Microsoft Intune -mobiililaitehallinnan yleistä tietoa

1. Taustaa ja termejä

Mobiililaitehallinnan ohjeissa puhutaan yksinkertaisuuden vuoksi vain puhelimista, mutta järjestelmää sovelletaan samoin myös Android-tableteissa ja iPadeissa ja kaikki ohjeet toimivat myös niissä.

Käytämme Microsoftin laitehallintatuotetta nimeltään Intune. Puhelimeen asennettavan hallintasovelluksen nimi on Yritysportaali. Tämän sovelluksen nimi on kuitenkin Play Kaupassa ja App Storessa muodossa Intune-yritysportaali.

Termejä mobiililaitehallinta, hallintajärjestelmä, Intune ja Yritysportaali käytetään ohjeissamme hiukan ristiin tilanteesta riippuen, kyse on kuitenkin pitkälti yhdestä ja samasta järjestelmästä ja asiasta.

2. Mitä tietoja hallintajärjestelmä näkee puhelimestani?

Kaikkien Tampereen korkeakouluyhteisön käyttämien järjestelmien ja laitteiden yksityisyydensuoja otetaan vakavasti, niin on luonnollisesti myös Intune-mobiililaitehallinnan suhteen. Kerromme tarkasti, mitä tietoja hallintajärjestelmä näkee puhelimestasi ja mitä ei. Kaikkia tietoja käsitellään luottamuksellisesti ja vain perusteltuun tarpeeseen.

Kaikenlainen valvonta ja hallinta luonnollisesti epäilyttää, kun se näyttää kohdistuvan henkilökohtaisiin asioihin, kuten omassa puhelimessasi oleviin omiin tietoihin ja tiedostoihin. Moni asia voi epäilyttää: Tekeekö hallintajärjestelmä juuri sitä, mitä lupaa, eikä muuta? Onko hallintajärjestelmässä vikoja? Onko hallintajärjestelmä oikein konfiguroitu? Voiko luottaa, että hallintaa operoiva henkilöstö ei lue tietojani? Kriittinen suhtautuminen on aina paikallaan, mutta on kuitenkin useita syitä, miksi tähän järjestelmään voi luottaa:

- Microsoft Intune on laajasti käytetty järjestelmä, käytössä noin 3000 firmassa.
- Intunen dokumentointi (katso luku 2) kertoo tarkkaan, mitä Intune näkee ja mitä ei. Intune ei saa mitään tietoja henkilökohtaisesta profiilista eli omista sovelluksistasi, niiden tiedoista ja tiedostoista.
- Intune on kaikissa organisaatioissa tietohallinnon ammattilaisten valvonnan alla oleva hallintajärjestelmä. Siinä olevat poikkeamat dokumentoinnista ja viatkin löytyvät siis paljon todennäköisemmin kuin kuluttajajärjestelmistä.
- Puhelimessa suuri osa mobiililaitehallinnan toiminnoista tulee Googlen ja Applen tekemistä käyttöjärjestelmistä, ja edellä mainittu jatkuva valvonta auttaa huomaamaan niidenkin relevantit viat.
- Käytät todennäköisesti hyvin monia sovelluksia salaistenkin tietojesi tallentamiseen ja välittämiseen, kuten: Google Drive, OneDrive, iCloud, WhatsApp, Signal, sähköposti. Jos voit luottaa riittävästi niiden virheettömyyteen ja ylläpitohenkilöstöön, miksi se luottamus ei yltäisi Intuneen ja mobiililaitehallintaan?
- Tampereen yliopiston tietohallinnon työntekijät noudattavat tiukkaa tietosuojaa ja ammattietiikkaa, ja kaikki tietosi pidetään hyvin salassa. Ylläpitohenkilöstön työtä säädellään tarkoin Tietotekniikkapalveluiden ylläpitosäännössä ja korkeakoulukonsernin Lokipolitiikassa. Noudatamme tietenkin kaikkia yliopiston hyvän hallinnon periaatteita, joista tässä mielessä relevantein asia on tietosuoja.

Hallintajärjestelmä näkee puhelimestasi seuraavat tiedot:

- Puhelinmalli ja -valmistaja
- Käyttöjärjestelmän versio
- Puhelimen omistajan nimi
- Puhelimen nimi, sarjanumero ja IMEI
- Puhelinnumeron neljä viimeistä numeroa (paitsi työnantajan omistamassa puhelimessa, katso alla)
- Hallintajärjestelmän asentamien sovellusten nimet

Työnantajan omistamassa puhelimessa hallintajärjestelmä näkee edellisten lisäksi seuraavat tiedot:

- Koko puhelinnumero
- Itse asentamiesi sovellusten nimen ja version työnantajan omistamassa iPhonessa.
- Sijainti: Jos työnantajan omistama iPhone katoaa tai varastetaan, puhelimen käyttäjä voi iCloud-palvelussa asettaa puhelimen erityiseen Kadonnut-tilaan. Myös IT Helpdesk voi tehdä tämän käyttäjän pyynnöstä. Tällöin puhelinta ei voi käyttää, siihen tulee ilmoitus paikannuksesta ja puhelimen sijainti rupeaa näkymään myös tietohallinnon hoitamassa Intune-hallintapalvelussa. Tämä on ainoa tilanne, jossa minkään puhelimen sijainti voi tulla tietohallinnon tietoon.
    - Applen dokumentaatio: https://support.apple.com/fi-fi/guide/icloud/mmfc0f0165/icloud
    - Microsoftin dokumentaatio: https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-lost-mode.

Hallintajärjestelmä ei näe puhelimestasi seuraavia tietoja:

- Soitto- ja verkkoselaushistoria
- Sähköpostit ja tekstiviestit
- Yhteystiedot
- Kalenteri
- Salasanat
- Kuvat
- Tiedostot
- Sijainti (paitsi työnantajan omistamassa iPhonessa, katso yllä)
- Itse asentamiesi sovellusten nimet ja tiedot (paitsi työnantajan omistamassa iPhonessa, katso yllä)

Microsoftin dokumentaatio tästä aiheesta on täällä: https://docs.microsoft.com/fi-fi/mem/intune/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune.

3. Työsovellukset

TUNI-tunnusta vaativien Microsoftin ns. M365-palveluiden (ennen: Office 365) käyttö on työntekijöille mahdollista vain hallituilla työsovelluksilla, jotka mobiililaitehallinta on asentanut työprofiiliin. Osa sovelluksista jaetaan kaikille puhelimiin ja osa on valinnaisia, joista voit itse asentaa haluamasi. M365-palveluita voi käyttää M365-sovellusten lisäksi myös selaimella, joka on asennettu työprofiiliin.

Jos tarvitset jonkin sovelluksen jaettavaksi puhelimiin tai tabletteihin itse asennettavana työsovelluksena, voit lähettää siitä pyynnön IT Helpdeskiin hyvillä perusteluilla. Vahvin peruste, jolla sovellus on syytä saada jaettuna puhelimiin työsovelluksena, on, että sinulle tulee työsähköpostiin linkkejä palveluun, joka ei toimi riittävän hyvin selaimella, vaan sinun pitäisi voida käynnistää linkistä kyseinen sovellus.

4. Jos et ota käyttöön mobiililaitehallintaa

Yliopiston ja TAMK:n työntekijöiden pääsyä M365-järjestelmiin rajoitetaan puhelimissa ja tableteissa, joissa ei ole käytössä mobiililaitehallintaa. Työntekijä tarkoittaa tässä työsopimussuhteisia ja niitä resurssisopimuslaisia, joilla on työpuhelin yliopistolta tai TAMK:sta. Työntekijä tarkoittaa tässä myös sellaista työntekijää, joka on samaan aikaan yliopiston tai TAMK:n opiskelija.

Rajoitus on, että pääsy M365-palveluihin estetään työntekijälle kyseisestä puhelimesta. Jos olet aiemmin käyttänyt M365-sovelluksia (kuten Outlook, Teams, Office, OneDrive), joissa olet kirjautuneena TUNI-tilillesi, sovellukset rupeavat antamaan virheilmoituksia TUNI-tilistä.

Kaksivaiheisen tunnistuksen hyväksyminen esimerkiksi Microsoft Authenticator -sovelluksella toimii. Authenticator:n muut toiminnot, kuten ”Tarkista äskettäinen toiminta”, eivät kuitenkaan toimi.

5. Opiskelija työntekijänä

Edellä kuvatut vaatimukset mobiililaitehallinnan käyttämisestä koskevat kaikkia työntekijöitä eli myös opiskelijoita. Opiskeleminen tai työsuhteen lyhyys eivät ole päteviä syitä tinkiä tietoturvasta.

Mobiililaitehallinnan käyttövelvoite hallitaan käyttäjätunnuskohtaisesti. Jokaisella henkilöllä on vain yksi käyttäjätunnus, eli ei ole erillisiä tunnuksia opiskeluun ja työntekemiseen. Tämä käyttövelvoite koskee siis myös opiskelukäyttöä ja kaikkia puhelimia, myös opiskelijan omia puhelimia.

Näin ollen, jos olet opiskelija ja aloitat työsuhteen yliopistossa tai TAMK:ssa, sinun tulee ottaa käyttöön mobiililaitehallinta kaikissa niissä puhelimissa, joissa haluat käyttää M365-sovelluksia ja palveluja (kuten Outlook, Teams, Office, OneDrive). Käyttövelvoite määräytyy työsuhteen mukaan ja tulee voimaan automaattisesti työsuhteen alkaessa. Sinun tulee siis ottaa mobiililaitehallinta käyttöön myös omassa puhelimessasi.

Kun työsuhde loppuu, mobiililaitehallinnan käyttövelvoite poistuu automaattisesti ja M365-sovellukset toimivat jälleen henkilökohtaisessa profiilissa tai ilman mobiililaitehallintaa samoin kuin ennen työsuhdetta. Mobiililaitehallintaa ja sen asentamien sovelluksien käyttämistä voi jatkaa työsuhteen päättymisen jälkeen, mutta uusia työsovelluksia ei voi asentaa.

6. Microsoft Intune tarkemmin

Intune-järjestelmän dokumentaatio käyttäjille löytyy osoitteesta https://docs.microsoft.com/fi-fi/mem/intune/user-help/ ja se pätee pääosin meidän käyttöönottoommekin. Osa Intunen ominaisuuksista ja puhelimen toiminnasta on tietohallinnon aseteltavissa ja sitä kehitetään. Jos haluat muutosta jonkin ominaisuuden toimintaan, ota yhteyttä IT Helpdesk:iin ja selosta tarpeesi ja pyyntösi.

Jotta voit tulkita Microsoftin Intune-dokumentaatiota, alla ohjeet puhelimesi käyttöönoton tietojen selvittämiseen.

Android:

- Jos olet itse asentanut Intune-Yritysportaali -sovelluksen ja tehnyt käyttöönoton, käyttöönottoprofiilisi on ”personally-owned with a work profile”.
    - Jos puhelimesi on työnantajan omistama, sen omistajuus on ”corporate”.
    - Jos puhelimesi on omasi, sen omistajuus on ”personal”.
- Jos olet saanut uuden puhelimen ja Intunen käyttöönotto käynnistyi automaattisesti, kun pistit puhelimen päälle, käyttöönottoprofiilisi on ”corporate-owned with a work profile” ja puhelimen omistajuus on ”corporate”.

iOS:

- Jos olet itse asentanut Intune-Yritysportaali -sovelluksen ja tehnyt käyttöönoton, puhelin ei ole hallinnaltaan ”Supervised”.
    - Jos puhelimesi on työnantajan omistama, sen omistajuus on ”corporate” ja käyttöönoton tyyppi on ”Device enrollment”.
    - Jos puhelimesi on omasi, sen omistajuus on ”personal” ja käyttöönoton tyyppi on ”User enrollment”.
- Jos olet saanut uuden työpuhelimen ja Intunen käyttöönotto käynnistyi automaattisesti, kun pistit puhelimen päälle, se on hallinnaltaan ”Supervised”, puhelimen omistajuus on ”corporate” ja käyttöönoton tyyppi on ”Automated Device Enrollment”.