
Eetu Luoto

# Oppimispäiväkirja vastaavan IT-asiantuntijan työstä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

1.6.2025

## Tiivistelmä


| | |
|---|---|
| Tekijä: | Eetu Luoto |
| Otsikko: | Oppimispäiväkirja vastaavan IT-asiantuntijan työstä |
| Sivumäärä: | 22 sivua |
| Aika: | 1.6.2025 |
| Tutkinto: | Insinööri (AMK) |
| Tutkinto-ohjelma: | Tieto- ja viestintätekniikka |
| Ammatillinen pääaine: | Älykkäät IoT-järjestelmät |
| Ohjaajat: | Osaamisaluepäällikkö Janne Salonen |


---


Tämä opinnäytetyö toimii oppimispäiväkirjana ja käsittelee kolmea aihealuetta: tietoturvaa, Microsoft- ja mobiililaiteympäristöjen hallintaa sekä teknistä asiantuntijuutta asiakasprojektissa. Tavoitteena oli kuvata käytännön ratkaisuja ja reflektoida omaa ammatillista kehittymistäni.

Tietoturvaosuudessa tarkastelin, miten tekniset ratkaisut, kuten VPN, pääkäyttäjäoikeudet ja varmuuskopiointi, muodostavat yhdessä henkilöstön koulutuksen kanssa kokonaisvaltaisen suojan. Havaitsin, että tehokas tietoturva vaatii sekä teknologiaa että organisaation sitoutumista turvallisuuteen.

Koostaessani ohjeistuksia syvennyin käyttämiini Microsoft- ja mobiililaitehallinnan työkaluihin, kuten Admin Centeriin, Entra ID:hen, Intuneen, MobiControliin sekä erilaisiin komentorivityökaluihin. Opin, miten näiden työkalujen avulla voidaan hallita laitteita tehokkaasti ja keskitetysti. Ohjeistusten laatiminen puolestaan kehitti kykyäni jäsentää teknistä tietoa ja esittää se ymmärrettävästi eri käyttäjäryhmille.

Asiakasprojektissa vahvistin suunnittelu-, viestintä- ja ongelmanratkaisutaitojani sekä opin toimimaan tehokkaammin eri sidosryhmien välissä. Samalla syvensin ymmärrystäni teknisten projektien toteuttamisesta ja niihin liittyvistä haasteista.
Työ vahvisti teknistä osaamistani ja ymmärrystäni siitä, että IT-asiantuntijuus perustuu tekniseen tietoon, yhteistyöhön ja jatkuvaan oppimiseen.



Avainsanat: tietoturva, tietoturvatietoisuus, projektisuunnittelu

## Abstract


| | |
|---|---|
| Author: | Eetu Luoto |
| Title: | A Learning Diary on the Work of a Lead IT Specialist |
| Number of Pages: | 22 pages |
| Date: | 1 June 2025 |
| Degree: | Bachelor of Engineering |
| Degree Programme: | Information and Communication Technology |
| Professional Major: | Smart IoT Systems |
| Supervisors: | Janne Salonen, Director of school (ICT) |


---


This thesis serves as a learning diary and focuses on three main areas: information security, the management of Microsoft and mobile device environments, and technical expertise in a customer project. The aim was to describe practical solutions and reflect on my professional development.

In the information security section, I examined how technical solutions such as VPNs, administrative privileges, and backups, together with staff training, form a comprehensive protection strategy. I learned that effective information security requires both technology and organizational commitment to security.

While compiling user guides, I deepened my understanding of the Microsoft and mobile device management tools I used, such as Admin Center, Entra ID, Intune, MobiControl, and various command-line tools. I learned how these tools enable efficient and centralized device management. Creating the guides also improved my ability to structure technical information and present it in a user-friendly way for different audiences.

In the customer project, I strengthened my skills in planning, communication, and problem-solving, and learned to work more effectively between different stakeholders. At the same time, I deepened my understanding of how technical projects are implemented and the challenges they involved.
This work reinforced my technical competence and my understanding that IT expertise is built on technical knowledge, collaboration, and continuous learning.



Keywords: Information security, cybersecurity awareness, project planning

## Sisällys

## Lyhenteet

## Lyhenteet

MFA: *Multi-Factor Authentication* eli monivaiheinen tunnistautuminen, jossa käyttäjän on todistettava henkilöllisyytensä useammalla kuin yhdellä tavalla (esim. salasanan lisäksi tekstiviestillä tuleva vahvistuskoodi).

VPN: *Virtual Private Network* eli virtuaalinen erillisverkko, joka salaa internet-yhteyden ja mahdollistaa turvallisen etäyhteyden esimerkiksi yrityksen sisäverkkoon.

ABR: *Admin By Request* on työkalu, joka mahdollistaa käyttäjille tilapäisen järjestelmänvalvojan oikeuden hallitusti ja turvallisesti.

MSP: *Managed Service Provider* eli ulkoistettu IT-palveluntarjoaja, joka hallinnoi asiakkaan IT-infrastruktuuria ja -palveluita, kuten verkkoja, tietoturvaa ja tukipalveluita.

MDM: *Mobile Device Management* eli mobiililaitteiden hallinta on järjestelmä, jonka avulla organisaatio voi etähallita, suojata ja valvoa organisaation mobiililaitteita, kuten älypuhelimia ja tabletteja.

# 1 Johdanto

Tässä oppimispäiväkirjassa tarkastelen, mitä opin toimiessani organisaatiomme IT-osaston vastaavana alkuvuonna 2025. Tämä ajanjakso valittiin tarkastelun kohteeksi, koska teimme yhdessä johdon kanssa keväälle suunnitelman, jonka mukaisesti vastuulleni tuli työtehtäviksi ja kehitettäväksi useita laajempia kokonaisuuksia. Nämä kokonaisuudet olivat organisaatiomme tietoturvan parantaminen sekä IT-osaston työtehtävien ja työkalujen dokumentointi, ja näihin liittyvien ohjeiden ja koulutusmateriaalien tuottaminen nykyisille ja uusille työntekijöille. Lisäksi osallistuin teknisenä asiantuntijana asiakasprojektiin. Tässä päiväkirjassa nostan esiin näistä aiheista nousseita havaintoja ja tarkastelen niistä oppimiani asioita.

# 2 Tietoturva organisaatiossa

Tässä luvussa tarkastelen organisaatiomme nykyistä tietoturvan tasoa sekä siihen liittyviä suunnittelukäytäntöjä. Esittelen myös konkreettisia kehitystoimia, joilla pyritään parantamaan tietoturvallisuutta. Näihin toimiin sisältyvät sekä tekniset ratkaisut että henkilöstön koulutus, joiden avulla vahvistetaan koko organisaation kykyä suojautua tietoturvauhilta. Tavoitteena on luoda kokonaisvaltainen ja jatkuvasti kehittyvä tietoturvastrategia, joka vastaa sekä nykyisiin että tuleviin haasteisiin.

## 2.1 Tietoturvan suunnittelu ja kehittäminen

Seuraavissa alaluvuissa avaan tietoturvan käsitettä, miten tietoturvan kehittämistä on suunniteltu ja millaisin erilaisin ratkaisun sitä on organisaatiossa toteutettu.

### 2.1.1 Tietoturvan peruskäsitteet

Tietoturva tarkoittaa toimenpiteitä ja käytäntöjä, joilla suojataan tietoa luvattomalta käytöltä, muutoksilta ja tuhoutumiselta (Solms & Niekerk, 2013). Se

kattaa laajan kirjon teknologioita, prosesseja ja toimintamalleja, joiden tavoitteena on varmistaa tiedon luottamuksellisuus, eheys ja käytettävyys (Traficom, 2025). Nämä kolme peruspilaria muodostavat tietoturvan ytimen: luottamuksellisuus tarkoittaa, että tieto on vain oikeutettujen henkilöiden saatavilla; eheys varmistaa, että tieto pysyy muuttumattomana ja virheettömänä; ja käytettävyys takaa, että tieto on käytettävissä silloin, kun sitä tarvitaan.

Tietoturvan merkitys on kasvanut merkittävästi digitalisaation myötä. Digitalisaatio luo useita mahdollisuuksia, mutta samalla se on muuttanut ympärillä vallitsevien riskien ja uhkien laatua (Ivaska, 2025). Yhä suurempi osa tiedosta tallennetaan ja käsitellään sähköisessä muodossa, mikä tekee siitä herkemmän erilaisille uhille, kuten tietomurroille, haittaohjelmille ja identiteettivarkauksille. Tietoturva ei suojaa ainoastaan teknisiä järjestelmiä, vaan myös yksilöiden yksityisyyttä ja organisaatioiden mainetta. Esimerkiksi tietovuodot voivat aiheuttaa merkittäviä taloudellisia tappioita ja heikentää luottamusta organisaatioon (IBM). Siksi tietoturva on olennainen osa sekä yksityishenkilöiden että organisaatioiden arkea ja riskienhallintaa. Tietoturvatoimenpiteet tulee aina toteuttaa huolellisesti ja huomioiden häiriön vakavuus (Traficom, 2025).

Tietoturvaa ajatellessa ajatukset suuntautuvat usein uhkiin, kuten verkkohyökkäysten ja tietovuotojen aiheuttamiin ongelmiin, ja niistä syntyviin uhkailuihin ja kiristyksiin. Tietoturva on kuitenkin laaja käsite, jonka alle mahtuu myös tiedonkeruuseen, kohdentamiseen ja profilointiin liittyviä kysymyksiä (Ivaska, 2025.)

### 2.1.2 Tietoturvan kehittämisen suunnittelu ja toteutus

Vuoden 2024 strategiaprosessin yhteydessä sain organisaatiomme johdolta tehtäväksi selvittää nykyisen tietoturvamme tilan ja esittää konkreettisia kehitysehdotuksia sen parantamiseksi. Tämä tehtävä nousi esiin osana laajempaa digitaalisen toimintaympäristön kehittämistä, jossa tietoturva nähtiin keskeisenä osana organisaation riskienhallintaa ja toimintavarmuutta. Ensimmäinen vaihe oli kartoittaa olemassa olevat käytännöt ja tunnistaa niiden mahdolliset heikkoudet. Tätä varten järjestin palaverin IT-kumppanimme kanssa, jonka kanssa

kävimme läpi nykyiset järjestelmät, käytännöt ja tunnistetut riskit. Yhteistyössä laadimme alustavan listan kehityskohteista ja mahdollisista toimenpiteistä.

Projektin virallinen käynnistys tapahtui starttipalaverissa, jossa määritettiin projektin tavoitteet, aikataulu ja vastuunjako. Minulle annettiin vetovastuu koko projektista, ja samalla muiden osallistujien roolit ja vastuualueet kirjattiin selkeästi. Tämä vaihe oli tärkeä projektinhallinnan näkökulmasta, sillä se loi perustan systemaattiselle ja tavoitteelliselle etenemiselle.

Kehitystoimenpiteet päätettiin jakaa useisiin osa-alueisiin, jotka yhdessä muodostavat kokonaisvaltaisen lähestymistavan tietoturvan parantamiseen. Ensimmäinen konkreettinen toimenpide oli monivaiheisen tunnistautumisen (MFA) käyttöönoton laajentaminen, jolloin siitä tuli pakollinen kaikille käyttäjille. Kyberturvallisuuskeskuksen Pilvipalveluiden turvallisuuden arviointikriteeristön mukaisesti salausratkaisut ovat monesti ainoita menetelmiä datan eheyden ja luottamuksellisuuden varmistamiseksi käytettäessä huonosti suojattua verkkoa (Kyberturvallisuuskeskus, 2020). Tämä lisäsi merkittävästi käyttäjätunnusten suojaa erityisesti etäyhteyksien ja pilvipalveluiden käytön yhteydessä.

Toisena toimenpiteenä organisaatiossamme otettiin käyttöön pakollinen VPN-yhteys kaikessa etätyössä, mikä varmistaa, että organisaation sisäisiin järjestelmiin päästään vain suojatun yhteyden kautta.

Kolmantena kehityskohteena keskityimme työkoneiden hallintaan. Toteutimme järjestelmänvalvojan oikeuksien hallinnan uudistuksen, jossa pääkäyttäjäoikeudet myönnetään vain tilapäisesti ja tarkoin määritellyissä tilanteissa. Tämä vähentää riskiä siihen, että haittaohjelmat tai käyttäjävirheet pääsevät vaikuttamaan järjestelmän kriittisiin osiin. Lisäksi varmistimme, että organisaation tiedon tallennus tapahtuu keskitetysti, ja varmuuskopiointi on säännöllistä sekä testattua.

Käyttöönottojen jälkeen laadin koko organisaatiolle uuden tietoturvaohjeistuksen, joka kokosi yhteen keskeiset käytännöt ja toimintamallit. Järjestin tämän lisäksi myös henkilöstölle koulutuksen, jossa käytiin läpi ohjeistuksen sisältö ja

keskusteltiin tietoturvan merkityksestä arjen työssä. Tulevaisuuden kehitystoimena suunnittelimme tietoturvan suorituskykytyökalun käyttöönottoa, joka tulisi käyttöön myöhemmässä vaiheessa vuotta 2025.

## 2.2 Uudet teknologiset ratkaisut tietoturvan parantamiseksi

Tietoturvan kehittämiseksi päätimme ottaa käyttöön useita erilaisia sovelluksia ja teknisiä ratkaisuja, jotka tukevat organisaation suojaustasoa eri näkökulmista. Sovellusten valinta perustui huolelliseen arviointiin siitä, millaisia uhkia ja tarpeita organisaatiollamme on, sekä siihen, miten eri työkalut voivat täydentää toisiaan kokonaisvaltaisen tietoturvan rakentamisessa. Valinnassa painotettiin erityisesti käytettävyyttä, yhteensopivuutta olemassa olevien järjestelmien kanssa sekä kykyä vastata nykyaikaisiin tietoturvahaasteisiin.

Seuraavissa alaluvuissa esittelen tarkemmin ne sovellukset ja työkalut, jotka osoittautuivat keskeisiksi osiksi tietoturvamme kehittämistä. Kunkin sovelluksen kohdalla käyn läpi sen käyttötarkoituksen, käyttöönoton vaiheet sekä sen, miten kyseinen ratkaisu tukee organisaation tietoturvatavoitteita. Näin lukija saa kokonaiskuvan siitä, miten teknologiaa voidaan hyödyntää osana organisaation suunnitelmallista ja tavoitteellista tietoturvatoimintaa.

### 2.2.1 VPN-ratkaisu

Virtuaalinen erillisverkko eli VPN (Virtual Private Network) on teknologia, jonka avulla käyttäjä voi muodostaa suojatun yhteyden organisaation sisäverkkoon internetin yli. VPN salaa tietoliikenteen käyttäjän laitteen ja organisaation palvelimien välillä, mikä estää ulkopuolisia – kuten hakkereita tai avoimen Wi-Fi-verkon ylläpitäjiä – pääsemästä käsiksi tietoihin. Tämä on erityisen tärkeää etätyössä, esimerkiksi julkisissa tiloissa, joissa verkkoyhteydet eivät ole yhtä turvallisia kuin organisaation sisäverkossa.

Tietoturvan parantamiseksi otimme käyttöön Cisco AnyConnect -ratkaisun, joka mahdollistaa turvallisen ja salatun pääsyn organisaation resursseihin sijainnista

riippumatta. Käyttöönoton yhteydessä varmistimme, että VPN-yhteyden käyttö on pakollista kaikille toimiston ulkopuolella työskenteleville.

### 2.2.2 Admin By Request -käyttöoikeuksien hallinta

Admin By Request (ABR) on tietoturvaratkaisu, joka hallitsee ja valvoo pääkäyttäjäoikeuksia. Organisaatiossamme se rajoittaa käyttäjien järjestelmänvalvojan oikeuksia ilman, että työnteko keskeytyy tai IT-tuki kuormittuu tarpeettomasti. ABR:n avulla käyttäjät voivat ottaa tilapäisiä pääkäyttäjäoikeuksia hallitusti ja valvotusti, mikä vähentää riskiä haittaohjelmien asentamisesta tai järjestelmän väärinkäytöstä.

Aiemmin monilla käyttäjillä oli jatkuvat järjestelmänvalvojan oikeudet, mikä altisti järjestelmät sisäisille ja ulkoisille uhille. ABR:n käyttöönoton myötä oikeudet myönnetään vain pyynnöstä, ja kaikki tapahtumat kirjautuvat lokiin. Hallintapaneelin kautta voidaan seurata, kuka on käyttänyt oikeuksia, milloin ja mihin tarkoitukseen.

Ratkaisu tukee myös Zero Trust -periaatetta, jonka mukaan mikään käyttäjä tai laite ei ole automaattisesti luotettava. Pääkäyttäjäoikeuksien rajoittaminen ja hyväksyntäprosessin vaatiminen konkretisoivat tämän periaatteen käytännössä.

### 2.2.3 Cove Data Protection -varmuuskopiointiratkaisu

N-able Cove Data Protection on pilvipohjainen varmuuskopiointi- ja palautusratkaisu, joka tarjoaa tehokkaan ja skaalautuvan tavan suojata organisaation kriittistä dataa. Ratkaisu on suunniteltu erityisesti hallittujen palveluntarjoajien (MSP) tarpeisiin, mutta se soveltuu erinomaisesti myös sisäiseen IT-hallintaan. Cove Data Protectionin avulla voidaan varmistaa, että tärkeät tiedot ovat turvassa ja palautettavissa nopeasti erilaisissa häiriötilanteissa, kuten laiterikoissa, inhimillisissä virheissä tai kyberhyökkäysten, kuten kiristyshaittaohjelmien, yhteydessä.

Cove Data Protectionin käyttöönotto oli keskeinen osa organisaatiomme tietoturvastrategiaa, sillä se mahdollistaa jatkuvan ja automatisoidun varmuuskopioinnin ilman raskasta infrastruktuuria. Ratkaisu hyödyntää kevyttä agenttipohjaista arkkitehtuuria ja tallentaa varmuuskopiot suoraan pilveen, mikä vähentää paikallisten tallennusratkaisujen tarvetta ja parantaa palautuskykyä myös katastrofitilanteissa.

Tietoturvan näkökulmasta Cove Data Protection tarjoaa useita etuja. Ensinnäkin se tukee vahvaa salauskäytäntöä sekä siirrettäessä että tallennettaessa dataa, mikä suojaa tietoja luvattomalta käytöltä. Toiseksi järjestelmä mahdollistaa yksityiskohtaisen valvonnan ja raportoinnin, jolloin varmuuskopioiden onnistumista ja palautusvalmiutta voidaan seurata reaaliaikaisesti.

Yhteenvetona voidaan todeta, että N-able Cove Data Protection on moderni ja luotettava ratkaisu varmuuskopiointiin ja tietojen palautukseen. Se tukee organisaatiomme tietoturvatavoitteita tarjoamalla vahvan suojan datalle, parantamalla palautusvalmiutta ja mahdollistamalla tehokkaan valvonnan.

## 2.3 Tekoälyn turvallinen käyttö ja ohjeistus

Organisaatiossamme on otettu käyttöön Microsoft Copilot, joka on koko henkilökunnan käytössä oleva generatiivinen tekoälyratkaisu. Copilot on tekstipohjainen tekoälyavustaja, joka toimii Microsoftin kaupallisen tietosuojan piirissä, kun käyttäjä kirjautuu sisään organisaatiomme Microsoft-tunnuksillaan. Tämä tarkoittaa, että keskustelut eivät tallennu eikä niitä käytetä tekoälymallien kouluttamiseen, toisin kuin monissa muissa avoimissa tekoälypalveluissa. Copilotin käyttö on mahdollista selaimessa tai Microsoft Edgen sivupalkissa tai muissa Officen ohjelmissa, ja se tukee sekä tekstin että kuvien käsittelyä.

Laadin organisaatiollemme ohjeistuksen, jossa määritellään tekoälyn tietoturvallinen käyttö. Ohjeessa korostin, että Copilotin kanssa voi käsitellä myös yksilöiviä tietoja, koska keskustelut poistuvat automaattisesti istunnon päättyessä. Käyttäjiä ohjeistetaan hyödyntämään Copilotia esimerkiksi sisällöntuotannossa, tietojen analysoinnissa, tekstien muokkauksessa ja koodin tulkinnassa, mutta

samalla muistutetaan suhtautumaan vastauksiin kriittisesti ja tarkistamaan niiden oikeellisuus.

Yleisesti tekoälyn käytössä korostetaan tietoturvan näkökulmasta luotettavien palveluiden valintaa, käyttöehtojen tuntemista ja henkilötietojen välttämistä, ellei käytössä ole suojattu yritysympäristö, kuten Copilot. Tekoälyn käyttöön liittyvä ohjeistus on osa laajempaa tietoturvakulttuurin kehittämistä, jossa työntekijöiden tietoisuus uhkista ja heidän vastuunsa tietoturvan toteutumisessa ovat keskeisessä roolissa.

## 2.4 Henkilöstön tietoturvaohjeistus ja koulutus

Osana organisaatiomme tietoturvan kehittämistä tein koko henkilökunnallemme suunnatun tietoturvaohjeistuksen, jossa käydään läpi meidän toimintaympäristöömme soveltuvat tietoturvalliset käytännöt. Ohjeessa käydään myös läpi yleiset säännöt, joiden avulla varmistetaan tietoturvan toteutuminen arjessa. Ohjeistus toimii käytännön työkaluna, jonka avulla jokainen työntekijä voi ymmärtää, miten oma toiminta vaikuttaa koko organisaation kyberturvallisuuteen.

Ohjeistuksessa käsitellään muun muassa turvallinen salasanojen hallinta ja monivaiheinen tunnistautuminen, sähköpostin ja liitetiedostojen turvallinen käsittely, mobiililaitteiden ja etätyön tietoturva sekä tietojen luokittelu ja käsittely eri suojaustasojen mukaan. Lisäksi ohjeessa annetaan selkeät toimintaohjeet tilanteisiin, joissa epäillään tietoturvaloukkauksia tai havaitaan poikkeavaa toimintaa. Erityisen tärkeää tietoturvallisuuden kannalta on, että työntekijöillä on tieto kyberuhista ja ymmärrys siitä, että heidän tietoturvatietoisuutensa ja osaamisensa ovat keskeisiä suojatekijöitä.

Ohjeistuksen lisäksi järjestin henkilöstölle koulutuksen, jonka tavoitteena oli ylläpitää ja kehittää henkilöstön tietoturvaosaamista. Koulutuksia tulisi olla säännöllisesti ja suunnitelmana on jatkossa hankkia koulutuksia myös ulkopuolisilta tahoilta. Näin varmistamme, että tietoturva ei jää pelkäksi dokumentiksi, vaan siitä tulee osa organisaation arkea ja kulttuuria.

## 2.5 Tietoturvan tason testaaminen ja jatkuva koulutus

Tietoturvan kehittäminen ei ole pelkästään teknisten ratkaisujen käyttöönottoa, vaan siihen kuuluu olennaisena osana myös henkilöstön osaamisen ja tietoisuuden jatkuva kehittäminen. Ihmisten tekemät virheet ovat yhä yksi suurimmista tietoturvariskeistä: esimerkiksi CybSafe:n (2020) mukaan jopa 90 prosenttia tietomurroista johtuu ihmisvirheistä. Tämä korostaa sitä, kuinka tärkeää on panostaa henkilöstön tietoturvatietoisuuteen ja osaamiseen.

Tämän tarpeen pohjalta otimme käyttöön työkalun, joka yhdistää käyttäjien osaamisen testaamisen, simuloidut hyökkäykset sekä kohdennetun mikrokoulutuksen. Käyttäjät altistuvat säännöllisesti simuloiduille tietojenkalasteluyrityksille ja muille kyberuhkia jäljitteleville testeille, jotka on räätälöity organisaation toimialan, koon ja maantieteellisen sijainnin mukaan. Kun käyttäjä lankeaa simuloituun hyökkäykseen, järjestelmä käynnistää automaattisesti lyhyen, tilanteeseen liittyvän mikrokoulutuksen. Näin oppiminen tapahtuu oikea-aikaisesti ja kontekstissa, mikä parantaa tiedon omaksumista ja muistamista.

Jatkuvalla tietoturvakoulutuksella on tutkitusti merkittävä vaikutus organisaation kyberturvallisuuteen. Esimerkiksi 2NS:n (2022) mukaan yli 50 prosentissa hyökkäyksistä hyödynnetään henkilöstön tietämättömyyttä, ja koulutuksen avulla näitä riskejä voidaan merkittävästi vähentää. Koulutuksen vaikutus näkyy paitsi vähentyneinä tietoturvaloukkauksina myös parantuneena reagointikykynä ja tietoturvakulttuurin vahvistumisena.

Ratkaisun hallinta on suunniteltu mahdollisimman kevyeksi: järjestelmä toimii pitkälti automaattisesti, eikä se vaadi jatkuvaa manuaalista ylläpitoa. Ylläpitäjät saavat käyttöönsä selkeät kuukausittaiset raportit, jotka tiivistävät käyttäjien edistymisen, koulutusten suorittamisen ja tietoturvatietoisuuden kehityksen. Näin organisaatio saa konkreettista dataa siitä, miten henkilöstön osaaminen kehittyy ja missä mahdollisia puutteita vielä esiintyy.

Yhteenvetona voidaan todeta, että jatkuva koulutus ja tietoturvatason testaaminen ovat keskeisiä elementtejä organisaation kyberturvallisuuden

vahvistamisessa. Käyttöönotettu työkalu mahdollistaa systemaattisen, ajantasaisen ja käyttäjälähtöisen lähestymistavan, joka tukee koko organisaation tietoturvakulttuurin kehittymistä.

# 3 Microsoft- ja mobiililaiteympäristöjen hallinta

Organisaatiomme IT-ympäristö koostuu pääasiassa Microsoftin pilvipalveluista sekä Android-pohjaisista mobiililaitteista, joita hallitaan useilla eri työkaluilla. Tässä luvussa esittelen keskeiset hallintaratkaisut, joita käytämme Microsoftin O365-ympäristön ja mobiililaitteiden hallintaan. Tavoitteena on kuvata, miten eri hallintatyökalut tukevat organisaatiomme IT-infrastruktuurin ylläpitoa, tietoturvaa ja tehokasta käyttöä.

## 3.1 Microsoft-ympäristön hallintaratkaisut

Organisaatiomme käyttää Microsoftin O365-ympäristöä, joka tarjoaa laajan valikoiman työkaluja hallintaan, viestintään ja yhteistyöhön. Hallintatoiminnot jakautuvat useisiin eri palveluihin, joista keskeisimmät ovat M365 Admin Center, SharePoint, Entra ID ja Intune.

### 3.1.1 Microsoft 365 Admin Center

Microsoft Admin Center on Microsoftin tarjoama selainpohjainen hallintaportaali, jonka avulla IT-asiantuntijat voivat hallita Microsoft 365 -ympäristöä keskitetysti (Microsoft, 2024). Se kokoaa yhteen useita hallintatoimintoja, jotka tukevat käyttäjien, lisenssien, tietoturvan ja palveluiden hallintaa. Admin Center on keskeinen työkalu organisaatiomme IT-henkilöstölle.

Toimiessani IT-vastaavana yhdeksi tärkeimmistä työkaluista olen havainnut käyttäjähallinnan. IT-asiantuntijat voivat lisätä ja poistaa käyttäjiä, muokata käyttöoikeuksia, palauttaa salasanoja ja määrittää rooleja. Tämä mahdollistaa sen, että käyttäjillä on pääsy vain niihin resursseihin, joita he työssään tarvitsevat. Lisäksi Admin Centerin kautta voidaan hallita Microsoft 365 -lisenssejä, kuten

jakaa, siirtää tai poistaa niitä tarpeen mukaan. Tämä auttaa optimoimaan lisenssien käyttöä ja kustannuksia.

Tietoturvan lisääminen on olennainen osa Admin Centerin toimintoja. IT-asiantuntijat voivat ottaa käyttöön monivaiheisen tunnistautumisen (MFA), hallita kirjautumiskäytäntöjä ja seurata tietoturvaraportteja. Näin voidaan havaita poikkeamia, kuten kirjautumisyrityksiä epätavallisista sijainneista, ja reagoida niihin nopeasti. Admin Center integroituu myös muihin Microsoftin tietoturvapalveluihin, kuten Microsoft Defenderiin ja Security & Compliance Centeriin.

Portaalin kautta voidaan hallita myös yksittäisiä Microsoft 365 -palveluita, kuten Outlookia, Teamsia ja SharePointia. Jokaiselle palvelulle on omat hallintanäkymänsä, joiden kautta voidaan säätää asetuksia ja seurata käyttöä. Lisäksi Admin Center tarjoaa reaaliaikaisen näkymän palveluiden tilaan, mikä mahdollistaa nopean reagoinnin mahdollisiin häiriöihin.

Yhteenvetona Microsoft Admin Center tarjoaa IT-asiantuntijalle tehokkaan ja keskitetyn työkalun Microsoft 365 -ympäristön hallintaan. Olen havainnut organisaatiossamme sen parantavan hallinnan tehokkuutta, lisäävän tietoturvaa ja tukevan sujuvaa käyttäjien ja palveluiden hallintaa.

### 3.1.2 SharePointin käyttö ja hallinta

SharePoint on Microsoftin kehittämä alusta, jota käytetään laajasti organisaatioiden sisäiseen viestintään, dokumenttien hallintaan ja tiimityöhön. IT-asiantuntijoiden rooli SharePointin hallinnassa on keskeinen, sillä he vastaavat sivustojen rakenteen suunnittelusta, käyttöoikeuksien määrittelystä sekä tietoturvan varmistamisesta.

Sivustot voidaan rakentaa tiimien tai osastojen tarpeiden mukaan, ja niiden näkymiä voidaan mukauttaa käyttäjäryhmittäin, kuten teemme organisaatiossamme. Esimerkiksi henkilöstöhallinnon (HR) sivustolle voidaan luoda oma kansiorakenne, johon pääsy rajataan vain HR-päällikölle. Tämä toteutetaan luomalla erillinen käyttöoikeusryhmä ja määrittämällä kansiolle yksilölliset

käyttöoikeudet. Näin varmistetaan, että arkaluonteiset henkilötiedot pysyvät suojattuina ja tietosuojavaatimukset täyttyvät.

IT-asiantuntijana hallinnoin myös SharePointin käyttöoikeuksia keskitetysti Microsoft 365 -hallintaportaalin kautta. Hallintaportaalissa voidaan luoda ryhmiä, määrittää rooleja ja valvoa käyttöä, mikä mahdollistaa tehokkaan ja turvallisen tiedonhallinnan.

Lisäksi Power Automate -työkalun avulla voidaan automatisoida erilaisia työnkulkuja. Esimerkiksi tiimit voivat saada automaattisia muistutuksia dokumenttien tarkastuksesta, hyväksynnästä tai määräpäivistä. Tämän olen havainnut vähentävän manuaalista työtä ja parantavan prosessien sujuvuutta. Automatisoidut ilmoitukset voidaan kohdistaa tiettyihin käyttäjäryhmiin, jolloin viestintä on kohdennettua ja ajankohtaista.

Yhteenvetona SharePoint tarjoaa joustavan ja turvallisen alustan, jonka tehokas hallinta edellyttää IT-asiantuntijoilta teknistä osaamista ja ymmärrystä organisaation tarpeista.

### 3.1.3 Entra ID ja Intune -identiteetti- ja laitehallinta

Microsoft Entra ID ja Microsoft Intune muodostavat yhdessä kattavan ratkaisun organisaation identiteetin- ja laitehallintaan. IT-asiantuntijan näkökulmasta nämä työkalut mahdollistavat turvallisen, automatisoidun ja skaalautuvan hallintamallin, joka tukee nykyaikaisia hybridityöympäristöjä.

Entra ID vastaa käyttäjien ja ryhmien identiteetinhallinnasta. Sen avulla hallitaan kirjautumista, käyttöoikeuksia ja monivaiheista tunnistautumista (MFA). Microsoftin mukaan MFA:n avulla voidaan estää jopa 99,9 prosenttia käyttäjätilejä uhkaavista hyökkäyksistä (Maynes, 2019). Yksi keskeinen toiminto on Conditional Access, jonka avulla voidaan määrittää tarkkoja ehtoja pääsylle eri palveluihin. Esimerkiksi pääsy voidaan sallia vain tietyiltä laitteilta, tietyistä sijainneista tai jos laite täyttää tietyt tietoturvavaatimukset. Tämä mahdollistaa joustavan, mutta turvallisen pääsynhallinnan ilman tarvetta manuaaliseen valvontaan.

Microsoft Intune täydentää kokonaisuutta laitehallinnan näkökulmasta. Sen avulla IT-asiantuntijat voivat määrittää ja ottaa käyttöön laitekäytäntöjä, jotka koskevat esimerkiksi VPN-yhteyksien määrityksiä, salausasetuksia, sovellusten automaattista asennusta ja tietoturvapolitiikkojen soveltamista. Uudet laitteet voidaan liittää automaattisesti organisaation hallintaan, jolloin ne saavat tarvittavat ohjelmistot ja asetukset ilman manuaalista konfigurointia.

Yhdessä Entra ID ja Intune tarjoavat IT-tiimille tehokkaan ja ennakoivan hallintamallin, jossa käyttäjien identiteetit ja laitteet ovat jatkuvassa valvonnassa ja hallinnassa. Tämä vähentää riskejä, parantaa käyttökokemusta ja vapauttaa IT-resursseja muihin kehitystehtäviin.

## 3.2 Mobiililaitteiden hallinta ja käytännöt

Tässä luvussa esittelen, miten organisaatiossamme hallitaan Android-pohjaisia mobiililaitteita eri menetelmillä. Käytössä on sekä keskitettyjä hallintaratkaisuja että valmistajakohtaisia ja komentorivipohjaisia työkaluja, joiden avulla voidaan vastata erilaisiin hallintatarpeisiin ja vikatilanteisiin.

### 3.2.1 MobiControl Android-laitteiden hallinnassa

MobiControl on SOTI:n kehittämä mobiililaitteiden hallintaratkaisu (Mobile Device Management, MDM), jonka avulla voimme hallita, valvoa ja suojata mobiililaitteitamme keskitetysti. Se tukee useita käyttöjärjestelmiä, kuten Android, iOS ja Windows, mutta organisaatiossamme sitä käytetään erityisesti Android-pohjaisten mobiiliskannereiden hallintaan. MobiControl mahdollistaa laitteiden etähallinnan, sovellusten jakelun, asetusten määrittelyn sekä tietoturvapolitiikkojen soveltamisen ilman, että laitteita tarvitsee käsitellä fyysisesti.

MobiControlin avulla voidaan esimerkiksi rekisteröidä uusia laitteita, määrittää automaattisesti asennettavat sovellukset, rajoittaa laitteen käyttöä vain tiettyihin toimintoihin sekä seurata laitteiden tilaa ja sijaintia reaaliaikaisesti. Esimerkiksi meidän kulunvalvontasovelluksemme on lukittu Android Kiosk -tilaan, jossa käyttäjä ei pääse poistumaan sovelluksesta. Lisäksi järjestelmä tukee skriptien

käyttöä, joiden avulla voidaan automatisoida hallintatehtäviä, kuten laitteen nimeäminen, verkkoasetusten määrittely tai ongelmatilanteiden ratkaisu. Tämä tekee MobiControlista tehokkaan ja joustavan työkalun erityisesti suurten laitemäärien hallintaan.

### 3.2.2 Laitteiden omat hallintatyökalut

Monilla mobiiliskannereiden valmistajilla on omat hallintasovelluksensa, joilla voidaan säätää laitteiden asetuksia tarkasti. Näihin kuuluu esimerkiksi skannerin herkkyyden säätö, näppäinten ohjelmointi ja käyttöliittymän mukautus. Esimerkkejä tällaisista työkaluista ovat Zebra StageNow ja Honeywellin Enterprise Provisioner.

Uuden laitteen käyttöönotossa on myös huomioitavaa, että joissakin tapauksissa laitteen omia asetuksia täytyy säätää manuaalisesti, jotta ne toimivat yhteen organisaation oman sovelluksen kanssa. Tämä voi olla tarpeen erityisesti silloin, kun MobiControl-profiilista ei löydy kyseiselle laitteelle sopivaa asetusta.

### 3.2.3 Komentorivipohjaiset hallintamenetelmät

ADB (Android Debug Bridge) on komentorivipohjainen työkalu, jonka avulla voidaan hallita Android-laitteita tietokoneen kautta USB-yhteydellä tai langattomasti. ADB on osa Android SDK -kehitystyökaluja ja se tarjoaa tehokkaan tavan suorittaa komentoja laitteella, siirtää tiedostoja, asentaa sovelluksia, ottaa lokitietoja ja hallita laitetta ilman fyysistä käyttöä.

ADB:n käyttö edellyttää, että laitteessa on kehittäjätila ja USB-virheenkorjaus (USB debugging) aktivoituna. Tyypillisiä ADB-komentoja ovat:

- adb devices – listaa yhdistetyt laitteet

- adb install *.apk – asentaa APK-tiedoston laitteeseen

- adb push tiedosto /kohdepolku – siirtää tiedoston tietokoneelta laitteeseen

- adb pull /lähdepolku – siirtää tiedoston laitteesta tietokoneelle

- adb shell – avaa komentorivin laitteen sisällä

- adb logcat – näyttää laitteen lokitiedot reaaliajassa

ADB on erityisen hyödyllinen tilanteissa, joissa laite ei ole täysin toimintakykyinen, mutta siihen saadaan vielä yhteys. Näitä tilanteita varten meillä on laitteisiimme tarkoitetut tehdasasetuksiin nollaavat apk-tiedostot.

Recovery-tila on Android-laitteen erillinen käynnistysympäristö, joka toimii käyttöjärjestelmästä riippumatta. Se mahdollistaa laitteen huoltotoimenpiteet, kuten tehdasasetusten palautuksen, päivitysten asentamisen SD-kortilta tai ADB:n kautta sekä välimuistin tyhjentämisen. Recovery-tila on hyödyllinen erityisesti silloin, kun laite ei käynnisty normaalisti tai kun halutaan suorittaa järjestelmän korjaustoimia ilman pääsyä käyttöliittymään.

Fastboot on toinen matalan tason tila, jota käytetään erityisesti laitteen käynnistyslataimen (bootloader) hallintaan. Fastboot-tilassa voidaan suorittaa komentoja, jotka liittyvät laitteen ohjelmiston syvempään hallintaan, kuten käyttöjärjestelmän osien (boot, recovery, system) päivittämiseen tai laitteen lukituksen avaamiseen.

Fastboot-komentoja ovat esimerkiksi:

- fastboot devices – tunnistaa fastboot-tilassa olevan laitteen

- fastboot flash recovery recovery.img – asentaa uuden recovery-osion

- fastboot oem unlock – avaa laitteen bootloaderin (jos sallittu)

- fastboot reboot – käynnistää laitteen uudelleen normaalisti

Fastboot-tila on erityisen hyödyllinen silloin, kun käyttöjärjestelmä on vioittunut tai halutaan asentaa laitteeseen uusi ohjelmistoversio kokonaan.

### 3.2.4 Hallintamenetelmien vertailu ja käyttökohteet

Eri hallintamenetelmillä on omat vahvuutensa ja rajoitteensa. MobiControl soveltuu parhaiten keskitettyyn ja skaalautuvaan hallintaan, kun taas valmistajien omat työkalut tarjoavat tarkkaa laitekohtaista säätöä. Komentorivipohjaiset menetelmät ovat hyödyllisiä erityisesti vikatilanteissa ja laitteiden palautuksessa. Käytännön tilanteissa valitaan menetelmä sen mukaan, mikä on tehokkain ja turvallisin ratkaisu kyseiseen tarpeeseen.

# 4 Tekninen asiantuntijuus projektissa

Minut kutsuttiin mukaan asiakasprojektiin, jonka tavoitteena oli suunnitella ja toteuttaa autonomisesti toimiva kulunvalvontaportti. Projektin tarkoituksena oli kehittää järjestelmä, joka mahdollistaa vierailijoiden pääsyn alueelle ilman manuaalista valvontaa. Portin tuli aueta automaattisesti, kun vieras esittää sisäänpääsyyn oikeuttavan lipun.

Käytännössä järjestelmä rakennettiin siten, että vieras esittää lippunsa viivakoodin asiakaskioskin viivakoodinlukijalle. Kun viivakoodi on luettu ja todettu kelvolliseksi, portti avautuu automaattisesti. Tämä edellytti sekä laitteiston että ohjelmiston yhteensovittamista, jotta viivakoodinlukija, portin ohjausyksikkö ja taustajärjestelmä toimivat saumattomasti yhteen.

Projektissa pääsin seuraamaan ja osallistumaan käytännön suunnittelutyöhön, yhdessä asiakkaan ja muiden yhteystyökumppaneiden kanssa ja vaikuttamaan järjestelmän toimintavarmuuteen sekä käyttäjäystävällisyyteen.

## 4.1 Suunnitteluvaihe ja tekniset lähtökohdat

Projekti käynnistyi, kun minulle kerrottiin lyhyesti, että organisaatiossamme ollaan aloittamassa asiakasprojekti, joka liittyy kulunvalvonnan ratkaisun

toteuttamiseen. Sain kutsun suunnittelupalaveriin, johon osallistuisivat asiakasyrityksen edustajat, meidän organisaatiomme sekä yhteistyökumppanimme, joka vastaa kulunvalvontasovelluksen teknisestä kehityksestä.

Minulle kerrottiin, että roolini projektissa olisi seurata sen etenemistä, toimia yhteyshenkilönä meidän organisaatiomme ja sovelluskehittäjän välillä sekä osallistua suunnitteluun. Meillä oli jo entuudestaan käytössä oma taustajärjestelmä sekä kulunvalvontasovellus, mutta koska ohjattava portti toimii autonomisesti, näihin järjestelmiin oli tehtävä muutoksia, jotta ne tukisivat uudenlaista toimintalogiikkaa.

Ensimmäisessä palaverissa käytiin läpi projektin aikataulu ja määriteltiin, mitä tietoja ja toimenpiteitä tarvitaan eri osapuolilta. Meidän organisaatiomme kehittäjät vastaavat tarvittavista muutoksista taustajärjestelmäämme ja testaavat niiden toimivuuden. Tämän jälkeen toimitamme tarvittavat tiedot yhteistyökumppanillemme, joka vastaa asiakaspäätteen kehityksestä ja toimituksesta.

Yhteistyökumppani puolestaan on suoraan yhteydessä asiakasyritykseen asennukseen liittyvissä asioissa ja vastaa siitä, miten ohjattava portti liitetään asiakaspäätteeseen. Palaverissa sovittiin myös, että kun nämä alkuvaiheen toimet on saatu liikkeelle, järjestetään erillinen kehityspalaveri meidän ja teknisen toteutuksen tekevän kumppanin kesken. Tässä palaverissa on tarkoitus suunnitella tarkemmin asiakaspäätteen toiminnallisuudet ja varmistaa, että ratkaisu vastaa asiakkaan tarpeita.

## 4.2 Projektin edistyminen ja seurannan menetelmät

Projektin edetessä sovimme, että asiakasyritys luo yhteisen Microsoft Teams -työtilan, johon kutsutaan mukaan asiakasyrityksen edustajat, meidän organisaatiomme sekä teknisestä toteutuksesta vastaava yhteistyökumppanimme. Tarkoituksena oli käyttää tätä työtilaa projektin ensisijaisena viestintä- ja dokumentointikanavana. Käytännössä työtilan luomisessa kuitenkin kesti, minkä seurauksena keskustelu siirtyi osittain sähköpostiketjuihin ja meidän organisaatiomme sisällä Slackiin.

Pidimme myös erillisen palaverin yhteistyökumppanimme kanssa, jossa kävimme tarkemmin läpi, mitä portilta halutaan ja miten sen tulisi toimia. Koin, että heidän ohjelmistosuunnittelijansa ei täysin ymmärtänyt toivottuja toiminnallisuuksia, ja hän esitti useita tarkentavia kysymyksiä. Pyrin tämän vuoksi esittämään mahdollisimman selkeästi, mitä sovelluksen uuteen versioon tarvitaan. Huomasin myös, että aiemmat meiltä tulleet toiveet eivät olleet välittyneet ohjelmistosuunnittelijalle riittävän ymmärrettävästi. Tämän vuoksi kävimme yhdessä läpi, mitkä toiminnot ovat toteutettavissa ja mitkä eivät ole teknisesti tai ajallisesti järkeviä tässä vaiheessa projektia.

## 4.3 Alustava kehitys ja toiminnallinen testaus

Kun suunnitteluvaiheen keskustelut oli käyty ja alustavat vaatimukset määritelty, siirryttiin kehitystyön alkuvaiheeseen. Meidän organisaatiomme kehittäjät tekivät taustajärjestelmäämme tarvittavia muutoksia, joita asiakasyrityksen porttiratkaisu edellytti. Testasin uusia ja muokattuja toimintoja järjestelmämme testiympäristössä ja huomasin, etteivät muutokset toimineet suoraan Android-sovelluksessamme.

Otin yhteyttä yhteistyökumppanin kehittäjiin ja selitin, miten ja miksi kyseisiä toimintoja tarvitaan. Tämän jälkeen he lisäsivät puuttuvat ominaisuudet myös sovelluksen uuteen versioon. Seurasin kehitystyön etenemistä ja pidin aktiivisesti yhteyttä sekä sisäisiin kehittäjiimme että yhteistyökumppaniin, joka vastasi asiakaspäätteen ohjelmiston toteutuksesta. Toimitin heille myös testitunnukset ja loin erillisen testiympäristön, jossa he pystyivät testaamaan sovelluksen toimintaa käytännössä.

## 4.4 Muutokset kesken kehitystyön ja kohdatut haasteet

Kehitystyön aikana asiakasyritykseltä tuli joitakin lisätoiveita ja mahdollisia muutoksia kesken projektin. Kävimme näistä keskustelun sisäisesti ja yhteistyökumppanin kanssa, ja päädyimme siihen, että jatkamme alkuperäisen suunnitelman mukaisesti, jotta aikataulu ja kokonaisuuden hallinta säilyvät hallinnassa.

Yksi merkittävä haaste liittyi käyttöliittymän suunnitteluun. Käyttöliittymäsuunnittelijamme sai kiireellisen työpyynnön, mutta vain puutteelliset tiedot asiakaspäätteen näytön asettelusta. Tämän seurauksena he tekivät nopeasti ensimmäisen version käyttöliittymästä. Kun kuulin, ettei suunnittelijoilla ollut varmuutta näytön suunnasta, otin heti yhteyttä yhteistyökumppaniimme ja selvisi, että näyttö olikin vaakasuunnassa eikä pystysuunnassa, kuten oli oletettu. Tämän vuoksi käyttöliittymä jouduttiin osittain suunnittelemaan uudelleen.

Koska käyttöliittymä jouduttiin tekemään uudestaan, sen lopullinen versio saatiin toimitettua yhteistyökumppanillemme huomattavan myöhään. Tämä puolestaan aiheutti sen, että heillä jäi hyvin vähän aikaa käyttöliittymän implementointiin ennen sovittuja testausvaiheita. Viivästys vaikutti myös testauksen aikatauluun ja toi lisäpainetta projektin loppuvaiheeseen.

Projektin aikana ilmeni myös viestintään liittyviä haasteita. Meiltä oli mukana useampi henkilö, mutta osa keskusteluista käytiin erillisissä sähköpostiketjuissa, joissa eivät aina olleet mukana ne henkilöt, joilla oli paras ymmärrys projektin teknisistä yksityiskohdista. Tämä johti hetkellisiin väärinymmärryksiin asiakasyrityksen kanssa ja sisäiseen tuplavarmisteluun. Lisäksi minut kutsuttiin kesken erään ison sisäisen palaverin mukaan, koska minut oli mahdollisesti unohdettu alkuperäisestä kutsusta tai kokouksen järjestäjä ei tiennyt tarkasti vastuualueestani projektissa.

## 4.5 Asennus, järjestelmätestaus ja käyttöönotto

Asennuksen aikataulu venyi alkuperäisestä suunnitelmasta noin viikolla. Viivästykseen vaikutti se, että yhteistyökumppanillamme oli vielä kehitystyö kesken, eikä asiakasyrityksen tiloissa ollut vielä vedetty kaikkia tarvittavia sähköjä. Asiakaspäätteen fyysinen asennus saatiin kuitenkin tehtyä edellisellä viikolla ennen käyttöönottoa, mutta portin liitäntä saatiin valmiiksi vasta käyttöönottoa edeltävänä päivänä.

Testausaikaa jäi tämän vuoksi hyvin niukasti – ehdimme tehdä vain muutaman tunnin toiminnallisen testauksen ennen käyttöönottoa. Tämä osoittautui

riittämättömäksi, sillä käyttöönoton aamuna kohdattiin heti ensimmäinen ongelmatilanne: laite ei toiminut odotetusti. Lähdin nopeasti paikan päälle selvittämään tilannetta. Onneksi ongelma saatiin ratkaistua nopeasti yhteistyössä sovelluskehittäjän kanssa. Päättelimme, että ongelma johtui laitteen pitkästä käynnissä oloajasta, mikä ei ollut tullut esiin aiemmassa testauksessa, koska pitkäaikaistestausta ei ehditty tehdä.

Lisäksi käyttöönoton yhteydessä ilmeni puutteita päätteen ja portin käytännön toiminnassa sekä opastuksessa. Nämä puutteet johtivat siihen, että joitakin toimintoja jouduttiin muuttamaan jälkikäteen. Osa näistä asioista oli jäänyt huomiotta, koska suunnitteluvastuu oli osittain ollut sovelluskehittäjällä, eikä kaikkia käytännön yksityiskohtia ollut käyty riittävän tarkasti läpi etukäteen.

Dokumentoin tarkasti portin toiminnan ja laadin siitä ohjeistukset asiakasyritykselle. Lisäksi lähetin yhteistyökumppanille korjauslistan, jossa kuvattiin havaitut ongelmat ja tarvittavat muutokset.

## 4.6 Virheiden korjaus ja jatkokehityksen huomiointi

Käyttöönoton jälkeen kävin yhteistyökumppanin sovelluskehittäjän kanssa läpi havaitut ongelmat ja pohdimme niihin yhdessä toimivia ratkaisuja. Yksi keskeinen ongelma liittyi laitteen pitkään käynnissä oloaikaan, joka aiheutti toimintahäiriöitä. Ratkaisuksi päätimme, että laite asetetaan käynnistämään itsensä automaattisesti joka yö. Tämä on nopea ja kustannustehokas muutos, joka todennäköisesti ehkäisee vastaavia ongelmia jatkossa.

Toinen havaittu kehityskohde liittyi lukijan luentanopeuteen. Aiemmin portin piti sulkeutua kokonaan ennen kuin seuraava lippu voitiin lukea, mikä hidasti käyttöä. Sovelluskehittäjä muutti toimintalogiikkaa siten, että lippuja voidaan nyt lukea nopeammin peräkkäin, ja portti pysyy auki vain viimeisimmästä luennasta määritellyn ajan. Tämä paransi käyttökokemusta merkittävästi.

Jatkokehityksen osalta pohdimme myös, miten toteutusta voitaisiin hyödyntää tulevaisuudessa muissa kohteissa. Tämän vuoksi sovellukseen lisättiin

säätöpainikkeita, joilla voidaan hallita erilaisia viiveitä ja portin ohjausta. Näiden avulla järjestelmää voidaan mukauttaa erilaisiin käyttötarpeisiin ilman, että koko sovellusta tarvitsee muokata uudelleen.

## 4.7 Projektin onnistumisen arviointi ja vertailu

Projekti saatiin päätökseen aikataulussa ja tärkeimmät toiminnot olivat valmiina käyttöönottoon. Alkuperäisessä aikataulussa oli varauduttu mahdollisiin viivästyksiin, mikä osoittautui tarpeelliseksi, sillä kehitystyössä ja asennuksessa ilmeni odottamattomia viiveitä. Tämä osoittaa, kuinka tärkeää ohjelmistoprojekteissa on varata riittävästi lisäaikaa mahdollisten ongelmien ja muutostarpeiden varalle – tutkimusten mukaan yli puolet ohjelmistoprojekteista myöhästyy tai ylittää budjetin (Project.co, 2024).

Projektin seurannassa ilmeni kuitenkin useita kehityskohteita. Vastuualueet eivät olleet kaikilta osin selkeitä, ja tiedonkulussa oli puutteita. Yhteistä viestintäkanavaa ei saatu käyttöön ajoissa, ja keskustelu hajaantui eri sähköpostiketjuihin ja sisäisiin viestintäalustoihin. Tämä johti hetkellisiin väärinymmärryksiin ja epäselvyyksiin asiakasyrityksen suuntaan. Jatkossa olisi ollut tärkeää määrittää projektijohtaja, laatia projektin seurantataulu ja nimetä vastuuhenkilöt viestinnän seuraamiseen. Selkeä viestintäsuunnitelma ja roolitus ovat keskeisiä onnistuneessa projektinhallinnassa (Parallel Project Training, 2019).

Suunnitteluvaiheeseen olisi myös pitänyt varata enemmän aikaa ja resursseja. Asiantuntijoita olisi pitänyt hyödyntää laajemmin, ja yhteistyökumppanilta olisi pitänyt tilata tarkasti määritellyt toiminnot sen sijaan, että heille jätettiin tilaa tehdä omia tulkintoja. Tämä olisi todennäköisesti vähentänyt käyttöönoton jälkeisiä korjauksia ja nopeuttanut kehitystyötä. Hyvin toteutettu vaatimusanalyysi ja selkeä suunnittelu ovat keskeisiä tekijöitä ohjelmistoprojektien onnistumisessa (InformaTecDigital, 2024).

Lisäksi käyttöliittymäsuunnittelijat olisi pitänyt ottaa mukaan projektiin aikaisemmassa vaiheessa ja varmistaa, että heillä on kaikki tarvittavat tiedot

suunnittelutyön tueksi. Tämä olisi voinut estää käyttöliittymän uudelleensuunnittelun ja siihen liittyvän viivästyksen.

Vaikka projekti saavutti tavoitteensa, sen aikana opitut asiat osoittavat, kuinka tärkeää on panostaa suunnitteluun, viestintään ja selkeään vastuunjakoon. Näiden osa-alueiden kehittäminen parantaa tulevien projektien sujuvuutta ja lopputuloksen laatua.

# 5 Pohdinta

Tietoturvan kehittämisprojektissa havaitsin, kuinka tärkeää on yhdistää tekniset ratkaisut, kuten VPN, pääkäyttäjäoikeuksien hallinta ja varmuuskopiointi, henkilöstön koulutukseen ja selkeisiin ohjeisiin. Ymmärsin, että tietoturva ei ole vain järjestelmien suojaamista, vaan myös ihmisten toimintaa – ja juuri siinä piilee usein suurin riski. Opin laatimaan ohjeistuksia, järjestämään koulutuksia ja hyödyntämään työkaluja, jotka tukevat jatkuvaa oppimista ja tietoturvatietoisuuden kehittymistä. Kokonaisuutena tietoturva on jatkuva prosessi, jossa teknologia ja käyttäjät toimivat yhdessä organisaation suojaksi.

Microsoft ja mobiilihallinta ympäristöjä käyttäessä sekä niistä ohjeita tehdessä olen oppinut, kuinka tärkeää on hallita käyttäjiä ja laitteita keskitetysti ja turvallisesti. Microsoftin työkalut, kuten Admin Center, Entra ID ja Intune, auttoivat ymmärtämään, miten identiteetti- ja laitehallinta tukevat tietoturvaa ja tehokasta työskentelyä. Mobiililaitteiden hallinnassa opin hyödyntämään MobiControlia, valmistajien työkaluja ja komentorivipohjaisia menetelmiä eri tilanteisiin. Kokemukseni mukaan oikean työkalun valinta riippuu tarpeesta – ja että hyvä hallinta vaatii sekä teknistä osaamista että käytännön ymmärrystä.

Asiakasprojektin aikana opin, mitä tekninen asiantuntijuus käytännössä tarkoittaa – ei pelkästään teknistä osaamista, vaan myös viestintää, ongelmanratkaisua ja yhteistyötä eri osapuolten välillä. Selkeä suunnittelu, vastuunjako ja dokumentointi osoittautuivat keskeisiksi projektin sujuvuuden kannalta. Käytännön tilanteet, kuten käyttöliittymän uudelleensuunnittelu ja viestintäkatkokset, opettivat minulle, miten pienetkin epäselvyydet voivat vaikuttaa lopputulokseen. Opin

myös reagoimaan nopeasti ongelmatilanteisiin ja viemään asioita eteenpäin yhteistyössä muiden kanssa. Kokonaisuutena projekti kehitti taitojani toimia vastuullisessa roolissa teknisenä linkkinä eri sidosryhmien välillä.

Kokonaisuutena opinnäytetyöni aikana syvensin ymmärrystäni siitä, miten teknologia, prosessit ja ihmiset muodostavat yhdessä toimivan ja turvallisen IT-ympäristön. Opin yhdistämään teknisiä ratkaisuja käytännön ohjeistuksiin, kehittämään hallintakäytäntöjä ja toimimaan asiantuntijana yhteistyöprojektissa eri toimijoiden kesken. Työ vahvisti osaamistani sekä teknisellä että viestinnällisellä tasolla ja antoi valmiuksia toimia vastuullisissa rooleissa tulevaisuudessa. Jatkossa haluan kehittää osaamistani erityisesti tietoturvan, projektisuunnittelun ja -johtamisen osa-alueilla, sillä koen niiden olevan keskeisiä taitoja IT-asiantuntijana kehittymisessä.

## Lähteet

2NS. 2022. Palvelut. https://www.2ns.fi/palvelut/koulutus/

CybSafe. 2020. Human error to blame for 9 in 10 UK cyber data breaches in 2019. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

IBM. What is database security? https://www.ibm.com/think/topics/database-security

Ivaska, I. 2025. Tietoturva tekoälyn aikakaudella. Teoksessa Teknologiapedagogiikkaa kielten opetukseen. Turun yliopisto. https://www.utupub.fi/bitstream/handle/10024/180143/Veivo_Makinen_Teknologiapedagogiikkaa_27022025.pdf?sequence=1#page=34

InformaTecDigital. 2024. Ohjelmiston käyttöönotto: Tehokkaat strategiat riskien minimoimiseksi ja hyötyjen maksimoimiseksi. https://informatecdigital.com/fi/ohjelmiston-toteutus/

Kyberturvallisuuskeskus. 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Maynes, Melanie. 2019. One simple action you can take to prevent 99.9 percent of attacks on your accounts. Microsoft. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Microsoft. 2024. What is Windows Admin Center? https://learn.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/what-is

Parallel Project Training. 2019. Why should a project manager use a communication plan? https://www.parallelprojecttraining.com/blog/feedback-please-communication-plan-practice-question/

Project.co. 2024. Project Management Statistics: Everything You Need to Know (2024). https://www.project.co/project-management-statistics/

Traficom. 2025. Sähköisen viestinnän tietoturva. Liikenne- ja viestintävirasto. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoisen-viestinnan-tietoturva

Von Solms, R., & Van Niekerk, J. 2013. From information security to cyber security. Computers & Security. https://doi.org/10.1016/j.cose.2013.04.004