OULUN AMMATTIKORKEAKOULU

Casandra Andersson

MICROSOFT E5 SECURITY -PALVELUIDEN VAIKUTUS HOIVATIE OY:N TIETOTURVAAN JA LIIKETOIMINNAN TURVALLISUUTEEN

MICROSOFT E5 SECURITY -PALVELUIDEN VAIKUTUS HOIVATIE OY:N TIETOTURVAAN JA LIIKETOIMINNAN TURVALLISUUTEEN

Casandra Andersson
Opinnäytetyö
Kevät 2024
Tieto- ja viestintätekniikka
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tieto- ja viestintätekniikka (insinööri), Ohjelmistokehityksen suuntautumisvaihtoehto

---

Tekijä: Casandra Andersson
Opinnäytetyön nimi: Microsoft E5 -palveluiden vaikutus Hoivatie Oy:n tietoturvaan ja liiketoiminnan turvallisuuteen
Työn ohjaaja: Jukka Nevalainen
Työn valmistumislukukausi ja -vuosi: Kevät 2024 Sivumäärä: 23

Tämän opinnäytetyön aiheena on Microsoft E5 -palveluiden vaikutus yrityksen tietoturvaan ja liiketoiminnan turvallisuuteen. Tarkoituksena oli laatia esitelmä siitä, miten E5-palvelut otettiin käyttöön, mitä se vaati ja mikä oli tulos palvelun käyttöönoton jälkeen. Aihe on valikoitunut perustuen opiskelijan omiin mielenkiinnon kohteisiin sekä yrityksen tarpeisiin.

Työ on tehty projektimuodossa ja työtä on kirjoitettu reaaliajassa sitä mukaa, kun Microsoft E5 -työkalua on otettu käyttöön Hoivatie Oy:llä. Käyttöönotosta on raportoitu vaiheittain ja eri vaiheet ja niiden selitykset on jaoteltu erikseen.

Opinnäytetyön tulos osoittaa sen, että niin kaiken kokoisten yritysten kuin myös yksityishenkilöiden tulee panostaa tietoturvaan kattavasti. On huojentavaa tietää, että on olemassa työkaluja, joilla omat tiedot, tunnukset ja tilit pysyvät suojattuina erilaisilta kyberuhilta. Kaikkia uhkia tietoturvatyökalut eivät kuitenkaan yksin voi estää, vaan on syytä muistaa käyttää maalaisjärkeä.

Avainsanat: Microsoft 365, E5, Hoivatie Oy

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Technology (engineer), Option of Software Development

---

Author: Casandra Andersson
Title of thesis: The impact of Microsoft E5 services on Hoivatie Oy's cybersecurity and business security.
Supervisor: Jukka Nevalainen
Term and year when the thesis was submitted: Spring 2024 Number of pages: 23

The topic of this thesis was the impact that Microsoft E5 services had on the company's cybersecurity and business security. The aim was to create a presentation on how the E5 services were implemented, what it required, and what the outcomes were after the implementation. The topic was chosen based on the student's own interests as well as the needs of the company.

The work has been conducted in a project format, and it has been written in real-time as Microsoft E5 tools have been implemented at Hoivatie Oy. The implementation has been reported in stages and the different stages and their explanations have been separately divided.

The result of this thesis shows that companies of all sizes as well as private persons should invest in cybersecurity. It is reassuring to know that there are tools to keep your information, credentials and accounts protected from various cyber threats. However, not all threats can be prevented by information security tools alone, so one should always remember to use common sense.

Keywords: Microsoft 365, E5, Hoivatie Oy

SISÄLLYS

TERMIT JA LYHENTEET

Compliance	Täytäntöönpano
SaaS	Ohjelmistopalvelu, joka toimii verkon kautta (pilvipalvelu).
CAP	Conditional Access policy eli ehdollinen pääsykäytäntö
MFA	Monivaiheinen tunnistautuminen
Policies	Politiikat, eli säännöt, jotka on määritelty etukäteen. Takaavat turvallisen ja lainmukaisen käytön organisaation tunnuksilla ja/tai laitteilla
CASB	Cloud access security broker eli pilvipalveluiden tietoturvaohjelmisto
DLP	Data Loss Prevention eli politiikka, joka estää tietojen menetyksen
Sensitivity Labels	Tietoaineiston luokittelu
EOP	Exchange Online Protection eli sähköpostin suojaus
MDO	Microsoft Defender for Office 365 eli Microsoftin sovellusten suojaus
Windows PowerShell	Microsoftin kehittämä komentotulkki
Microsoft Intune	Päätepisteen hallintapalvelu (pilvipohjainen)
Azure Entra ID	Pääsynhallintaratkaisu (pilvipohjainen)

1 JOHDANTO

Tietoturvavuodot ja niiden mukanaan tuomat ongelmat ovat nykypäivänä suuri ongelma kaiken kokoisille yrityksille ja yksityishenkilöille. Tämän vuoksi on entistä tärkeämpää pysyä ajan tasalla mahdollisista uhista ja pyrkiä siihen, että omat laitteet sekä käyttäjätilit ovat mahdollisimman hyvin suojattuja.

Tässä opinnäytetyössä otetaan käyttöön kattava tietoturvapalvelu Microsoftilta, joka varmistaa sen, että yrityksen työntekijöiden ja asiakkaiden tiedot, käyttäjätunnukset, laitteet ja muut tiedostot ovat turvassa ja suojattuja. Projekti on aloitettu tammikuussa 2024 ja saatettu päätökseen huhtikuussa 2024. Opinnäytetyössä käydään kattavasti läpi työkalun käyttöönottoa ja selvitetään sen vaikutus Hoivatie Oy:n tietoturvaan ja liiketoimintaan. Tämä työ on yksi osa tietoturvakehityshanketta ja sillä pyritään varmistamaan turvallinen työympäristö kaikille käyttäjille ja asiakkaille.

Opinnäytetyö kirjoitetaan perinteisen raportin mallin mukaisesti ja siinä käydään läpi tietoturvan keskeisiä asioita ja Microsoft E5-työkalun eri osa-alueita, arvioidaan työn tuloksia sekä mahdollisia kehityskohteita. Microsoft E5-työkalun vaikutus tietoturvaan ja liiketoimintaan selviää pidemmän ajanjakson aikana.

2 HOIVATIE OY

Hoivatie Oy on vuonna 2020 perustettu yhtiö, jonka omistajina ovat Nuorten Ystävät ry ja Oulun Diakonissalaitoksen Säätiö sr. (ODL). Hoivatie on jo yksi Suomen suurimmista sosiaalialan toimijoista. Kuvassa 1 on Hoivatien logo.

Hoivatie tarjoaa 18 paikkakunnalla ja yli 60 eri yksikössä sosiaalipalveluita hyvinvointialueille kuten lasten- ja nuortenpalveluita, vammaispalveluita, ikääntyneiden palveluita, perhepalveluita, mielenterveys- ja päihdepalveluita sekä työllistämispalveluita.

Päätoimipaikka sijaitsee Oulussa, jossa sijaitsee myös Hoivatien oma tietohallintoyksikkö, joka vastaa mm. laitetilauksista, verkkoyhteyksistä, järjestelmistä sekä sisäisestä IT-tuesta. Tietohallinto vastaa tietotekniikan ja tietojärjestelmien hallinnasta ja niiden kehittämisestä. Palveluita tuotetaan sisäisesti, mutta ulkoistettuja palveluita on myös. (1.)

KUVA 1. Hoivatien logo

3 MICROSOFT E5

Microsoft E5 -työkalu kuuluu Microsoftin korkeimman tason tilaukseen (Microsoft 365). Se tarjoaa käyttäjälleen laajan valikoiman työkaluja ja ominaisuuksia, joilla yrityksen järjestelmävalvojat voivat hallita tietoturvaa, viestintää ja määräyksiä (engl. compliance). Tietoturvatyökalut ovat kuitenkin E5:n pääominaisuus. (2.)

Kaiken kokoiset yritykset hyötyvät E5 -palvelusta, sillä se takaa turvalliset työkalut ja sen avulla yritykset voivat seurata sekä ehkäistä mahdollisia tietoturvauhkia. Microsoft E5 hallitsee seuraavia tuotteita: Advanced Threat Protection (ATP), Azure Information Protection (AIP), Microsoft Cloud App Security (MCAS) ja Microsoft Defender for Endpoint. (3.)

3.1 Azure Advanced Threat Protection (ATP)

ATP-sovellus kuuluu Microsoftin tietoturvapalveluihin ja sovelluksella yritykset saavat laajan suojauksen sähköposteille, tiedostoille ja sovelluksille. ATP:n avulla yritysten omat verkot pystyvät estämään, havaitsemaan ja vastaamaan erilaisiin kyberhyökkäyksiin. Sovelluksen keskeisiä toimintoja ovat uhan tiedustelu, pilviturvallisuuden analysoiminen ja käyttäytymisen sensorit, joiden avulla päätelaitteita voi seurata ja analysoida.

ATP-sovellus keskustelee saumattomasti muiden Microsoft-sovellusten kanssa. Tämä mahdollistaa yhtenäisen ja tehokkaan hallinnan ja reagoinnin mahdollisiin tietoturvauhkiin. (4.)

3.2 Azure Information Protection (AIP)

AIP-sovelluksella yritykset saavat käyttöön tehokkaat työkalut, joiden avulla voi suojata ja hallita yrityksen tietoja. Työkalu mahdollistaa tietojen luokittelun, suojauksen ja seurannan tietovirran ajan niin sisäisesti kuin ulkoisesti. AIP laajentaa Microsoft Purview'n (tietosuojaratkaisu) tarjoamaa luokittelun ja luokittelutoiminnallisuuden toimintoja seuraavilla ominaisuuksilla: yhdistetty luokittelun asiakasohjelma, paikallinen skanneri ja SDK.

Yhdistetty luokittelun asiakasohjelma laajentaa luokittelun ja suojauksen toimintoja lisätiedostotyyppeihin sekä File Exploreriin ja PowerShelliin. **Paikallinen skanneri** mahdollistaa järjestelmänvalvojien skannata paikalliset tiedostojärjestelmänsä herkän sisällön löytämiseksi, joka tulee luokitella, määritellä tai suojata. Se asennetaan PowerShell-komentosarjoina, jotka ovat osa yhdistettyä luokittelun asiakasohjelmaa, ja sitä voidaan hallita PowerShellin ja tietosuojan skannerialueen avulla Microsoft Purview -noudattavuusportaalissa. **SDK** laajentaa herkkyysluokkia kolmannen osapuolen sovelluksiin ja palveluihin. Kehittäjät voivat käyttää SDK:ta integroidakseen tuen herkkyysluokkien ja suojauksen käyttämiseen tiedostoille. (5.)

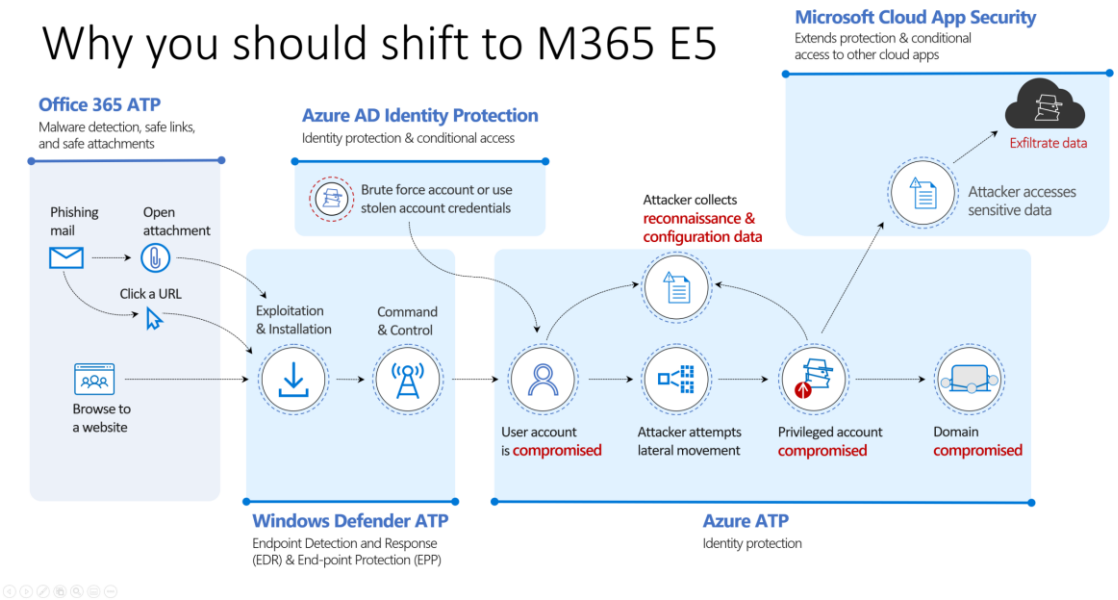
3.3 Microsoft Cloud App Security

Cloud App Security on pilvipalveluiden käyttöön liittyvän turvallisuuden tuottaja (Cloud Access Security Broker, CASB), joka on yhteensopiva monien johtavien palveluiden kanssa (esimerkiksi AWS, Dropbox ja Google Cloud). CASB:nä Microsoft Cloud App Security toimii lisäturvana kaikissa SaaS-sovelluksissa, joita yritykset käyttävät liiketoimintaansa varten. Cloud App:ssa järjestelmävalvojat voivat valvoa ja korjata epätavallista toimintaa, estää riskialttiita SaaS-sovelluksia ja määrittää sääntöjä tarkasti. Lisääntynyt näkyvyys ja vahvempi hallinta korostavat yrityksen tietoturvaa siirtäessään enemmän tietoa pilveen. Cloud App tarjoaa ns. kojelaudan, jossa ylläpitäjä voi nähdä reaaliajassa tiedot kaikista pilvisovelluksista ja hälytyksistä. (6.)

3.4 Microsoft Defender for Endpoint

Defender for Endpoint on kehittynyt turvallisuusratkaisu, joka on suunniteltu suojaamaan yritysten laitteita kuten tietokoneita, kannettavia, palvelimia ja mobiililaitteita erilaisilta tietoturvauhilta ja haittaohjelmilta. Työkalu tarjoaa jatkuvaa reaaliaikaista suojausta, uhkien havaitsemista ja niiden torjuntaa. Se käyttää tekoälyä tunnistamaan ja estämään haitallisia toimintoja ja hyökkäyksiä kuten haittaohjelmien leviämistä, tunkeutumisyrityksiä ja muita tietoturvauhkia. (7.)

Microsoft Defender for Endpoint kerää tietoja laitteista, analysoi niitä ja tarjoaa turvallisuusanalyysejä, jotka auttavat yrityksiä tunnistamaan tietoturvapoikkeamia ja uhkia ja reagoimaan niihin nopeasti. Se myös tarjoaa laajaa näkyvyyttä organisaation laitekannasta ja auttaa vähentämään tietoturvahyökkäysten riskiä. Kuvassa 2 selviää useita syitä, miksi yrityksen tulisi valita E5-työkalu. (7.)

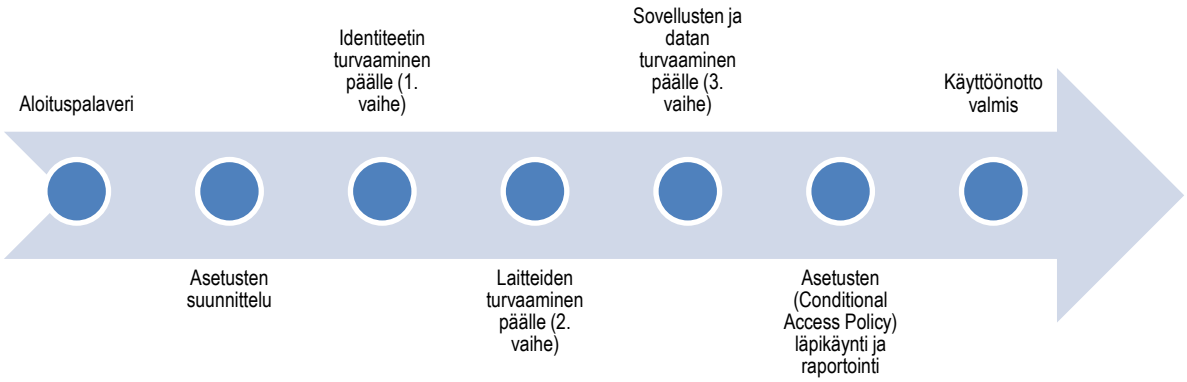


KUVA 2. Miksi valita E5 (8.)

4 KÄYTTÖÖNOTON VAIHEET

Microsoft E5 -työkalun käyttöönotto alkoi tammikuun alussa Microsoft Teams -palaverilla. Palaverissa olivat läsnä projektin osapuolet Crayon ja Hoivatie Oy.

Palaverissa käytiin läpi asetusten ja sovellusten käyttöönoton vaiheet sekä aikataulutukset. Sovellusten käyttöönotto tapahtui vaiheittain, jolloin osapuolet pystyivät helpommin huomaamaan mahdollisia ongelmia tai vikatiloja. Vaiheittainen käyttöönotto takaa myös sujuvamman käyttäjäkokemuksen, jolloin on helpompi ylläpitää niitä asetuksia, joita taustalle tehdään yksitellen. Alla olevasta kuvasta selviää suunniteltu eteneminen.



Kuva 3. Käyttöönoton etenemisjärjestys

Asetuksen käyttöönotto liittyy ehdollisten käyttöoikeuksien asetuksiin ja se on jaettu kolmeen vaiheeseen, jotka esitellään seuraavaksi.

Ensimmäisessä vaiheessa on jalkautettu MFA-vaatimus eli monivaiheinen tunnistautuminen (engl. Multi-factor Authentication). Tämä tarkoittaa sitä, että vahva tunnistautuminen vaaditaan kaikilta käyttäjiltä. Vahva tunnistautumisen mahdollistaa sen, että yritys voi taata, että oikealla henkilöllä on pääsy hänen omiin tietoihinsa, ohjelmistoihin ja sovelluksiin, jotka on suojattu.

Toisessa vaiheessa jalkautettiin ne politiikat (policyt), jotka koskevat yrityksen laitteita. Tämä tarkoittaa sitä, että E5-työkaluun on syötetty ehdolliset säännöt, jotka koskevat laitteita ja niiden yhteensopivuutta tietoturvasovelluksen kanssa. Eli mikäli käyttäjä avaa laitteensa ja se ilmoittaa yhteensopivuusongelmasta, tarkoittaa se sitä, että laitetta ei voida suojata vaatimusten mukaisesti eikä näin ollen sitä voi myöskään käyttää ennen kuin tarvittavat toimenpiteet on järjestelmävalvojan toimesta tehty.

Kolmannessa ja viimeisessä vaiheessa jalkautettiin politiikat, jotka koskivat datan ja sovellusten suojaamista. Tämä tarkoitti sitä, että Microsoft 365 -sovellukset kuten esimerkiksi Exchange (sähköposti) ovat entistä suojatumpia. Kiristetty suojaus ilmeni esimerkiksi siten, että jos käyttäjä sai tuntemattomalta lähettäjältä sähköpostiviestin, tuli siitä automaattinen ilmoitus. Tällä tavoin organisaatio pystyi paremmin ehkäisemään mahdolliset sähköpostikalastelut tai haittaohjelmat.

5 IDENTITEETIN TURVAAMINEN

E5-työkalu otettiin käyttöön vaiheittain ja ensimmäinen vaihe oli identiteetin turvaaminen, mikä tarkoittaa sitä, että työn tuottaja (Crayon) toimittaa Hoivatien ympäristöön ehdollisen käyttöoikeuden asetukset (Conditional Access Policy). Tietoturvan perustasoon kuuluivat seuraavat asetukset: Block Legacy authentication ja Require MFA all users and browser access.

5.1 Block legacy authentication

Block Legacy authentication -asetuksella estetään vanhempien ja vähemmän turvallisten autentikointimenetelmien käyttö. Legacy-autentikointi viittaa esimerkiksi vanhempiin menetelmiin ja protokolliin, joita ei välttämättä enää tueta uusimmissa turvatoimissa ja jotka näin tekevät laitteesta haavoittumaisemman.

5.2 Require MFA all user and browser access

MFA:n vaatiminen kaikille käyttäjille tarkoittaa sitä, että jokaisen työntekijän tulee autentikoitua sovelluksen avulla (esimerkiksi Microsoft Authenticator), jotta hän pääsee kirjautumaan työnantajan sovelluksiin. Vahva tunnistautuminen edellytetään kaikilta käyttäjiltä.

6 LAITTEIDEN TURVAAMINEN

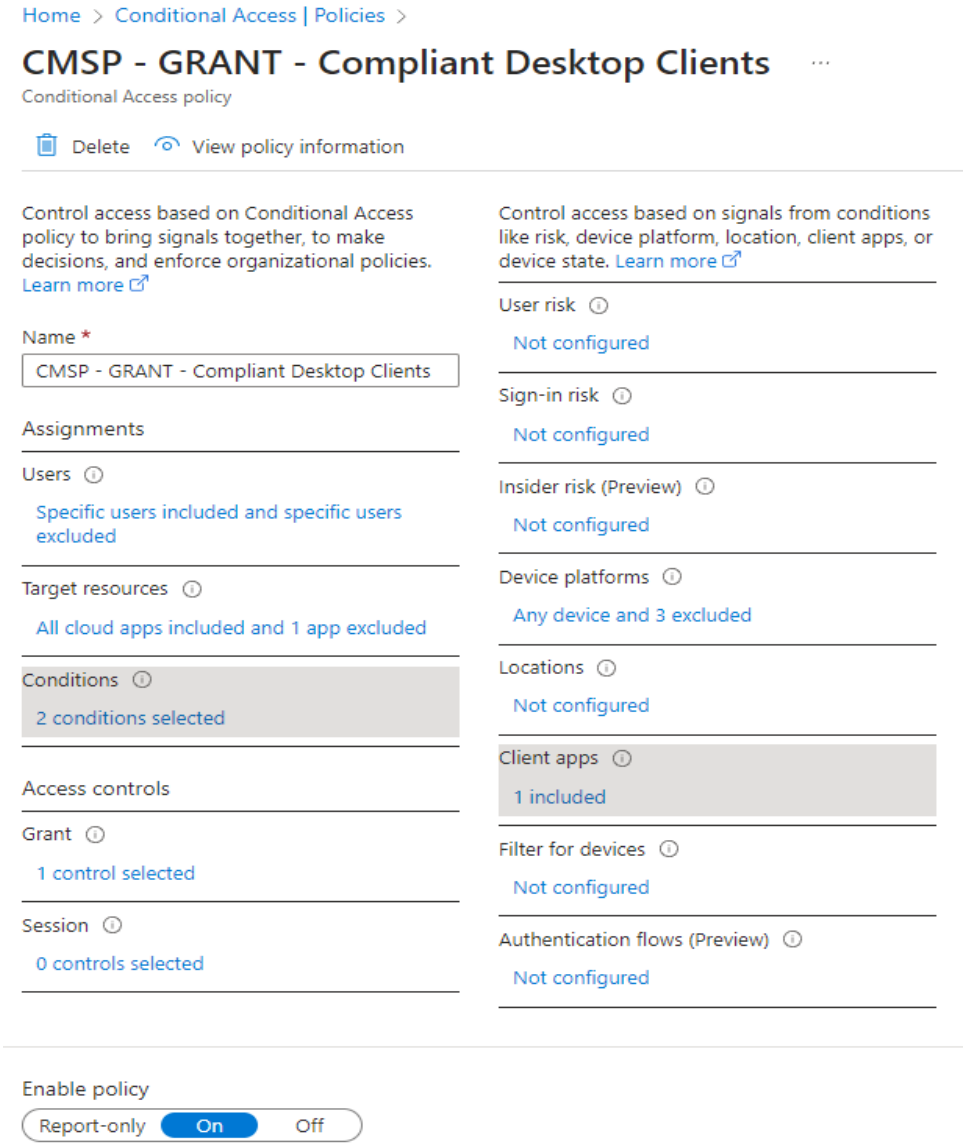
Toinen käyttöönoton vaihe on laitteiden turvaaminen eli miten organisaatio pystyy E5-työkalun avulla turvaaman sen hallinnoimia laitteita. Kaikille laitteille asetetaan tietyt vaatimukset eli politiikat (engl. policies), joiden avulla järjestelmävalvojat pystyvät takaamaan turvallisen ja suojatun käytön. Kyseiset politiikat ovat require mobile app protection policy /compliant device, require managed device for O365+ block unknown browser access, require compliant device + MFA for admin ja require compliant device for access-to-access Desktop clients.

Require mobile app protection policy/ compliant device- asetus tarkoittaa sitä, että mobiililaitteeseen on asetettu politiikka (engl. policy), joka koskee laitteen turvatoimia kuten salausta ja tietojen säilyttämistä.

Require managed device for O365 + block unkown browser access- asetus tarkoittaa sitä, että organisaation hallinnoimassa laitteessa on tietyt asetukset, jotka mahdollistavat käyttäjän pääsyn Microsoftin Office365 -palveluihin kuten sähköpostiin, PowerPointiin ja Teamsiin. Asetus mahdollistaa myös sen, että käyttäjän selainvierailu on rajoitettu eli tietoturvasyistä potentiaaliset haitalliset verkkosivut on estetty.

Require compliant device + MFA for admin- asetus vaatii sen, että käyttäjällä on organisaation suositusten tai vaatimusten mukainen laite, jonka käyttö vaatii myös vahvaa tunnistautumista eli MFA-autentikointia. Tämä varmistaa sen, että hallinnollinen pääsy myönnetään vain laitteille, jotka täyttävät organisaation asentamat vaatimukset ja vahvistaa niiden tietoturvaa MFA:n kautta. MFA for admin tarkoittaa sitä, että järjestelmävalvojien tunnuksille vaaditaan tunnistautumista MFA:n kautta 12 tunnin välein.

Require compliant device for access-to-access Desktop clients- asetus tarkoittaa sitä, että käyttäjällä on lupa käyttää työpöytäkoneen sovelluksia vain, jos laite täyttää määritellyt vaatimukset. Kuvasta 4 nähdään, miten kyseinen politiikka on rakennettu järjestelmään.



KUVA 4. Compliant Desktop Client -politiikka

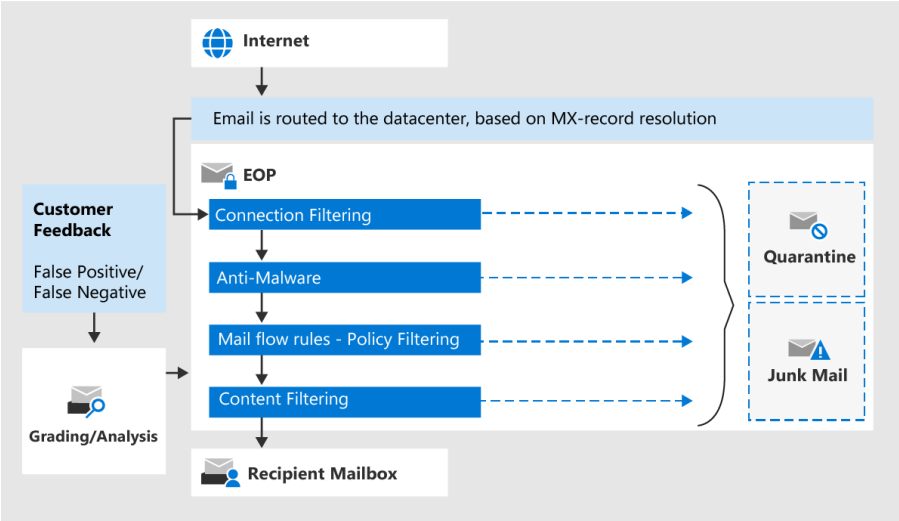
7 SOVELLUSTEN TURVAAMINEN

Kolmannessa vaiheessa otettiin käyttöön ne asetukset, jotka koskivat sovellusten ja datan turvaamista. Sovellusten turvaaminen on olennainen osa E5-työkalua ja sillä varmistetaan, että työntekijöiden käyttämät sovellukset kuten Exchange, OneDrive ja SharePoint pysyvät suojattuina.

Microsoft Exchange eli Microsoftin tarjoama yritys- tai oppilaitoksen sähköpostitili on suojattu niin, että jos käyttäjä saa epätavalliselta lähettäjältä sähköpostin, sovellus ilmoittaa siitä. Kuvassa 5 näkyy, millainen ilmoitus voi olla kyseessä. Asetettu suojaus osaa suodattaa saapuvia sähköposteja niin, että mahdolliset haittapostit menevät automaattisesti roskapostikansioon ja se osaa ilmoittaa epätavallisesta lähettäjästä.

KUVA 5. Microsoftin ilmoitus

Esiasetetut EOP (Exchange Online Protection) ja MDO (Microsoft Defender for Office) -suojausprofiilit suojaavat ja turvaavat yrityksen sähköposteja sekä Office-dataa. Kuvassa 6 näkyy miten EOP suojaus toimii.



KUVA 6. Miten EOP suojaus toimii (9.)

8 DATAN TURVAAMINEN

Datan turvaaminen tarkoittaa sitä, että organisaation tulee turvata arkaluontoisia tiedostoja niin että niihin ei kukaan ulkopuolinen pääse käsiksi. Sähköpostit, viestit, jaetut tiedostot, pilvisovellukset ja laitteet sisältävät paljon dataa, joten ne tulee kaikki olla suojattuja. Koska dataa on niin valtavasti, voi sen suojaaminen olla hankalaa ilman siihen tarkoitettuja työkaluja.

Taulukosta 1 selviää yleisimmät tietoturvariskit.

TAULUKKO 1. Tietoturvariskit

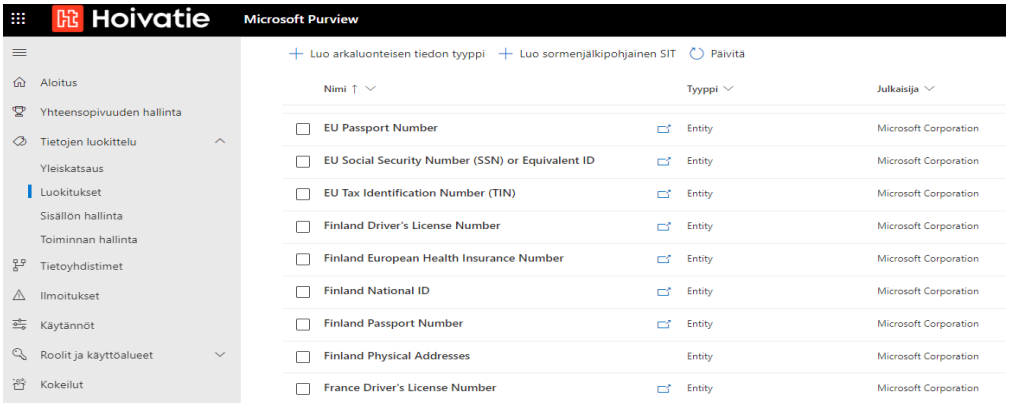
Käyttö	**Riski**
Sähköposti	Kalastelu, haittaohjelmat, tietomurrot, säädösten rikkoutuminen (GDPR), vakoilu
Viestit	Vakoilu, väärentäminen, kalastelu, haittaohjelmat, tietovuoto
Jaetut tiedostot	Luvaton pääsy, tietovuoto, tietojen menetys, haittaohjelmat, sisäiset uhat
Pilvisovellukset	Tietomurrot, tietojen menetys, haittaohjelmat, tilin kaappaus
Laitteet	Tietomurrot, haittaohjelmat, identiteettivarkaus, yksityisyyden menetys, palvelunestohyökkäykset

Jotta organisaatio voi taata turvallisen käytön ja datan suojauksen, tulee sen turvata arkaluontoista dataa missä ikinä sitä onkaan ja miten ikinä sitä jaetaankaan. Lisäksi organisaation tulee ymmärtää, kuinka työntekijät ymmärtävät ja käyttävät dataa. Organisaation tulee myös osata identifioida mahdolliset riskit sekä ehkäistä ne.

Microsoft E5 -työkaluilla (Microsoft Purview) organisaatio voi suorittaa automaattisen tietoturva-analyysin, joka osaa hakea kaikista Microsoftin sovelluksista tietoturvariskejä sekä identifioida arkaluontoista dataa.

Cloud App Securityssä järjestelmävalvojat voivat estää tietojen menetyksiä käyttämällä tai aktivoimalla DLP-politiikat, ja DLP määrittää sen, miten arkaluontaista dataa käytetään.

Microsoft Purview:n tietoluokittelu (engl. sensitivity labels) mahdollistaa sen, että tiedostoja tai dataa voidaan luokitella ja suojella ilman, että itse tiedosto vahingoittuu tai aiheuttaa käyttäjälle toimimattomuutta. Käytetyimmät tietoluokat, jotka näkyvät kuvassa 7 ovat esimerkiksi suomalainen henkilöturvatunnus, passin numero tai IBAN-tilinumero. Luokkia on kuitenkin erittäin monta ja järjestelmänvalvojat voivat lisätä ja poistaa niitä. Kuvassa 8 näkyy tarkemmat tiedot suomalaisen henkilöturvatunnuksen tietoluokasta. (10.)



KUVA 7. Sensitivity labels -lista

KUVA 8. Suomalaisen henkilöturvatunnuksen tietoluokituksen tiedot

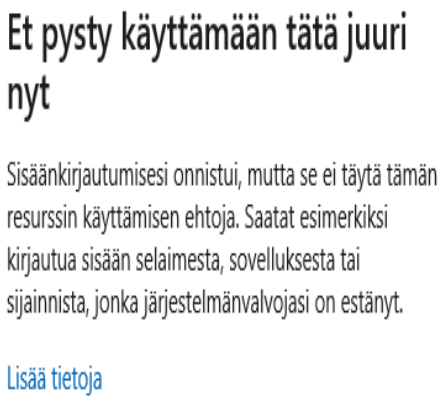
9 YHTEENVETO

Microsoft E5 -työkalun käyttöönotto Hoivatiellä onnistui hyvin. Käyttöönoton onnistumiseen vaikuttivat eri asiat kuten tarkka suunnittelu, tiivis yhteistyö Crayon Oy:n ja Hoivatien välillä ja palvelun helppokäyttöisyys ja sen hallinta. Kokonaisuudessaan E5 -palvelu pystyi tarjoamaan Hoivatielle suojatun ja turvallisen työympäristön kaikille työntekijöille ja asiakkaille.

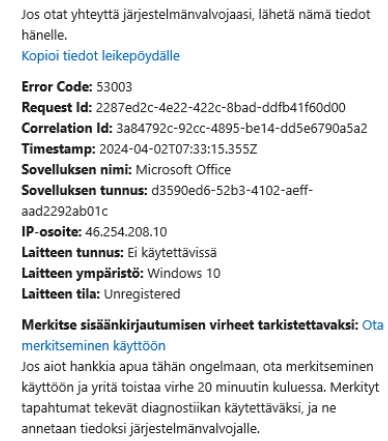
Käyttöönoton alussa laadittiin pilottiryhmät Microsoft E5 -työkaluun, mikä tarkoitti sitä, että ryhmiin lisättiin ne henkilöt, joille ensimmäisenä asetettiin valmiiksi säädetyt politiikat. Tämän myötä oli helppo selvittää, jos uudet politiikat olisivat enemmän haitaksi kuin hyödyksi. Microsoftin luomat raportit kertoivat, miten asetetut politiikat vaikuttivat pilottiryhmän jäseniin ja raportin tulosten perusteella jalkautettiin politiikat lopuille käyttäjille.

Ensimmäisen käyttöönoton vaiheen aikana ei juuri huomattu muutosta palveluiden käytössä, eikä peruskäyttäjä pystynyt huomaamaan, että taustalla on kiristetty suojauksia. Yksi ongelma kuitenkin nousi esille joillakin Android-käyttäjillä. Asetetut säännöt aiheuttivat sen, että käyttäjät eivät pystyneet kirjautumaan työsähköpostiinsa Android-laitteella, vaikka heillä oli vahva tunnistautuminen (MFA) käytössä. Tämä johtui siitä, että Android-käyttöjärjestelmän yksityisprofiili ja työprofiili eivät keskustelleet keskenään eikä vanhempi tapa hallita työprofiilia enää tukenut uusia asetettuja sääntöjä. Ongelma ratkaistiin luomalla käyttäjille uusi työprofiili, jonka kautta Microsoft Intune pystyi lataamaan uudelleen yritystilit. Kyseistä ongelmaa ei esiintynyt iOS-laitteissa.

Toinen vaihe käyttöönotosta sujui hyvin, vaikka sääntöjä (politiikkoja) oli jonkin verran enemmän. Laitevaatimusten kohdalla kiristettiin suojausta entistäkin enemmän ja sen myötä ilmeni, että osa laitteista ei täyttänyt laitevaatimuksia. Näiden laitteiden tila oli ”not compliant” eli ei yhteensopiva. Kuvissa 9 ja 10 on ne virheilmoitukset, jotka ilmestyivät käyttäjille, joilla ei ollut yhteensopivaa laitetta.



KUVA 9. Virheilmoitus



KUVA 10. Virheilmoituksen lisätiedot

Ongelmat ilmeni käyttäjillä, joilla oli laitteessa toinen virustorjuntaohjelma, jota Microsoftin palomuuri ei pystynyt ohittamaan tai jos käyttäjä ei kuulunut Azure Entra ID -ryhmään ”M365 E5 Security Computers”. Azure Entra ID -ryhmä ei ole dynaaminen ryhmä eli sinne piti käsin lisätä jäseniä. Ongelmat ratkaistiin poistamalla vanha virustorjuntaohjelma käsin ja lisäämällä laite vaadittuun Azure Entra ID -ryhmään.

E5-työkalun käyttöönotto mahdollisti sen, että Hoivatie Oy:n oma tietohallinto pystyy jatkossa omatoimisesti havaitsemaan tietoturvauhkia ja reagoimaan niihin. Tällä tavalla Hoivatiellä on laajempi kuva omasta tietoturvasta ja sen toimivuudesta. Voidaan todeta, että omatoiminen tietoturvahallinta ja nopea reagointi on tärkeä osa Hoivatie Oy:n kokonaisuutta ja se tuo mukanaan monia erilaisia hyötyjä kuten asiakkaiden luottamusta, kustannustehokkuutta sekä nopeaa reagointia ja ongelmien ratkaisuja.

LÄHTEET

1. Hoivatie Oy. Kotisivu. Hakupäivä 12.3.2024. https://hoivatie.fi

2. Microsoft. Microsoft 365 E5. Hakupäivä 2.3.2024 https://www.microsoft.com/en-us/microsoft-365/enterprise/e5?activetab=pivot:overviewtab

3. Houssier, Emily 2023. The Security features of Microsoft 365. Powell Software. Hakupäivä 8.3.2024. https://powell-software.com/resources/blog/microsoft-365-security/

4. Microsoft Tech Community. 2018. “Introducing Azure Advanced Threat Protection”. Hakupäivä 19.3.2024. https://techcommunity.microsoft.com/t5/security-compliance-and-identity/introducing-azure-advanced-threat-protection/ba-p/250332

5. Microsoft Learn. What is Azure Information Protection? Hakupäivä 19.3.2024. https://learn.microsoft.com/en-us/azure/information-protection/what-is-information-protection

6. Microsoft Learn. Microsoft Defender for Cloud Apps Documentation. Hakupäivä 19.3.2024. https://learn.microsoft.com/en-us/defender-cloud-apps/

7. Microsoft Learn. Microsoft Defender for Endpoint. Hakupäivä 20.3.2024. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide

8. Bernaers, Jasper. 2020. "The Value of Microsoft 365 E3 or E5." Hakupäivä 4.3.2024. https://jasperbernaers.com/the-value-of-microsoft-365-e3-or-e5/

9. Micrsoft Learn. Exchange Online Protectionin yleiskatsaus. Hakupäivä 24.3.2024. https://learn.microsoft.com/fi-fi/microsoft-365/security/office-365-security/eop-about?view=o365-worldwide

10. Microsoft Learn. Get started with sensitivity labels. Hakupäivä 23.3.2024. https://learn.microsoft.com/en-us/purview/get-started-with-sensitivity-labels