HAMK
Hämeen ammatti-
korkeakoulu

Erillistyöaseman asennus ja dokumentointi

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

Syksy 2023

Mikko Hannukka

HAMK
Hämeen ammatti-
korkeakoulu

Tietojenkäsittelyn koulutus
Tekijä Mikko Hannukka
Ohjaaja Pentti Ojaniemi

Tiivistelmä
Vuosi 2023

Työn nimi Erillistyöaseman asennus ja dokumentointi

Opinnäytetyön aiheena on erillistyöaseman asennus ja dokumentointi. Opinnäytetyössä asennettavalla erillistyöasemalla asiakas käsittelee turvallisuusluokitukseltaan IV olevia asiakirjoja. Opinnäytetyön toimeksiantaja oli Mikropolix Oy.

Opinnäytetyön tietopohja nojaa vahvasti tietoturvallisuuden auditointityökalu Katakriin. Katakrin määritykset ohjaavat erillistyöaseman asennusta. Keskeisessä osassa ovat BIOSin ja käyttöjärjestelmän koventaminen. Opinnäytetyössä kuvataan tarkasti erillistyöaseman asennusprosessi. Erillistyöaseman käyttöjärjestelmän ja ohjelmien päivittäminen esitellään omassa luvussaan. Tutkimusaineisto kerättiin päiväkirjan avulla asennuksen aikana. Opinnäytetyö on toiminnallinen.

Asennetusta opinnäytetyöstä täytettiin tietojärjestelmän turvallisuusseloste, josta ilmenevät toteutetut kovennukset. Opinnäytetyössä asennettava erillistyöasema auditoitiin Puolustusvoimien turvatarkastajan toimesta hyväksytysti. Asiakas oli tyytyväinen työasemaan, täytettyihin asiakirjoihin ja päivityksiin ja ylläpitoon liittyviin ohjeisiin.

Avainsanat Katakri, erillistyöasema, turvallisuusluokitus
Sivut 22 sivua ja liitteitä 8 sivua

HAMK
Hämeen ammatti-
korkeakoulu

Degree Programme in Business Information Technology Abstract
Author Mikko Hannukka Year 2023
Subject Installation and documentation of a standalone workstation
Supervisors Pentti Ojaniemi

The purpose of the thesis was installing a standalone secure workstation. With the workstation customer handling restricted documents. The restricted documents security class is IV (TL IV). The thesis focuses on workstations informational security. The necessary installation-related documents can be found in the attachment. The research questions are: How to setup standalone workstation that is used for processing restricted documents? What is restricted document? How to update virus databases when workstation is not online?

The thesis introduces cyber security's audition tool Katakri. All the Defense forces documents are based on Katakri. The thesis shows BIOS and operating system hardening. The thesis presents the Finnish national safety classes. This is practical thesis, and the primary research method was diary. Diary was written during the installation.

The research demonstrates installation of a standalone secure workstation. Whole secure environment, including workstation, was audited by Defence forces security officer. Audition was passed and customer was happy about result. After all there were few problems during installation, but the result was great.

Keywords Standalone workstation, hardening, restricted document.
Pages 22 pages and appendices 8 pages

Sanasto

Katakri	Tietoturvallisuuden auditointityökalu viranomaisille
BitLocker	Windowsin salaustekniikka
TPM	Trusted Platform Module -turvapiiriä käytetään tietokoneen suojauksen parantamiseen. Sitä käyttävät palvelut muun muassa BitLocker salausavainten turvalliseen luomiseen ja tallentamiseen.
GPO	Group Policy Object, ryhmäkäytännöillä tehdyt määrittelyt tallentuvat ryhmäkäytäntöobjekteiksi
Policy Analyzer	Työkalu, jolla analysoidaan ja verrataan ryhmäkäytäntöobjekteja
BIOS	Basic Input-Output System. Tietokoneohjelma, joka etsii ja lataa käyttöjärjestelmän keskusmuistiin sekä käynnistää sen tietokoneen käynnistyessä. BIOS hoitaa myös matalan tason kommunikoinnin tietokonelaitteiston kanssa.

Sisällys

Kuvat, komennot, ohjelmakoodit, taulukot ja kaavat

Liitteet

1 Johdanto

Opinnäytetyössä kuvataan erillistyöaseman asennusprosessi. Erillistyöasemalla tarkoitetaan kaikista tietoverkoista pysyvästi erotettua tietokonetta. Erillistyöaseman suojaamisessa tulee huomioida sen koko elinkaari. Erillistyöasemaa käytetään turvallisuusluokaltaan IV olevien asiakirjojen käsittelyyn. Asiakirjojen turvallisuusluokitusten määritelmät esitellään tarkemmin opinnäytetyössä.

Minun työpaikallani Mikropolix Oy:ssä vastaavaa asennusta ei ole koskaan aikaisemmin tehty, joten projekti on mielenkiintoinen. Puolustusvoimien meille toimittavat ohjeet ja asiakirjat määrittävät lopputuloksen, mutta toteutustapa on suhteellisen vapaa. Toteutus tapahtuu osin kokeilemisen ja erehtymisen kautta. Koska erillistyöasema tullaan auditoimaan puolustusvoimien toimesta, lopputulos täytyy olla tehtynä tarkasti ja huolellisesti. Prosessin aikana pääsee toteuttamaan ja oppimaan uusia asioita, joita ei ole aikeisemman työurani aikana päässyt tekemään.

Koska työnantajaltani tilattiin pelkästään työaseman teknillinen asennus, opinnäytetyöstä rajataan pois erillistyöaseman fyysinen turvallisuus.

Vastaavanlaista asennusdokumentointia ei ole julkisesti saatavilla, joten opinnäyte tulee vastaamaan seuraaviin kysymyksiin:

- Kuinka asennetaan erillistyöasema, jolla käsitellään turvallisuusluokan IV asiakirjoja?
- Mitä tarkoitetaan, kun asiakirjan turvallisuusluokitus on IV?
- Kuinka haittaohjelmatorjuntaohjelmisto päivitetään, kun tietokone ei ole verkossa?

2 Erillistyöaseman asennuksen määritykset

Tässä luvussa käydään läpi määritykset, jotka on huomioitava erillistyöaseman asennuksessa. Erillistyöaseman asennus perustuu puolustusvoimien asiakirjaan ”Erillistyöaseman toteutus ja dokumentointi” (Liite 2), jonka perustana on tietoturvallisuuden auditointityökalu Katakri. Asiakirja toimii myös pohjana, josta luodaan erillistyöaseman tietojärjestelmän turvallisuusseloste.

Turvallisuusselosteeseen kirjataan toteutetut kovennukset. Koventamisella tarkoitetaan laitteiden, ohjelmistojen ja käyttöjärjestelmän teknisen hyökkäyspinta-alan pienentämistä. Tämä toteutetaan esimerkiksi poistamalla tarpeettomia sovelluksia ja palveluita. Turvallisuusselosteessa suluissa olevat kirjainnumeroyhdistelmät viittaavat suoraan Katakriin. Esimerkiksi I09 viitta kohtaan Monitasoinen suojaaminen - haittaohjelmasuojaus. Asiakirja on luotu jo vuonna 2017, mutta puolustusvoimien ohjeistuksen mukaan sitä sovelletaan edelleen. Käyttöjärjestelmän ja BIOSin kovennukset esitellään omissa alaluvuissaan.

2.1 Katakri – tietoturvallisuuden auditointityökalu viranomaisille

Katakri on viranomaisten auditointityökalu, jota voidaan käyttää kohdeorganisaation kykyyn suojata salassa pidettävää tietoa. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset.

Ensimmäinen Katakri on julkaistu vuonna 2009. Tässä keskitytään neljänteen versioon, joka on julkaistu vuonna 2020. Tämän version hallinnointi ja päivitystyö on ollut Kansallisen turvallisuusviranomaisen (NSA) vastuulla.

Katakri on jaettu kolmeen osa-alueeseen: turvallisuusjohtaminen (T), fyysinen turvallisuus (F), Tekninen tietoturvallisuus (I). Opinnäytetyössä pääpaino on teknisessä tietoturvallisuudessa.

2.1.1 Turvallisuusjohtaminen (T) ja fyysinen turvallisuus (F)

Turvallisuusjohtaminen-osiossa käsitellään vaatimuksia, joilla varmistetaan, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä ja turvaluokiteltua tietoa käsittelevä henkilöstö toimii asianmukaisesti. Osio jakautuu kahteen osaan: hallinnollinen tietoturvallisuus ja henkilöstöturvallisuus. Hallinnollinen tietoturvallisuus osiossa määritellään organisaation turvallisuusperiaatteiden vaatimukset. Siihen sisältyy myös tietoturvallisuuden vastuiden määrittäminen, riskien arviointi ja turvallisuusohjeistus. (Kansallinen turvallisuusviranomainen, 2020)

Henkilöstöturvallisuus-osiossa käsitellään henkilöstöön liittyviä turvallisuusasioita. Työsuhteen eri vaiheissa pitää huomioida erilaisia toimenpiteitä. Esimerkiksi työsuhteen alussa tehdään henkilöstöselvitykset ja määritellään käyttö- ja pääsyoikeudet. Työsuhteen päättyessä on hyvä muistuttaa salassapito- ja vaitiolovelvollisuuksista. Henkilön luotettavuus selvitetään turvallisuusselvityksellä, joka haetaan joko Suojelupoliisilta tai Pääesikunnalta riippuen siitä minkälaisia tietoja käsitellään. Turvallisuuskoulutus on myös määritelty henkilöstöturvallisuus osiossa. Turvallisuuskoulutuksella varmistetaan, että henkilöstöllä on riittävä tuntemus tiedonhallinnasta, tietojenkäsittelystä, salassapitovelvollisuudesta ja organisaation ohjeista. (Kansainvälinen turvallisuus viranomainen, 2020, ss. 17–20)

Fyysinen turvallisuus -osio käsittelee fyysisten ja teknisten turvatoimien toteutumista. Turvallisuusluokiteltujen tietojen käsittelyssä on kahdenlaisia turvallisuusalueita: hallinnolliset alueet ja turva-alueet. Fyysisillä turvatoimilla estetään luvaton pääsy turvallisuusluokkien tietoihin. Menetelmiin kuuluu muun muassa kulunvalvonta, valaistus ja kameravalvonta. Turvallisuusluokiteltujen tietojen käsittelyssä sovelletaan niin sanottua need-to-know-periaatetta. Tietoja suojataan henkilöiltä, joilla ei ole tiedon saanti tarvetta. Hallinnollisilla alueilla tarkoitetaan esimerkiksi toimistotiloja. Alueelle on oltava selkeästi määritelty näkyvä raja. Turva-alueella tarkoitetaan hallinnollista aluetta paremmin suojattuja alueita, jossa voidaan säilyttää turvallisuusluokiteltuja tietoja. (Kansainvälinen turvallisuus viranomainen, 2020, ss. 22–42)

2.1.2 Tekninen tietoturvallisuus (I)

Katakrin tekninen tietoturvallisuus -osa-alue esittelee vaatimukset, joita soveltavalla pyritään varmistamaan riittävät turvallisuusjärjestelyt turvallisuusluokitellun tiedon sähköiseen käsittelyyn. Jos organisaation tavoitteena on saada toimivaltaisen viranomaisen hyväksyntä,

tulee organisaation toteuttamien suojauksien olla riittäviä. (Kansainvälinen turvallisuus viranomainen, 2020, s. 63)

Turvallisuusluokituksen mukaisesti tietojenkäsittely-ympäristö on eroteltu muusta ympäristöstä. Erottelun tavoitteena on rajata turvallisuusluokitellun tiedon käsittely vain riittävän turvalliseen ympäristöön. Turvallisuusluokan IV tietojenkäsittely-ympäristö on mahdollista kytkeä internettiin, mikäli kytkennän tuomaa riskiä voidaan pienentää riittävästi. Riskien pienentäminen edellyttää ohjelmistopäivityksistä huolehtimista, vähempien oikeuksien periaatteen mukaisia käyttöoikeuksia, järjestelmänkovennuksia ja kykyä poikkeamien havainnointiin. (Kansainvälinen turvallisuus viranomainen, 2020, ss. 65, 66)

Tietoliikenneverkossa toteutetaan vähempien oikeuksien periaatetta (least privilege). Eri verkkoalueiden välillä sallitaan vain tarpeelliset yhteydet. Kaikkia liitettyjä tietoliikennejärjestelmiä tulisi lähtökohtaisesti käsitellä epäluotettavana. (Kansainvälinen turvallisuus viranomainen, 2020, s. 69)

Pääsyoikeuksien hallinnoissa määritellään tietojärjestelmien käyttöoikeudet. Käyttöoikeudet voidaan myöntää vain henkilöille, joiden käsittelyoikeus on varmistettu. Oikeuksien antamisessa noudatetaan vähempien oikeuksien periaatetta eli annetaan vain välttämättömät käyttöoikeudet. Käyttöoikeudet katselmoidaan tasaisiin väliajoin esimerkiksi 6 kuukauden välein. (Kansainvälinen turvallisuus viranomainen, 2020, s. 75)

Katakri 2020 (Kansainvälinen turvallisuus viranomainen, 2020, ss. 75, 76) sisältää seuraavanlaisen esimerkin:

> Turvallisuusluokan IV käsittely-ympäristöissä vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
>
> 1. Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).
>
> 2. Järjestelmän käyttäjistä on olemassa lista.
>
> 3. Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu.
>
> 4. Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu.

5. On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen.

6. Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen) (vrt. I-10).

7. Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti.

8. Tietojärjestelmissä turvallisuusluokitellut tiedot on eritelty vähimpien oikeuksien periaatteen mukaisesti käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä.

9. Tietojärjestelmissä ko. turvallisuusluokan tiedot pidetään erillään julkisista ja muiden turvallisuusluokkien tiedoista, tai eri tason tietoja käsitellään korkeimman turvallisuusluokan mukaisesti.

10.Tietojärjestelmissä tarkastusoikeuden varaavien tiedon omistajien tiedot säilytetään toisistaan ko. turvallisuusluokalle toimivaltaisen viranomaisen hyväksymällä menetelmällä eroteltuna.

Tietojenkäsittely-ympäristöä käyttävät henkilöt ovat tunnistettava riittävän luotettavasti. Minitaso todennuksessa on salasanankäyttö. Mikäli todennus epäonnistuu liian monta kertaa peräkkäin tunnukset lukittautuvat. Salasanalle asetetaan turvallisuuden vähimmäisvaatimukset ja vanhenemisaika. (Kansainvälinen turvallisuus viranomainen, 2020, s. 78)

Järjestelmä kovennetaan siten, että vain tietojen käsittelyn kannalta välttämättömät prosessit, laitteet ja palvelut ovat käytössä. Koventamisen tarkoituksena on haavoituspinta-alan pienentäminen. Kovennukseen olennaisesti kuuluu ohjelmistojen päivittäminen. Päivitysten jälkeen on varmistettava, että kovennukset ovat edelleen voimassa. Kovennuksella estetään tietojärjestelmän käynnistäminen muulla kuin ensisijaiseksi määrätyllä laitteella. (Kansainvälinen turvallisuus viranomainen, 2020, ss. 79–82)

Haittaohjelmatorjuntaohjelmistot on asennettava sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille. Tällaisia ovat esimerkiksi julkisessa verkossa toimivat järjestelmät sekä laitteet, joihin liitetään ulkoisia laitteita esimerkiksi USB-media. Virustietokantoja on

päivitettävä säännöllisesti. Järjestelmät, jotka eivät ole kytkettynä julkiseen verkkoon, virustietokantojen päivitys järjestetään käyttämällä päivitystenhakupalvelinta. Palvelimelta tietokannat siirretään manuaalisesti järjestelmään esimerkiksi 1–3 kertaa viikossa. Järjestelmään voidaan liittää luotettavaksi määriteltyjä muistitikkuja, joita ei kytketä mihinkään muuhun järjestelmään. (Kansainvälinen turvallisuus viranomainen, 2020, ss. 83, 84)

Turvallisuuteen liittyvien tapahtumien jäljitettävyydellä tarkoitetaan järjestelmäympäristön tapahtumien kirjaamista. Tärkeimpinä ovat kirjautumistiedot ja työaseman lokitiedot. Sieltä voidaan poikkeustilanteessa selvittää mitä toimia on tehty. Suositeltu tapa on lokien ohjaaminen keskitetylle lokipalvelimella, jossa on säännöllinen varmuuskopiointi. (Kansainvälinen turvallisuus viranomainen, 2020, ss. 85, 86)

2.2 Asiakirjojen turvallisuusluokitukset

Suomalaisten viranomaisten salassa pidettäviksi luokitellut asiakirjat sijoitetaan neljään turvallisuusluokkaan. Turvallisuusluokkien määritykset havainnoidaan taulukossa 1.

Taulukko 1 Suomessa käytössä olevat asiakirjojen turvallisuusluokat

Turvallisuusluokka I	**Turvallisuusluokka II**	**Turvallisuusluokka III**	**Turvallisuusluokka IV**
ERITTÄIN SALAINEN	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖRAJOITETTU

Opinnäytetyössä asennettavalla erillistyöasemalla käsitellään asiakirjoja, jotka kuuluvat turvaluokkaan IV. Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa säädöksessä (1101/2019) turvallisuusluokan IV asiakirjat ovat määritelty seuraavasti: ”Turvallisuusluokan IV asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa tiedonhallintalain 18 §: 1 momentissa tarkoitetulle suojattavalle edulle.”

Turvallisuusluokiteltujen asiakirjojen käsittelyyn määritetään fyysisesti suojatut turvallisuusalueet.:

1. Hallinnolliset alueet, jotka ovat selkeästi rajattu ja joihin pääset vain valtuutetut henkilöt.
2. Turva-alueet, joilla on selkeästi merkityt ja suojatut rajat ja kulunvalvonta on järjestetty kulkuluvin tai henkilökohtaisesti tunnistamalla.

Turvallisuusluokan IV tietojen käsittely ja säilytys on mahdollista myös turvallisuusalueiden ulkopuolella, kunhan päätelaitteessa olevat tiedot ovat suojattu riittävän turvallisella salausratkaisulla. Tietoa voi käsitellä virkapaikan ulkopuolella, mikäli näkyvyys tai muu pääsy tietoon on estetty sivullisilta. (Valtioneuvosto, 2019, § 10)

2.3 Käyttöjärjestelmän koventaminen

Käyttöjärjestelmän kovennuksella tarkoitetaan perusominaisuuksien, ohjelmistojen ja palveluiden poistoa tai käytön rajoittamista. Se voi tarkoittaa myös konfiguraatiomuutoksia, jotka vaikeuttavat väärinkäytöksiä. Koventaminen tehdään ennen käyttöönottoa ja oletuksena käyttäjällä ja laitteella on vain välttämättömät oikeudet. (Suomen Automaatioseura ry, 2010, ss. 73–74)

Tässä tapauksessa käyttöjärjestelmän kovennus perustuu Windows 11 version 22H2 Security Baselineen. Muita mahdollisia kovennusreferenssejä ovat esimerkiksi CIS Microsoft Windows 11 Stand-alone Bencmark ja DISA Microsoft Windows 11 Security Tecnical Implementation Guide (STIG). (Kroder, 2022, s. 4)

Windows Security Baseline sisältää Microsoftin suosittelemia asetuksia, jotka parantavat työaseman turvallisuutta. Baselinen avulla asetetaan työaseman turvallisuudelle standardi. (Microsoft, 2023)

Suuri osa Baselinen muutoksista liittyy ryhmäkäytäntöjen (Group Policy) muuttamiseen. Ryhmäkäytäntö on hierarkkinen infrastruktuuri, jolla voidaan muokata tietokoneen ja käyttäjän asetuksia. Ryhmäkäytäntö on ensisijaisesti turvallisuustyökalu tietokoneiden ja käyttäjien turvallisuuskäytäntöjen muuttamiseen. Näytä käytäntöjä kutsutaan ryhmäkäytäntöobjekteiksi (Group Policy Object, GPO). Ryhmäkäytännöt prosessoidaan tietokoneessa tasojen mukaan.

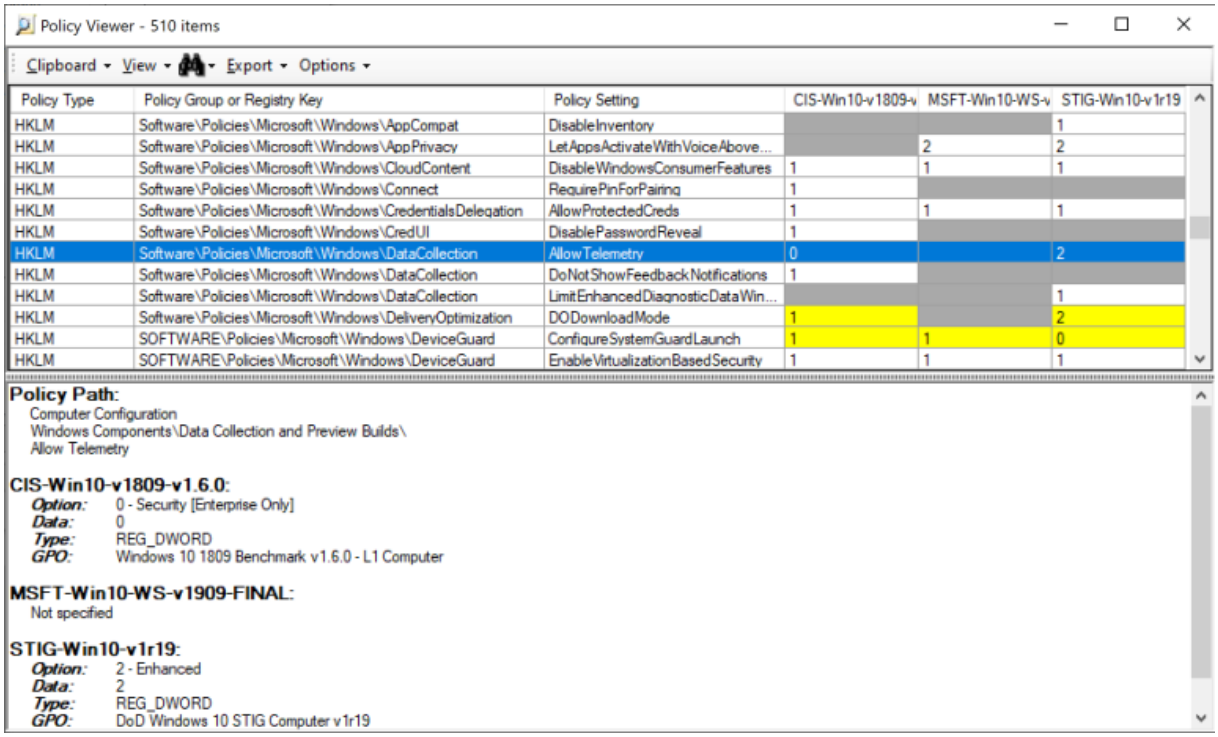
1. Paikalliset ryhmäkäytännöt
2. Toimipaikan ryhmäkäytännöt

3. Toimialueen ryhmäkäytännöt
4. Organisaation ryhmäkäytännöt

Ryhmäkäytännöillä määritellään esimerkiksi salasanan minimipituusvaatimus ja vanhenemisaika. (Posey, 2019)

Policy Analyzer on työkalu ryhmäkäytäntöjen vertailuun ja analysointiin. Sillä löydetään helposti eroavaisuudet tietokoneelle asetettujen ryhmäkäytäntöjen ja suositeltujen ryhmäkäytäntöjen välillä. Kuvassa 1 on esimerkki Policy Analyzerin käytöstä. Esimerkissä Analyzeriin on valittu kolme eri ryhmäkäytäntöä (CIS-Win10-v1809-v1.60, MSFT-Win10-WS-v1909-FINAL, STIG-Win10-v1r19), joita verrataan keskenään. Ryhmäkäytäntöjen väliset eroavaisuudet ovat merkitty keltaisella.

Kuva 1 Esimerkki Policy Analyzerin käytöstä



Policy Type	Policy Group or Registry Key	Policy Setting	CIS-Win10-v1809-v	MSFT-Win10-WS-v	STIG-Win10-v1r19
HKLM	Software\Policies\Microsoft\Windows\AppCompat	DisableInventory			1
HKLM	Software\Policies\Microsoft\Windows\AppPrivacy	LetAppsActivateWithVoiceAbove...		2	2
HKLM	Software\Policies\Microsoft\Windows\CloudContent	DisableWindowsConsumerFeatures	1	1	1
HKLM	Software\Policies\Microsoft\Windows\Connect	RequirePinForPairing	1		
HKLM	Software\Policies\Microsoft\Windows\CredentialsDelegation	AllowProtectedCreds	1	1	1
HKLM	Software\Policies\Microsoft\Windows\CredUI	DisablePasswordReveal	1		
HKLM	Software\Policies\Microsoft\Windows\DataCollection	AllowTelemetry	0		2
HKLM	Software\Policies\Microsoft\Windows\DataCollection	DoNotShowFeedbackNotifications	1		
HKLM	Software\Policies\Microsoft\Windows\DataCollection	LimitEnhancedDiagnosticDataWin...			1
HKLM	Software\Policies\Microsoft\Windows\DeliveryOptimization	DODownloadMode	1		2
HKLM	SOFTWARE\Policies\Microsoft\Windows\DeviceGuard	ConfigureSystemGuardLaunch	1	1	0
HKLM	SOFTWARE\Policies\Microsoft\Windows\DeviceGuard	EnableVirtualizationBasedSecurity	1	1	1

Työkalun etuna on, että sillä voidaan yhdistää useita ryhmäkäytäntöjä samaan listaan, jolloin vertailu on helpompaa. Policy Analyzerin tiedot voidaan siirtää Exceliin. Analyzer kuuluu Microsoftin Security Compliance Toolkit -pakettiin. (Margolis, 2019)

BitLocker on Windowsin levynsalausmenetelmä, joka suojaa tietoja salaamalla koko kiintolevyn. Maksimaalisessa suojauksessa BitLocker toimii yhdessä TPM (Trusted Platform

Module) -turvapiirin kanssa. Kaikissa uudemmissa tietokoneissa on TPM-turvapiiri, koska Windows 11 -käyttöjärjestelmää ei virallisesti voi asentaa ilman sitä. Lisäksi TPM mahdollistaa normaalin käynnistysprosessin lukitsemisen, joka alkaa vasta kun käyttäjä on syöttänyt PIN-koodin tai ulkoisenlaitteen, joka sisältää käynnistysavaimen. (Microsoft, 2023)

BitLockerin haitta puolena Windows 11 Pro -käyttöjärjestelmää käyttäessä on se, että BitLockerin käyttö hidastaa SSD (Solid-state drive) -levyn suorituskykyä jopa 45 prosenttia. Tämä johtuu siitä, että Windows 11 Pro -käyttöjärjestelmä käyttää oletuksena ohjelmistoon perustuvaa BitLocker-salausta. Vaikka monet SSD-levyt tukevat laitteistopohjaista salausta Microsoft on päätynyt ohjelmistopohjaiseen salaukseen, koska SSD-levyjen laitevalmistajien salauksista on löytynyt haavoittuvuuksia, jotka on jouduttu korjaamaan. (Kolokythas, 2023)

2.4 Haittaohjelmatorjuntaohjelmistot

Haittaohjelmatorjuntaohjelmistolla tarkoitetaan tietoturvaohjelmaa, joka suojaa tietokonetta tallennusvälineiden ja verkon kautta saapuvilta viruksilta ja muilta haittaohjelmilta. Tieturvaohjelmat pitävät itsensä ja virustietokannat ajantasaisena, jos tietokone on yhdistettynä verkkoon. Tietoturvaohjelmat tarkkailevat tiedostojärjestelmää taustalla koko ajan aktiivisesti. Viruksen havaittuaan se ilmoittaa siitä käyttäjälle varoitusikkunalla. (Helsingin yliopisto, 2023)

WithSecure Policy Manager on tietoturvaohjelma, jolla voidaan valvoa yrityksen tietoturvaa keskitetysti. Policy Managerilla päivitetään virustietokannat ja hallitaan tietoturvasovelluksia yhdessä paikassa. Policy Manageriin liitettyihin työasemiin asennetaan WithSecure Client Security, joka toimii työaseman tietoturvaohjelmana. (WithSecure, n.d.)

2.5 Windows 11 -käyttöjärjestelmän päivitykset

Microsoft julkaisee Windows 11 -käyttöjärjestelmälle kahdenlaisia päivityksiä, ominaisuuspäivityksiä ja suojauspäivityksiä. Windows 11 -käyttöjärjestelmän ominaisuuspäivitykset julkaistaan, Microsoftin aikaisemmasta linjasta poiketen, kerran vuodessa kalenterivuoden toisella vuosipuoliskolla. Ominaisuuspäivitys sisältää uusia toimintoja ja ominaisuuksia sekä mahdollisia korjauksia ja suojauspäivityksiä. Laatupäivitys, jota kutsutaan myös kumulatiiviseksi päivitykseksi, julkaistaan kerran kuussa kuukauden toisena torstaina. Nämä päivitykset sisältävät yleensä laadun parantamiseen ja tietoturvaan liittyviä korjauksia. Olennaisena osana Windowsin päivitykseen kuuluu myös Microsoft Store

sovellusten päivitys. Sovelluksilla ei ole erillistä päivitysaikataulua vaan niitä päivitetään tarpeen mukaan. Windowsin päivitys tapahtuu Windows Updaten kautta. Käyttäjän tarvitsee vain asentaa päivitykset ja käynnistää tarvittaessa tietokone uudelleen. Windowsin päivitykset voi asentaa myös manuaalisesti lataamalla ne Microsoft Update -luettelo verkkosivuilta. (Microsoft, 2023)

3 Erillistyöaseman asennus

Erillistyöaseman asennuksen aikana seurattiin tarkasti Puolustusvoimien toimittamaa Erillistyöaseman kovennus tarkistuslistaa (Liite 3). Asennuksen aikana pidin päiväkirjaa ja otin kuvakaappauksia tarvittaessa.

3.1 Käyttöjärjestelmän asennus

Erillistyöaseman asennus aloitettiin asentamalla Windows 11 Pro -käyttöjärjestelmä puhtaana asennuksena uudelta USB-muistitikulta. USB-muistitikulle oli luotu asennusmedia käyttäen Windows Media Creation Toolia. Asennusohjelman käynnistyessä painettiin Shift + F10, jotta saatiin Komentokehote auki. Komentokehote-ikkunaan kirjoitettiin komento ”oobe\bypassnro”. Tämä komento mahdollistaa Windows 11 -käyttöjärjestelmän asentamisen ilman Microsoft-tiliä. Kun Windows oli asennettu ja käynnistynyt työpöydälle, työasema yhdistettiin verkkoon. Tämän jälkeen käyttöjärjestelmä päivitettiin Windows Updaten kautta. Työasemalle haettiin HP Support Assistant internetistä ja Support Assistantia hyödyntäen päivitettiin tarvittavat ajurit ja BIOS. Kun Windows ja ajurit olivat ajan tasalla, poistettiin Windowsista tarpeettomat oletussovellukset kuten Maps, OneDrive, Teams ja Paint.

3.2 Käyttäjätilit

Työasemalle luotiin kaksi käyttäjätiliä. Pääkäyttäjätili ”administrator” ja päivittäisessä käytössä oleva ”user”. Oletuskäyttäjätilit otettiin pois käytöstä ohjeen mukaisesti. User-käyttäjätiliä käytetään, kun käsitellään turvallisuusluokitukseltaan IV:n mukaisia asiakirjoja. Käyttäjätilillä on minimaaliset oikeudet. Tämä tarkoitta esimerkiksi sitä, että käyttäjä ei voi asentaa mitään työasemalle tai muokata lokitietoja. Administrator-käyttäjätiliä käytetään käyttöjärjestelmän ja ohjelmien päivitykseen ja tarvittaessa lokitietojen tarkasteluun.

3.3 Käyttöjärjestelmän koventaminen

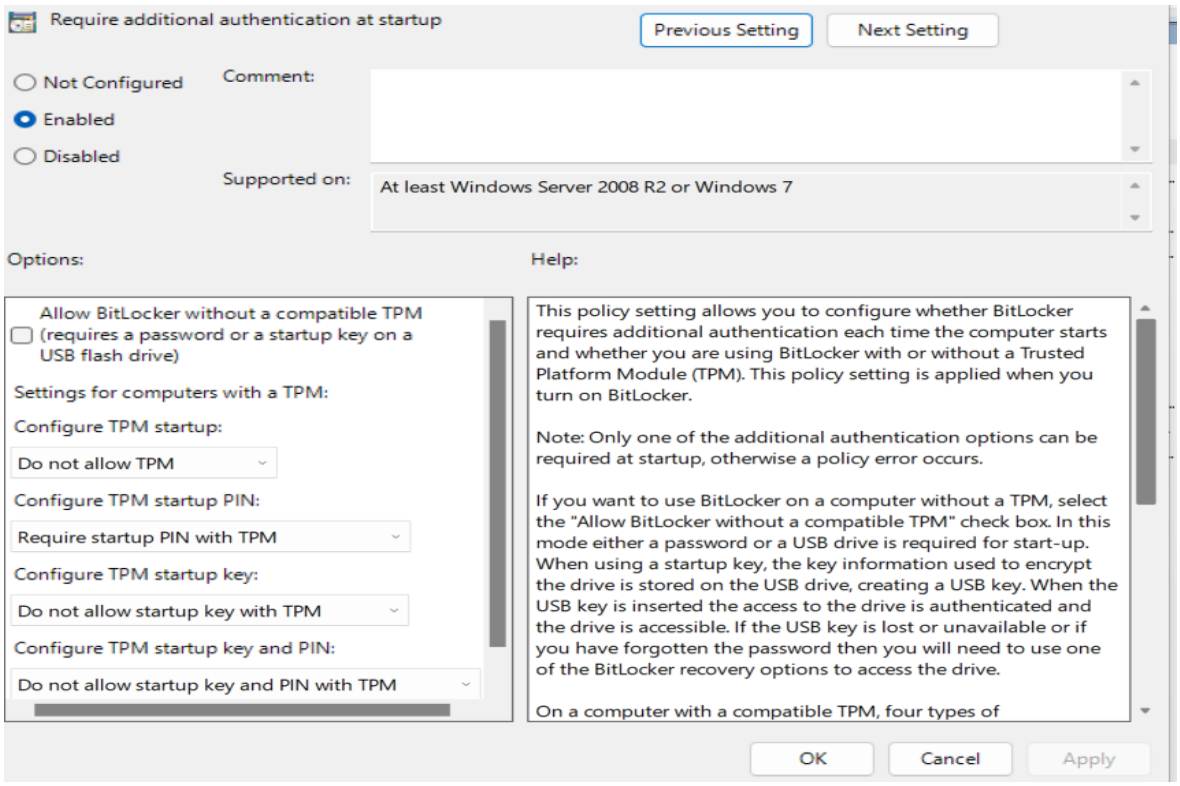
Käyttöjärjestelmä kovennettiin Windows 11 version 22H2 Security Baselinen mukaan. Microsoftin lataussivuilta ladattiin Security Compliance Toolkit (SCT), josta löytyivät työkalut automaattisten muutosten tekemiseen. Windows 11 version 22H2 Security Baseline.zip purettiin kansioon C:\Baseline. Koska työasemaa ei liitetty toimialueelle, ladattiin samaan

Security Compliance Tookittiin kuuluva LGPO. LGPO.zip purettiin Tools-alikansioon. Scripts-alikansiosta löytyvä baseline-localInstall.ps1 ajettiin käyttäen Windows PowerShelliä. Näin Security Baselinen mukaiset käyttöjärjestelmän kovennukset tulivat voimaan. Puolustusvoimien ohjeasiakirjan mukaisesti muutettiin vielä paikallista ryhmäkäytäntöä (Local Group Policy), joka lukitsee näytön 5 minuutin käyttämättömyyden jälkeen.

3.4 BitLockerin asettaminen

Työasemaan asetettiin BitLocker-asemasalaus, joka käyttää TPM-turvapiiriä. Bitlocker laitettiin päällä Ohjauspaneelista (Control Panel) BitLocker Drive Encryption kohdasta. Bitlockerin palautusavain (recovery key) tulostettiin paperille, koska työasemaa ei ole liitetty Microsoft-tiliin. Kun asemasalauksen määritys oli saatettu loppuun, muutettiin paikallisia ryhmäkäytäntöjä, jotta PIN-koodin kysely ennen käynnistysprosessin aloittamista saatiin päälle (Kuva 2).

Kuva 2 Kaikki muut pois päältä, paitsi Require startup PIN with TPM



Uudelleen käynnistyksen jälkeen, avattiin komentokehote (Command Prompt) järjestelmänvalvojan oikeuksilla. Komennolla ”manage-bde -protectors -add c: -TPMAndPIN”

päästiin asettamaan PIN-koodi, jota työasema kysyy ennen käyttöjärjestelmän käynnistysprosessin aloittamista. PIN-koodiksi asetettiin 8-merkkinen yhdistelmä.

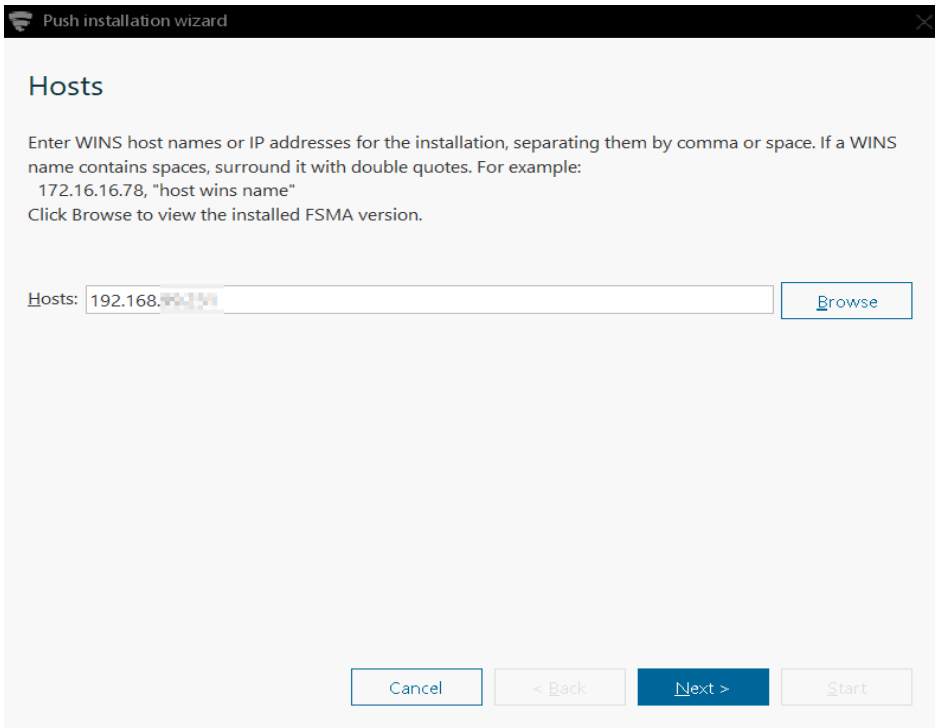
3.5 Microsoft Office Home & Business 2021

Microsoft Office asennettiin sähköisellä asennuskoodilla. Asennusta varten luotiin geneerinen sähköpostiosoite, johon Office-lisenssi sidottiin. Tilin luomisen jälkeen asennuspaketti noudettiin kirjautumalla office.com-osoitteeseen. Kun Office oli asennettu, se aktivoitiin kirjautumalla Office-sovellukseen. Makrojen käyttö estettiin kaikista Microsoft Office ohjelmista.

3.6 WithSecure Client Security 15.30

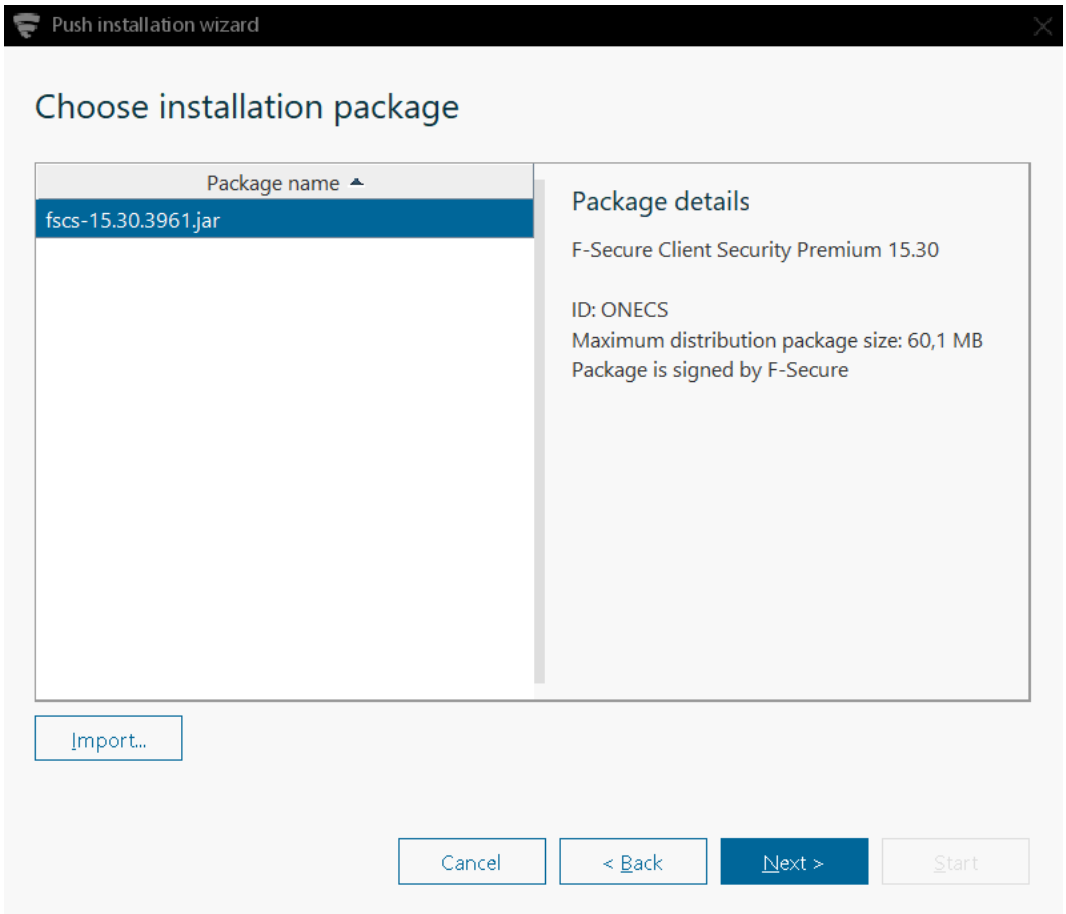
WithSecure Client Security -ohjelma asennettiin käyttäen WithSecure Policy Manageria, joka on asennettu jatkossakin verkossa olevalle työasemalle. Samaisella työasemalla hoidetaan myös Client Securityn päivitykset. Asennuksen aikana työasemat olivat samassa verkossa, joten tämän työaseman pystyi liittämään Policy Manageriin käyttäen IP-osoitetta (Kuva 3).

Kuva 3 Client Securityn asentaminen Policy Managerilla



Kun työasema oli yhdistetty Policy Manageriin valittiin asennettavapaketti (Kuva 4), joka tässä tapauksessa oli Client Security. Asennuspaketti oli aiemmin ladattu WithSecuren verkkosivulta.

Kuva 4 Asennettavan paketin valinta Policy Managerissa



Asennus viimeisteltiin syöttämällä vastaanottavan työaseman järjestelmänvalvojan käyttäjätunnus ja salasana.

3.7 Asiakkaan tietokoneohjelmat

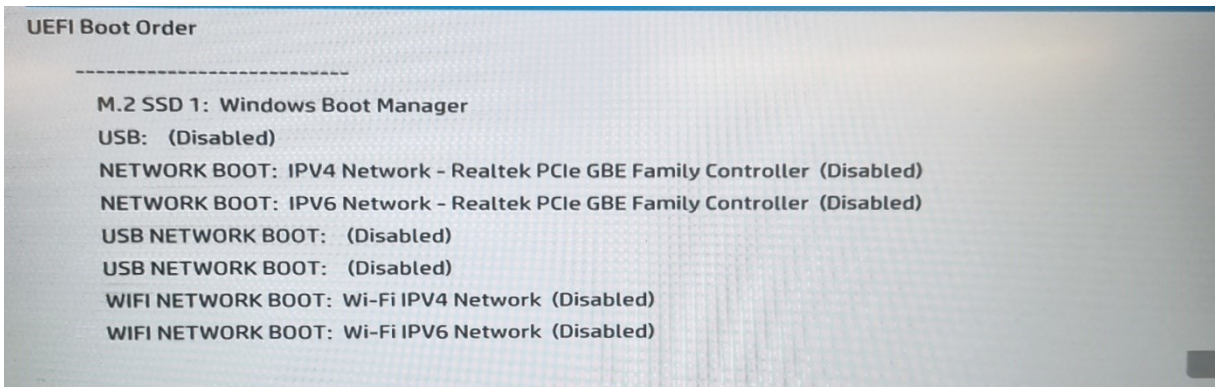
Asiakkaan ohjeiden mukaan erillistyöasemalle asennettiin seuraavat tietokoneohjelmat. Ohjelmat asennettiin tässä vaiheessa, kun tietokoneella oli vielä verkkoyhteys.

- CDBurnerXP 4.5.8.7128. CD:n ja DVD:n polttamiseen tarkoitettu ohjelma.
- VeraCrypt 1.25.9. Tiedostojen salaukseen käytetty ohjelma.

3.8 BIOSin koventaminen

BIOSin koventaminen aloitettiin estämällä kaikki muut käynnistysmenetelmät kuin Windows Boot Manager, kuten kuvassa 5 on tehty.

Kuva 5 BIOSissa sallitaan käynnistys vain Windows Boot Managerilla

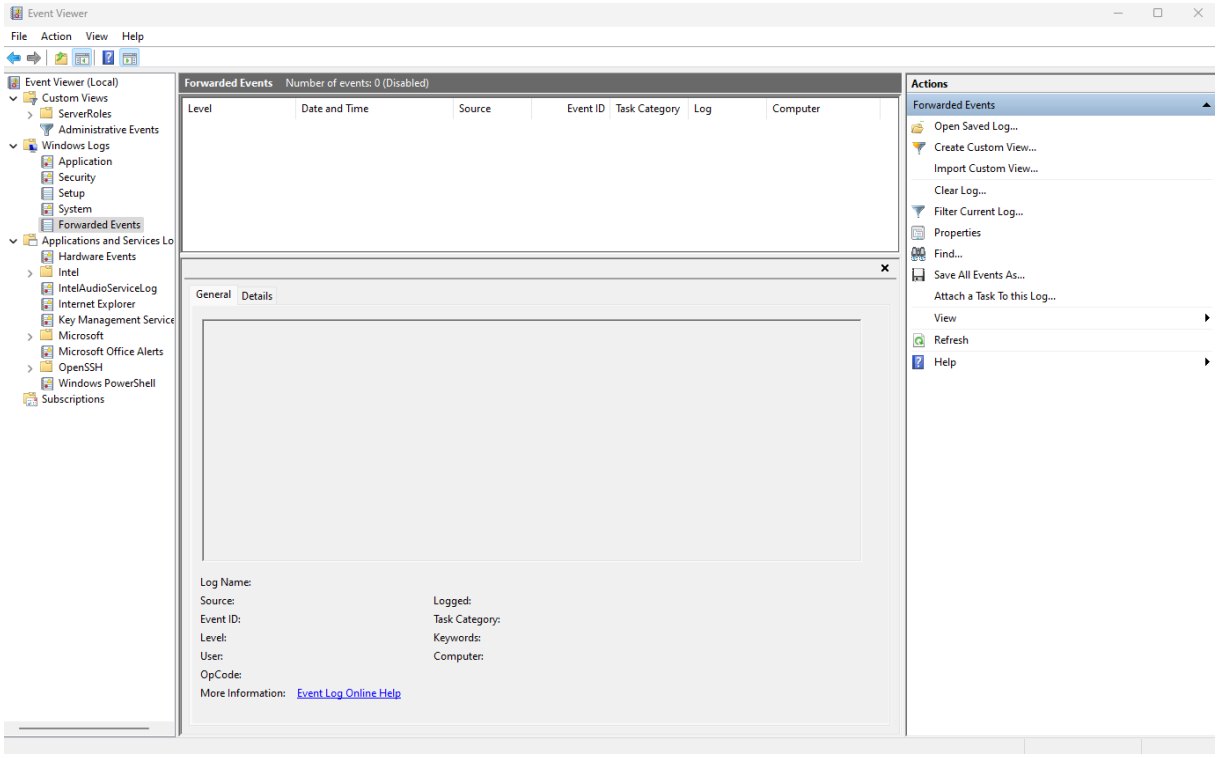


BIOS tasolla poistettiin verkkoyhteys LAN ja langatonverkkoyhteys WLAN- ja Bluetooth-yhteydet käytöstä. Asetettiin vahva 17-merkkinen BIOS-salasana, jota voi käyttää vain järjestelmänvalvoja tasolla.

3.9 Windows lokit

Käyttöjärjestelmän ja sovellusten lokitiedot näkyvät Tapahtumienvalvonnassa (Event Viewer). Lokitietojen valvonnasta vastaa Administrator-käyttäjätili. Kuvassa 6 on esimerkki kuva tapahtumienvalvonnan etusivusta.

Kuva 6 Event Viewerissä näkyy sovellusten ja Windowsin lokit



Koska asennettava työasema ei ole verkossa, niin lokien varmuuskopiointi on loppuasiakkaan vastuulla. Lokitiedot varmuuskopioidaan säännöllisesti USB-muistitikun avulla.

4 Käyttöjärjestelmän ja ohjelmien päivittäminen

Koska erillistyöasema ei ole verkossa, niin käyttöjärjestelmän ja ohjelmien päivitykset hoidetaan manuaalisesti. Päivitykset ladataan internetistä työasemalle, jolla on verkkoyhteys. Asiakas siirtää päivitykset USB-muistitikun avulla erillistyöasemaan. Käyttöjärjestelmän ja ohjelmien ajantasaisuus on asiakkaan vastuulla.

4.1 Windows 11 -käyttöjärjestelmä

Windows 11 -käyttöjärjestelmän päivitykset ladataan Windows Update -luettelo verkkosivustolta. Asiakkaalla on käytössä samanlainen työasema kuin tässä asennettu erillistyöasema, mutta siinä on käytössä verkkoyhteys. Sitä kautta asiakkaan on helppo seurata Windows päivityksiä. Kun verkossa oleva työasema on päivittynyt, niin Knowledge Base -artikkelin (esimerkiksi KB9123456) avulla asiakkaan on helppo hakea sama päivitys Windows Update -luettelo verkkosivulta ja siirtää se erillistyöasemaan USB-muistitikun avulla. Siirtämisen jälkeen päivitys asennetaan erillistyöasemalle.

4.2 Microsoft Office Business & Student 2021

Officen päivitystä varten luodaan Office_update-kansio verkossa olevan työaseman työpöydälle. Microsoftin sivulta ladataan xml-tiedosto config.xml, joka muokataan muotoon:

```
<Configuration>
  <Add SourcePath="C:\Temp" OfficeClientEdition="64" >
    <Product ID="HomeBusiness2021Retail">
      <Language ID="en-us" />
    </Product>
  </Add>
  <Remove All="True" />
  <!--  <RemoveMSI All="True" /> -->
  <!--  <Display Level="None" AcceptEULA="TRUE" />  -->
  <!--  <Property Name="AUTOACTIVATE" Value="1" />  -->
</Configuration>
```

Kopioidaan config.xml ja Officen asennuksen yhteydessä käytetty setup.exe työpöydällä olevaan Office_update-kansioon. Komentokehotteessa suoritetaan seuraava komento:

C:\Users\Omistaja\Desktop\Office_update\setup.exe /download C:\Users\Omistaja\Desktop\Office_update\config.xml

Kopioidaan c:\temp-kansiossa oleva office-kansio USB-muistitikulle ja siirretään sieltä erillistyöaseman c:\temp-kansioon. Temp-kansioon kopioidaan myös setup.exe ja config.xml. Erillistyöasemalla kirjoitetaan komentokehotteeseen seuraava komento: c:\temp\setup.exe /configure c:\temp\config.xml. Office-kansion kopiointi tehdään aina vanhan kansion päällä, jotta ohjelma päivittää vain viimeisimmät muutokset.

4.3 WithSecure Client Security -virustietokannat

WithSecuren Client Securityn virustietokannat päivitetään verkossa olevan työaseman avulla, jossa on WithSecure Policy Manager asennettuna. Verkossa olevan työaseman komentokehotteeseen kirjoitetaan seuraava komento: C:\"Program Files (x86)"\F-Secure\"Management Server 5"\bin\prepare-fspm-definitions-update-tool.bat c:\fs. Tämä komento luo prepare-fspm-definitions-update-tool.bat-tiedoston c:\fs-kansioon. Tämän jälkeen käynnistetään C:\fs\fspm-definitions-update-tool kansiossa oleva fspm-definitions-update-tool. Tämä työkalu luo f-secure-updates.zip -tiedoston C:\fs\fspm-definitions-update-tool\data -kansioon. Zip -tiedosto kopioidaan USB-muistitikun avulla erillistyöaseman C:\Program Files (x86)\F-Secure\Client Security -kansioon. Kansiosta käynnistetään fsaua-update.exe.

5 Tulokset

Ennen kuin erillistyöasema luovutetaan asiakkaalle, käyttöjärjestelmänkovennukset on tarkistettava Microsoftin Policy Analyzer työkalulla. Policy Analyzer antoi yhden poikkeaman Baselinen ja työaseman ryhmäkäytäntöjen välillä (Kuva 7).

Kuva 7 Poikkeama Policy Analyzerissä

A	B	C	D	E
Policy Type	**Policy Group or Registry Key**	**Policy Setting**	**Baseline**	**windows11**
HKLM	Software\Microsoft\Windows\CurrentVersion\Polic	InactivityTimeoutSecs	900	300

Poikkeama johtuu siitä, että puolustusvoimien tarkastuslistassa näytönlukitus on ohjeistettu menemään päälle 5 minuutin käyttämättömyyden jälkeen. Baselinessä on ohjeistettu 15 minuuttia. Tarkastuslistaa on päivitetty työn edetessä. Tässä vaiheessa täytetään Kovennetun erillistyöaseman turvallisuusseloste, joka muokataan Erillistyöaseman toteutus ja dokumentointi pohjasta.

Työasemaan tehdyt kovennukset ovat tiukempia kuin turvallisuusluokitukseltaan IV olevien asiakirjojen käsittely vaatii. Katakrin mukaan työasema on mahdollista kytkeä internettiin, edellyttäen että kytkennän tuomia riskejä on pienennetty riittävästi. Tämä tapahtuu esimerkiksi palomuurin avulla. Katarin ohjeet ovat ympäripyöreitä, mutta asiakkaan toimittavissa Puolustusvoimien asiakirjoissa on selkeät ohjeet mikä on haluttu lopputulos.

6 Johtopäätökset ja pohdinta

Opinnäytetyössä kuvattiin erillistyöaseman asennusprosessi ja päivittäminen. Asennus jouduttiin aloittamaan kertaalleen alusta, koska käyttöjärjestelmä ei käynnistynyt TPM-turvapiiriin PIN-koodin asettamisen jälkeen. PIN-koodi asetetaan komentokehotteessa. Asettamisen jälkeen, ennen uudelleenkäynnistämistä, kannattaa käydä graafisessa käyttöliittymässä varmistamassa, että PIN-koodin asettaminen onnistui. Opinnäytetyö helpottaa välttämään edellä mainitut virheet, koska vastaavaa erillistyöaseman asennukseen liittyvää dokumenttia ei ole aikaisemmin tehty.

Erillistyöaseman käyttöönotto jäi kokonaan asiakkaan vastuulle, koska asiakas käsittelee käyttörajoitettuja asiakirjoja. Käytännössä tämä tarkoittaa sitä, että asiakas nouti työaseman, salasanat ja kovennetun erillistyöaseman turvallisuusselosteen liitteineen, joka oli tallennettu USB-muistitikulle. Asiakkaan kanssa katsottiin etäyhteydellä WithSecure Client Securityn toiminta verkossa olevalla työasemalla. Samaa ohjetta hyödynnetään erillistyöasemassa.

Puolustusvoimien turvatarkastaja kävi auditoimassa työaseman, kun asiakas oli saanut erillistyöaseman fyysisen turvallisuuden kuntoon. Turvatarkastaja oli tyytyväinen työaseman kovennukseen.

Tutkimuskysymyksiin saatiin vastaus opinnäytetyön aikana. Erillistyöaseman asennusprosessi on esitetty selkeäasti vaihe kerrallaan. Tämä helpottaa vastaavaa asennusta jatkossa. Viranomaisten asiakirjojen turvallisuusluokituksien määrityksistä kerrottiin pääpaino turvallisuusluokitus IV:ssä. Haittaohjelmatorjuntaohjelmiston virustietokantojenpäivitys esitettiin käytössä olevan WithSecure Client Securityn osalta.

Opinnäytetyön valmistumisen loppupuolella Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus julkaisi ohjeen nimeltään ”Ohje erillistyöaseman tietoturvallisuuden varmistamisesta”. Ohje vastaa sisällöltään ”Erillistyöaseman toteutus ja dokumentointi” asiakirjaa. Uskon, että jatkossa päivitetty ohje tulee myös Puolustusvoimien käyttöön.

7 Yhteenveto

Johdannossa esitettyihin tutkimuskysymyksiin, opinnäytetyö vastaa mielestäni hyvin. Erillistyöaseman asennus on esitetty kronologisessa järjestyksessä, joka mahdollistaa asennuksen toistamisen. Asennus seuraa Puolustusvoimien toimittamaa Erillistyöaseman kovennus tarkistuslistaa.

Asiakirjojen turvallisuusluokitukset ja turvallisuusluokiteltujen asiakirjojen käsittely ovat esitelty omassa luvussaan. Pääpaino on turvallisuusluokassa IV.

Haittaohjelmatorjuntaohjelmiston päivityksen osalta opinnäytetyössä päivitettiin WithSecuren Client Securityn virustietokanta. Sen osalta päivitysohjeistus ei ole yleispätevä. Virustietokantojen päivitys on esitetty seikkaperäisesti, joten ohjeita seuraamalla päivitys onnistuu helposti.

Omalta osalta koko asennusprosessin aikana pääsin oppimaan paljon uutta. Ennen projektin aloitusta, minulla ei ollut mitään käsitystä asiakirjojen turvallisuusluokituksista tai missä kyseisiä asiakirjoja voidaan käsitellä. Osa työaseman kovennuksista oli yksinkertaisia, mutta toiset toteutettiin yrityksen ja erehdyksen kautta. Oman haasteensa asetti Puolustusvoimien tarkistuslista, jossa on vanhentunutta tietoa. Esimerkiksi Microsoft Baseline Analyzer ei ole enää käytössä.

Työssä vaadittiin tarkkuutta ja huolellisuutta, koska asennettu erillistyöasema auditoitiin.

Jatkossa oli mukava päästä asentamaan erillistyöasema alusta loppuun, johon sisältyisi myös fyysinen turvallisuus. Opinnäytetyön käytännönosuutta seuraamalla onnistuu erillistyöaseman tekninen toteutus tietoturvallisesti.

Lähteet

Helsingin Yliopisto. (n.d.). *Haittaohjelmilta suojautuminen*. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-2-suojautuminen-uhkatekijoilta/haittaohjelmilta-suojautuminen/

Kansallinen turvallisuusviranomainen. (2020). *Katakri 2020*. Kansallinen turvallisuusviranomainen. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Kolokythas, P. (2023). *Default Windows 11 feature slows SSDs up to 45%: How to fix it*. https://www.pcworld.com/article/2113846/default-windows-11-feature-slows-ssds-up-to-45-you-can-fix-it.html

Kroder, J. (ei pvm.). Windows 11 system hardening: Essential measures und tips. *2022*. https://www.fb-pro.com/windows-11-system-hardening-measures-und-tips/

Microsoft. (2023a). *BitLocker overview*. Microsoft. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/

Microsoft. (2023b). *Microsoft Update -luettelo*. Micrososft. https://www.catalog.update.microsoft.com/home.aspx

Microsoft. (2023c). *Security Baselines*. https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines

Microsoft. (2023d). *Windows Update: Usein kysytyt kysymykset—Microsoft-tuki*. Microsoft. https://support.microsoft.com/fi-fi/windows/windows-update-usein-kysytyt-kysymykset-8a903416-6f45-0718-f5c7-375e92dddeb2

Microsoft. (n.d.). *Jatkuvan innovaation tuottaminen Windows 11—Microsoft-tuki*. Microsoft. https://support.microsoft.com/fi-fi/windows/jatkuvan-innovaation-tuottaminen-windows-11-b0aa0a27-ea9a-4365-9224-cb155e517f12

Morgolis, A. (2019). *New tool: Policy Analyzer*. Microsoft. https://techcommunity.microsoft.com/t5/microsoft-security-baselines/new-tool-policy-analyzer/ba-p/701049

Posey, B. (2019). *What is Group Policy? - Definition from WhatIs.com (techtarget.com)*. https://www.techtarget.com/searchwindowsserver/definition/Group-Policy

Valtioneuvosto. (2019). *Lainsäädäntö 1101/2019*. https://www.finlex.fi/fi/laki/alkup/2019/20191101

WithSecure. (n.d.). *WIthSecure Policy Manager*. WithSecure. https://www.withsecure.com/userguides/product.html#business/policy-manager/16.00/en/concept_F46303878393460CA4890BD092F4BB3E-16.00-en

Liite 1: Aineistonhallintasuunnitelma

Asennusprojektin aikana pidetään päiväkirjaa, johon kerätään teknistä tietoa projektista. Uutta aineistoa saadaan myös kokeilemalla ja kyselemällä. Tämä tieto analysoidaan opinnäytetyötä varten. Päiväkirjaa säilytetään tekijän tietokoneen C-asemalla, ja USB-tikulla. Päiväkirjaa säilytetään USB-tikulla ainakin vuoden verran opinnäytetyön valmistumisesta.

Koko opinnäytetyössä kyseessä olevan erillistyöaseman asennuksen aikana täytetään puolustusvoimien dokumentteja, jotka löytyvät liitteenä. Täytettyjen dokumenttien kopiot säilytetään USB-tikulla.

Valmiin projektin onnistumisesta kerätään tietoa päiväkirjaan. Päiväkirjaa täydennetään kuvakaappauksilla.

Liite 2. Erillistyöaseman toteutus ja dokumentointi

Erillistyöaseman toteutus ja dokumentointi (11.10.2017)

Koventamisen lähtökohtana on dokumentoitu (*tietojärjestelmän turvallisuusseloste*) tieto kovennettavan laitteen tarjoamista palveluista, toimintaympäristöstä, ja käyttötapauksista.

Palveluiden osalta myös erillistyöaseman tarjoamien palveluiden määrä tulee minimoida, jolloin voidaan pienentää yksittäisen palvelun väärästä toiminnasta muille palveluille aiheutuvia vaikutuksia.

Seuraavat asiat on vähintään toteutettava, tarkastettava ja kuvattava erillistyöaseman (ei kiinni tietoverkoissa) toteutuksessa ja dokumentoinnissa:

Toteutettavat kovennukset

- BIOS-asetukset:
  - BIOS-suojaus (salasana)
  - Käynnistys sallittu vain kovalevyltä
  - Tarpeettomat palvelut ja portit on poistettu käytöstä
    - WLAN, LAN, Bluetooth, Sarjaportit, Firewire, 3/4G modeemit, jne. poistettu käytöstä
- Haittaohjelmatorjuntaohjelmisto asennettu (I09 ja I11).
- PDF-lukijat, toimisto ohjelmistot, jne ovat turvallisesti konfiguroituja.
- Ajettavan koodin (erityisesti JavaScript ja makrot) suorittaminen on oletuksena estetty.
- Käyttäjätilien määrittely ja hallinta
  - Tarpeettomien käyttäjätunnusten ja -tilien poistaminen
  - Järjestelmiin asennuksen yhteydessä automaattisesti luoduille tileille (esim. “administrator” ja “guest”) on oikeudet rajattu minimiin tai poistettu käytöstä.
  - Oletussalasanat vaihdettu
- Käyttöjärjestelmä kovennettu (I08)
- Tarpeettomat palvelut on suljettu (alusta sisältää vain järjestelmän tarvitsemia ohjelmistokomponentteja.)
- Tarpeettomat työkalut, kirjastot ja tiedostot on poistettu käyttöjärjestelmästä
- Tarjottavien palveluiden tietoturva-asetusten koventaminen (käyttö- ja pääsyoikeudet, pääsyn rajoittaminen, käytettävät protokollat jne.) (I06, I07, I13)
- Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi on toteutettu

luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen (I10).
- Käyttöjärjestelmän tunnettuja turvallisuusuhkia sisältävät automaattisen ohjelmakoodin suorituksen mahdollistavat ominaisuudet on kytketty pois päältä (erityisesti PDF-tiedostojen automaattinen esikatselu sekä “autorun” ja ”autoplay”-toiminnallisuudet).
- Erillistyöaseman tilan todennus ennen käyttöönottoa ja muutosten yhteydessä
    - täydellinen haittaohjelmatarkastuksen ajo => raportti
    - MBSA:n ajo (Microsoft Baseline Analyzer) => raportti
- Erillistyöaseman käyttöpaikan hyväksyminen ennen käyttöönottoa
    - Tilan hallinnolliset ja fyysiset vaatimukset
    - TEMPEST-vaatimusten huomioiminen (I14)

Kovennetun erillistyöaseman turvallisuusseloste (kovennusten dokumentointi)

- Työaseman käyttötarkoitus
- Työaseman merkki/malli
- Työaseman sarjanumero
- Kuvataan tehdyt kovennukset:
    - BIOS-asetusten muutokset ja suojaus
    - BIOS-suojaus (salasana)
- Kovalevyn salauksen dokumentointi
- Käyttöjärjestelmän ja sovellusohjelmistojen dokumentointi
    - Luettelo asennetuista ohjelmista
    - Tietoturvapäivitysten (Microsoft, Adobe jne.) ja haittaohjelmatorjuntaohjelmiston päivitysten toteutusprosessi ja sen kuvaaminen
    - Käyttöjärjestelmään ja sovellusohjelmistoihin on asennettu tarpeelliset turvapäivitykset.
    - Ohjelmistohaavoittuvuuksien hallinnasta on huolehdittu (I23)
- Käyttäjätilien määrittely ja hallinta on dokumentoitu
    - peruskäyttäjä(t)
    - pääkäyttäjä
    - yhteiset levyalueet
- käyttö- ja pääsyoikeuksien hallinnan kuvaaminen ja dokumentointi
    - Käyttöoikeuksien hyväksymisprosessi, kuka hyväksyy
- Erillistyöaseman toipumissuunnitelma
    - varautuminen todennäköisempiin uhkiin/riskeihin
    - toiminta huoltotilanteissa
- Toiminta tietoturvapoikkeamatilanteessa
- Erillistyöaseman seurattavien lokitiedostojen määrittely ja kuvaaminen (I10)
    - mitä seurataan, miten, kuka vastaa, dokumentointi, lokien talteenotto, säilytys

    - väliaikaistiedostojen hallinta ja poistaminen
- Tietojen varmuuskopiointi toteutuksen määrittely ja kuvaaminen (I 24)
    - miten, kuka vastaa, dokumentointi, seuranta, säilytys
- Muutoksenhallintamenettely on kuvattu (I20)
- Käytettävät muistitikut, ulkoiset kovalevyt, tulostimet:
    - käyttötarkoitus, sarjanrot (vast. yksilöinti), säilytys/käyttö
    - Tietojen siirtoprosessin kuvaaminen/ohjeistaminen erillistietokoneeseen ja -koneesta
- Menettely erillistyöasemasta tai siihen liittyvien laitteiden hävittämisen tai luopumisen osalta (I19)
    - kovalevy
    - ulkoiset muistivälineet
    - tulostimet
    - muut oheislaitteet

Liite 3. Erillistyöaseman kovennuksen tarkistuslista

Erillistyöaseman kovennus checklist (eräitä tärkeitä huomioitavia asioita)		
Toimenpide	**Status**	**Toteutus dokumentoitu**
Työaseman turvallinen asennus		
Asenna käyttöjärjestelmä "puhtaalle" ylikirjoitetulle (vaatimukset täyttävä) levylle luotettavalta medialta	☐ Ok	
Asennusprosessi		☐ Ok
Tarpeettomien fyysisten komponenttien poisto (mm.)		
Langattomat verkkokortit	☐ Ok	
Kamera (tai kameran teippaus)	☐ Ok	
Dokumentoi tuotteiden tiedot (myös miltä laitteelta irrotettu), aseta turvalliseen paikkaan (esim. sinettipussiin ja kassakaappiin)	☐ Ok	☐ Ok
BIOS-kovennukset (Laitekohtainen, mutta disabloi / estä tarpeettomat mm.)	☐ Ok	
Estetään käynnistäminen muulta kuin ensisijaiseksi määritellyltä laitteelta	☐ Ok	
BIOS-version tarkistaminen	☐ Ok	
Secure Boot	☐ Ok	
Aseta vahva BIOS salasana (väh. 16 merkkiä)	☐ Ok	
Password Bypass: Disabled	☐ Ok	
Password Change, allow non-admin password changes: Disabled	☐ Ok	
Tarpeettomien asetusten disablointi	☐ Ok	
Tarpeettomien porttien disablointi	☐ Ok	
Verkkokortin disablointi	☐ Ok	
Windows työaseman ja käyttöjärjestelmän perustiedot		
Käyttöjärjestelmäversio / build		☐ Ok
Työaseman käyttötarkoitus		☐ Ok
Työaseman merkki ja malli		☐ Ok
Työaseman sarjanumero		☐ Ok
Käytössä oleva kovennusreferenssi		☐ Ok
Tehtyjen kovennusten kuvaus		☐ Ok

Haittaohjelman torjuntaohjelmiston asennus & tunnisteet		
Tunnisteiden päivitys toteutetaan erillisellä verkkoon kytketyllä laitteella ja toimitetaan turvallisella tavalla offline-työasemaan	☐ Ch	
Tietoturvapäivitysten ja haittaohjelman torjuntaohjelmistojen päivitysten toteutusprosessi ja sen kuvaaminen		☐ Ch
Ajettavan koodin (JavaScript, makrot) suorittaminen oletuksena estetään mm.		
Selain	☐ Ch	
Office	☐ Ch	
PDF-lukija	☐ Ch	
PowerShell	☐ Ch	
Muista paikoista mikäli käytössä	☐ Ch	
Tarpeettomien työkalujen, ominaisuuksien sekä ohjelmien poistaminen ja estäminen käyttöjärjestelmästä		
Minimoi sovellusten määrä, jätä vain välttämättömät sovellukset	☐ Ch	
Ylimääräisten Windows ominaisuuksien (feature) poistaminen	☐ Ch	
AppLocker-sääntöjen luominen	☐ Ch	
Luettelo asennetuista ohjelmista		☐ Ch
Ohjelmistohaavoittuvuuksien hallinnan kuvaus		☐ Ch
Käyttäjätilit- ja hallinta		
Käyttäjätilien määrittelyt ja hallinta		☐ Ch
Käyttäjä- ja pääsyoikeuksien hallinnan kuvaaminen ja dokumentointi		☐ Ch
Käyttöoikeuksien hyväksymisprosessi		☐ Ch
Disabloi Guest	☐ Ch	
Rajaa Administrator-ryhmään kuuluvien oikeudet	☐ Ch	
Käytä työasemaa "normaali"-tunnuksella	☐ Ch	
Aseta vahva salasana	☐ Ch	
Salasanan vaihtuminen	☐ Ch	
Tilien suojaamiseen liittyvien asetusten käyttöönotto	☐ Ch	

Ylläpitotunnusten säilytys tietoturvallisella tavalla siten, että salasanat ovat suojattuna sekä saatavilla	☐ Ch	
Services		
Katselmoi ja disabloi tarpeettomat servicet	☐ Ch	
Katselmoi Service Accountit (principle of least privilege)	☐ Ch	
Servicen liittyvien käyttöoikeuksien katselmointi ja koventaminen	☐ Ch	
Jäljitettävyys		
Toiminnan vaatimukset huomioiva työaseman lokitus	☐ Ch	
Lokien säilytys ja suojaus	☐ Ch	
Ylikirjoitusasetuksen tarkistaminen	☐ Ch	
Lokien siirto tasaisin väliajoin turvalliseen paikkaan	☐ Ch	
Lokitietoihin pääsyn rajoitus	☐ Ch	
Työaseman seurattavien lokitiedostojen määrittely ja kuvaaminen	☐ Ch	☐ Ch
Salasanasuojattu näytön lukitus 5 minuutin käyttämättömyyden jälkeen	☐ Ch	
Erillistyöaseman tilan todennus ennen käyttöönottoa ja muutosten yhteydessä		
Täydellinen haittaohjelmatarkastuksen ajo --> raportti	☐ Ch	
MBSA:n (Microsoft Baseline Analyzer) ajo --> raportti	☐ Ch	
Levynsalauksen (esim. BitLocker) käyttöönotto		
BitLocker: PIN with TPM (vahva PIN asetettava)	☐ Ch	
Recovery Key saatavilla tarvittaessa, säilytys turvallisessa paikassa		☐ Ch
Levyn salauksen dokumentointi		☐ Ch
Windows palomuuri		
Sääntöjen katselmointi: (inbound, outbound), oletuksena kaikki kielletään ja erikseen sallitaan ne säännöt, joita tarvitaan	☐ Ch	
Palomuuri päällä	☐ Ch	

Erillistyöaseman käyttöpaikan hyväksyminen ennen käyttöönottoa		
Tilan hallinnolliset ja fyysiset vaatimukset	☐ Ch	
TEMPEST-vaatimusten huomioiminen	☐ Ch	
Työaseman säilytyspaikka	☐ Ch	
Päivitykset		
Päivitysten ajantaisuuden tarkistaminen	☐ Ch	
Päivityssyklin tarkistaminen	☐ Ch	
Kovennuksen huomioiminen	☐ Ch	
Käyttöjärjestelmän ja sovellusohjelmistojen turvapäivitykset		☐ Ch
Käytössä olevat levyt ja tiedostojärjestelmä		
Käytössä olevan tiedostojärjestelmän tarkistaminen	☐ Ch	
Fyysisten levyjen tarkistus (tarkista ettei levyjä ole "unmountattuna")	☐ Ch	
USB-laitteiden käyttö työasemassa		
Vain sallittujen tikkujen käyttö työasemassa	☐ Ch	
Muiden usb-laitteiden rajaaminen	☐ Ch	
Kuvaus käytettävistä muistitikuista, ulkoisista levyistä, tulostimista		☐ Ch
Toipuminen, huolto ja elinkaaren päättyminen		
Varmuuskopio	☐ Ch	☐ Ch
Varautumissuunnitelma todennäköisimpiin riskeihin/uhkiin		☐ Ch
Toiminta työaseman huoltotilanteessa		☐ Ch
Prosessi levyllä olevan tiedon hävittämiseen elinkaaren päättyessä		☐ Ch
Muutoshallinta		
Muutoshallintamenettelyn kuvaus		☐ Ch
Turvallisuuskoulutus		
Tilakoulutus		☐ Ch
Työasemakoulutus		☐ Ch