KARELIA-AMMATTIKORKEAKOULU
Tieto- ja viestintätekniikan koulutus

Aleksi Reinikainen

SALASANAJÄRJESTELMÄ TIETOTEKNIIKAN ALAN YRITYKSELLE

Opinnäytetyö
Kesäkuu 2019

Karelia AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Kesäkuu 2019
Tieto- ja viestintätekniikan koulutus

Tikkarinne 9
80200 JOENSUU
p. (013) 260 600

Tekijä
Aleksi Reinikainen

Nimeke
Salasanajärjestelmä tietotekniikan alan yritykselle

Tiivistelmä

Tietoturvan merkitys on nykyaikana kasvanut yrityksissä huomattavasti. Heikot salasanat ovat suuri riski yrityksen tietoturvalle. Tämän vuoksi yritykset hyödyntävät salasanajärjestelmiä välttääkseen heikkojen salasanojen muodostumisia. Salasanajärjestelmillä mahdollistetaan myös salasanojen turvallinen säilyttäminen ja hallitseminen. Opinnäytetyön tavoitteena oli parantaa tietotekniikan alan yrityksen tietoturvaa ottamalla käyttöön yritykselle sopiva salasanajärjestelmä.

Opinnäytetyössä valittiin neljä salasanajärjestelmää arvioitavaksi. Arvioinnissa selvitettiin, mitkä kaksi järjestelmää olisivat sopivimmat ratkaisut yritykselle. Nämä kaksi järjestelmää asennettiin yritykselle ilmaisversioilla testaukseen. Testausvaiheessa selvitettin, kumpi järjestelmistä vastaa parhaiten yrityksen tarpeita. Sopivin järjestelmä ostettiin yritykselle käyttöön. Kaikissa salasanajärjestelmissä oli kaikki salasanajärjestelmiltä vaaditut ominaisuudet. Ostetussa järjestelmässä oli kuitenkin yritykselle tuttu KeePass-integraatio, joka haluttiin yritykselle käyttöön. Ostettu järjestelmä oli on-premise-palvelin, joka asetettiin yrityksen omiin tiloihin. Järjestelmä ostettiin kertamaksulla, joten järjestelmästä ei tule tulevaisuudessa kuluja. Järjestelmän ostamisen jälkeen viimeisteltiin järjestelmän käyttöönotto yritykselle.

Kieli
suomi

Sivuja 26

Asiasanat
tietotekniikka, salasanajärjestelmä, tietoturva

THESIS
June 2019
Degree Programme in Information Technology
Tikkarinne 9
FI 80200 JOENSUU
FINLAND
Tel. +358 13 260 600

Author
Aleksi Reinikainen

Title
Password Manager for an Information Technology Company

Abstract

The importance of information security has grown considerably in companies today. Weak passwords are an enormous risk to enterprise security. As a result, companies use password managers to avoid weak passwords. Password managers also make it possible to safely store and manage passwords. The aim of the thesis was to improve information security of the information technology company by introducing a suitable password manager for the company.

In the thesis four password managers were selected for evaluation. The aim of the evaluation was to examine which two password managers would be the most appropriate solutions for the company. These two password managers were installed in the company for free testing. At the testing stage, it was examined which of the password managers best suits the needs of the company. The most suitable password manager was purchased for use by the company. All password managers had all the features required by password managers. However, the purchased password manager had KeePass integration familiar to the company, and thus it was desired by the company. The purchased password manager was an on-premise server that was placed in the company's own premises. The system was purchased on a one-off payment, so there will be no future costs for the password manager. After the purchase of the password manager, the introduction of the password manager for the company was finalized.

Language

Finnish

Pages 26

Keywords

information technology, password manager, information security

Sisältö

Lyhenneluettelo

AD	Active Directory, aktiivihakemisto
IIS	Internet Information Services
LDAP	Lightweight Directory Access Protocol
LDAPS	Secure Lightweight Directory Access Protocol
MFA	Multi-factor authentication
PMP	Password Manager Pro
PPS	Pleasant Password Server
RDP	Remote Desktop Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSO	Single Sign-On
URL	Uniform Resource Locator

1 Johdanto

Vahvat salasanat ovat yrityksen tietoturvan kannalta välttämättömiä. Heikko salasana voi vaarantaa pahimmassa tapauksessa koko yrityksen tiedot, kun taas vastaavasti vahva salasana voi suojata yrityksen mahdolliselta kyberhyökkäykseltä. Useiden monimutkaisten salasanojen hallinta ja säilyttäminen tuo kuitenkin yritykselle usein haasteita. Kuinka jakaa salasanat oikeille henkilöille henkilöstön kesken ja missä salasanoja säilytettäisiin turvassa? Tässä kohtaa salasanajärjestelmät astuvat kuvioon. Salasanajärjestelmällä saadaan hallittua salasanoja yrityksen sisällä ja säilöttyä nämä turvalliseen paikkaan. [1.]

Suoritin harjoitteluni tietotekniikan alan yrityksessä, jossa työskentelee noin 50 henkilöä. Harjoitteluni aikana sain idean opinnäytetyötäni varten. Yritys tarvitsi käyttöönsä salasanajärjestelmän yrityksen salasanojen hallinnointia varten. Yritys, jolle tämä työ tehtiin, halusi pysyä salaisena, joten jatkossa tästä käytetään nimeä ”Yritys”. Yrityksellä oli jo ollut jonkin aikaa tavoitteena parantaa salasanojen hallintaa ja näiden säilyttämistä Yrityksen sisällä. Salasanat ovat suuri osa yrityksien tietoturvaa, joten katson työstäni olevan suuri hyöty Yritykselle.

Yritys käytti aiemmin KeePass Password Safe-ohjelmistoa salasanojen säilyttämiseen. Sovellus mahdollisti salasanojen säilyttämisen yhden tiedoston sisään ja tiedosto saatiin salattua salasanalla ja erillisellä avaintiedostolla. Tällä ohjelmalla ei kuitenkaan saatu hallittua salasanoja millään tavalla. Uuden salasanajärjestelmän myötä oli tarkoitus saada salasanat valvottuun hallintaan. Salasanajärjestelmän pääosainen tarkoitus oli parantaa yrityksen tietoturvaa salasanajärjestelmän erilaisten ominaisuuksien avulla. Yrityksen toiveena oli, että salasanojen hallinta ja jakaminen onnistuisi selaimen tai erillisen sovelluksen kautta. Salasanajärjestelmän tulisi sisältää AD eli Active directory-integraatio, ja järjestelmästä tulisi löytyä tarpeellinen raportointi salasanoista. Lisäksi käyttäjiä tulisi pystyä lisäämään erilaisiin rooleihin, jolloin Yrityksen käyttäjien hallinnointi olisi helppoa. Järjestelmässä pitää olla myös ominaisuus varmuuskopioiden ottamiseen salasanoista ja järjestelmän asetuksista. Opinnäytetyö aloitettiin näiden toiveiden pohjalta.

Opinnäytetyössä esitellään aluksi salasanojen merkitystä yrityksille ja sitä, mistä vahva salasana koostuu. Tämän jälkeen aloitetaan opinnäytetyön tekeminen Yritykselle valitsemalla neljä salasanajärjestelmää arvioon. Näistä neljästä järjestelmästä valitaan kaksi Yritykselle sopivinta salasanajärjestelmää testaukseen. Testauksessa asennetaan salasanajärjestelmistä ilmaiset kokeiluversiot Yritykselle ja arvioidaan salasanajärjestelmien sopivuus Yritykseen. Testauksen jälkeen ostetaan Yritykselle sopivin salasanajärjestelmä. Lopuksi jalkautetaan salasanajärjestelmä käyttöön Yritykselle.

2 Salasanojen merkitys

Salasanoilla todistetaan luvallinen käyttö laitteisiin tai sovelluksiin. Salasanat voivat kuitenkin päätyä vääriin käsiin, jolloin voi tapahtua tietomurto. Kaikki tietotekniset laitteet, kuten tietokoneet, läppärit ja tabletit ovat alttiita joutumaan hakkerointihyökkäyksen kohteiksi. Seurauksena voi olla muun muassa tärkeiden tietojen menetys, pankkikorttitietojen varastus ja identiteettivarkaus. Tietomurron kohteeksi joutuneen uhrin nimissä pystytään tekemään rikoksia, mistä voi aiheutua oikeudellisia seuraamuksia. Yritykset voivat menettää tietojensa lisäksi myös maineensa. Heikot salasanat ovat yksi useimmista syistä tietomurroille. Helposti arvattavissa oleva ja yleisesti käytetty salasana on tunkeutujalle helppo kohde, joka johtaa helppoon tietomurtoon. [2.] Heikko salasana on lyhyt, koostuu pelkästään pienistä kirjaimista ja sisältää sanoja, jotka löytyvät sanakirjasta. Tällainen salasana on todella nopea purkaa brute force -hyökkäyksellä. Brute force -hyökkäys on väsytyshyökkäys, jossa tietokoneohjelma käy läpi mahdollisia salasanoja, kunnes löytää sopivan osuman. [3.]

Hyökkäystä vastaan voidaan kuitenkin puolustautua vahvalla salasanalla. Vahva salasana koostuu vähintään 12 merkistä, sisältää erikoismerkkejä, sekä pieniä ja isoja kirjaimia. [4.] Useita vahvoja salasanoja on kuitenkin vaikea muistaa. Sala-

sanajärjestelmät tallentavat vahvat salasanat muistiin, jolloin käyttäjän itse ei tarvitse näitä muistaa. Käyttäjän tarvitsee pelkästään muistaa yksi salasana, joka käy salasanajärjestelmään ja salasanajärjestelmä säilyttää loput salasanoista. [1.] Salasanoilla ei kuitenkaan pystytä suojautumaan kaikkia hyökkäyksiä vastaan. Tällainen hyökkäys on esimerkiksi phishing eli kalasteluhyökkäys. Tässä hyökkääjä esittää ja huijaa uhrille olevansa luotettava lähde. Tällä tavoin hyökkääjä kalastelee uhrin tiedot sähköpostilinkkien ja pikaviestien avulla. Hyökkäyksessä käytetään usein hyödyksi käyttäjän kiirettä erilaisin aikarajoituksin, jolloin käyttäjä saattaa avata saastuneen linkin. [5.]

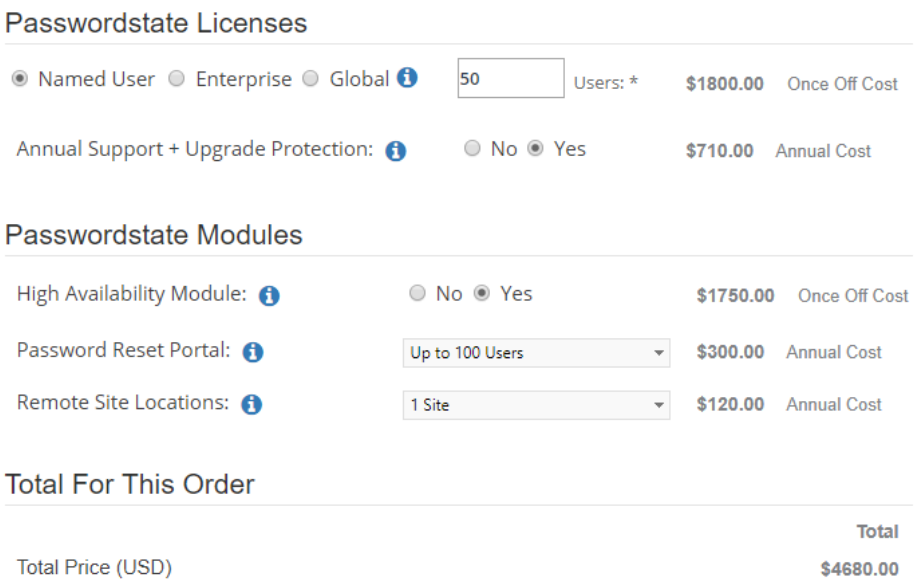
3 Arviointiin valitut salasanajärjestelmät

3.1 Passwordstate

Passwordstate on Clickstudios -yrityksen päätuote keskitettyyn salasanojen hallintaan. Tuote on tarkoitettu yrityksen omiin tiloihin sijoitettavaksi eli on-premise -palvelimeksi. Järjestelmänvalvojahallinta tapahtuu nettiselaimen avulla. Peruskäyttäjät käyttävät tuotetta selainvälilehden tai selainliitännäisen kautta. Tähän tuotteeseen voidaan liittää kaksi pääosin isommille yrityksille tarkoitettua lisätuotetta, Self-Service Password Reset Portal ja Remote Site Locations Module for MSPs. [6.] Password Reset Portalin avulla yrityksen henkilöstö voi itsenäisesti vaihtaa salasanansa, tai salasanan unohdettuaan palauttaa tämän erilaisia turvakysymyksiä käyttäen. [7.] Remote Site Locations Module on tarkoitettu yrityksille, joilla on palomuureja verkkojen välissä ja useita toimipisteitä. Tämä vaatii agentin asennuksen jokaiseen eri toimialueeseen ja agentit keskustelevat Passwordstaten päähallinnan kanssa. Näin salasanoja ja käyttäjiä saadaan hallittua useaan toimipisteeseen Passwordstaten kautta. [8.]

Passwordstate vaatii toimiakseen Windows 7- tai Windows Server 2008 R2 -käyttöjärjestelmän tai näistä uudemmat versiot. Palvelimelle tulee asentaa Internet

Information Services eli IIS versio 7.0 Windows Server, tai 7.5 Windows 7. Tietokannaksi vaaditaan vähintään Microsoft SQL Server 2012 Express -versio. [9.] Tuotteessa on AD-integraatio käyttäjien helppoon lisäämiseen ja hallintaan. Käyttäjät voidaan synkronoida passwordstaten ja AD:n kanssa, jolloin tulisipa muutos passwordstaten tai yrityksen toimialueen kautta, niin tiedot pysyvät samoina. Passwordstate tukee molempia AD-integraatio yhteyksiä, LDAP- ja LDAPS-yhteyttä. [10.] Järjestelmän internet-selain liitännäisellä tai erikseen asennettavalla etäyhteys sovelluksella pystytään kierrättämään salasanajärjestelmän kautta SSH- ja RPD-yhteydet. Tämä mahdollistaa yhteyksien nauhoituksen ja raportoinnin. Raportit saadaan kaikesta salasanojen käytöstä ja myös etäyhteyksien käytöstä. [11.]



Kuva 1. Passwordstate hinnoittelu.

Kuvassa 1 näkyvät Passwordstaten erilaiset lisenssit ja hinnoittelut. Itse päätuotteella on kolmea erilaista lisensointia, käyttäjäpohjainen-, yritys- ja globaali-lisensointi. Käyttäjäpohjaiseen valitaan haluttujen käyttäjien määrä ja yksi asennuskerta tuotteelle. Yrityslisenssiin saadaan loputtomasti käyttäjiä ja yksi asennuskerta. Globaalilisenssillä saadaan myös loputtomat käyttäjät, mutta tuotteelle tulee loputtomasti asennuksia. Yrityslisenssin hinta on 5 700 dollaria ja globaalilisenssin 15 100 dollaria. Yrityksen tapauksessa kiinnostaa tuotteen hinta 50 käyttäjälle ja mahdollisesti vuosittainen tuki. Tuotteen hinnaksi siten tulee 1 800 dollaria ja lisäksi tulisi 360 dollarin vuosikustannus. [12.]

3.2 Pleasant Password Server

Toinen valitsemani tuotteista on Pleasant Password Server (myöhemmin PPS). PPS on Pleasant Solutionsin tuote. Kuulin tuotteesta harjoittelijaohjaajaltani, joka oli käyttänyt tätä aikaisemmassa työpaikassaan. PPS tulee sijoittaa myös on-premise -palvelimeksi. Pleasant Solutionsilta on tarjolla myös tuotteet Pleasant Reset Server ja Universal Single Sign-on (SSO). Pleasant Reset Server on samankaltainen salasanojen vaihtojärjestelmä kuin Passwordstatelta löytyvä Self-Service Password Reset Portal. Universal SSO ottaa käyttöön single-sign on -teknologian, jolla pystytään kirjautumaan kaikkiin järjestelmiin käyttäen yhtä salasanaa. [13.]

PPS on tarkoitettu käytettäväksi yhdessä KeePass Password Safe tai Bruce Schneierin Password Safe -ohjelmistojen kanssa. Tuotetta voidaan myös käyttää nettiselaimen kautta. PPS vaatii toimiakseen Windows Vista- tai Windows Server 2008 -käyttöjärjestelmän tai näistä uudemmat versiot. Oletus tietokantana järjestelmälle on SQLite. [14.] Järjestelmästä löytyy neljä erilaista lisenssiä: community, enterprise, enterprise+ ja enterpise+SSO. Community on tarkoitettu yleiskäyttöön, joten tämä valinta jää Yritykseltä pois. Enterprise+ eroaa enterprisestä ominaisuuksiltaan tietyin hienosäädöin ja kosmeettisin puolin. Enterpise+ mahdollistaa yrityksen logon lisäämisen järjestelmään ja taustateeman muokkaamisen. Enterprise+ lisenssin ominaisuuksia ovat esimerkiksi automaattinen salasanan vaihto, pakollisen kommentin jättäminen salasanaa käytettäessä, järjestelmänvalvojilta oikeuden pyytäminen salasanaan ja tietty aikarajoitus, jos salasanaa tarvitaan väliaikaiseen käyttöön. Hinnoittelu määräytyy valitun lisenssin, vuosikustannuksen ja käyttäjämäärän mukaan. [15.] PPS ostetaan kertaostona ja järjestelmälle tulee mukaan yhden vuoden tuki. Jos tukea halutaan jatkaa, niin tuki tulee maksamaan yhden neljäsosan tuotteen hinnasta. Taulukossa 1 näkyy järjestelmän hinnoittelu. [16.]

Taulukko 1. Pleasant Password Server -järjestelmän hinnoittelu.

Käyttä-jät	Enter-prise	Enter-prise+	Enter-prise+SSO
30	2,355 $	3,179 $	3,534 $
40	2,808 $	3,791 $	4,183 $
50	3,485 $	4,705 $	5,201 $
75	4,754 $	6,418 $	7,049 $
100	5,561 $	7,508 $	8,339 $

3.3 ManageEngine Password Manager Pro

Password Manager Pro (jäljempänä PMP) on yksi monista ManageEnginen tuotteista salasanojen hallintaa varten. PMP sijoitetaan myös on-premise -palvelimeksi. PMP voidaan asentaa Windows- ja Linux-käyttöjärjestelmille. PMP käyttää oletuksena PostgreSQL-tietokantaa, mutta PMP tukee myös MySQL- ja MS SQL -tietokantoja. PMP:tä hallinnoidaan ja käytetään nettiselaimen kautta. Selaimeen voidaan myös asentaa selainliitännäinen tuotteesta, jolloin erillistä selainvälilehteä ei vaadita tuotteen käyttöön. [17.]

PMP:ssä on kolme erilaista lisenssiä: Standard, Premium ja Enterprise. Standard-lisenssillä päästään jo pitkälle salasanojen hallinnan kanssa. Tässä tulee jo lähes kaikki pienelle tai keskisuurelle yritykselle halutut ominaisuudet, kuten AD-integraatio, multi-factor authentication (MFA) ja varmuuskopiot. Premium-lisenssissä saadaan käyttöön käyttäjien etäyhteydet ja näiden valvominen. Premiumiin tulee mukaan myös synkronointi sovelluksiin, salasanojen hälytykset ja ilmoitukset poikkeuksista. Enterprise-lisenssi on tarkoitettu isommille yrityksille, jotka tarvitsevat käyttöönsä erilaisia integraatioita ja laajempaa hallinnointia. Tällä voidaan hallita yrityksen varmenteita, muokata raportteja, mahdollistaa kirjautuminen smart cardilla ja salasanojen synkronointi laitteille. [18.] Hinnoittelu tuotteelle menee lisenssin ja järjestelmänvalvojakäyttäjien määrän mukaan. Järjestelmänvalvojat pystyvät hallinnoimaan salasanoja ja lukemaan raportteja. Salasanojen peruskäyttäjät eivät pysty muokkaamaan salasanoja. Password Manager Pron

viralliselta sivustolta ei löytynyt minkäänlaista hinnoittelua tuotteelle, vaan yritykseltä pitää kysyä hintatarjous. [19.]

3.4 LastPass

LastPass on ainut tuotteista, joka toimii pilvipalveluna salasanojen hallintaa varten. Pilvipalvelu tallentaa salasanat internetin välityksellä pilveen, joten tiedot ovat aina saatavilla. Pilvipalvelun ansiosta LastPass ei vaadi mitään erillisiä asennuksia yrityksen tiloihin. LastPassin käyttäminen tapahtuu pääosin internet-selaimeen asennettavan liitännäisen avulla tai kirjautumalla yrityksen sivustolle. Tämä koskee peruskäyttäjiä ja järjestelmänvalvojia. Ohjelma ei siis vaadi mitään erillisiä asennuksia hallinnointiin. Mobiilikäyttö on kuitenkin poikkeus, joka vaatii toimiakseen asennettavan sovelluksen käytettävälle laitteelle. [20.]

LastPassissa on tavalliseen käyttöön tarkoitettujen lisenssien lisäksi kaksi yrityksille tarkoitettua lisenssiä, teams ja enterprise. Teams on nimensä mukaan tarkoitettu tiimeille tai pienille yrityksille ja enterprise pelkästään yrityksille. Teams sisältää hallinnointitarpeet, kuten salasanojen vaatimukset ja MFA-pakotuksen käyttäjille. [21.] Enterprise sisältää kaikki samat ominaisuudet kuin teams ja tuo lisäksi yrityksille lisää ominaisuuksia ja vaihtoehtoja jo teamsissa oleville asetuksille. Huomattavimmat lisäykset enterprise-lisenssiin ovat AD-synkronointi, roolit ja SSO. [22.] LastPassia ei voi ostaa ollenkaan kertaostolla, vaan hinnoittelu menee SaaS-mallin mukaan. LastPassin hinnoittelu näkyy taulukossa 2. [23.]

Taulukko 2. LastPass kuukausihinnoittelu [23.]

Käyttäjät	Teams €/kk	Enterprise €/kk
30	105,60	158,40
40	140,80	211,20
50	176	264
60	211,20	316,80

3.5 Testiin valitut järjestelmät

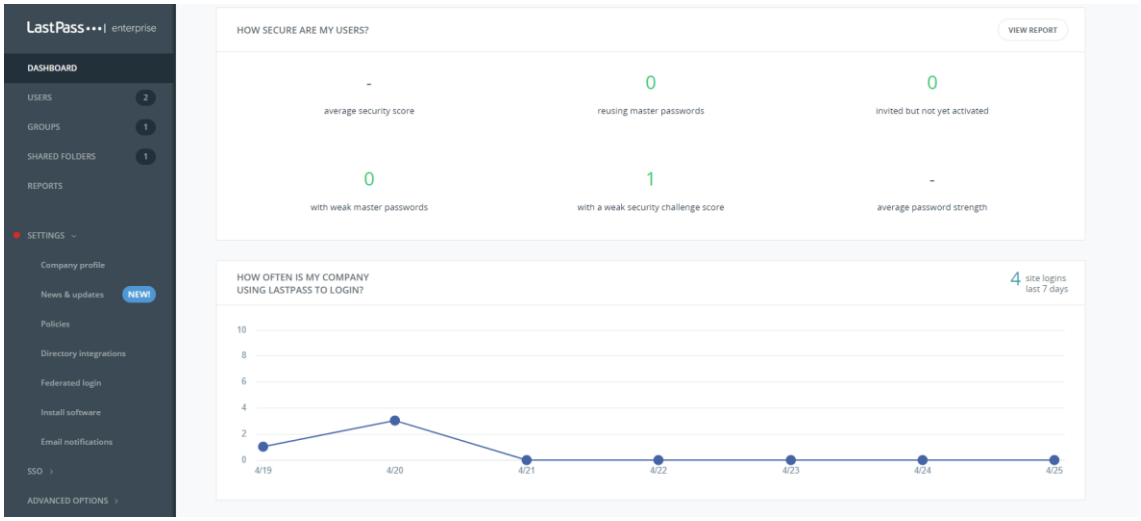
Jokaisessa arvioitavassa salasanajärjestelmässä oli vaaditut ominaisuudet, joita Yritys tarvitsi järjestelmältä. Järjestelmissä oli kuitenkin eroja, joiden perusteella valittiin kaksi järjestelmää testiin. Testaukseen valitut järjestelmät olivat Pleasant Password Server ja LastPass. PPS:n osalta valintaan vaikutti suuresti jo yritykselle tuttu KeePass-ohjelmiston integraatiomahdollisuus. Toinen vaikuttava tekijä oli on-premise-palvelin sijoitus. Tämä olisi edullinen vaihtoehto Yritykselle, koska kyseessä olisi kertaosto tuotteesta ja tukea voisi ostaa lisää tuotteelle, jos ohjelmistopäivityksiin on tarvetta. Tällöin salasanajärjestelmästä ei aiheutuisi jatkuvia kustannuksia Yritykselle. Tuote pystytään asentamaan Windows 10 -käyttöjärjestelmän tietokoneelle, joten Windows Server -lisenssiäkään ei tarvita ostaa, mikä karsii kuluja huomattavasti.

LastPass valittiin testaukseen pääosin pilvipalveluratkaisun vuoksi. Ohjelma toimii internetselain liitännäisen avulla ja tämä helpottaa käytettävyyttä huomattavasti. Tuote oli ainut vertailussa olleista järjestelmistä, joka toimii pilvipalveluna. Passwordstate vaikutti hyvin samankaltaiselta ratkaisulta kuin PPS, mutta PPS:n KeePass-integraation vuoksi PPS valittiin testaukseen. Password Manager Prossa oli kaikista järjestelmistä kattavimmat ominaisuudet, mutta hinnoittelu tapahtuu järjestelmänvalvojakäyttäjillä. Yritys halusi, että peruskäyttäjillä olisi myös oikeudet hallita heille jaettuja salasanoja, mikä olisi vaatinut kaikille järjestelmänvalvojaoikeudet. Tämän vuoksi PMP ei ollut sopiva vaihtoehto Yritykselle. Mielestäni PMP on tarkoitettu suuremmille yrityksille tämän kattavien ominaisuuksien vuoksi.

4 Testaukseen valittujen järjestelmien käyttöönotto

4.1 LastPass-kokeiluversion käyttäminen

LastPass enterprise-lisenssistä on 14 päivän kokeilujakso. Ohjelman käyttö saadaan aloitettua heti käyttäjän luonnin jälkeen yrityksen sivuston kautta. [24.] Asennusvaiheessa huomattiin, että luodulla käyttäjällä on järjestelmänvalvojatason oikeudet organisaation LastPass-hallintaan. Kuvassa 2 näkyy LastPass-järjestelmänvalvojan hallintanäkymä.

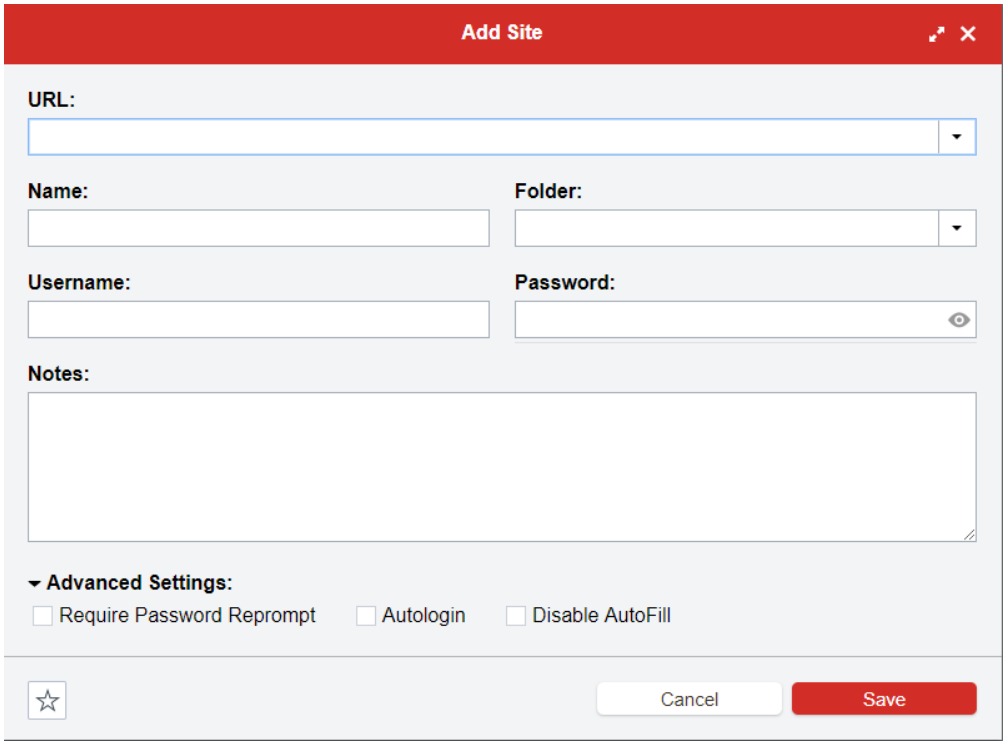


Kuva 2. LastPass-järjestelmänvalvojan hallintanäkymä.

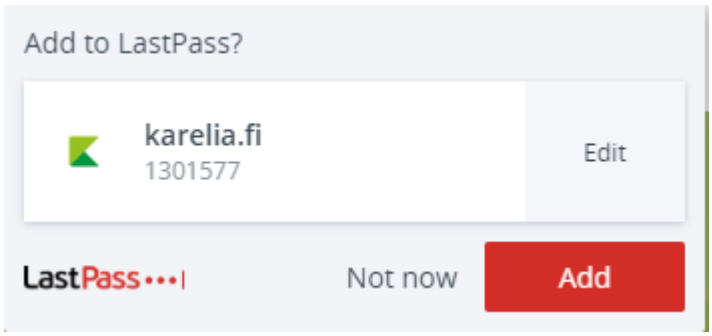
Testauksen myötä selvisi, että käyttäjiä LastPassiin saadaan lisättyä AD-integraatiolla tai lähettämällä kutsu sähköpostiin lisättäville henkilöille. Käyttäjien lisäyksen jälkeen lisätyt käyttäjät lataavat selainliitännäisen, tai halutessaan Windows-sovelluksen LastPassista. AD-integraatio vaatii toimiakseen Active Directory Connector -sovelluksen. Sovellus asennetaan Windows-käyttöjärjestelmän tietokoneelle ja tämän kautta hallinnoidaan, mitä tietoja halutaan synkronoida ADsta LastPassiin.

Salasanat tallentuvat LastPassiin Sites (sivusto) -kohteina. Sivustoon voidaan täyttää URL-osoite, tunnistenimi, kansio, käyttäjätiedot ja muistiinpano.

Sivustoja pystytään tallentamaan, joko manuaalisesti hallinnan kautta kuvan 3 mukaisesti, tai hyväksymällä LastPassin kysely jokaisen uuden salasanan kirjoittamisen jälkeen kuvan 4 mukaisesti.



Kuva 3. Salasanojen lisääminen sivustoille hallinnan kautta.



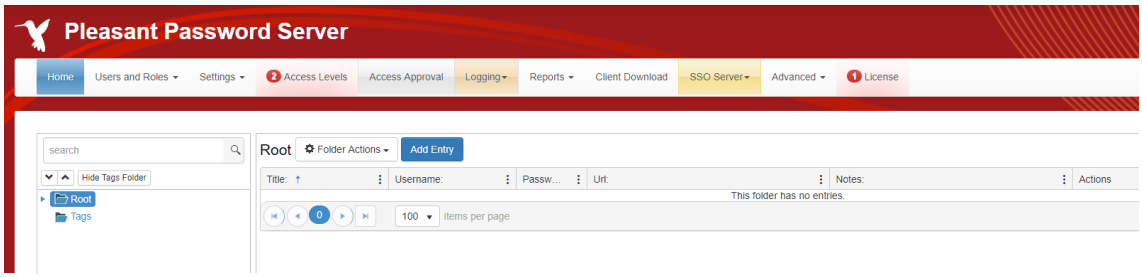
Kuva 4. LastPass kysyy salasanan tallennusta kirjauduttua uudelle sivustolle.

Järjestelmää tutkiessa ilmeni, että sivustojen ja kansioiden jakaminen tapahtuu helposti Share Item -ominaisuutta käyttämällä. Tähän vaaditaan vain sähköposti, jolle sivusto halutaan jakaa. Sivustojen jakaminen useille käyttäjille tapahtuu helpoiten hyödyntämällä ryhmiä. Testauksessa luotiin jokaiselle Yrityksen henkilöstöosastolle oma ryhmänsä ja lisättiin osastojen henkilöt omiin ryhmiinsä, jolloin

saatiin helposti jaettua henkilöstölle heille kuuluvat salasanat. Järjestelmänvalvojahallinta mahdollistaa helpon tarkkailun, kenelle mikäkin kansio on jaettuna ja mitä oikeuksia henkilöillä on kansioihin. Raportointi näkyy järjestelmänvalvojan hallinnasta ja tätä kautta näkyvät kaikki tapahtumat, joita Yrityksen LastPassissa on tehty. Tietoja voidaan etsiä niin pitkältä ajalta taaksepäin kuin vain halutaan. Käyttäjille voidaan myös asettaa sähköpostihälytyksiä tietyistä tilanteista. Näitä tilanteita voivat olla esimerkiksi heikot salasanat, samat salasanat useissa sivustoissa ja LastPassin vähäinen käyttö. Järjestelmänvalvojan hallinnan kautta kuitenkin selviää, että sähköpostihälytyksiä ei pysty lainkaan luomaan tai muokkaamaan jo olemassa olevia. Policy-välilehden kautta pystytään säätelemään LastPassiin erilaisia sääntöjä. Tämän kautta saadaan pakotettua MFA käyttäjille ja säädettyä salasanojen vähimmäismerkkimäärää sekä monia muita samankaltaisia sääntöjä.

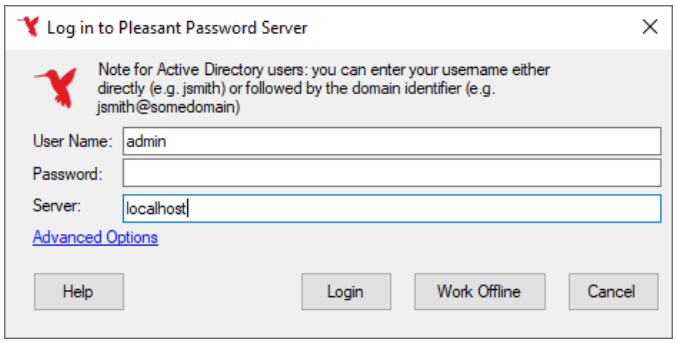
4.2 Pleasant Password Server kokeilun käyttäminen

PPS:stä saadaan ladattua loputon kokeiluversio ilmaiseksi. Kokeiluversioon ei sisälly enterprise-ominaisuuksia. Käyttäjiä ja salasanoja voidaan lisätä vain tiettyyn rajaan asti. Ohjelmisto tulee asentaa Windows-käyttöjärjestelmälle. Tässä työssä asennus tehtiin Yrityksen tiloihin Windows 10 -käyttöjärjestelmän tietokoneelle. Ohjelma ladataan Pleasant Password Serverin sivustolta ja asennus vaatii vain sijainnin tietotokoneelta, johon PPS tullaan asentamaan. Kaikki muu asennuksessa asentuu automaattisesti valmiiksi ja ohjelmaa päästään käyttämään heti internetselaimen kautta. Kuvassa 5 näkyy PPS admin -tason käyttäjän selainhallinta. [17.]



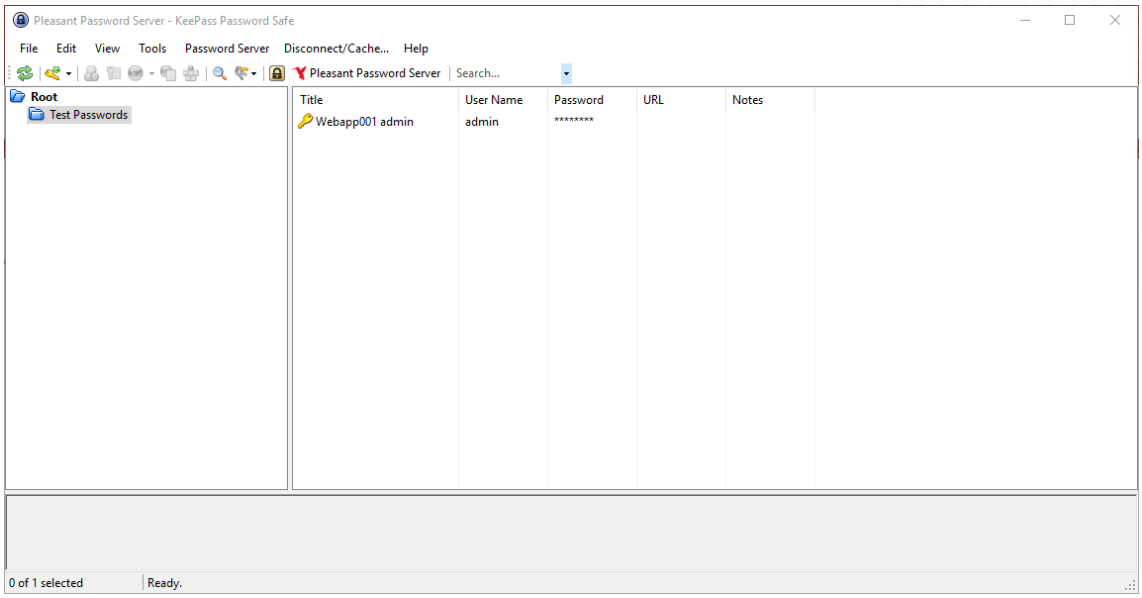
Kuva 5. Admin-näkymä PPS-selainhallinnasta.

Kuten kuvasta 5 näkyy Pleasant KeePass-sovellus saadaan ladattua juuri asennetusta PPS:stä välilehden Client Download -kautta. Tällä sovelluksella voidaan ottaa yhteys PPS:ään ja käyttää tuotetta ilman selainta. Yrityksellä aikaisemmin ollut KeePass-sovellus ei ole yhteensopiva Pleasant Password Serverin kanssa. Kuvassa 6 näkyy Pleasant KeePass -sovelluksen kirjautumisruutu.



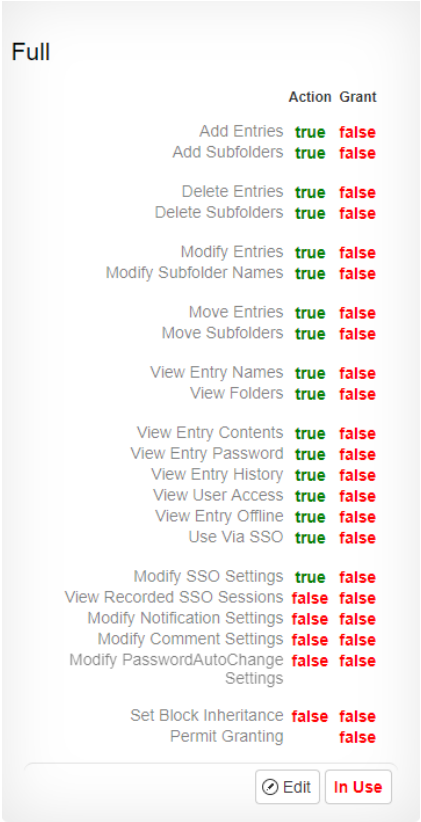
Kuva 6. Pleasant KeePass-sovelluksen kirjautumisruutu.

Kun oikeat tiedot on syötetty, avautuu KeePass-sovelluksen näkymä (kuva 7). Sovelluksessa nähdään kaikki käyttäjälle sallitut kirjaukset. Työssä huomattiin, että tätä kautta voidaan myös lisätä uusia salasanoja valitsemalla add entry, eli lisää kirjaus. Kirjaukseen voidaan syöttää käyttäjän kirjautumistiedot, otsikko, selainsivu sekä muistiinpanot. Kirjauksen tallennettua kirjaus ilmaantuu KeePassiin ja tämä sama kirjaus toimii selainhallinnan kautta. Kirjaukset voidaan tuoda entisestä KeePassista uuteen Pleasant KeePass-sovellukseen käyttämällä KeePassin tuo ja vie -ominaisuuksia. Entinen KeePass luo KeePass kdbx -päätteisen tiedoston, joka tuodaan Pleasantin KeePassiin. Tällä tavoin saatiin kaikki Yrityksen jo olemassa olevat kirjaukset tuotua entisestä KeePassista uuteen Pleasant KeePassiin.



Kuva 7. Pleasant KeePass-sovelluksen näkymä.

Testauksessa käyttäjiä lisättiin PPS:ään hakemalla nämä AD:n kautta. AD-synkronointi ei vaadi mitään erillisiä asennuksia. Käyttöä varten tarvitsee vain tietää, mistä haluttu AD löytyy, millä käyttäjällä tiedot haetaan ja mistä kansiosta käyttäjät haetaan. Salasanakirjausten oikeuksien hallinnointi järjestelmässä tapahtuu pääsytasoilla. Pääsytasoilla saadaan hallinnoitua, mitä oikeuksia käyttäjillä tai rooleilla on salasanakirjauksiin. Kuvassa 8 näkyy, mitä oikeuksia voidaan sallia tai estää pääsytasoilla. PPS:ään voidaan luoda rooleja ja näihin rooleihin voidaan lisätä käyttäjiä. Roolien avulla voidaan lisätä useille käyttäjille samat salasanat ja pääsytasot.



Kuva 8. Pääsytason oikeudet.

4.3 Ostettavan järjestelmän valitseminen

LastPassin ja Pleasant Password Serverin testaamisen jälkeen näistä sopivammaksi valinnaksi Yritykselle osoittautui Pleasant Password Server. PPS valittiin parhaaksi ratkaisuksi tutun KeePass-ohjelmiston, on-premise-sijoituksen ja kertaostohinnan vuoksi. PPS enterprise-lisenssi maksoi viidellekymmenelle käyttäjälle 3 115 euroa. Tähän sisältyi yhden vuoden tuki uusille järjestelmäpäivityksille. LastPass enterprise-lisenssi olisi tullut maksamaan 264 euroa kuukaudessa viidellekymmenelle käyttäjälle, joten tämä olisi tullut yritykselle kalliimmaksi jo yhden vuoden jälkeen. Pleasant Password Serverin on-premise-sijoituksen vuoksi salasanat tulevat olemaan pelkästään Yrityksen verkosta käsin saatavilla, mikä nostaa huomattavasti järjestelmän tietoturvaa. Järjestelmien hallinnan kannalta testauksessa ei ilmennyt kummassakaan suuria puutteita. Molempiin järjestelmiin saadaan AD-liitos ja käyttäjiä saadaan hallittua tarpeellisin tavoin. Raportointi ja logikirjaus olivat järjestelmissä myös molemmissa hyvällä tasolla.

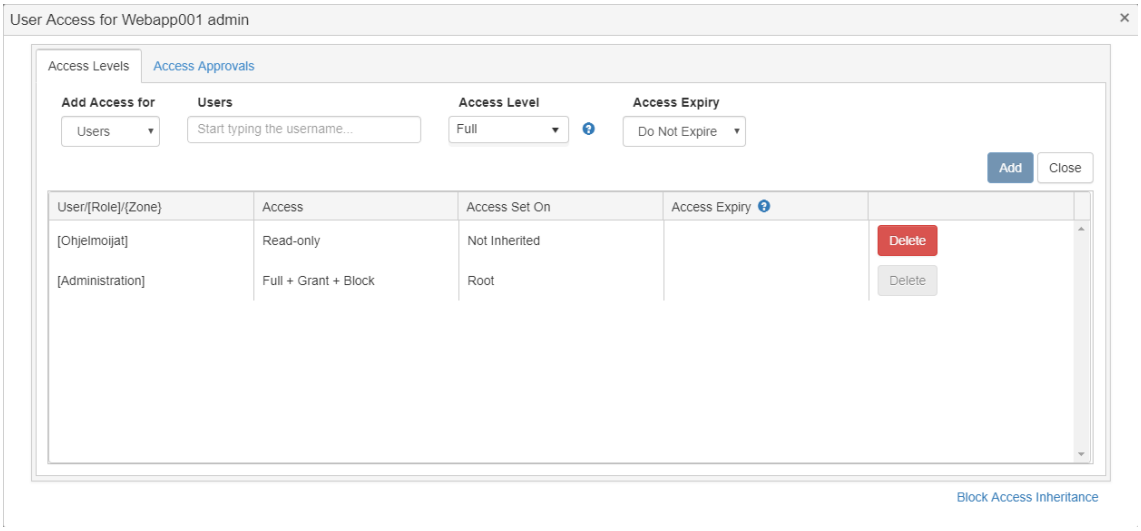
5 Pleasant Password Serverin lopullinen järjestelmän käyttöönotto

Pleasant Password Server enterprise-lisenssi ostettiin Yritykselle Pleasant Solutionsin sivustolta. Ostamisen jälkeen saatiin haltuun aktivointilisenssi tuotteelle. Lisenssi asetettiin testausvaiheessa asennetulle Pleasant Password Serverille. Tämän jälkeen enterprise-ominaisuudet saatiin järjestelmään käyttöön. Enterprise-lisenssi mahdollisti AD-liitoksen, pääsytasot, tietokantavarmistukset ja KeePass-asetuksien konfiguroimisen. AD yhdistettiin, kuten jo luvussa 4.2 mainittiin menemällä Active Directory -välilehdelle, syöttämällä yrityksen AD:n sijainti ja käyttäjätiedot. Yhdistyksen jälkeen pystyttiin valitsemaan henkilöt, jotka haluttiin synkronoida järjestelmään. Käyttäjien tuonnin jälkeen luotiin pääsytasot ja huomattiin, että PPS tarjoaa neljä valmiiksi luotua pääsytasoa käyttäjien ja roolien oikeuksien hallinnointia varten. Valmiit pääsytasot ovat seuraavat:

- Full
- Read-only
- Full + Grant
- Full + Grant + Block.

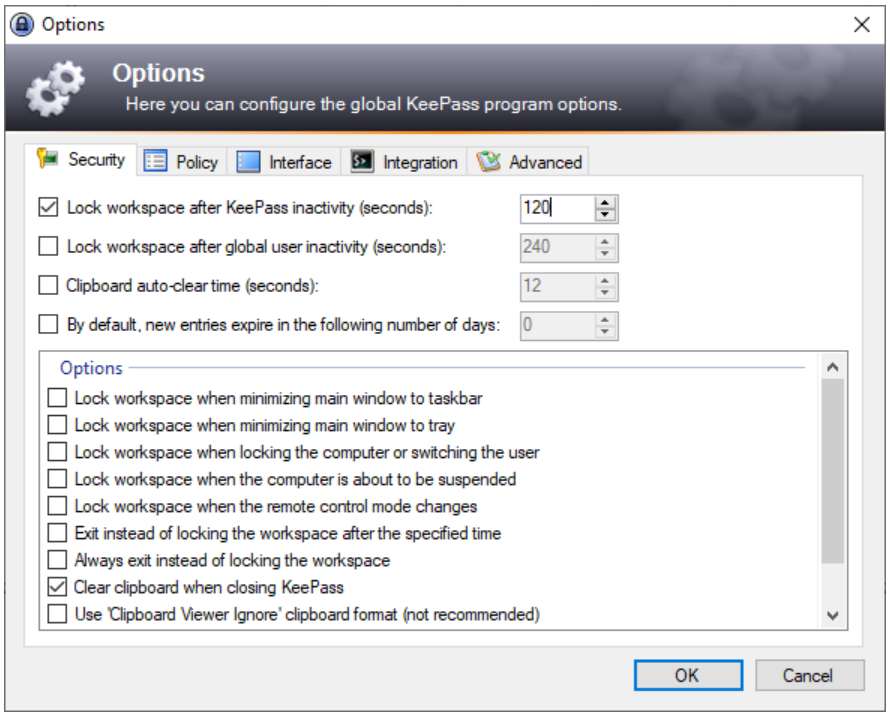
Salasanakirjausten hallinnointia varten työssä tarvittiin järjestelmän viimeistelyyn pelkästään kahta ensimmäistä pääsytasoa: Full ja Read-only. Full antaa käyttäjille kaikki oikeudet muokata ja käyttää heille jaettuja kirjauksia. Työssä huomattiin, että tämä ei anna kuitenkaan oikeuksia jakaa salasanoja muiden käyttäjien kesken. Read-Only antaa käyttäjille pelkästään lukuoikeudet salasanoihin. Kaksi viimeistä tasoa ovat tarkoitettu pelkästään järjestelmänvalvojia varten. Nämä tasot antavat kaikki oikeudet kirjauksiin mukaan lukien kaikkien asetuksien muokkaamisen ja jakamisen. Pääsytasoja voidaan luoda uusia ja näin muokata oikeuksia mieleisiksi. Pääsytasojen ja käyttäjien tuonnin jälkeen luotiin käyttäjille roolit. Roolit lisättiin Roles-valikosta. Roolit luotiin yrityksen henkilöosastojen mukaan

järjestelmään ja käyttäjät sijoitettiin heille kuuluviin rooleihin. Tämän jälkeen asetettiin salasanakirjauksiin juuri luodut roolit ja pääsytasot kuvan 9 mukaisesti.



Kuva 9. Webapp001 admin -salasanakirjauksen roolit ja pääsytasot.

Järjestelmää testatessa huomattiin, että PPS on myös varautunut tietojen menetyksiin tietokantavarmistuksilla. Työssä säädettiin tietokantavarmistukset Database Backups -valikosta. Varmistuksien otoille säädettiin aika ja paikka sekä valittiin, minne varmistus luodaan. Varmistuksien palautus vaatii aina salausavaimen, joka löytyy saman valikon alta. Pleasant KeePass-sovelluksen asetuksiin kuuluu useita käyttäjäkohtaisia asetuksia, kuten pienennä sovellus automaattikirjoituksen jälkeen. Nämä ovat kuitenkin pieniä muokattavia asetuksia, joita voidaan muokata jatkossa. Sovelluksen suojauksessa on suurimmaksi osaksi kyse lukituksesta. Alla olevassa kuvassa 10 näkyvät sovelluksen suojausasetukset.



Kuva 10. Pleasant KeePass -sovelluksen suojausasetukset.

Kuvasta 10 näkyy, että sovellus voi lukkiutua monin eri tavoin, mutta huomattavasti tehokkain ja paras vaihtoehto mielestäni tähän on lukitseminen tietyn käyttämättömyyden jälkeen. Lukitusta testatessa huomattiin, että sovellus vaatii lukitseminen jälkeen uudelleen kirjautumisen. Tämä estää, ettei sovellus voi unohtua vahingossa päälle, mikä saattaa aiheuttaa luvattoman salasanoihin käsiksi pääsyn. Asetukset saatiin vietyä kaikille käyttäjille muokkaamalla aluksi käyttöönotetun sovelluksen asetuksia haluamiksi ja käyttämällä sovelluksen ominaisuutta export configuration eli vie asetukset. Tämä loi sovelluksen asetuksista tiedoston, joka vietiin järjestelmän hallinnasta löytyvän Client Configuration -valikon kohtaan Default Rule. Käyttäjien Pleasant KeePass -sovellus hakee nyt tämän asetustiedoston heidän seuraavan kirjautumisen yhteydessä.

6 Pohdinta

Salasanajärjestelmiä arvioidessani huomasin, että järjestelmistä löytyi hyvin samankaltaiset ominaisuudet. Järjestelmissä oli kuitenkin eroja, joiden perusteelta valinta tehtiin. LastPass käytti hyväkseen pilvipalvelua, jolloin tämä oli käytettävissä kaikkialta internetistä. Tämä kuitenkin tallentaa salasanat pilveen, jolloin salasanat eivät ole yrityksen verkossa. Pleasant Password Server, Password Manager Pro ja Paswordstate sen sijaan säilyttävät salasanat on-premise-palvelimille, jolloin salasanat pysyvät yrityksen sisällä ja tämä nostaa järjestelmien tietoturvaa. Tämä hankaloittaa kuitenkin salasanajärjestelmään pääsyä, koska järjestelmät toimivat pelkästään yrityksen verkon sisältä. Password Manager Prossa oli kaikkein kattavimmat ominaisuudet suuremmille yrityksille, mutta järjestelmänvalvojakäyttäjien mukaan tuleva hinnoittelu ei ollut sopiva Yritykselle, jolle opinnäytetyö tehtiin. Pleasant Password Server käytti hyödykseen KeePass-integraatiota, joka oli jo tuttu yritykselle ja tämä osoittautui parhaaksi valinnaksi Yritykselle.

Mielestäni opinnäytetyölle asetetut tavoitteet täyttyivät. Yritys sai sille sopivimman salasanajärjestelmän käyttöönsä. Salasanajärjestelmä otettiin Yrityksessä hyvin vastaan, koska tietoturvan merkitys on nykyaikana kasvanut yrityksissä huomattavasti. Opinnäytetyön aiheesta oli vaikea löytää aineistoa, koska aihetta ei ole Suomessa paljoa tutkittu. Siksi katson tämän opinnäytetyön olevan hyödyllinen tietoperusta, jos halutaan käyttöönottaa salasanajärjestelmä yritykselle.

Jatkokehityksenä salasanajärjestelmälle olisi varmuuskopioiden siirto pois Pleasant Password Server -palvelimelta. Tällä vältyttäisiin tietojen katoamisilta laitteistovian sattuessa. Simple Mail Transfer Protocol (SMTP) on myös mahdollista asettaa käyttöön järjestelmään. Tämä vaatisi kuitenkin erillisen SMTP -palvelimen käyttämistä. SMTP mahdollistaisi automaattiset sähköpostihälytykset raporteista ja hälytyksistä. Tämä auttaisi järjestelmänvalvojia huomaamaan sähköpos-

tin kautta, miten käyttäjät käyttävät salasanajärjestelmää. Tällä huomattaisiin helposti myös salasanojen luvaton käyttö, joka antaa lisäturvaa hakkerointihyökkäystä vastaan.

Lähteet

1. How to geek. 2018. Why you should use a password manager, and how to get started. https://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started [21.5.2019]
2. Bauman, A. 2018. The importance of strong, secure passwords. Secure data recovery. https://www.securedatarecovery.com/resources/the-importance-of-strong-secure-passwords [17.4.2018]
3. Calyptix. 2016. Brute-force. https://www.calyptix.com/top-threats/password-security-how-to-thwart-hackers-with-a-strong-password [25.4.2019]
4. How to Geek. 2018. The Traditional Password Advice. https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/ [25.4.2019]
5. Imperva. 2019. Phishing techniques. https://www.imperva.com/learn/application-security/phishing-attack-scam [24.5.2019]
6. Clickstudios. 2018. Etusivu. https://www.clickstudios.com.au/ [5.3.2019]
7. Clickstudios. 2018. Password Reset Portal. https://www.clickstudios.com.au/resetportal/default.aspx [5.3.2019]
8. Clickstudios. 2018. Remote Site Locations for MSPs. https://www.clickstudios.com.au/remotesitelocations/default.aspx [5.3.2019]
9. Clickstudios. 2018. Passwordstate laitevaatimukset. https://www.clickstudios.com.au/passwordstate-system-requirements.aspx [7.3.2019]
10. Clickstudios. 2018. Active directory integraatio. https://www.clickstudios.com.au/about/active-directory-integrated.aspx [5.3.2019]
11. Clickstudios. 2018. Passwordstate etäyhteys kirjautuminen. https://www.clickstudios.com.au/about/remote-session-logins.aspx [26.5.2019]
12. Clickstudios. 2018. Passwordstate hinnoittelu. https://www.clickstudios.com.au/buy-now.aspx [7.3.2019]
13. Pleasant Solutions. 2019.Etusivu. https://www.pleasantsolutions.com/PasswordServer [24.5.2019]
14. Pleasant Solutions. 2019. Laite -ja sovellusvaatimukset. https://info.pleasantsolutions.com/Documentation/Pleasant_Password_Server/A._Install_Pleasant_Password_Server/Hardware_and_Software_Requirements [28.2.2019]
15. Pleasant Solutions. 2019. Lisenssien vertailu. http://www.pleasantsolutions.com/passwordserver/details/features/ [28.2.2019]
16. Pleasant Solutions. 2019. Hinnoittelu. http://www.pleasantsolutions.com/passwordserver/purchase/?users=50&tier=C [28.02.2019]

17. Manage Engine. 2019. User Guide. https://download.manageengine.com/products/passwordmanagerpro/images/pmp-help.pdf [13.3.2019]
18. Manage Engine. 2019. Lisensointi. https://www.manageengine.com/products/passwordmanagerpro/download.html#licensing [13.3.2019]
19. Manage Engine. 2019. Käyttäjät. https://www.manageengine.com/products/passwordmanager-pro/help/user_management.html [13.3.2019]
20. LastPass. 2019. How It Works. https://www.lastpass.com/how-lastpass-works [24.5.2019]
21. LastPass. 2019. Teams lisenssi. https://www.lastpass.com/team-password-manager [24.5.2019]
22. LastPass. 2019. Enterprise lisenssi. https://www.lastpass.com/enterprise-password-management [24.5.2019]
23. LastPass. 2019. Hinnoittelu. https://www.lastpass.com/pricing [21.3.2019]
24. LastPass. 2019. Enterprise trial versio. https://lastpass.com/enterprise_trial.php?createacct=1 [21.4.2019]
25. Pleasant Solutions. 2019. Lataaminen. http://www.pleasantsolutions.com/passwordserver/download/ [21.4.2019]