Opinnäytetyö AMK

Tietojenkäsittely

2019

Joonas Lapinmäki

IT-OMAISUUDEN HALLINTA

– Case: Tietoturvalaboratorio

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2019 | 19 sivua

Joonas Lapinmäki

IT-OMAISUUDEN HALLINTA

- Tapaus: Tietoturvalaboratorio

Opinnäytetyön tilaajana on Turun ammattikorkeakoulun Tietoturvalaboratorio, joka toimii ICT-cityssä koulun tiloissa. Ongelma on IT-omaisuuden hallinta, joka on ollut vaikeaa ilman asianmukaista työkalua tai ohjelmistoa. Ongelma on alkanut oppilaiden vaihtuessa ja tiedon alkaessa kasaantua perimätiedoksi, sen sijaan että se olisi jollain tavalla hallittavassa muodossa opettajilla.

Tämän opinnäytetyön tarkoituksena oli löytää ohjelma tai ohjelmisto millä hallitaan IT-omaisuutta tietoturvallisesti ja helposti.

Opinnäytetyön aikana tutkittiin internetistä löytyviä vertailuja ja arvosteluja ohjelmistoista sekä muuta materiaalia kuten ohjelmistojen valmistajien sivustoja. Niistä opinnäytetyön tuloksena löytyi yksi ohjelma, mikä asennettiin virtuaalikoneelle ja testattiin toimivaksi ratkaisuksi haluttuun lopputulokseen.

Thycotic Secret Server toimii itsenäisenä palvelimena Tietoturvalaboratorion palvelimella, pitäen tallessa sisäänkirjautumistiedot ja koneiden sijainnit. Tietoturvalaboratorion johtaminen ja käyttäminen on nyt helpompaa.

ASIASANAT:

IT omaisuuden hallinta, VMware, Thycotic Secret server, salasanojen hallinta

BACHELOR´S / MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Data processing

2019 | 19 pages

Author(s)

IT ASSET MANAGEMENT

- Case: Tietoturvalaboratorio

The thesis is commissioned by the Turku University of Applied Sciences' Information Security Laboratory, which operates in ICT-City at the school premises. The problem is the management of IT assets, which has been difficult without the proper tool or software. The problem has begun as pupils change and as knowledge begins to accumulate as a tradition, rather than being in some way manageable form with teachers.

The purpose of this thesis was to find a program or software to manage IT assets safely and easily.

During the thesis, comparisons and reviews of software and other material found on the Internet were studied, such as software manufacturers' websites. As a result of this thesis, one program was found, which was installed on a virtual machine and tested as an effective solution for the desired end result.

Thycotic Secret Server acts as a standalone server on the Information Security Laboratory server, keeping login information and machine locations. Managing and using Information Security Laboratory is now easier.

KEYWORDS:

IT asset management, VMware, Thycotic Secret server, passwords management

SISÄLLYS

1 JOHDANTO **1**

2 IT-OMAISUUDEN HALLINTA **2**

2.1 Laitteiden ja ohjelmistojen parametrit ja luokittelut 2

2.2 Laitteiden skannaus 3

2.3 Laitteiden elinkaari 4

2.4 Lisenssit 6

3 TIETOJÄRJESTELMÄN VAATIMUKSET **7**

3.1 AMK:n Tietoturvalaboratorion nykytilanne IT-omaisuuden hallinnassa 7

3.2 Salasanojen hallinta 8

3.3 Toimintavarmuus, tietoturva ja käytettävyys 8

4 OHJELMAT JA VIRTUAALIKONEET **9**

4.1 Vertailtavat ohjelmat 9

4.2 Thycotic Secret Server 9

4.3 Asennus 11

4.4 Secret Serverin secretit 12

4.5 Salasanojen hallinta 15

4.6 Käyttäjät 17

4.7 Privileged Manager 17

5 LOPUKSI **19**

LÄHTEET **20**

KUVAT

Kuva 1. Secret Serverin ilmaisversion lataus (Thycotic 2019). 10
Kuva 2. Secretit (Thycotic 2019). 13
Kuva 3. Secret oppilas3:n sisäänkirjautumistiedoista (Thycotic 2019). 14
Kuva 4. Auditointi (Thycotic 2019). 15
Kuva 5. Salasanan vaatimusten muokkaus (Thycotic 2019). 16
Kuva 6. Roolien muokkaus (Thycotic) 17
Kuva 7. Privileged Manager (Thycotic 2019). 18

TAULUKOT

Taulukko 1. Parametrit (ManageEngine 2019). 2
Taulukko 2. Luokittelut (ManageEngine 2019). 3
Taulukko 3. Laitteiden skannaus (ManageEngine 2019). 4
Taulukko 4. Askel askeleelta laitteiden elinkaari (ManageEngine). 5
Taulukko 5. Secret serverin eri ominaisuudet (Thycotic 2019). 11
Taulukko 6. Privileged Manager lisenssien tarve (2019). 18

1 JOHDANTO

Turun ammattikorkeakoulun Tietoturvalaboratorion ongelmana on IT-omaisuuden hallinta: miten pidetään kirjaa erilaisista tietojärjestelmistä, jotka ovat laboratorion ylläpidossa. Tietojärjestelmistä pitää olla selvillä vähintään sijainti, palvelimen tai pilvipalvelun sijainti ja IP-osoite, käyttötarkoitus, projektin tilaaja, käyttäjätunnukset ja salasanat. Opiskelijahenkilöstö vaihtuu jatkuvasti, joten tieto on oltava saatavilla keskitetysti ja hallitusti.

Suurin ongelma on salasanojen hallinta, koska toisaalta ne pitää tallentaa salattuina ja toisaalta laboratorion henkilökunnan täytyy päästä niihin tarvittaessa käsiksi. Tämä ongelma on ihan yleinen, pienillä IT-alan yrityksillä ei yleensä ole yhdessä turvallisessa paikassa kaikkien koneiden IP-osoitteita ja sisäänkirjautumistietoja, eikä jotakuta hoitamaan niitä. Sekä fyysisiä että virtuaalikoneita saattaa olla missä tahansa, eikä kukaan välttämättä tiedä niihin ylläpitäjän sisäänkirjautumistietoja.

Tämän opinnäytetyön tarkoituksena on tutkia, mikä ratkaisu olisi hyvä IT-omaisuuden hallintajärjestelmäksi. Tutkimusmenetelmänä on case-tutkimus, jonka toimeksianto on Turun ammattikorkeakoulun Tietoturvalaboratoriolta. Etsin eri tapoja toteuttaa tämän ja aion testata käytännössä, mikä palvelee asiassa parhaiten.

Vaatimuslistalla on muutamia välttämättömiä asioita sekä lisäominaisuuksia, joiden saaminen voisi helpottaa hallintaa. Välttämättömiä ovat esimerkiksi koneiden IP-osoitteiden näkyvyys ja mahdollisuus nimetä ne, tämän lisäksi ylläpitäjän täytyy kyetä näkemään niiden käyttäjätunnukset ja salasanat. Lisäominaisuuksia ovat esimerkiksi peruskäyttäjän mahdollisuus pyytää käyttäjätunnus sekä salasana, jolloin jää jälki ylläpidolle, kenellä on tiedossa sisäänkirjautumistiedot. Testausta tehdessäni hyödynnän virtuaalikoneita, joille asennan eri ohjelmistot ja testaan niiden soveltuvuutta IT-omaisuuden hallintajärjestelmäksi.

2 IT-OMAISUUDEN HALLINTA

IT-omaisuuden hallinta on tapa, miten pidetään kirjaa erilaisista tietojärjestelmistä ja laitteista, jotka ovat yrityksen ylläpidossa. Se pitää sisällään laitteiden elinkaaren hallinnan kuten myös laitteiston hallinnan ja ohjelmiston hallinnan. Tietojärjestelmä on järjestelmä, joka koostuu ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista sekä ohjelmistoista. Sen tarkoituksena on tietojen tehokkaampi käsittely ja toiminnan helpottaminen tai mahdollisesti koko toiminnan toteuttaminen. Tietojärjestelmä sekoitetaan välillä pelkkään ohjelmaan tai ohjelmistoon, vaikka se on käsitteenä laajempi. IT-omaisuuden hallinta voi auttaa monessa asiassa: ylimääräisten huoltojen kustannuksien vähentämisessä, lisenssien optimaalisemmassa käytössä sekä vähentää käyttämättömien laitteiden määrää että tietoturvariskejä. (ManageEngine 2019)

2.1 Laitteiden ja ohjelmistojen parametrit ja luokittelut

Laitteiston hallinta (Hardware asset management) pitää tallessa tietoa fyysisistä tietokoneen osista(laitteiden elinkaari) ja tietoverkoista. Laitteiston hallinta (software asset management) on hyvin samanlainen prosessi kuin laitteiston hankinta, se keskittyy ohjelmistojen omaisuuteen sisältäen lisenssit. (ISO 2019) Taulukosta 1 näkee oleellisimmat seurattavat parametrit sekä laitteiston että ohjelmiston osalta. Niistä on tärkeää tietää mahdollisimman paljon, jotta niistä on jatkossa helpompi tehdä tärkeitä päätöksiä.

Taulukko 1. Parametrit (ManageEngine 2019).

Laitteiston parametrit	Ohjelmiston parametrit
Määritettävän laitteiston luokka	Ohjelmiston versionumero
Laitteen nykyinen tila	Ohjelmiston asennusten lukumäärä
Hankintahinta	Valmistajan nimi
Toimittajan nimi	Luokka ja alaluokka mihin ohjelmisto kuuluu
Takuun voimassaolo	

Taulukosta 2 näkee laitteiden luokittelut, ne kannattaa jakaa kolmeen alla näkyvään osioon seurattavuuden vuoksi. Kun näiden tietoja jaksetaan pitää päivitettyinä ja oikeina, on niistä helpompi tehdä päätöksiä. Kun yritys tai organisaatio kasvaa isommaksi, tarvitaan myös enemmän laitteistoa tukemaan yrityksen tehtävien määrän kasvua. Ajan tasalla oleva laitteiston seuranta prosessi helpottaa asioiden ylläpitoa ja seuraamista, ei väliä kuinka paljon yritys kasvaa. (ManageEngine 2019) Asian tärkeys tulee sesonkiaikoina esille, silloin on oltava sopiva ylimäärä laitteita. Esimerkiksi joulusesongin aikana kaupoissa tarvitaan enemmän henkilökuntaa ja heille laitteistoa, täytyy tietää missä laitteisto on ja onko niitä riittävästi.

Taulukko 2. Luokittelut (ManageEngine 2019).

Laitteistot	Komponentit	Ohjelmistot
Serverit	Näppäimistö	Ohjelmisto
Työasemat	Hiiri	Ohjelmiston lisenssit
Tulostimet	Web-kamera	
Skannerit	Projektorit	
Reitittimet		
Älypuhelimet		
Tabletit		
Virtuaalikoneet ja niiden hostit		

2.2 Laitteiden skannaus

Tehtävä aloitetaan havaitsemalla laitteet sisäverkon sisältä. Taulukossa 3 näkyy mitä kaikkea voidaan skannata. Windows toimialueen skannaus näyttää kaikki Windows-käyttöjärjestelmällä olevat laitteet. Verkko skannauksella nähdään Linux tai Mac käyttöjärjestelmän laitteet, virtuaaliset koneet, tulostimet, reitittimet ja kytkimet. Niiden valmistajilla tai malleilla ei ole vaikutusta asiaan. (ManageEngine 2019)

Taulukko 3. Laitteiden skannaus (ManageEngine 2019).

Windows toimialue skannaus	Verkko skannaus
Windows laitteet	Linux, Solaris
	Mac, AIX
	VMHost koneet
	Tulostimet
	Reitittimet ja kytkimet

Laitteiden etsinnän tulos agentti-pohjaisella toimintatavalla tarkoittaa, että kaikissa työasemissa otetaan käyttöön agentti, joka skannaa tiedot laitteistosta ja lähettää tiedot keskuspalvelimelle. Myöhemmät skannaukset lähettävät vain muuttuneen tiedon, kuluttaen näin vähemmän tehoa ja tietoverkkoa. Tällä tavoin voidaan skannata myös laitteita, jotka eivät ole sisäverkossa tai ovat kannettavia laitteita. Näitä skannauksia voidaan tehdä myös valikoivasti. Jos halutaan käyttää laitteiden etsintää ilman agenttia, täytyy kaikkien laitteiden olla sisäverkossa ja kytkettynä päälle. Näin ollen ei myöskään tule agenttien asennusten kuluja, käyttökustannuksia eikä päivityksiä. (ManageEngine 2019)

2.3 Laitteiden elinkaari

Laitteiden elinkaaren hallinnan tärkeimmät ja kriittisimmät kohdat ovat käyttöönotto ja käytöstä poistaminen. Käyttöönoton kuuluu olla helppoa ja sujuvaa. Käytöstä poiston pitää tapahtua tietoturvallisesti; kukaan ulkopuolinen ei käytöstä poiston jälkeen saa saada käsiinsä mitään tietoa laitteen sisältä. Kaikki elektroniset laitteet näytöstä tulostimeen otetaan uutena käyttöön ja vanhetessaan ajan kuluessa poistuvat käytöstä. Toiset laitteet nopeammin kuin toiset, mutta työn sujuvuuden ja tietoturvallisuuden vuoksi yritysten ja organisaatioiden pitäisi ottaa huomioon laitteiden elinkaari kokonaisuudessaan. (Centero 2019)

Taulukosta 4 on nähtävillä laitteiden elinkaari anomuksesta hävitykseen. Prosessi etenee aika lailla samoin, oli mikä vain laite kyseessä. Ensin käyttäjä tai osasto tekee anomuksen uudesta omaisuudesta ja ostohakemus lähtee hyväksyttäväksi. Tämän jälkeen omaisuus otetaan käyttöön siellä, minne se on tilattu. Jos omaisuuden sijainniksi laitetaan säilytys, se on joko varastossa tai korjauksessa. Lopulta omaisuuden käyttö päättyy

ja pitää miettiä laitetaanko laite poistoon vai keksitäänkö sille uusiokäyttöä. (ManageEngine 2019) Esimerkiksi näyttöpäätteen kohdalla valinta riippuu laitteen iästä, resoluutiosta, koosta ja mahdollisesti paneelityypistä. Vanhahtavat huonot paneelit pienellä tuumakoolla ja resoluutiolla joutavat ser-jätteeseen. Sen sijaan paremmalla paneelilla varustetut vähintään 23 tuumaiset 1080 korkeuspikselin näytöt voidaan monissa yrityksissä ottaa uudelleen käyttöön. Vuokranäyttöjen kohdalla tätä ei tarvitse miettiä, ne menevät lähes poikkeuksetta takaisin vuokrayritykselle.

Taulukko 4. Askel askeleelta laitteiden elinkaari (ManageEngine).

Anomus uudesta omaisuudesta (Anottu)
Hyväksyntä (Odotus hyväksynnälle, hyväksytty)
Hankinta (Ostettu tai vuokrattu)
Käyttöönotto (Asennuksessa, asennettu)
Käyttö (Käytössä)
Varasto (Varastossa tai korjauksessa)
Käytön päättyminen (Poisto käytöstä tai poistoon)
Hävitys (Hävitetty)

Laitteiden käyttöaste voi vaihdella, esimerkiksi Tietoturvalaboratoriossa osa koneista on päivittäisessä käytössä ja osaa käytetään yhdestä kolmeen kertaan viikossa, mahdollisesti eri käyttäjien toimesta. Laitteiden elinkaaressa tämä tarkoittaa tärkeää vaihetta kohdissa käyttö ja varasto. Varasto on huono termi kuvaamaan sitä, että laite on olemassa mutta sitä ei käytetä, eihän sitä varsinaisesti siirretä varastoon silloin kun kukaan ei käytä sitä, vaan sitä ei yksinkertaisesti kukaan käytä silloin. Mutta jos on hyvin seurattu, missä tilassa koneet ovat ja milloin, tiedetään, tarvitaanko koneita lisää vai riittääkö vähempikin. Turha makuuttaa koneita mitä kukaan ei käytä. (ManageEngine 2019)

Laitteiden tagit ovat nykyaikaa ja niitä käytetään tarvittaessa. Tageina toimivat esimerkiksi viivakoodit, RFID eli radiotaajuinen etätunnistus tai GPS, jotka mahdollistavat laitteen seurannan. Tällä ei tarkoiteta pelkkää fyysistä seurantaa, että nähdään kartalla missä kännykkä menee, vaan myös laitteen tila, onko se käytössä vai ei. Niistä myös

selviävät jatkuvasti omistajuus tai hallinnointi sekä laitteiston kokoonpano. (ManageEngine 2019)

2.4 Lisenssit

Lisenssien hankkimisessa on hyvä edetä asia kerrallaan. Ensin täytyy esimerkiksi selvittää ja tunnistaa mitä lisenssejä jo omistetaan, milloin ne päättyvät ja onko ne yhdistetty mihinkään sopimukseen. Lisenssien tyypeistä tarvitsee tietää määrä, yksilöllisyys, alkuperäinen laitevalmistaja, CAL (client access licence, käyttäjän mahdollisuus käyttää palvelin ohjelman palveluita), rinnakkaisuus ja mistä lisenssi hankitaan. Riippuen siitä, millainen yritys on ja mitä ohjelmistoja omistetaan, tutkitaan ja valitaan sopivimman tyyppiset lisenssit tai yhdistelmät lisenssejä. Tärkeimmät lisenssit ovat jatkuvia, kun taas uusi ohjelmisto mitä testataan, otetaan määräaikaisella lisenssillä. Lisenssien täsmäytys vaatii paljon manuaalista vaivannäköä. Jos käytössä oleva ohjelmisto sisältää työkalut IT-omaisuuden hallinnalle lisenssien suhteen, sieltä saa kolme tärkeää yksityiskohtaa: asennusten määrä, käytettävissä olevat lisenssit ja jo käytössä olevat lisenssit. (ManageEngine 2019)

3 TIETOJÄRJESTELMÄN VAATIMUKSET

Vaatimuslistalla ovat Tietoturvalaboratorion puolesta seuraavat asiat: ohjelmiston täytyy kyetä pitämään tallessa tietoa tietojärjestelmistä vähintään sijainti, käyttötarkoitus, tilaaja, käyttäjätunnukset ja salasanat. Koska opiskelijahenkilöstö vaihtuu jatkuvasti, kaiken tiedon tulee olla saatavilla keskitetysti ja hallitusti. Lisäominaisuuksia ovat esimerkiksi peruskäyttäjän mahdollisuus pyytää käyttäjätunnus sekä salasana, jolloin jää jälki ylläpidolle, kenellä on tiedossa sisäänkirjautumistiedot.

3.1 AMK:n Tietoturvalaboratorion nykytilanne IT-omaisuuden hallinnassa

Virtuaalikoneiden sijainnit ovat osaksi tallessa VMwaren vSpheressä ja Oraclen VM Servereillä. Näiden sisäänkirjautumistiedot ovat tallessa missä ovat, osa sähköpostiviesteissä ja osa tiedoston sisällä esimerkiksi opettajan koneella. Minä olen tehnyt Tietoturvalaboratoriolle pari koekonetta. Tällä hetkellä vain minä ja opettaja, jolle lähetin tiedot koneista, tiedämme koneiden sijainnit ja sisäänkirjautumistiedot. Kun minä tämän kevään jälkeen valmistun koulusta, minulla ei enää ole koulusähköpostia, joten minulta ei kukaan voi sitä kautta kysyä tiedoista. Tällöin ainoastaan opettaja tietää koneista. Hän voi kuitenkin vaihtaa työpaikkaa, jäädä sairauslomalle, unohtaa nimeni ja sen milloin olen tiedot koneista lähettänyt, joten tieto koneista voi kadota kokonaan. On myös mahdollista, että joku muu opettaja tai oppilas tarvitsee tietoja tekemistäni koekoneista, eikä tiedä mistä kysyä.

Tällä hetkellä tieto voi myös siirtyä opiskelijalta seuraavalle, jos joku jatkaa samoista hommista mihin edeltäjä on jäänyt. Jo vuodessa kahdessa väki vaihtuu paljon ja välttämättä kukaan ei ole jatkanut samoista jutuista mihin edeltäjä on jäänyt, vaan uudessa projektissa. Tämän takia käy helposti niin, ettei koneiden sijainnista tai ylläpitäjän tunnuksista ole mitään tietoa kenellekään. Ei vaikka ne olisi tallennettu samaan paikkaan, koska niiden nimeämiskäytäntö ei välttämättä ole kovin looginen. On myös verkkokiintolevy, jonka olemassa olosta osa opiskelijoista ei tiennyt mitään.

Tietoturvalaboratoriolla on kaksi eri ohjelmistoa tietojärjestelmille projekteista riippuen. Tämä ja muut edellä mainitut asiat eivät ole tulevaisuudessa ongelma, kunhan saadaan Tietoturvalaboratoriolle IT-omaisuuden hallinta ohjelmisto. Se tekee sekä laboratorion johtamisesta että siellä työskentelystä helpompaa ja tehokkaampaa, tietoturvallisesti.

3.2 Salasanojen hallinta

Salasanat ovat vaikea asia tässä työssä. Toisaalta ne pitää tallentaa salattuina, ja toisaalta laboratorion henkilökunnan täytyy päästä niihin tarvittaessa käsiksi. On myös mietittävä, tuleeko yhteiskäyttötunnuksia vai jokaiselle omat. Vaihtuvuuden takia jokaiselle omat aiheuttaisi ylimääräistä työtä. Toisaalta silloin jäisi tarkalleen jälki ylläpitäjille, kuka on käynyt hakemassa salasanan ja mihin tietojärjestelmään. Jossain kohtaa käyttäjiä alkaa kuitenkin olla paljon ja monet jo valmistuneet koulusta, joten tarvitaan joku hoitamaan asiaa, ja se taas vie ylimääräistä aikaa. Yhteistunnukset tai paremminkin useammat tunnukset, joissa riittää oikeudet tiettyihin projekteihin, olisivat paremmat. Siinäkin voi tulla tilanteita, joissa ei oikeudet riitä, ja asiaa joutuu kysymään opettajalta, jolloin taas tulee ylimääräistä työtä.

Ilmaiset ohjelmat saattavat rajoittaa enimmäismäärän käyttäjiä tarpeisiin sopimattoman pieneksi. Täten valitsen luultavasti yhteiskäyttäjätunnukset, sillä ne voi sitten voi myöhemmin Tietoturvalaboratorio vaihtaa, jos yksilötunnukset koetaan paremmaksi. Tämä tietysti sillä edellytyksellä, ettei ilmaisen ohjelman rajoitus rajoitu yhteen tai kahteen käyttäjään, joka olisi aivan liian vähän.

3.3 Toimintavarmuus, tietoturva ja käytettävyys

Ohjelmiston olisi hyvä olla omana serverinään ja sinne pääsy selaimella vain Tietoturvalaboration verkosta. Ohjelmiston täytyy osata salata salasanat, jonka uskoisin kaikkien nykyaikaisten ohjelmistojen osaavan. Nykyaikaiset ohjelmat ovat varmasti muutenkin kaikin puolin tietoturvallisia. Käyttö ei saisi olla raskasta tietokoneelle eikä käyttäjälle, koska muuten ei olisi mitään hyötyä edes muuttaa mitään.

4 OHJELMAT JA VIRTUAALIKONEET

Virtuaalikoneiden hallintaan ja käyttöön valitsin VMwaren Workstation, joka ei ole ilmainen, mutta Tietoturvalaboratiolla on lisenssit siihen ja sen käyttö on minulle tuttua. Käyttöjärjestelmäksi valitsin Windows 10:n ja asensin 3 eri virtuaaliympäristöä, eri kokoisilla massamuisteilla. Tämä siksi, että on turha olla tarpeettoman suuri massamuisti, jos suurinta osaa tilasta ei koskaan käytetä. Liian pieneen taas ei mahdu mitään, mutta en vielä tässä vaiheessa tiennyt mikä on sopiva.

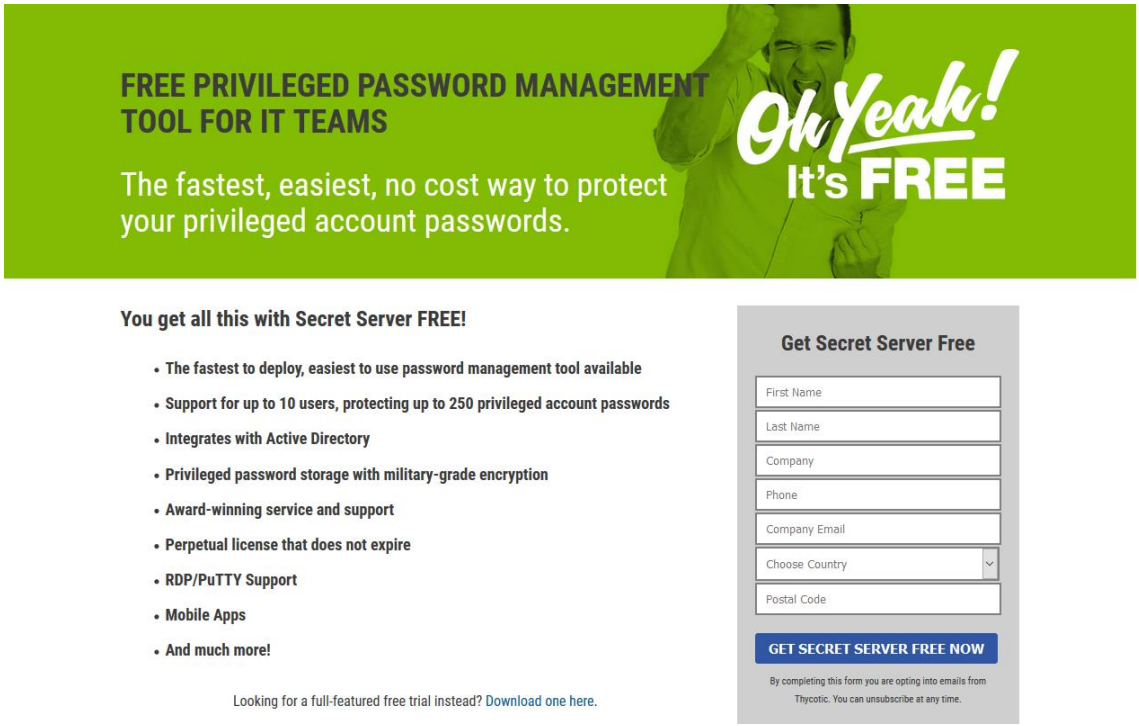
4.1 Vertailtavat ohjelmat

Empiiristen tutkimuksien tuloksena selvisi, että ilmaisena versiona haluttavaa ohjelmaa ei ole kuin yksi. Lähes kaikki ohjelmat on suunniteltu isoille yrityksille, joissa liikkuvat miljoonat eurot. Monesta ohjelmasta sai demon tai ilmaisen kokeilujakson, mutta niiden lisenssit pienellekin käyttäjämäärälle olivat useiden tuhansien arvoisia, ja hinta nousi huomattavasti joidenkin ominaisuuksien myötä, kuten auditointi. Yhdestä ohjelmasta on saatavilla ilmainen versio, josta seuraavaksi lisää.

4.2 Thycotic Secret Server

Kuvasta 1 on nähtävissä, että ohjelman lataus edellyttää tietojen täyttämistä, samalla tavalla on kaikissa muidenkin valmistajien ohjelmissa, vaikka kyse olisi vain kokeiluversiosta tai demosta.

Ohjelman ilmaisella versiolla lähdettiin liikkeelle ottaen selvää riittääkö se vaatimuksiin. Kysyin myös chatissa ohjelman hintaa, jos halusin sen sisältävän tiettyjä asioita, mutta siinä käskettiin valtuutetun henkilön pyytää tarjous. Sain kuitenkin sen verran selville, että puhutaan tuhansista euroista jo alle 10 käyttäjän määrällä.



Kuva 1. Secret Serverin ilmaisversion lataus (Thycotic 2019).

Kuten taulukosta 5 ilmenee, ilmaisversiossa ei ole kovin montaa asiaa, mutta mahdollisesti riittävästi. Tehostettu auditointi ja raportointi ovat saatavilla vasta Professionalissa ja sen hinta ei selviä tästä. Taulukko ei sisällä kaikkea: ominaisuudet, jotka on tarkoitettu isoille, miljoonaluokan yrityksille on jätetty pois. Platinum versio sisältää kaikki ominaisuudet. Secret Serverissä on erikseen Privileged Manager ja Secret Server. Ensimmäisessä on oikeuksien hallintaa ja jälkimmäisessä pidetään tallessa salasanoja.

Taulukko 5. Secret serverin eri ominaisuudet (Thycotic 2019).

Ominaisuus	Ilmainen	Vault	Professional
	10 käyttäjän rajoitus	25 käyttäjän rajoitus	
Sijainti	Oma palvelin	Oma palvelin ja pilvi	Oma palvelin ja pilvi
Secretit	250	Rajaton	Rajaton omalla palvelimella, 10000 pilvessä
Tekninen tuki, tietopohja, forumit	tietopohja ja forumit	Kyllä	Kyllä
Secure Vault ja salasana hallinta AD liitännällä	Kyllä	Kyllä	Kyllä
Havaitse paikalliset ja AD:n ylläpitäjätilit	Ei	Kyllä	Kyllä
Laajennettu auditointi ja raportointi	Ei	Ei	Kyllä
Edistynyt skriptaus	Ei	Ei	Lisäosa

Sekä Secret Serverin, että muidenkin ohjelmien hintojen kohdalla on vain ”Pyydä tarjous”. Hintaan vaikuttavat käyttäjämäärä, mahdolliset halutut lisäosat ja joissain tapauksissa se tuleeko tuote opiskelu tai tutkimuskäyttöön. Ohjelmien lisenssit on uusittava vuoden välein, joten hinta on aina per vuosi ja kaikissa puhuttiin useista tuhansista. Tällöin ohjelmissa tulee muutakin kuin välttämättömimmät. Näistä syistä sekä myös tietämättömyydestä tietoturvaan, on hyvin useiden suomalaisten pk-yritysten salasanojen hallinta tai koko IT-omaisuuden hallinta tietoturvattomasti tai kömpelösti toteutettu.

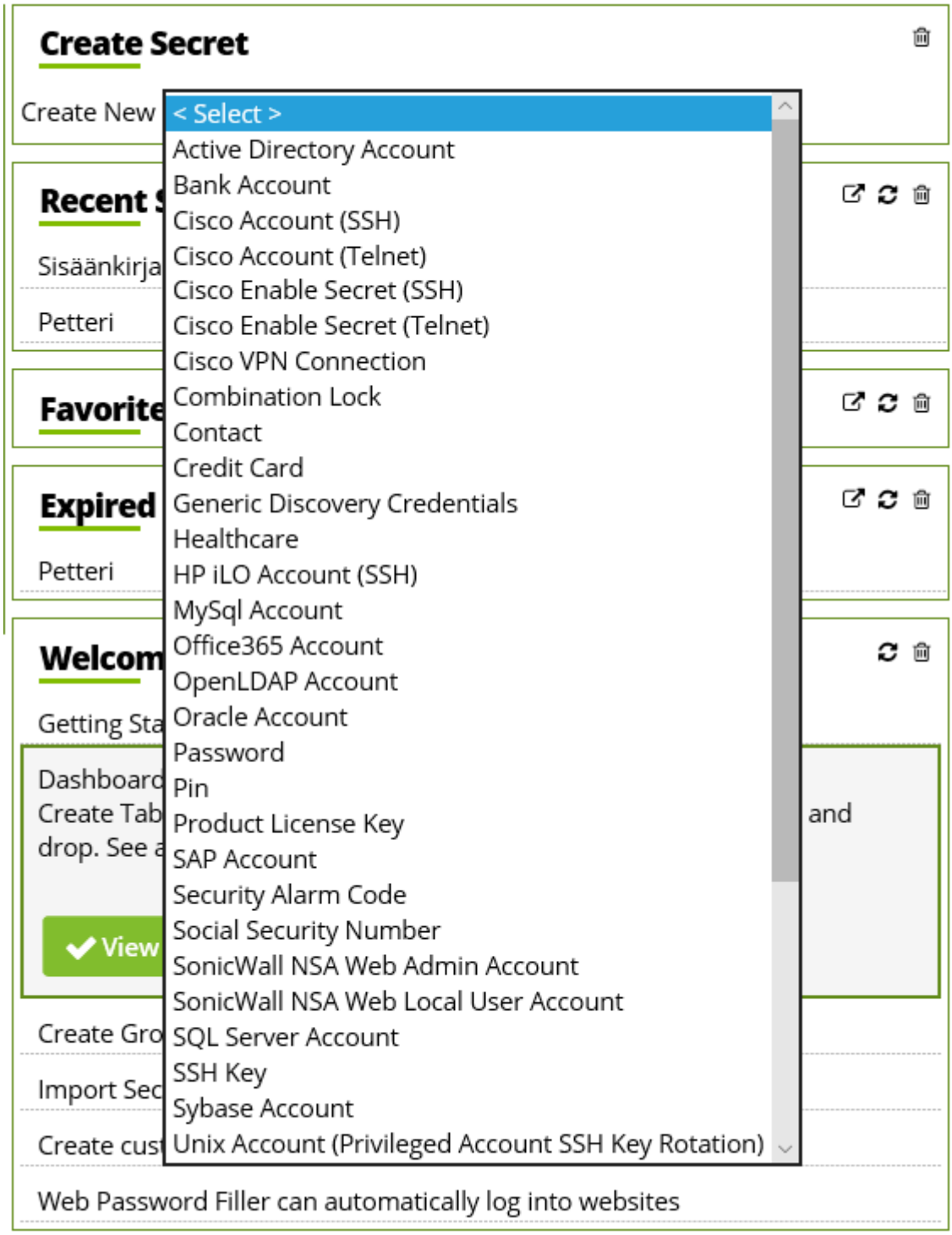
4.3 Asennus

Asennus on 15 minuutin työ ja siinä painetaan lähes koko ajan ”seuraava” painiketta. Asennuksen eteneminen näkyy koko ajan ja rivittäin lukee mitä tapahtuu. Jos asennus jostain syystä jää jumiin tai ei onnistu, asennusohjelma osaa kertoa missä vika on.

4.4 Secret Serverin secretit

Secret Serverissä käytetään termiä secret eli salaisuus tiedoista, jotka tallennetaan järjestelmään. Käytän jatkossa sanaa secret, koska se on ohjelmassa esiintyvä termi. Niitä on pitkä template-(pohja) lista valmiina ja itse saa lisättyä, osa niistä on näkyvissä kuvassa 2. Templatet ovat todella hyvin muokattavissa ja esimerkiksi salasanojen vaatimusten kohdalla SAP salasanan on oltava vähintään 12 merkkiä pitkä, koska se on SAPin vähimmäismerkkivaatimus. Maksimissaan secretejä voi olla 250 kpl ilmaisversiossa. Yleisimmät ja useimmin tarvittavat kuten password, SSH key ja Oracle account löytyvät suoraan.

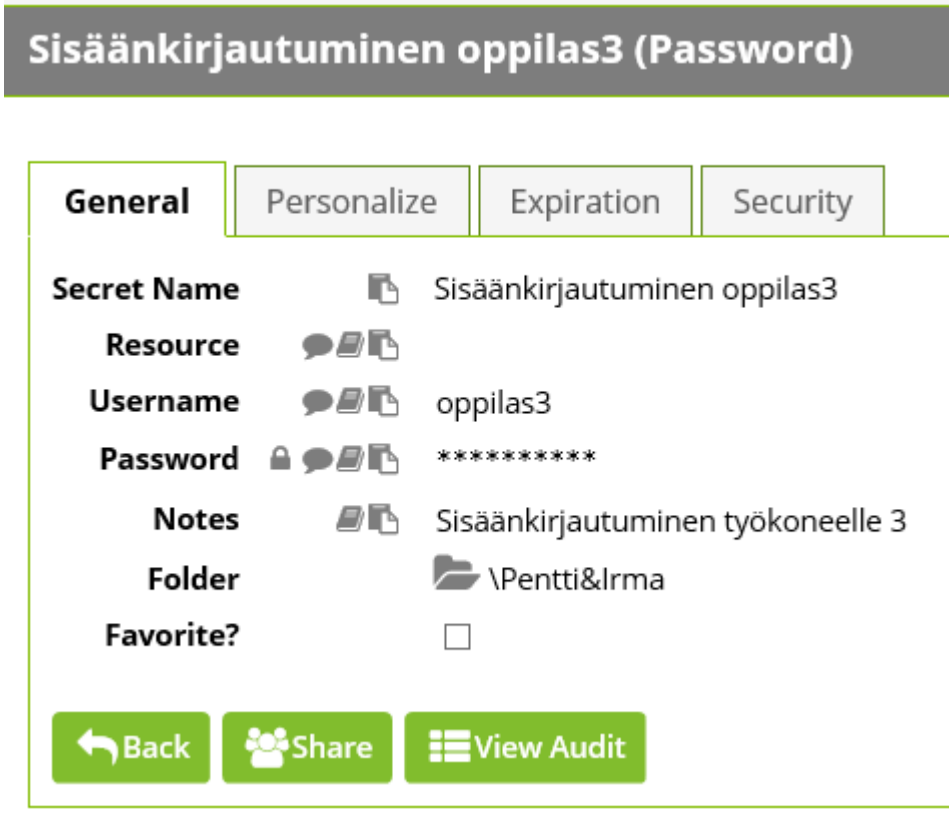
Käyttöliittymän oletuksena käytössä oleva laajennettu kotinäkymä sisältää pienoisohjelmia kuten viimeisimmät, suosikki ja päättyneet secretit. Pienoisohjelmat ovat hyvin muokattavissa. Perusnäkymässä näkyy pelkästään secretit, etsiminen ja mahdollisuus lisätä uusia secretejä.



Kuva 2. Secretit (Thycotic 2019).

Kuvassa 3 näkyvässä kohdassa Password on ensimmäisenä painike, josta näkee salasanan, tässä tapauksessa käyttäjän oppilas3 käyttäjätunnuksella sisäänkirjautumiseen. Lukon jälkeinen painike näyttää salasanan NATO-aakkosina eli A=Alfa, B=Bravo, C=Charlie ja niin edelleen. Kolmas painike secretin arvojen historia. Viimeinen painike

on kopiointi leikepöydälle. Nämä neljä näkyvät vain ylläpitäjälle, normaalilla käyttäjällä on näkyvissä lukko ja kopiointi leikepöydälle.



Kuva 3. Secret oppilas3:n sisäänkirjautumistiedoista (Thycotic 2019).

Kuvassa 4 näkyy auditointi. Kaikki tapahtunut on lokina, mikä sisältää ajan, käyttäjän nimen, tapahtuman ja merkinnän. Tämä on riittävä auditointi, eikä rasita ylläpitoa. Jos jotain epäilyttävää tapahtuu, päästään auditoinnista tarkistamaan kuka tai ketkä ovat käyneet secretiä katsomassa.

Audit View - Sisäänkirjautuminen oppilas3 (\Pentti&Irma)

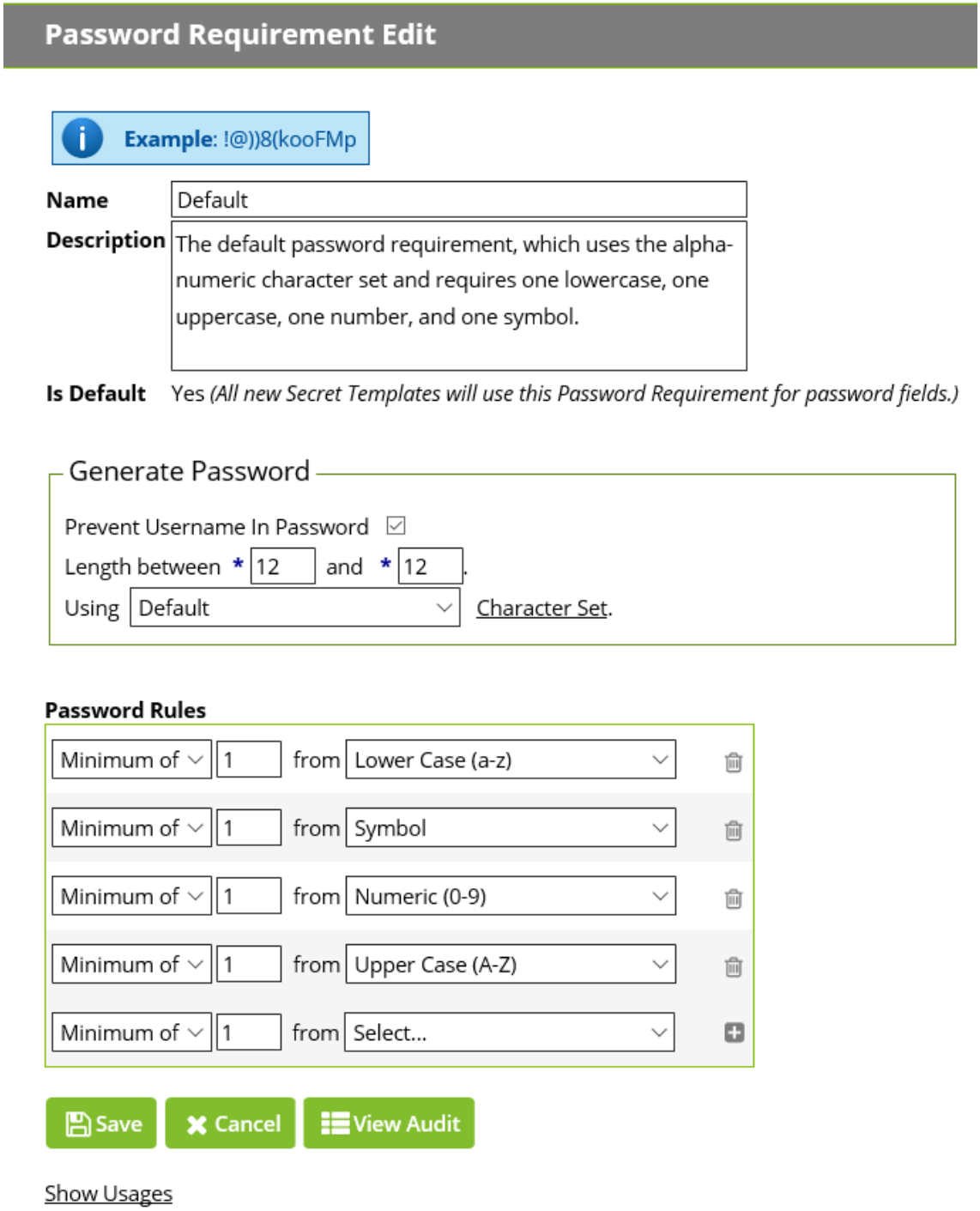
Explain

Date	Full Name	Action	Notes
6/6/2019 10:29 AM	admin	VIEW	
6/6/2019 10:04 AM	admin	VIEW	
5/15/2019 08:52 AM	Oppilas Yksi	PASSWORD DISPLAYED	
5/15/2019 08:52 AM	Oppilas Yksi	VIEW	
5/15/2019 08:50 AM	admin	PASSWORD DISPLAYED	
5/15/2019 08:50 AM	admin	VIEW	
5/12/2019 12:05 PM	Pentti	PASSWORD DISPLAYED	
5/12/2019 12:05 PM	Pentti	VIEW	
5/12/2019 12:04 PM	admin	UPDATE	Team oracle (Granted View)
5/12/2019 12:04 PM	admin	DISABLEINHERITANCE	
5/12/2019 12:04 PM	admin	UPDATE	Settings: (Inherit Permissions)
5/12/2019 12:03 PM	admin	VIEW	
5/12/2019 11:45 AM	admin	VIEW	
5/12/2019 11:30 AM	admin	SECRET COPIED TO	Copied To Sisäänkirjautuminen oppilas4 (Id:3)
5/12/2019 11:28 AM	admin	VIEWED EDIT	

Kuva 4. Auditointi (Thycotic 2019).

4.5 Salasanojen hallinta

Salasanojen vaatimusten editointi onnistuu Secret Templates hallinnan kautta. Oletuksena siellä on 3 eri pohjaa ja lisää voi luoda. Oletus pohjan saa valittua ja pohjia saa muokattua. Kuvasta 5 näkee salasanan sääntöjä kuten vähintään 1 merkki symboleja ja vähintään 1 numero.

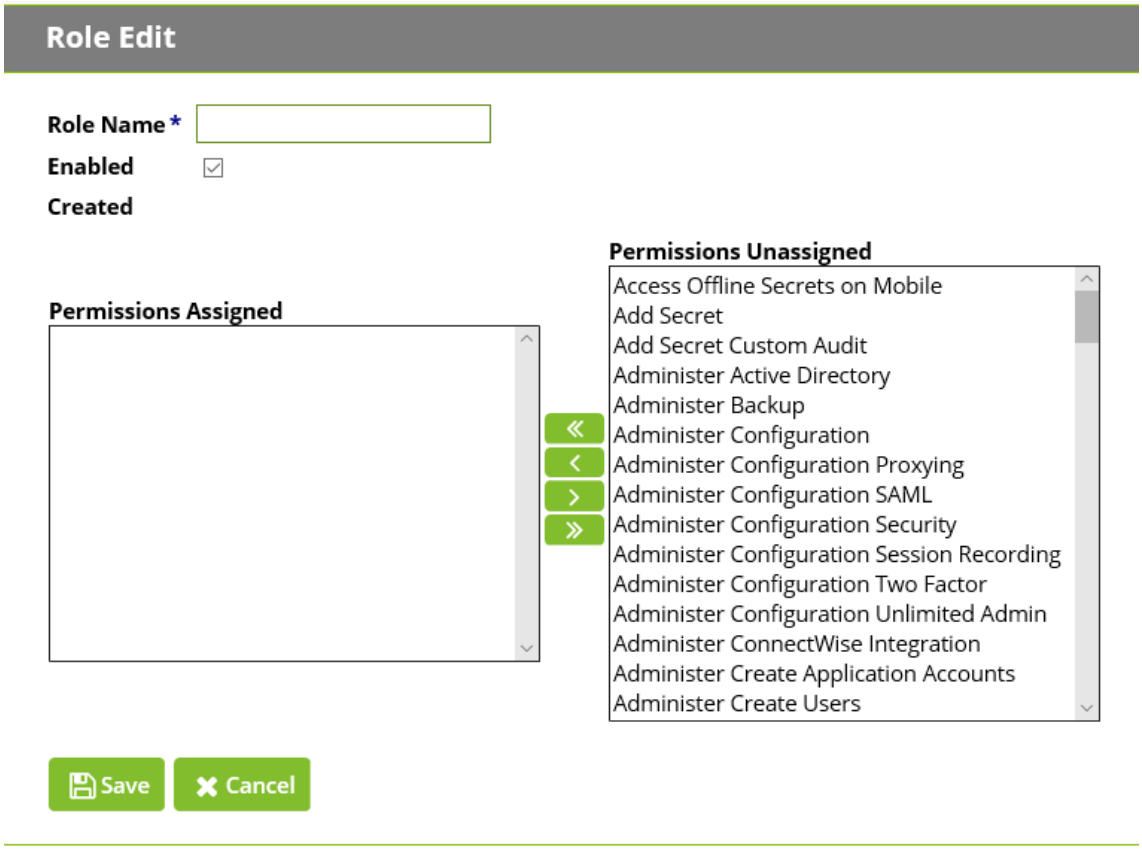


Kuva 5. Salasanan vaatimusten muokkaus (Thycotic 2019).

4.6 Käyttäjät

Ilmaisversiossa käyttäjiä voi olla enimmillään 10. Tietoturvalaboratoriossa oppilaita yhtenä lukuvuonna on 5-15 ja vaihtuvuus on suuri. Luultavasti siellä otetaan käyttöön yhteiskäyttötunnukset, tiimin saman asian kanssa työskenteleville yksi tunnus ja toisen osan kanssa työskenteleville toinen tunnus, mikäli tarvitaan useampia secretejä.

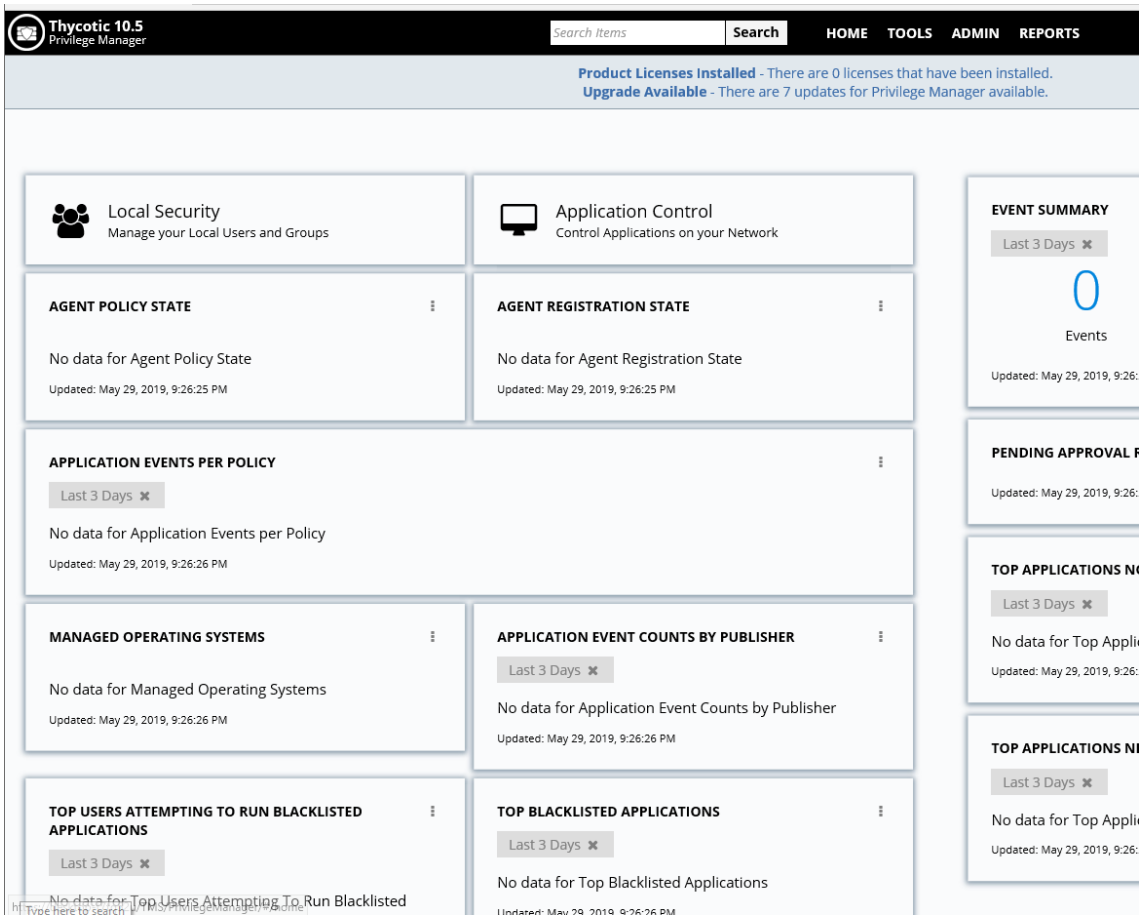
Oletuksena käytössä on eri rooleja käyttäjille, kuten ylläpitäjä, tavallinen käyttäjä sekä ryhmän omistaja. Niitä voi muokata, luoda itse lisää tai ottaa pois käytöstä ja takaisin käyttöön. Kuvasta 6 näkee käyttöliittymää niiden muokkaamiseen. Jokaiselle roolille saa valittua pitkästä listasta mitä ominaisuuksia haluaa roolilla olevan.



Kuva 6. Roolien muokkaus (Thycotic)

4.7 Privileged Manager

Kuvasta 7 näkee että Secret Server on muutakin kuin pelkkä salasananhallinta ohjelma. Tietoturvalaboratorion tapauksessa ei tällä hetkellä ole tarvetta Privileged Managerille (Käyttöoikeuksien hallinta) joten käyn sen hyvin pintapuolisesti läpi.



Kuva 7. Privileged Manager (Thycotic 2019).

Kaikkea ohjelmassa mukana olevaa ei saa käyttöönsä ilmaisversiossa, niihin tarvitsee lisenssin. Taulukosta 6 näkee, että hakemistopalveluiden yhdistäjä ja tavaraluettelo ratkaisu eivät tarvitse lisenssiä.

Taulukko 6. Privileged Manager lisenssien tarve (2019).

Tuotteen nimi	Tarvitsee lisenssin
Sovelluksen hallinta ratkaisu	Kyllä
Hakemistopalveluiden yhdistäjä	Ei
Tavaraluettelo ratkaisu	Ei
Paikallinen turvallisuus ratkaisu	Kyllä
Käyttöoikeuksien hallinta	Kyllä

5 LOPUKSI

Opinnäytetyön tavoitteena oli Turun ammattikorkeakoulun Tietoturvalaboratorion toive saada jollain tavalla toteutettuna toimiva IT-omaisuuden hallinta. Aiemmin se toteutettiin välttävästi, dokumentaatio saattoi sijaita yhdellä fyysisellä koneella Tietoturvalaboratoriossa, tietyllä käyttäjätilillä tai se oli lähetetty sähköpostilla opettajalle tai toiselle oppilaalle. Kenelläkään ei myöskään ole ollut riittävästi aikaa perehtyä asiaan. Laboratoriolla on ollut toiveissa jo pitempään saada toimiva systeemi ja nyt sellainen saatiin.

Asia oli paljon vaikeampi kuin osasin kuvitella. Suomeksi ei aiheesta ollut kirjoitettu kovin paljoa, eikä netissä ollut tietoa laajasti englanniksikaan. Koska kenelläkään ei tästä myöskään toimeksiantajan puolesta ollut tietoa aiheesta, ei valitettavasti tullut apua sieltäkään. Tutkimustyö eteni hitaasti mutta varmasti.

Monet halutut asiat kuten auditointi saatiin jo ilmaisella versiolla Thycotic Secret Serverillä, joten sitä ei lähdetty päivittämään maksulliseen. Tulevaisuudessa kaikki koneiden nimet, IP-osoitteet ja sisäänkirjautumistiedot ovat yhdessä paikassa helposti asianomaisten saatavilla. Tätä ohjelmaa ja näitä tietoja voin hyödyntää tulevaisuudessa, mahdollisesti työllistää itseni PK-yrityksiin heidän IT-omaisuuden hallinnan helpottamiseksi.

LÄHTEET

Centero. *Centero.* 2019. https://centero.fi/ratkaisut/it-ympariston-hallinta/moderni-laitteiden-elinkaaren-hallinta/ (haettu 6. 5 2019).

ISO. *IT asset management.* 2019. https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:ed-3:v1:en (haettu 26. 05 2019).

ManageEngine. *Manage Engine.* 2019. https://www.manageengine.com/products/service-desk/it-asset-management/what-is-it-asset-management.html (haettu 29. 4 2019).