuttumassa. Microsoft on viime vuosien aikana kehittänyt Applen Device Enrollment Program (DEP) vastaavan AutoPilot-palvelun, jolla Windows 10 -työasemat voidaan mukauttaa organisaation tarpeisiin ilman perinteistä organisaation tarpeisiin räätälöityä asennuspakettia. Työasemien asetuksia voidaan hallita MDM-ratkaisuilla ml. Microsoftin oma Intune-palvelu.

Windows 10 -laitteet voivat olla Azure AD:yyn liitettyinä seuraavin tavoin:

- Azure AD Registered; työntekijän omistama pääteaite, joka rekisteröidään Azure Active Directory:yn ja mahdollisesti organisaation MDM-järjestelmään
- Azure AD Joined; organisaation omistama laite on liitetty vain Azure Active Directory:yn
- Azure AD Hybrid Joined; laite on liitetty sekä on-prem Active Directory:yn että Azure Active Directory:yn.

Jos käytössä on federoitu identiteetti ja AD FS -palvelu, voidaan sääntöjen avulla rajoittaa Office 365:n käyttö organisaation omiin päätelaitteisiin.

3.6 Huolehdi käyttäjien ja ylläpitäjien koulutuksesta

Käyttäjien koulutus on erittäin tärkeää, koska usein juuri käyttäjä on tietoturvan heikoin lenkki. Toisaalta esimerkiksi tuhannen hengen organisaatiossa ei millään päästä tilanteeseen, etteikö yksikään käyttäjä vuosien varrella koskaan tekisi virhettä, kun hänen tietojaan yritetään kalastella. Kuitenkin jos käyttäjät ovat osaavampia ja tiedostavampia, hyökkääjän onnistumismahdollisuudet ovat huonommat.

Kunkin Office 365 -käyttäjän tulisi tietää, miten varjella omaa salasanaansa, tunnistaa huijausviestit ja miten toimia, jos joutuu huijausyrityksen kohteeksi tai se on onnistunut.

Tarkemmin koulutus voisi sisältää mm. seuraavia asioita:

- Millaista salasanaa pitäisi käyttää? Esim. https://pidempiparempi.fi/
- Lähestyminen on yleensä sähköpostiviesti, mutta voi olla myös puhelinsoitto tai tekstiviesti.
- Jos viestissä on huonoa kieltä, se on todennäköisemmin huijausta.
- Jos hyperlinkin näkyvä osa ja taustalla oleva linkki ovat eri, se on todennäköisemmin huijausta.
- Jos hyperlinkin kohdeosoite on numeerinen, kyseessä on luultavasti huijausviesti.
- Jos hyperlinkin kohdeosoite muistuttaa kunniallista yhtiötä, kyseessä on luultavasti huijausviesti. Esimerkiksi ei www.gigantti.fi vaan www.gigamtti.fi.
- Jos viestissä pyydetään kiirehtimään ja uhataan rahan menettämisellä, se voi olla huijausta.
- Jos puhuttelutapa on teennäinen, kyseessä on luultavasti huijausviesti.
- Viesti voi olla sikäli aito, että se tulee oman johtajan tai työkaverin sähköpostista. Lähettämisen kuitenkin aiheutti murtautuja, joten viestissä oleva pyyntö tai käskykin on huijausta.
- Miten erottaa aidon kirjautumisruudun väärennetystä.
- Jos saa huijaussähköpostin, johon ei lankea, se riittää tuhota, eikä siitä tarvitse ilmoittaa.
- Jos vahingossa syöttää salasanansa paikkaan, jonka huomaa huijaukseksi tai epäilee sellaista, tulee asiasta heti ilmoittaa eteenpäin organisaation ohjeiden mukaan.

Asian tärkeyden ja toisaalta suppeuden vuoksi voisi olla hyvä, että kultakin käyttäjältä saadaan testin kautta tai muuten kuittaus siitä, että hän tietää kyseiset asiat.

Tekniikoiden tai tilanteiden muuttuessa täytyy myös koulutus päivittää.

Koulutuksen lisäksi käyttäjiä voidaan myös testata, mikä tosin sekin on heidän kouluttamistaan. Organisaation tietohallinto lähettää itse käyttäjille kalasteluviestejä. Jos käyttäjät erehtyvät linkkiä napsauttamaan, he päätyvät nettiosoitteeseen, jossa heitä informoidaan tilanteesta.

Office 365 sisältää Attack Simulator -toiminnon, jolla simuloitu hyökkäys voidaan toteuttaa. Vastaavia harjoituksia sekä koulutusta voidaan ostaa myös palveluna.

Ylläpitäjien osaamisesta ja sen ajantasaisuudesta pitää myös huolehtia. Microsoft on muuttanut sertifiointiohjelmaansa syksystä 2018 lähtien. Microsoft 365 -ympäristön suojaamisen ja tietoturvan ylläpidon kehittämisen asioita käsitellään mm. seuraavissa uusissa työroolipohjaisissa sertifioinneissa ja niihin valmentavissa koulutuksissa:

- Microsoft 365 Certified: Security Administrator Associate[60]
- Microsoft 365 Certified: Enterprise Administrator Expert[61]

3.7 Käytä tarkistuslistoja

Kalastelun yleisyyden takia sen torjumiseksi on olemassa monia eri tarkistuslistoja. Microsoft on julkaissut monitahoisen blogiartikkelien sarjan https://blogs.technet.microsoft.com/cloudready/2018/07/31/introduction-email-phishing-protection-guide-enhancing-your-organizations-security-posture/. Osa sen yksityiskohtaisista artikkeleista ei ole enää täysin ajantasaisia, mutta ohjeita voi soveltaa tässä dokumentissa esiteltyjen tietolähteiden kanssa.

Microsoft 365 identiteetti-infrastruktuurin käyttöönoton vaiheet https://docs.microsoft.com/en-us/microsoft-365/enterprise/identity-infrastructure puolestaan listaa toimenpiteet, joilla hybridi identiteetti tärkeimpine toimintoineen saadaan käyttöön.

Aiemmin tässä esitetyt Secure Score -portaalit listaavat toimintoja, joista useat auttavat rajoittamaan kalastelun mahdollisuuksia.

3.8 Kirjautuminen salasanoitta

Kuten tässä dokumentissa on useaan otteeseen todettu, kalastelun päätavoitteena on saada käyttäjän tunnistetiedot ts. käyttäjätunnus ja salasana selville ja väärinkäyttää niitä jollakin tavalla. Tunnistamisessa on mahdollista käyttää tapoja, joissa ei tarvita salasanaa lainkaan.

Microsoft on omissa palveluissaan esitellyt esim. Windows 10:n Hello for Business[62] -toiminnon, jossa tunnistus tehdään PIN-koodilla tai biometrisesti.

AD FS -toiminnolla voidaan federoiduissa ympäristöissä Azure MFA määrittää ensisijaiseksi todennustavaksi[63]. Vaatimuksena on vähintään Windows Server 2016 AD FS.

Salasanaton kirjautuminen voidaan toteuttaa myös puhelimeen asennettavalla Microsoft Authenticator -sovelluksella[64]. Tällöin käyttäjälle näytetään numerojonoa, jota vastaavaa kohtaa käyttäjä napsauttaa puhelimensa näytöllä hyväksyäkseen kirjautumisen.

Toimikorttikirjautuminen on myös käytössä joillakin toimialoilla ja organisaatioissa. Tällöin käyttäjä ei välttämättä edes tiedä salasanaansa ja kirjautuminen perustuu toimikorttiin ja sen PIN-koodiin.

[60] https://www.microsoft.com/en-us/learning/m365-security-administrator.aspx
[61] https://www.microsoft.com/en-us/learning/m365-enterprise-administrator.aspx
[62] https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification
[63] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa
[64] https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-phone-sign-in

Kalastelun uhkat ja niiden rajoittaminen

	SaaS-palvelu			Todennus ja valtuutus (identiteetti)		
	Office 365 -versio			AAD-versio		
Uhka	**Business**	**E3**	**E5**	**Basic ja Office 365**	**AAD P1**	**AAD P2**
Kalasteluviesti käyttäjälle						
Anti-spoof väärennetyt viestit	Tiettyjen kumppanien kanssa käytetään TLS:ää	‹	‹			
Linkkien turvallisuuden varmistaminen	›	›	Safe-linkit			
Tunnistetietojen joutuminen vääriin käsiin						
Salasanojen murtaminen (Brute force)				Salasanojen suojaaminen Jos käytössä federoitu kirjautuminen, Extranet Lockout	‹	‹
Käyttäjälle helpommin erottuvat kirjautumissivut				Kirjautumis-sivujen räätälöinti	‹	‹
Käyttäjätunnus-salasanaparin riittämättömyys				Kaksivaiheinen tarkistus (MFA for Office 365) käyttäjä-kohtaisesti Jos käytössä federoitu kirjautuminen, niin AD FS Conditional Access -säännöt	Kaksivaiheinen tarkistus (Azure MFA) - Conditional Access	‹ + MFA-rekisteröinnin pakotus Identity Protection
MFA:n kiertäminen						
Legacy-protokollien käyttö	Basic Authentication -esto Exchange-palvelussa	‹	‹	Basic Authentication -esto Exchange-palvelussa (Office 365 -toiminnossa, ei AAD toimintona) tai ›	Modern Authentication pakotus Conditional Access:in avulla	‹
Reaaliaikainen MFA Phishing (esim. vahvistus-SMS kalastelu)						
Tietovuoto - sähköposti						
Postin edelleenlähetyssääntöjen (mail forward) tekemisen estäminen	Automatic Forward -esto oletusarvoisessa Remote Domain -konfiguraatiossa Transport Rules	‹ + Data Loss Prevention (DLP)	‹			
Postin lajittelusääntöjen (Inbox rulet) tekemisen estäminen						
Lähtevä roskaposti	Välitettävän postin rajoittaminen (throttling) Connector:ien asetukset, esim. tunnistautuminen	‹	‹			
Tietovuoto muista palveluista						
Single sign-on -toiminnolla kirjautuminen muihin järjestelmiin					Monitoring - Sign-ins	‹
Dokumentin jakaminen SaaS-palvelusta luvattomasti	›	›	Office 365 Cloud App Security Microsoft Cloud App Security saatavilla EMS-lisenssillä.			
Tunnusten muu väärinkäyttö						
Lateral movement				›	ATA	Azure ATP
Protokollien heikkouksien hyödyntäminen				›	ATA	Azure ATP
Ylläpitoon käytettävien tunnusten väärinkäyttö						Privileged Identity Management

Merkkien selitykset: › Voi toteuttaa hankkimalla kalliimman lisenssin oikealta ‹ Voi toteuttaa samalla tavalla kuin vasemmalla on kuvattu

Uhka ei ole relevantti tässä kontekstissa tai siltä suojautuminen ei ole mahdollista

Havainnointi ja forensiikka

	SaaS-palvelu			Todennus ja valtuutus (identiteetti)		
	Office 365 -versio*			AAD-versio		
Uhka	**Business**	**E3**	**E5**	**Basic ja Office 365**	**AAD P1**	**AAD P2**
Lokitus						
Salasanojen murtaminen (Brute force tai spray attack) - on-prem				Tapahtumalokien seuranta	‹	‹
Salasanojen murtaminen (Brute force tai spray attack) - AAD				Kirjautumis-aktiviteettilokien seuranta	‹	‹
Tunnusten väärinkäytön yritykset - on-prem				On-prem: tapahtumalokien seuranta	‹	‹
Tunnusten väärinkäytön yritykset - AAD				Kirjautumis-aktiviteettilokien seuranta	‹	‹
Viestien lukemisen selvittäminen						
Postilaatikon sisältöön tehtyjen hakujen selvittäminen	Lokien tutkiminen	‹	‹			
Postin edelleenlähetyssääntöjen löytäminen	Lokien tutkiminen Postilaatikoiden asetusten tutkiminen	‹	‹			
Postin lajittelusääntöjen (Inbox rulet) löytäminen	Lokien tutkiminen Postilaatikoiden asetusten tutkiminen	‹	‹			
Murretulta tililtä lähetettyjen sähköpostien löytäminen	Lokien tutkiminen	‹	‹			
Postilaatikon sisältöön tehtyjen hakujen selvittäminen				›	Sign-in logs	‹
Ennaltaehkäisevä seuranta (Monitoring)						
Tunnusten väärinkäytön havaitseminen				›	Azure Active Directory risk events	‹
Kalastelun onnistumisen tunnistaminen				›	Azure Active Directory risk events	‹

Merkkien selitykset: › Voi toteuttaa hankkimalla kalliimman lisenssin oikealta ‹ Voi toteuttaa samalla tavalla kuin vasemmalla on kuvattu

Uhka ei ole relevantti tässä kontekstissa tai siltä suojautuminen ei ole mahdollista

Taulukkoon on vedetty yhteen Office 365 - kalasteluun ja tietomurtoihin liittyviä uhkia ja hyökkäysmenetelmiä sekä yleisimmillä Suomessa käytössä olevilla lisenssitasoilla saatavilla olevia suojautumis- tai havaitsemiskeinoja. Taulukko ei ole kattava palvelukuvaus, mutta sitä voi käyttää apukeinona nykyisten lisenssien puitteissa käytössä olevien keinojen määrittämisessä.

4 Toiminta hyökkäyksen tapahduttua

Organisaation tietoturvaohjeistuksen osana tulisi olla sisäinen toimintaohje eli tietoturvapoikkeamaprosessi. Tämän dokumentin ohjeistus tulisi soveltuvin osin integroida organisaation ohjeistukseen.

Lyhyenä muistilistana toiminta hyökkäyksen tapahduttua:

1. Kohteeksi joutuneiden uhrien ja tilien tunnistaminen ja jatkovahinkojen estäminen (käyttäjätilien haltuun otto, hyökkääjien lukitseminen ulos, välittömät estotoimenpiteet).
2. Sisäinen tiedotus tapahtuneesta jatkovahinkojen minimoimiseksi.
3. Alustava arvio hyökkääjien toimenpiteistä ja vahinkojen laajuudesta mahdollisuuksien mukaan
4. Ulkoinen tiedotus tapahtuneesta vahinkojen leviämisen minimoimiseksi; alustavat viranomaisyhteydenotot.
5. Tapahtumaketjun kattavampi selvitys lokitiedoista; mitä tapahtui, milloin ja kenen toimesta.
6. Mahdollisesti saastuneiden tiedostojen ja vastaavien siivous, lokitietojen arkistointi jatkoa varten.
7. Täydentävät ilmoitukset viranomaisille.
8. Pitkäkestoinen suojautuminen vastaavan varalta.

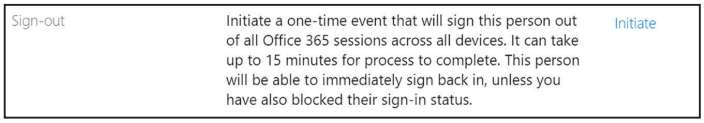
4.1 Kirjautuneen murtautujan sulkeminen pois

Jos tiedetään tai epäillään, että tietty käyttäjätunnus on väärissä käsissä, ja murtautuja saattaa käyttää sitä, voidaan tämän käyttäjätunnuksen pääsyä eri Office 365 -palveluihin estää. Nämä palvelut saattavat tosin jonkin aikaa muistaa vanhoja tietja, jotta normaalikäyttö olisi juohevampaa.

Edellisestä seuraa, että murtautuja saattaa pystyä käyttämään tunnusta vielä jonkin aikaa salasanan vaihdon jälkeenkin. Niinpä täytyy myös katkoa nykyisiä parhaillaan käytössä olevia yhteyksiä.

Katkominen aloitetaan Office 365 -hallintaportaalissa. Siellä avataan murron kohteena olevan käyttäjätunnuksen tiedot ja edelleen OneDrive-asetukset. Niissä on oheisen kuvan mukainen toiminto.

Initiate-linkin napsautus katkaisee seuraavien 15 minuutin aikana kyseisen käyttäjätunnuksen yhteydet kaikilta laitteilta. Jottei murtautuja voi saman tien kirjautua takaisin, täytyy myös uudet kirjautumiset estää. Käyttäjätietojen kohdassa Signin status voidaan esto laittaa päälle oheisen kuvan mukaisella toiminnolla.



Muutoksen tallennuksen jälkeen ruutuun tulee ehdotus myös salasanan vaihtamisesta, mikä kannattaakin tehdä saman tien.

Jos kohdekäyttäjä on synkronoitu paikallisesta Active Directory -hakemistosta, ja salasana muutetaan siellä, sen kulkeutuminen Azure AD -pilveen voidaan tarkastaa PowerShell-komennolla Get-MsolUser katsomalla tuloksista ajankohdat LastDir-SyncTime ja LastPasswordChangeTimestamp.

Lisäksi voidaan käyttää kahta PowerShell-komentoa yhteyksien katkomiseen:

- Revoke-SPOUserSession on SharePoint Online -komento, eli sillä voidaan katkaista kohdekäyttäjän SharePoint-yhteydet.
- Revoke-AzureADUserAllRefreshToken on Azure AD -komento, jolla katkaistaan tietyn käyttäjän yhteydet kaikkiin Azure AD:ta käyttäviin sovelluksiin.

Lopuksi on hyvä tarkastaa, onko kohdekäyttäjän postilaatikossa delegaatteja, koska jos heidän salasanansa on joutunut vääriin käsiin, niin sitäkin kautta voi päästä kohdekäyttäjän postilaatikkoon.

4.2 Torjunta/forensiikka/tapahtuneen selvittely

Ensimmäinen askel hyökkäyksen tapahduttua on koventaa tietoturvaa koko tenantin osalta pakottamalla kaksivaiheinen tunnistus kaikille käyttäjille. Jos käytössä on Azure AD Premium tai AD FS, käyttö organisaation ulkopuolelta ja ei-tunnistetuilla laitteilla tulisi myös estää. Näillä toimenpiteillä voidaan tehokkaasti katkaista käynnissä oleva hyökkäys ja silti sallia organisaation toiminnan jatkuvuus.

Seuraavaksi täytyy tunnistaa hyökkäyksen uhrit. Tunnistamisessa voidaan käyttää seuraavia tietolähteitä ja menetelmiä.

Kun hyökkäyksen uhrit on tunnistettu, estetään uhrien sähköpostien lähettäminen vastaanottajille käyttäen sääntöjä. Tällä estetään uusien kalasteluviestien ja roskapostin leviäminen ja siten myös uudet uhrit. Jos käytössä on Exhange Plan 2, uhrien laatikot tulisi asettaa välittömästi pitoon (Legal Hold), jolloin varmistetaan todisteiden säilyminen.

Tietolähde / menetelmä	Mitä tutkitaan?
Audit loki	Onko poikkeuksellisia tapahtumia, esimerkiksi toimialueiden luonteja tai niiden tunnistautumismenetelmien muutoksia? Onko lokitukseen tehty muutoksia?
Kirjautumisaktiviteetti	Onko poikkeuksellisia sisäänkirjautumisajankohtia ja -sijainteja.
Office 365 audit loki	Onko sähköposteihin luotu sääntöjä. Rikolliset saattavat lisätä postin uudelleenohjaussäännön omaan sähköpostiinsa seuratakseen tietyn sähköpostiliikennettä?

Tietoturvan koventamisen jälkeen kerätään kaikki saatavilla olevat lokit talteen todistusaineiston säilyttämiseksi ja analysoimiseksi.

Keskusrikospoliisin näkökulmasta Office 365 -tietomurtoilmiön tutkinnallisena haasteena on tiedonsaannin vaikeus. Tästä syystä olisikin ensiarvoisen tärkeää, että Office 365 -ohjelmistoissa otettaisiin käyttöön lokitietojen tallennus.

Kyseisistä Office 365 -auditlokeista voidaan havaita oikeudettomat kirjautumiset ja tutkia kirjautujien IP-osoitteet sekä havaita ainakin osa toimenpiteistä, joita järjestelmässä on oikeudetta tehty. Ilman lokien tarjoamaa tietoa näiden asioiden selvittäminen ja tietomurron toteennäyttäminen on lähes mahdotonta.

Ennaltaehkäisevässä mielessä onkin suositeltavaa, että asiakkaat tarkistavat, onko heillä lokitietojen tallennus käytössään, mistä lokit ovat saatavilla ja kuinka pitkältä ajalta ne ovat saatavilla.

Tietomurron sattuessa suosittelemme tekemään poliisille rikosilmoituksen (tai lähettämään Nettivinkin) asiasta mahdollisimman varhaisessa vaiheessa, jotta lokitiedot ovat vielä saatavilla riittävän pitkältä ajalta.

4.3 Yhteydenotto Kyberturvallisuuskeskukseen

Kyberturvallisuuskeskus on kiinnostunut Office 365 –aiheisista tietojenkalasteluviesteistä sekä tapahtuneista tietomurroista. Käytämme tietoja kansallisen tilannekuvan rakentamiseen sekä esimerkiksi tietojenkalastelusivustojen irtikytkentäpyyntöjen lähettämiseen.

Kyberturvallisuuskeskukselle voi ilmoittaa joko sähköpostilla osoitteeseen: cert@traficom.fi
tai verkkosivujen ilmoita tietoturvaloukkauksesta – lomakkeella: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/asioikanssamme

4.4 Yhteydenotto poliisiin

Käyttäjätileihin tunkeutuminen ja niiden oikeudeton käyttö täyttävät tietomurron tunnusmerkistön. Asiaan voi liittyä myös muita rikosnimikkeitä, jotka selviävät tai tarkentuvat asiaa peratessa ja poliisin rikostutkinnan edetessä. Rikosilmoituksen aiheesta voi tehdä joko paikallispoliisilaitokselle puhelimitse tai käymällä paikan päällä, tai sitten verkosta osoitteesta https://www.poliisi.fi/rikokset/sahkoinen_rikosilmoitus.

Jos tapaus jää yrityksen asteelle tai jos organisaatio ei halua tehdä aiheesta rikosilmoitusta jostakin syystä, tapauksesta kannattaa kuitenkin tehdä Nettivinkki poliisille. Kaikki lisätiedot tapahtumaketjuista ja

toimijoista voivat auttaa jonkin toisen rikoksen selvittämisessä tai muodostaessa kokonaiskuvaa laajemmista rikosvyyhdeistä. Nettivinkin voi tehdä verkossa osoitteessa https://www.poliisi.fi/nettivinkki

4.5 Ilmoittaminen tietosuojavaltuutetun toimistolle

Lähes aina organisaatioihin kohdistuneissa Office 365 -tietomurroissa on kyse myös henkilötiedosta.

Henkilötietoihin kohdistuneesta tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ja jos rekisteröidyille on aiheutunut korkeaa riskiä, myös loukkauksen kohteena oleville henkilöille.

Ilmoitettuaan tietosuojavaltuutetun toimistolle tietoturvaloukkauksesta rekisterinpitäjät voivat saada neuvontaa ja ohjausta henkilötietojen suojaamisesta. Ilmoitus auttaa myös tilannekuvan luomisessa organisaation johdolle. Tarvittaessa tietosuojavaltuutettu voi määrätä organisaation noudattamaan tietosuoja-asetuksen mukaisia velvoitteita.

Tietoturvaloukkausilmoituksen jälkeinen prosessi etenee Office 365 -murroissa seuraavasti:

1. Varmistetaan, että hyökkäys ei ole enää toiminnassa.
2. Selvitetään hyökkäyksen laajuus henkilötietojen osalta.
3. Selvitetään vuotaneiden henkilötietojen määrä ja laatu.
4. Tehdään riskiarvio, onko henkilöille aiheutunut korkeaa riskiä.
5. Tarvittaessa voidaan määrätä organisaation noudattamaan tietosuoja-asetuksen mukaisia velvoitteita.
6. Dokumentointi ja lisäohjeistus mikäli tarpeen Office 365 -hyökkäykseen liittyen pyydetään normaalisti seuraavat lisäselvitykset. Tiedot toimivat myös tietoturvaloukkauksen dokumentaationa. Tarvittaessa pyydetään myös enemmän esimerkiksi lokitietoja.

Tietoturvaloukkausilmoituksen lisätiedot, koskien Office 365 -murtoja:

1. Onko kyseessä Office 365 vai OWA-ympäristö?
2. Onko tarkastettu, ettei tileille ole tullut luvattomia uudelleenlähetyssääntöjä?
3. Jos on, niin mihin sähköpostiosoitteeseen?
4. Onko tarkastettu, ettei tilille ole kirjauduttu luvattomasti tuona aikana? (esim. Azure AD -tunnuksen audit log)
5. Jos on, onko tarkastettu, onko sähköposteja ladattu? (esim. Office 365 Exchange lokit)
6. Onko tilillä ollut käytössään OneDrive tai Sharepoint-palveluita?
7. Oliko tilien sähköposteissa tai OneDrivessa tai Sharepoint-palveluissa henkilötietoja?
8. Jos on, niin kuinka monen henkilön tietoja ja mitä henkilötietoryhmiä? (esim. nimi, HETU, sähköposti, osoite)
9. Onko harkittu käytettäväksi monen tekijän tunnistautumista (MFA)?
10. Toimittakaa tietosuojavaltuutetun toimistoon vuodettujen tunnusten osalta tunnusten Azure AD:n SIGN-INS -loki hyökkäyksen ajanjaksolta csv-tiedostona.

4.6 Taloushallinon kontrollit

Murrettuja tilejä on käytetty mm. väärennettyjen laskujen tekemiseen ja/tai lähettämiseen. Yrityksen tulee huomioida tämä uhka omassa laskujenmaksuprosessissa tai tilitietoja lisättäessä ja muokattaessa.

Kyberturvallisuuskeskuksen tietoon on tullut useampi tapaus, jossa sähköpostitileihin murtautumisen jälkeen organisaatioiden välisiin sähköpostikeskusteluihin on puututtu aiemmin mainituin edelleenohjaussäännöin ja postiarkistoinnein, ja olemassa olevia laskuja ja tilitietoilmoituksia on muokattu hyökkääjien toimesta. Tällöin validi lasku on voinut lähteä asiakkaalle tai kumppanille, mutta hyökkääjä on muokannut tietoja välissä, ja rahaliikenne ohjautuu täysin väärään suuntaan. Laskuvääränn östen osalta ongelma koskee etenkin PDF-muodossa välitettyjä laskuja; sähköiseen laskutukseen ei toistaiseksi ole hyökätty.

Tämän vuoksi organisaatioiden kannattaa käydä sisäisesti läpi, kuinka maksettavien laskujen tiedot varmistetaan, kuinka organisaatio toimittaa itse laskut asiakkailleen ja kuinka kumppanien ja asiakkaiden tilitietomuutokset varmistetaan.

4.7 Viestintä sidosryhmille

Tietomurtojen ja väärinkäytösten kohteeksi joutuminen ei ole poikkeuksellista, joten organisaation

kannattaa suunnitella etukäteen tiedotusmalli ja –politiikka erilaisia skenaarioita varten. Tietyissä tapauksissa on myös mahdollista, että tapaus herättää median huomion ja nousee julkisuuteen, joten tämänkin mahdollisuuden hallitseminen kannattaa miettiä ennakkoon.

Jos uhriksi joutuneen käyttäjän tililtä on lähetetty roskapostia tai kalasteluviestejä, on erittäin todennäköistä, että tämä kerää ilmoituksia ja kommentointia vastaanottajilta ja heidän organisaatioiltaan. Lisäksi on myös todennäköistä, että tästä aiheutuu uusia uhreja muissa organisaatioissa. Tämän vuoksi tilanteen havaitsemisen jälkeen on suotavaa viestiä asiasta proaktiivisesti.

Erityistä huomiota kannattaa panostaa organisaation sisäiseen tiedotukseen. Hyvin monissa tapauksissa ensimmäisen uhrin tililtä on lähetetty haitallisia viestejä muille samassa organisaatiossa vaikuttaville, jonka jälkeen hyökkääjä saa haltuunsa suuremman määrän käyttäjätilejä samasta organisaatiosta. Tämän vuoksi sisäistä tiedotusta kannattaa tehdä nopeasti ja matalalla toleranssilla, jotta vahinkojen määrä saadaan pidettyä mahdollisimman alhaisena.

Lisätietoja:

tietosuoja(at)om.fi
Tietoturvaloukkaukset:
https://tietosuoja.fi/tietoturvaloukkaukset
Ilmoitus tietoturvaloukkauksesta:
https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

Liitteet

Liite 1. Esimerkki Conditional Access -säännöistä

Esimerkissä on luotu kaksi ryhmää: sg_CA Excluded Cloud ja sg_CA Excluded On-prem, joiden jäseninä on käyttäjätunnukset ja palvelutunnukset, joihin Conditional Access -sääntöjen ei haluta vaikuttavan.

Nimi	**Users and Groups**		**Ehdot (Assignments)**		**Pääsykontrolli (Access controls)**	
	Include	**Exclude**	**Device Platforms**	**Client Apps**	**Block access**	**Grant access**
Allow modern authn from AADHJ or compliant devices - Clients	All Employees	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require device to be marked as compliant OR Require Hybrid AD joined device
Allow modern authn from AADHJ or compliant devices - Browser	All Employees	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require device to be marked as compliant OR Require Hybrid AD joined device
Require MFA for admins - Clients	Admin groups	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for admins - Browser	Admin groups	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require multi-factor authentication
Require MFA for Guests - Clients	All guest users	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for Guests - Browser	All guest users	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require multi-factor authentication
Require MFA for All other Users - Clients	All users	sg_CA Excluded Cloud sg_CA Excluded On-prem All Employees Admin groups All guest user	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for All other Users - Browser	All users	sg_CA Excluded Cloud sg_CA Excluded On-prem All Employees Admin groups All guest users	Android iOS Windows macOS	Browser		Require multi-factor authentication
Block ActiveSync	Cloud apps > Office 365 Exchange Online			Mobile apps and desktop cllients Exchange ActiveSync clients > Apply policy to supported platforms	Block	
Block legacy authn				Mobile apps and desktop clients > Other clients	Block	

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

TRAFICOM
Kyberturvallisuuskeskus