SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Evgeny Baranov

Salaisuuksien hallintapalvelin yrityskäyttöön

Opinnäytetyö
Kevät 2024
Insinööri (AMK), Tietotekniikka

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Tutkinto-ohjelma: Insinööri (AMK), Tietotekniikka

Tekijä: Evgeny Baranov

Työn nimi alaotsikoineen: Salaisuuksien hallintapalvelin yrityskäyttöön

Ohjaaja: Juha Hirvonen

Vuosi: 2024 Sivumäärä: 33 Liitteiden lukumäärä: 0

Opinnäytetyössä tutkittiin millaisia salasanojen ja salaisuuksien hallintaan tarkoitettuja palveluita ja palvelimia on saatavilla tällä hetkellä ja miten ne sopisivat Arnon Oy:n käyttöön. Vertailuun otetut ohjelmat olivat Hashicorp Vault, Bitwarden ja Passbolt.

Työn teoriaosuudessa käytiin läpi, mitä salasana on ja minkälaisia salasanan murtamistekniikat ovat olemassa. Lisäksi käsiteltiin, minkälaisia salasanahallintaohjelmatyyppejä on, niiden etuja ja haittoja.

Vertailu suoritettiin ennalta määritettyjen kriteerien mukaan. Ohjelman tuli olla itseisännöity, siinä oli oltava monivaiheinen tunnistautuminen ja REST API. Vertailun tuloksena saatiin selville, että kaikki valitut ohjelmat täyttävät määritellyt kriteerit, joten on yksiselitteisesti vaikea päätellä, mikä on paras.

[1] Asiasanat: salasana, todentaminen, salaus, tietomurto, tietoturva

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Degree programme: Bachelor of Engineering, Information Technology

Author: Evgeny Baranov

Title of thesis: Secret Management server for business use

Supervisor: Juha Hirvonen

Year: 2024 Number of pages: 33 Number of appendices: 0

The thesis examined what kind of services and servers there are currently available for managing passwords and secrets and if they would be suitable for the use of Arnon Oy. The programs selected for the comparison were Hashicorp Vault, Bitwarden and Passbolt.

In the theoretical part of the thesis, it was discussed what a password is and what kinds of password cracking techniques there are. In addition, the types of password management programs, their advantages and disadvantages were examined.

The comparison was performed according to predefined criteria. The program had to be self-hosted, have multi factor authentication and REST API. As the result of the comparison, it was found that all the selected programs met the defined criteria, so it was difficult to conclude which one was the best.

[1] Keywords: password, authentication, encryption, data break-in, data security

SISÄLTÖ

Kuva- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

API	Ohjelmointirajapinta (Application Programming Interface)
CLI	Komentorivikäyttöliittymä on ohjelmistomekanismi, jonka avulla voidaan olla vuorovaikutuksessa käyttöjärjestelmäsi kanssa näppäimistön avulla (Command Line Interface)
DNS	Verkkotunnuksen nimipalvelu (Domain Name Service)
GnuPG	Ilmainen ohjelma tietojen salaamiseen ja sähköisten digitaalisten allekirjoitusten luomiseen (Gnu Privacy Guard)
GUI	Graafinen käyttöliittymä (Graphical User Interface)
JSON	Tiedonvaihtomuoto, joka on tekstipohjainen ja perustuu JavaScript-kieleen (JavaScript Object Notation)
MFA	Monivaiheinen tunnistautuminen (Multi Factor Authentication)
OpenPGP	Yleisimmin käytetty sähköpostin salausstandardi
REST	REST-ohjelmointirajapintojen avulla voidaan lähettää HTTP- tai HTTPS-pyyntöjä palvelimille, jotka palauttavat esimerkiksi JSON- tai XML-muotoisia vastauksia (Representational State Transfer)
SMTP	Standardiprotokolla sähköpostien lähettämiseen ja vastaanottamiseen internetissä (Simple Mail Transfer Protocol)
SSL	Suojausmenetelmä, jolla luodaan suojattu ja turvallinen yhteys kahden tietokoneen välillä (Secure Socket Layout)
TOTP	Kaksivaiheinen todennusmenetelmä, joka käyttää kertaluonteisia salasanoja, jotka on luotu kellonajan perusteella (Time-Based One-Time Password)

1 JOHDANTO

1.1 Työn tausta

Yrityksissä salasanojen ja salaisuuksien kuten avaimien ja rajapintatunnusten käyttöön liittyy monenlaisia haasteita. Usein käyttäjät tietävät, että he eivät voi käyttää samoja salasanoja eri sovelluksiin, mutta he tekevät sen silti. Käyttäjät, jotka tallentavat tietoja tiedostoihin, eivät aina tiedä, kuka on vaihtanut salasanan tietyssä palvelussa tai järjestelmässä ja milloin. Usein ongelma tulee esiin kaikkein sopimattomalla hetkellä tai kun on liian myöhäistä tehdä jotain. Salasanojen hallintaohjelmien tarkoitus on ratkaista edellä mainittuja haasteita.

1.2 Työn tavoitteet

Opinnäytetyön tarkoituksena on vertailla kolmea eri salasanahallintaohjelmaa. Vertailuun otetaan seuraavat ohjelmat: Bitwarden, HashiCorp Vault, Passbolt. Tutkimuksen perusteella halutaan tehdä päätös, mikä ohjelma soveltuu parhaiten korvaamaan nykyisen ratkaisun.

1.3 Työn rakenne

Johdanto sisältää työn taustan ja työn tavoitteet. Luvussa 2 käydään läpi tietojen salausta, salasanoja ja niiden säilöntää. Luvussa käsitellään myös salasanojen murtamista ja varastamista. Seuraavaksi luvussa 3 selitetään mikä on salasanahallintaohjelma ja kerrotaan tarkemmin vertailtavista ohjelmista. Luvussa 4 kerrotaan ohjelmien asentamisesta ja niiden käytännöstä. Luvussa 5 kerrotaan tuloksista ja tehdään yhteenveto.

1.4 Toimeksiantaja

Arnon perustettiin vuonna 1978 (Arnon, i.a.). Se on kansainvälinen automaatioalan yritys, jolla on tuotantolaitokset Suomessa, Ruotsissa ja Puolassa. Tuotteita toimitetaan yli 100 maahan ympäri maailmaa. Pääsegmentit ovat meri-, kaivos-, energia- ja teollisuussovellukset.

2 KYBERTURVALLISUUS

2.1 Kyberturvallisuus ja miksi se on tärkeää

Kyberturvallisuus, jota voidaan kutsua myös tietoturvaksi, on prosessi, joka varmistaa tiedon eheyden, luottamuksellisuuden ja saatavuuden (Kiser, 2020). Siihen kuuluu työkaluja, riskienhallinnan lähestymistapoja, koulutuksia, teknologioita ja menetelmiä, jotka auttavat suojaamaan laitteita ja ohjelmia hyökkäyksiltä ja luvattomalta käytöltä.

Nykyään maailmassa on valtava kasvu tiedon luomisessa (Kiser, 2020). Yksityishenkilöt ja yritykset tallentavat tietoja tietokoneille, ja ne siirretään päivittäin muille tietokoneille verkon kautta. Valitettavasti tietokoneissa ja niiden käyttöjärjestelmissä on haavoittuvuuksia, joiden avulla hakkerit voivat hyökätä organisaation tietoturvaan. Tämän takia kyberturvallisuus on elintärkeää. Tietojen vuotaminen voi vaikuttaa yrityksen maineeseen ja aiheuttaa kumppaneiden ja asiakkaiden luottamuksen menetyksen. Ohjelmiston lähdekoodin varkaus voi olla vakavana ongelmana taistelussa kilpailijoita vastaan. Tästä syystä organisaatioiden on otettava käyttöön vahva ja tehokas kyberturvallisuus.

2.2 Salasana

Salasana on tärkeä osa tieto- ja verkkoturvallisuutta (The College of New Jersey (TCNJ), i.a.). Salasanoja käytetään estämään luvaton pääsy järjestelmään. Kuten tiedetään, heikko salasana voi uhata koko yritystä.

Salasana on tietokonetilien todennusmenetelmä ja henkilökohtainen avain käyttöjärjestelmään (TCNJ, i.a.). Niiden avulla saadaan pääsy tietokonejärjestelmiin vain valtuutetuille henkilöille ja voidaan seurata tietyn käyttäjän tekemiä muutoksia käyttöjärjestelmään, kuten esimerkiksi tietojen poistaminen tai siirtäminen. Siksi on hyvin tärkeää, että salasanoja ei jaeta muille. Vastuu tiedosta voi jäädä salasanan haltijalle.

Salasanojen suurin ongelma ja heikkous johtuu siitä, että käyttäjät luovat salasanoja, jotka on helppo arvata (Erickson, 2019, s. 88). Samaa salasanaa käytetään eri palveluihin ja ohjelmiin kirjautumiseen. Tämän takia hyökkääjä voi päästä moniin järjestelmän pisteisiin.

2.3 Mitä on salasanan murtaminen?

Salasanojen murtaminen on ollut aina suosittu toiminta kyberhyökkääjien keskuudessa (Stytch, 2023). Salasanan murtaminen on prosessi, jossa hyökkääjät yrittävät päästä käyttäjätileihin ohittamalla salasanasuojauksen. Hyökkääjät voivat käyttää erilaisia menetelmiä, kuten valmiita salasanaluetteloita tai erikoistuneita ohjelmistoja salasanojen arvaamiseen tai paljastamiseen. Tällaisten hyökkäysten tarkoituksena on saada luottamuksellisia tietoja ja resursseja, joita voidaan käyttää henkilökohtaiseen hyötyyn, sabotaasiin tai vain huvin vuoksi.

Salasanojen murtamisessa on kaksi pääluokkaa: online-hyökkäykset ja offline-hyökkäykset (Stytch, 2023). Online-hyökkäykset tapahtuvat suoraan palvelimella, kun hyökkääjä yrittää arvata oikean salasanan lähettämällä useita pyyntöjä verkon kautta. Niitä rajoittaa internetyhteyden nopeus ja ne voidaan havaita palvilimelle suuntautuvan lisääntyneen liikenteen vuoksi. Offline-hyökkäykset tarjoavat hyökkääjälle enemmän joustavuutta ja aikaa. Hakkeri sieppaa palvelimelle tallennetut salatut salasanatiivisteet. Salatut salasanatiivisteet ovat tapa tallentaa salasanoja tietokantaan käyttämällä hajautusalgoritmeja. Kun hyökkääjä pääsee käsiksi näihin tiivisteisiin, hän voi käyttää erityisiä ohjelmia niiden salauksen purkamiseen ja alkuperäisen salasanan hankkimiseen. Tämä menetelmä ohittaa verkkorajoitukset ja voi olla tehokkaampi.

2.4 Yleiset salasanan murtamistekniikat

On olemassa monia tapoja murtaa salasanoja. Tässä luvussa esitellään yleisimmin käytettyjä tapoja.

2.4.1 Väsytyshyökkäys

Väsytyshyökkäys (brute-force attack) voi murtaa melkein minkä tahansa salasanan, jos hyökkääjällä on tarpeeksi aikaa (Beaver, 2010, s. 95). Tässä tapauksessa kaikki mahdolliset merkkiyhdistelmät, numerot, kirjaimet ja erikoismerkit tarkistetaan peräkkäin, kunnes oikea salasana löytyy. Monet salasanan murto-ohjelmat antavat hyökkääjälle

mahdollisuuden mukauttaa testausparametreja, kuten salasanan pituutta, käytettyjä merkkejä ja jopa tunnettuja salasanamalleja.

On kuitenkin syytä huomata, että kaikkien mahdollisten yhdistelmien tarkistamiseen kuluva aika voi olla valtava (Beaver, 2010, s. 95). Se riippuu monista tekijöistä, kuten esimerkiksi salasanojen monimutkaisuudesta ja murto-ohjelmaa käyttävän tietokoneen nopeudesta. Jopa tehokkaiden laskentaresurssien avulla kaikkien salasanavaihtoehtojen läpikäyminen voi kestää loputtoman kauan, joten tämä menetelmä ei ole aina käytännöllinen tosielämän skenaarioissa.

2.4.2 Password spraying -hyökkäys

Password spraying -hyökkäyksessä hyökkääjät yrittävät päästä suureen määrään käyttäjätunnuksia muutamalla yleisesti käytetyllä salasanalla (Secret Double Octopus, i.a.). Tätä tekniikkaa käyttävä hyökkäys kohdistuu useisiin käyttäjätunnuksiin yhtä aikaa käyttämällä samaa salasanaa, eikä käyttäjätunnuksien lukitseminen liiallisten epäonnistuneiden kirjautumisyritysten vuoksi ole tämän vuoksi niin todennäköistä.

Password spraying -hyökkäyksessä, joka tunnetaan myös nimellä ”matala ja hidas” -hyökkäys, pahantekijä käyttää yleisiä käyttäjätunnuksia ja yksinkertaisia salasanoja, kuten ”Salasana 123” tai ”123456” (Secret Double Octopus, i.a.). Hyökkääjät voivat hankkia työntekijöiden tietoja eri lähteistä ja käyttää näitä tietoja hyökätäkseen yritystilejä vastaan, jotka käyttävät samoja käyttäjätunnuksia ja yleisesti käytettyjä salasanoja. Tämä tekee hyökkäyksestä huonommin havaittavan ja antaa hakkereille mahdollisuuden välttää havaitsemista.

2.4.3 Tunnusten täyttäminen

Tunnusten täyttäminen on toisenlainen väsytyshyökkäys (Stytch, 2023). Hyökkääjät käyttävät vaarantuneita tunnistetietoja (jotka he ovat saattaneet ostaa pimeiltä markkinoilta tai saada hakkeroinnin kautta) päästääkseen luvattomasti muille käyttäjätileille.

Toisin kuin tavalliset väsytyshyökkäykset, tunnusten täyttämistä hyödyntävät hyökkäykset eivät ole satunnaisia, koska ne perustuvat jo tunnettuihin käyttäjätunnus- ja salasanayhdistelmiin (Stytch, 2023). Koska työntekijät käyttävät usein samoja tunnistetietoja uudelleen eri tileillä, on suuri mahdollisuus, että yhden salasanan vuotaminen voi johtaa luvatta pääsyyn muihin heidän käyttämiinsä sovelluksiin tai verkkosivustoihin.

2.4.4 Sanakirjahyökkäys

Sanakirjahyökkäys on menetelmä, jossa hyökkääjät luottavat ennalta määritettyihin sana- tai lauseluetteloihin, jotka tunnetaan nimellä ”sanastot tai sanakirjat” (1Password, 2022). Toisin kuin tyypillinen väsytyshyökkäys, jossa kokeillaan kaikkia mahdollisia salasanayhdistelmiä, sanakirjahyökkäys on kohdennetumpi ja tehokkaampi.

Luettelo sisältää yleisiä sanoja, aiemmin varastettuja salasanoja tai yleisiä alueellisia sanoja tai lauseita (1Password, 2022). Hyökkääjät käyttävät sitten automaattisia ohjelmia kokeillakseen erilaisia käyttäjätunnusten ja salasanojen yhdistelmiä, kunnes he voivat murtautua tiliin.

Vaikka hyökkääjät voivat kokeilla sanakirjahyökkäystä suoraan profiilin kirjautumissivulla, monet turvajärjestelmät voivat estää tämän tapahtumisen (1Password, 2022). Jotkut tilit lukitaan automaattisesti useiden epäonnistuneiden kirjautumisyritysten jälkeen. Tämän suojan ohittamiseksi käytetään sanakirjahyökkäystä tietokantaan, joka sisältää hajautettuja salasanoja.

2.4.5 Väliintulohyökkäys

Kun käydään verkkosivustolla, pyyntö kulkee internetreitittimen kautta ja saavuttaa verkkosivuston palvelimen (Irwin, 2023). Palvelin käsittelee pyynnön ja lähettää tiedot takaisin laitteelle saman reitittimen kautta. Tämä prosessi tapahtuu hyvin nopeasti. Väliintulohyökkäykset (Man-in-the-Middle, MITM) voivat kuitenkin hyökätä tähän.

Hyökkääjät häiritsevät reitittimen toimintaa niin, että he voivat saada reaaliaikaista dataa, joka kulkee laitteiden välillä (Irwin, 2023). Tämän avulla heillä on mahdollisuus sekä

kuunnella tietoa että muuttaa sitä. Nämä hyökkäykset tapahtuvat useimmiten julkisissa Wi-Fi-verkoissa, joissa internetyhteydet ovat yleensä vähemmän turvallisia. Tämä ei ole tietoturvakysymys, vaan se on julkisten WI-FI-verkkojen ominaisuus, koska ne ovat suunniteltu kaikkien lähellä olevien käyttöön.

2.4.6 Sateenkaarihyökkäys

Useimmat sovellukset tallentavat salasanat hajautettuina merkkijonoina (Beyond Identity, i.a.). Tällaisten salasanojen murtamiseen käytetään menetelmää, jota kutsutaan sateenkaarihyökkäykseksi (rainbow table attack). Tämä menetelmä käyttää niin sanottua sateenkaaritaulukkoa, joka tallentaa ennalta luotuja salasanatiivisteitä. Kun käyttäjä syöttää salasanan, itse salasanaa ei verrata, vaan sen tiivistettä sateenkaaritaulukkoon tallennettuun tiivisteeseen.

Tällä hetkellä tehokas tapa torjua tällaisia hyökkäyksiä on käyttää menetelmää nimeltä suolaus (Beyond Identity, i.a.). Olemassa olevaan tiivisteeseen lisätään satunnainen arvo, jonka jälkeen luodaan uusi tiiviste.

Valitettavasti monet kehittäjät eivät vieläkään käytä tätä suojausmenetelmää, joten hakkerit voivat käyttää sateenkaaritaulukoita ohjelmiston hakkeroimiseen.

2.4.7 Kalastelu

Kalasteluhyökkäyksessä (phishing) yritetään huijata käyttäjiä luovuttamaan tunnistetietojaan tai muita arkaluonteisia tietoja (Stytch, 2023). Hyökkääjät lähettävät petollisia sähköposteja tai tekstiviestejä aiotuille uhreille saadakseen heidän tunnistetietonsa. Nämä viestit voivat sisältää linkkejä, joita napsautettuaan käyttäjä siirtyy väärennetylle verkkosivulle, jonne hänen on syötettävä tietonsa. Myös tällaisen linkin avulla laitteeseen voidaan asentaa haittaohjelmia.

Tietojenkalasteluhyökkäykset voivat olla satunnaisia tai kohdistettuja. Satunnaisissa hyökkäyksissä hakkerit lähettävät massaviestejä tekeytyen esimerkiksi testamenttien toimeenpanijoiksi saadakseen tunnukset (Stytch, 2023). Kohdennetut hyökkäykset voivat jäljitellä

tiettyjen yritysten viestejä, huijata käyttäjät syöttämään tunnuksensa tai nollaamaan salasanansa, mikä antaa hakkereille pääsyn käyttäjän tileille tai laitteille.

2.4.8 Haittaohjelmat

Haittaohjelmat on suunniteltu saamaan luvaton pääsy luottamuksellisiin tietoihin, kuten salasanoihin, käyttäjän laitteella (Stytch, 2023). Tämä voi sisältää tietojenkalasteluviestien tai liitteiden käytön sekä piilotetut linkit haitallisille verkkosivustoille.

Haittaohjelmilla voi olla erilaisia muotoja ja toimintoja (Stytch, 2023). Kaksi pääluokkaa, joita käytetään usein salasanojen varastamiseen, ovat vakoiluohjelmat ja näppäimistönlukijat (keyloggers). Vakoiluohjelmat asennetaan salaa käyttäjän laitteille, niiden avulla saadaan salasanat, joita käyttäjä käyttää.

Näppäimistönlukija on työkalu, joka tallentaa jokaisen näppäimistön painalluksen (Stytch, 2023). Tämän erittäin erikoistuneen työkalun avulla hyökkääjä voi päästä käsiksi suureen määrään luottamuksellisia tietoja käyttäjän huomaamatta. Näppäimistönlukija voi olla mikä tahansa ohjelmiston tai laitteiston osa, joka pystyy sieppaamaan ja tallentamaan kaikki käyttäjän toimet tietokoneen näppäimistöllä.

3 SALASANAHALLINTAOHJELMAT

3.1 Salasanahallintaohjelmatyypit

Monet ihmiset käyttävät salasanoja suojatakseen laitteita ja verkkotilejä hakkereilta, jotka saattavat yrittää saada heidän tietojansa (McAfee, i.a.). Tämä ei koske vain tietokoneita ja matkapuhelimia, vaan myös sähköposteja, sosiaalisia verkostoja ja verkko-ostoksia. Jokaisen salasanan on oltava ainutlaatuinen ja vain käyttäjän tiedossa. Monimutkaisten salasanojen keksiminen ja muistaminen ei ole helppoa. Tätä varten käytetään salasanahallintaohjelmia. Se on tehokas työkalu, joka tallentaa salasanoja salattuun muotoon. Tällöin käyttäjän ei tarvitse luoda ja muistaa salasanoja itse.

Kaikki salasanojen hallintaohjelmat eivät kuitenkaan ole samanlaisia (McAfee, i.a.). Jotkut niistä toimivat offline-tilassa, mikä tarkoittaa, että tiedot tallennetaan vain laitteelle ja ne on suojattu avainsalasanalla. Toiset tallentavat tietoja pilvitallennustilaan, jonka avulla tiedot voidaan synkronoida eri laitteiden välillä, mutta niiden käyttämiseen tarvitaan Internet-yhteys.

3.1.1 Selainpohjaiset salasanahallintaohjelmat

Selainten sisäänrakennetut salasananhallintaohjelmat on suunniteltu tallentamaan ja täyttämään käyttäjätiedot automaattisesti, kun kirjaudutaan verkkosivustoille (Zawalnyski, 2023). Nämä toiminnot on yleensä integroitu selaimen käyttöliittymään, ja niitä tarjotaan kätevänä tapana hallita salasanoja ilman erillistä sovellusta tai palvelua.

Selainpohjaisille salasanahallintaohjelmilla on etuja, kuten helppokäyttöisyys, integrointi selaimeen ja ilmaisuus, mutta niillä on myös merkittäviä haittoja (Zawalnyski, 2023). Esimerkiksi jotkut niistä eivät pysty luomaan vahvoja salasanoja käyttämällä riittävän erilaisia merkkejä. Niistä saattaa myös puuttua mukautustoimintoja, kuten kyky asettaa salasanan pituus ja muut suojauskäytännöt. Lisäksi tällaisen salasananhallintaohjelman toiminta rajoittuu tietyn selaimen käyttöön. Jos käyttäjä työskentelee eri selaimessa, on tarpeen käyttää eri työkalua.

3.1.2 Pilvipohjaiset salasanahallintaohjelmat

Pilvipohjaiset salasanahallintaohjelmat ovat sovelluksia tai palveluita, jotka tallentavat ja hallitsevat salasanoja pilvessä (Zawalnyski, 2023). Niiden avulla voidaan tallentaa, luoda ja täyttää automaattisesti salasanoja eri laitteissa, kuten tietokoneissa, älypuhelimissa ja tableteissa. Tämän työkalun tärkein etu on se, että sillä voidaan käyttää käyttäjän tunnistetietoja mistä tahansa, missä on internetyhteys. Tämä tekee salasanan käytöstä kätevää.

Näillä salasanahallintaohjelmilla on useita etuja (Zawalnyski, 2023):

1. Suojattu tallennus. Salasanat tallennetaan salattuna pilvitallennustilaan, mikä pitää käyttäjän kirjautumistiedot turvassa.
2. Varmuuskopiointi. Pilvitallennus takaa salasanojen turvallisuuden, vaikka laite kaatuu tai katoaa, joten pääsy voidaan palauttaa, kun internet on käytettävissä.
3. Korkeat turvallisuusstandardit. Nämä työkalut käyttävät yleensä vahvoja salausalgoritmeja, kuten AES-256-algoritmia, mikä tekee tiedoista käytännössä haavoittumattomia hyökkäyksille.

Negatiivinen puoli on, että tiedot ovat kolmannen osapuolen tallentamia. Vaikka palveluntarjoaja ei voi käyttää niitä, hän on edelleen vastuussa näiden tietojen hallinnasta.

3.1.3 Työpöytäpohjaiset salasanahallintaohjelmat

Työpöytäpohjaiset salasanahallintaohjelmat asennetaan yleensä käyttäjän tietokoneelle, ne tarjoavat laajan valikoiman ominaisuuksia salasanasuojauksen ja helppokäyttöisyyden varmistamiseksi (Zawalnyski, 2023). Salasanat tallennetaan käyttäjän paikalliselle laitteelle, mikä estää tiedon vuotamisen kolmannelta osapuolelta. Internetyhteys tarvitaan myös vain päivitysten vastaanottamiseen.

Tällainen työkalu on melko vaikea asentaa (Zawalnyski, 2023). Käyttäjän on myös muistettava varmuuskopiointi, sen manuaalinen tai automaattinen käyttö. Lisäksi kaikkien salasanojen tallentaminen yhteen paikkaan voi luoda haavoittuvuuden, jos hyökkääjä pääsee käsiksi tietokoneeseen tai tunnistetietoihin.

3.2 Ohjelmien valintakriteerit

Tällä hetkellä markkinoilla on suuri määrä salasanahallintaohjelmia. Osa on melko tunnettuja tuotteita, joita käyttää valtava määrä asiakkaita. Tältä osin yhdessä toimeksiantajan kanssa tunnistettiin useita kriteerejä, jotka valittujen salasananhallintaohjelmien tulisi täyttää.

3.2.1 Itseisännöity (self-hosted) salasanahallintaohjelma

Vaikka työskentely pilvipohjaisten salasanahallintaohjelmien kanssa on paljon mukavampaa ja helpompaa, on tietojen ja salasanojen tallentaminen kolmannen osapuolen toimesta huolenaihe. Istvanin ja Micaelan (2023) mukaan muutaman viime vuoden aikana hakkerit ovat yrittäneet useasti murtautua kolmannen osapuolen salasanatietokantoihin.

Itseisännöity salasanojen hallintaohjelmisto on eräänlainen salasananhallintaohjelmisto, jonka avulla henkilöt tai organisaatiot voivat tallentaa, hallita ja käyttää salasanojaan ja muita arkaluonteisia tietoja omilla palvelimillaan tai infrastruktuurillaan sen sijaan että luottaisivat kolmannen osapuolen palveluun tai pilvipalveluntarjoajaan (Psono, i.a.).

3.2.2 Monivaiheinen tunnistautuminen

Monivaiheinen tunnistautuminen (multi factor authentication, MFA) on menetelmä käyttäjän henkilöllisyyden todentamiseksi sisäänkirjautumisen tai tapahtuman suorittamisen yhteydessä, mikä edellyttää useiden eri todennusmenetelmien käyttöä (Yasar, 2023). Tämä prosessi yhdistää erityyppisiä tunnistetietoja käyttäjän henkilöllisyyden vahvistamiseksi. Esimerkiksi salasanan syöttämisen lisäksi käyttäjän pitää antaa lisätietoja, kuten matkapuhelimeen lähetettävän turvakoodi, tai käyttämällä biometrisiä tietoja, kuten sormenjälkitunnistusta tai kasvojentunnistusta. Useita eri menetelmiä käyttämällä järjestelmä tarjoaa paremman suojan luvattomalta käytöltä.

MFA-menetelmä pyrkii luomaan ylimääräisiä suojauskerroksia, jotta ei-toivottujen osapuolten on vaikeampi päästä käsiksi arvokkaisiin resursseihin, kuten fyysisiin paikkoihin, tietokoneisiin, verkkoihin tai tietokantoihin (Yasar, 2023). Vaikka yksi todennusmenetelmä

vaarantuisi hyökkääjän on silti voitettava muut suojaustasot, ennen kuin hän voi päästä käsiksi järjestelmään tai tietoihin. Tämä tekee tunkeutumisprosessista vaikeamman ja vähemmän todennäköisemmän, mikä lisää organisaatioiden ja käyttäjien turvallisuutta.

3.2.3 REST API

REST API on ohjelmistoarkkitehtuuristandardi verkkopalveluiden luomiseen (Buckler, 2022). Se tarjoaa käyttäjälle standardoidun tavan olla vuorovaikutuksessa salasanahallintaohjelman toimintojen kanssa HTTP:n kautta. REST API:n käyttöönotto salasanojen hallinnassa vaatii huolellista huomiota turvallisuusnäkökohtiin, kuten todennus, valtuutus, salaus ja validointi arkaluonteisten käyttäjätietojen suojan varmistamiseksi. Lisäksi kattavan sovellusliittymän dokumentaation tarjoaminen on välttämätöntä, jotta kehittäjät voivat käyttää sitä helpommin salasanojen hallinnan kanssa.

4 OHJELMIEN ESITTELY JA VERTALU

4.1 Valitut ohjelmat

Tässä luvussa esitellään vertailua varten valitut salasanahallintaohjelmat. Koska toimeksiantajan tärkein kriteeri oli itseisännöinti, kaikki valitut ohjelmat ovat itseisännöitäviä. Ohjelmat olivat Hashicorp Vault, Bitwarden ja Passbolt.

4.1.1 Hashicorp Vault

HashiCorp Vault on salaisuuksien (”secrets”) ja salauksen hallintatyökalu (HashiCorp Developer, i.a. -a). "Secrets" viittaa kaikkiin tietoihin, joiden luokse pääsyä halutaan valvoa tarkasti, kuten API-avaimia tai salasanoja. Vault tarjoaa salauksen, joka riippuu todennus- ja valtuutusmenetelmistä. Käyttöliittymän, komentorivin tai REST API:n avulla voidaan tallentaa ja hallita pääsyä salaisuuksiin ja muihin arkaluontoisiin tietoihin, asettaa tiukkoja käyttörajoituksia ja suorittaa turvatarkastuksia.

Vault käyttää tokenia eli salattua koneen luomaa koodia todennusmenetelmänä (HashiCorp Developer, i.a. -a). Token on kuin pääsylippu, joka oikeuttaa pääsyn tiettyihin palveluihin tietyksi ajaksi. Vaultin avulla voidaan luoda tokeneja manuaalisesti ja välittää ne asiakkaille, tai asiakkaat voivat kirjautua sisään ja luoda tunnuksia itse. Tämä prosessi tarjoaa tiukan hallinnan salaisuuksien ja muiden järjestelmän resurssien käyttöön.

HashiCorp Vault voidaan ottaa käyttöön sekä pilviympäristöissä että paikallisissa/itseisännöidyissä ympäristöissä (HashiCorp Developer, i.a. -a). On myös mahdollista käyttää ilmaista tai maksullista versiota.

4.1.2 Bitwarden

Bitwarden on monialustainen salasanahallintaohjelma (Bitwarden, i.a. -a). Käytön helpottamiseksi siinä on komentorivikäyttöliittymä. Laajennuksia on myös selaimille, kuten Chrome, Safari, Firefox ja monet muut. Ohjelmasta on verkkoversio, joka on käytettävissä millä tahansa internetyhteydellä varustetulla laitteella ja millä tahansa selaimella. Tiedot

synkronoidaan välittömästi keskitettyyn pilvitallennustilaan, mikä tarkoittaa, että kaikki yhteen laitteeseen lisätyt salaisuudet tulevat saataville lähes välittömästi muissa laitteissa. Lisäksi niille, jotka haluavat hallita tietojaan enemmän, on mahdollisuus käyttää omaa itseasennettua/itseisännöityä pilvitallennustilaa. Näin voidaan tallentaa kaikki salaisuudet ja tiedot henkilökohtaisesti valitsemalle laitteelle.

4.1.3 Passbolt

Passbolt on ilmainen, avoimen lähdekoodin salasanahallintaohjelma, joka on suunniteltu pienille ja suurille yrityksille (Containerize, i.a.). Toisin kuin monet muut salasanahallintaohjelmat, Passbolt asennetaan palvelimelle, mikä antaa tiimin jäsenille pääsyn salasanoihin ja mahdollisuuden jakaa ne koko tiimin kanssa. Passbolt käyttää tietojen suojaamiseen avoimen lähdekoodin salausta, joka tunnetaan nimellä GnuPG. Tämä standardi perustuu OpenPGP-tekniikkaan ja tarjoaa turvallisen päästä päähän -salauksen. Se käyttää pääavainta päästäkseen salasanatietokantaan, mikä tarjoaa korkean turvallisuustason. Google Chrome ja Mozilla Firefox -selainten lisäosat täyttävät salasanat automaattisesti vierailluilla verkkosivuilla. Passboltilla on myös mahdollisuus asentaa itseisännöity versio.

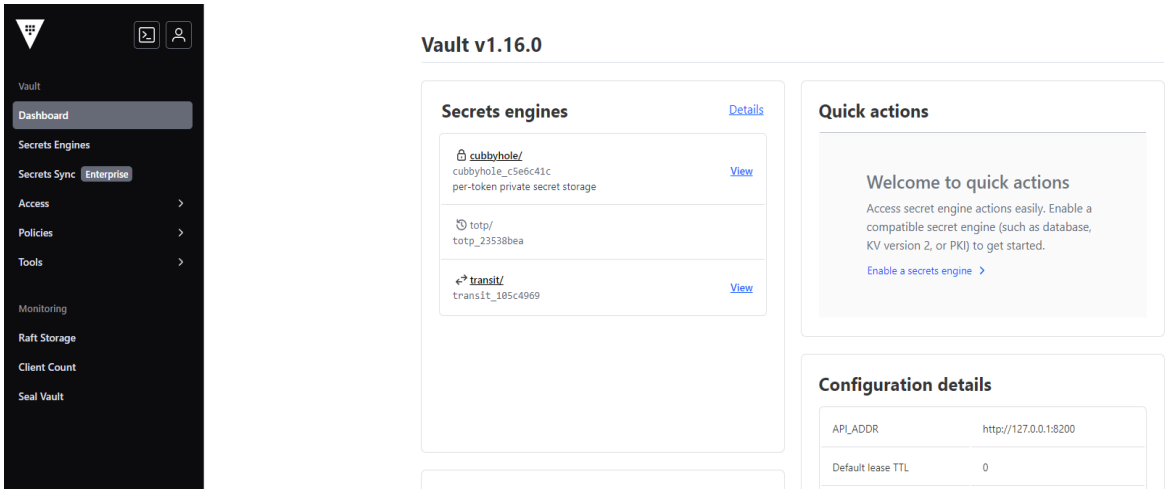
4.2 Asentaminen

Ohjelmien kokeilukäyttöön valittiin Linux Ubuntu 22.04 -palvelin, koska sillä on yksinkertainen asennusprosessi ja vakaa suorituskyky. Myös kaikki valitut ohjelmat, ohjeiden mukaan, voidaan asentaa tähän Linux-jakeluun. Jokaiselle ohjelmalle asennettiin oma erillinen palvelin Oracle VM VirtualBox -virtuaalikoneeseen. Tässä alaluvussa kerrotaan tarkemmin ohjelmien asentamisesta ja kokeilukäytöstä.

4.2.1 Hashicorp Vault

Hashicorp Vaultin asennus on kuvattu yksityiskohtaisesti virallisella tuotesivulla (HashiCorp Developer, i.a. -b). Valmistaja antaa erilliset ohjeet eri käyttöjärjestelmille (Linux, Windows, MacOs). Asennus suoritetaan muutamalla komennolla terminaalin avulla. Asennus ei ollut vaikeaa, dokumentaatiossa oli selkeät ohjeet. Asentamisen aikana saadaan

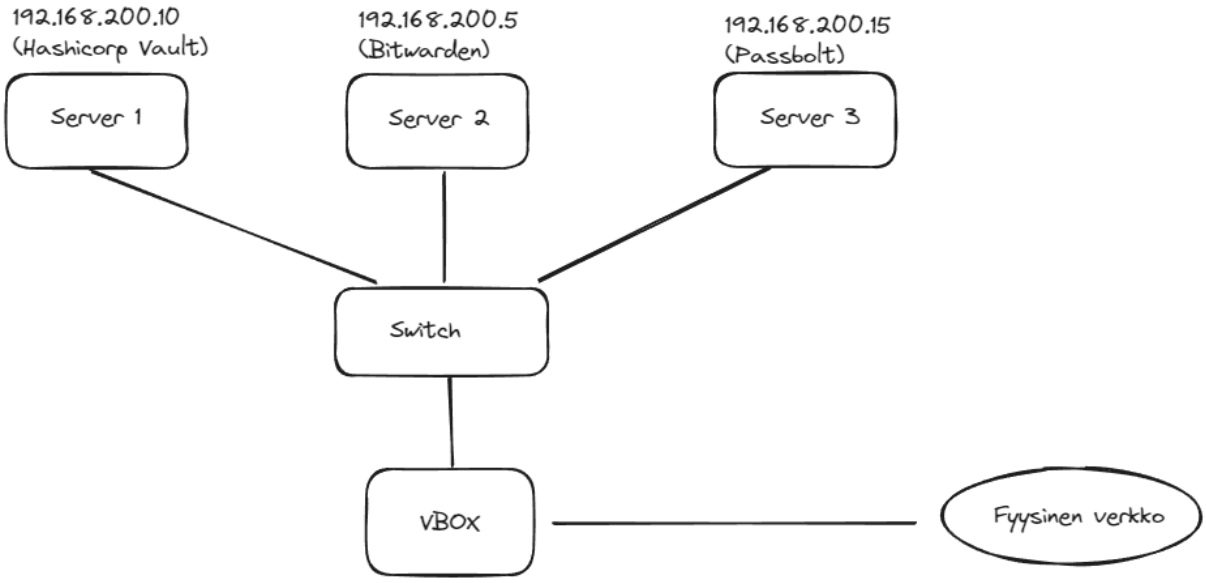
purkuavaimia, jotka tarvitaan graafisen käyttöliittymän sivulle pääsemiseen. Kuvassa 1 on Hashicorp Vaultin graafinen käyttöliittymä, joka on avattu selaimessa.



Kuva 1. Hashicorp Vaultin graafinen käyttöliittymä

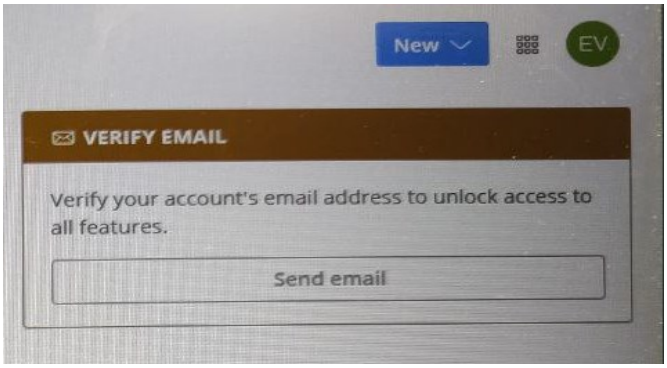
4.2.2 Bitwarden

Bitwardenin asentaminen on mahdollista myös Linux-palvelimelle, mutta ennen sitä on asennettava Docker-alusta palvelimelle, koska asennustiedostot puretaan Docker-kontista. Docker on työkalu, joka käyttää kontteja sovellusten kehittämiseen, asentamiseen ja suorittamiseen. Konttien avulla pakataan sovelluksen ja kaikki sen riippuvuudet yhdeksi paketiksi: kirjastot, järjestelmän apuohjelmat ja määritystiedostot (Docker.Docs, i.a.). Lisäksi asennus vaatii verkkotunnuksen, mikä aiheutti lisää verkkoasetuksia. Verkkoasetukset tuottivat hieman vaikeuksia ja vaativat ulkopuolista apua. Paikallisen verkkotunnuksen luomiseksi Ubuntu-palvelimelle tehtiin DNS-palvelun asennus. Tämän palvelun avulla muutetaan numeerisessa muodossa kirjoitettu IP-osoite tekstinimeksi, jota tarvitaan Bitwardenia asennettaessa. Kuvassa 2 näkyy verkko, joka on luotu käyttämään paikallista verkkotunnusta.



Kuva 2. Verkon asetukset.

Nämä asetukset valittiin siten, että virtuaalikoneet kommunikoivat keskenään ilman internetyhteyttä. Näin saadaan mahdollisuuden käyttää paikallisesti luotua verkkotunnusta. Asennuksen jälkeen Bitwarden-käyttöliittymä näkyy siirtymällä asennuksen aikana määritettyyn verkkotunnusosoitteeseen. Lisäksi, kun avataan Bitwardenin ensimmäisen kerran, pyydetään vahvistamaan sähköposti lisäominaisuuksien saamiseen. Kuva 3 esittelee vahvistuspyynnön, joka vaaditaan Bitwardenin asennuksen jälkeen.



Kuva 3. Sähköpostin vahvistuspyyntö.

Vahvistusta varten on määritettävä SMTP-palvelin sähköpostin lähettämistä ja vastaanottamista varten. Työssä käytettiin Googlen SMTP-palvelua. Tarvittavat asetukset on määritetty asetustiedostossa. Kuvassa 4 on SMTP-palvelimen asetukset, jotka on lisättävä global.override.env-tiedostoon.

```
globalSettings__mail__replyToEmail=evgeni.baranov@gmail.com
globalSettings__mail__smtp__host=smtp.gmail.com
globalSettings__mail__smtp__port=587
globalSettings__mail__smtp__ssl=true
globalSettings__mail__smtp__username=evgeni.baranov@gmail.com
globalSettings__mail__smtp__password=[redacted]
```

Kuva 4. SMTP-palvelimen asetukset asetustiedostossa global.override.env

4.2.3 Passbolt

Passboltin asentaminen vaatii uuden palvelimen, johon ei ole asennettu muita palveluita (Passbolt, i.a. -a). Myös asentaminen vaatii verkkotunnuksen, kuten Bitwarden-salasanahallintaohjelma. Tätä varten luotiin DNS-palvelu Ubuntu-palvelimelle samalla tavalla kuin palvelimelle, johon Bitwarden oli asennettu. Kehittäjäsivulla on yksityiskohtaiset ohjeet, joiden avulla voidaan asentaa Passbolt useisiin Linux-käyttöjärjestelmiin, kuten esimerkiksi Ubuntu 22.04, Debian 12, Fedora38.

On tärkeää huomata, että työssä käytettiin ohjelmia, jotka oli asennettu kokeilukäyttöön. Siksi SSL-avaimia, joita tarvitaan salatun yhteyden luomiseksi verkkopalvelimen ja selaimen välille, ei määritetty asennuksen aikana. Tämän takia, kuten kuva 5 näyttää, selaimessa ohjelmia avattaessa on selvää, että yhteys ei ole turvallinen. Ohjelman valinnan jälkeen käyttäjän on määritettävä SSL asennuksen aikana.

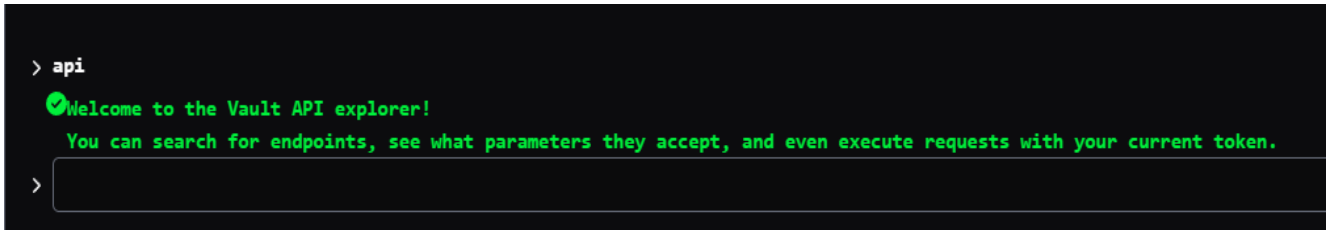
Kuva 5. Varoitus suojaamattomasta yhteydestä selaimessa

4.3 REST API:n saatavuus

Tässä alaluvussa kerrotaan tarkemmin REST APi:n saatavuudesta ja sen kokeilukäytöstä.

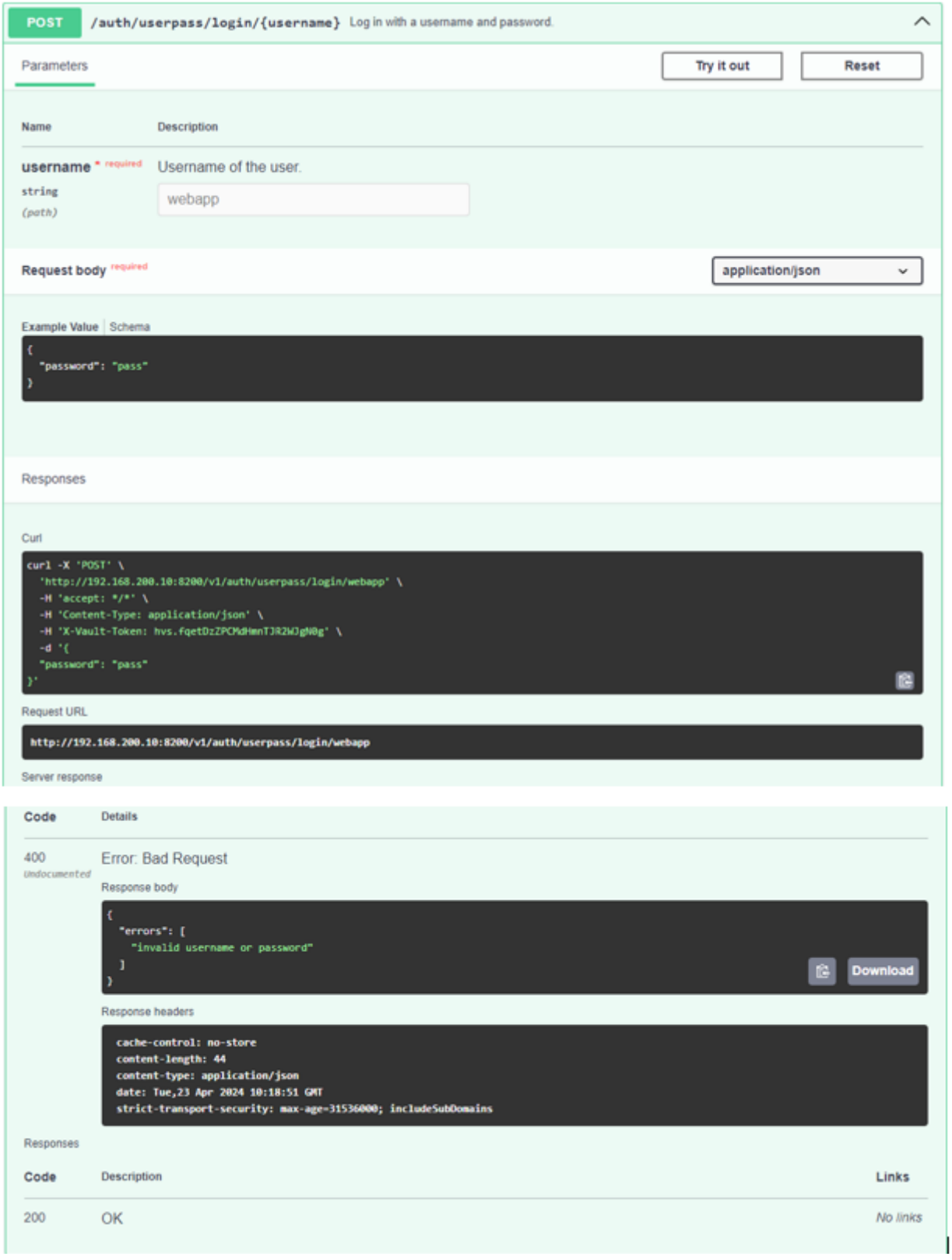
4.3.1 Hashicorp Vault

Hashicorp Vaultilla on REST API, jolla voidaan hallita Vaultin kaikkia osia. Kuva 6 näyttää, että API:n lista voidaan saada esimerkiksi sisäänrakennetun terminaalin kautta kirjoittamalla sinne komento ”api”.



Kuva 6. API:n käytön pääsykomento

Tämän jälkeen tulee näkyviin pitkä lista, joka sisältää API-polkuja. Jokaisen pyynnön toimintaa voidaan kokeilla käyttöliittymän avulla. Useimmat pyynnöt sisältävät myös kuvauksen jo itse otsikossa. Pyyntöjä ovat esimerkiksi todennukseen oikeutettujen käyttäjien listan saaminen (kosketuspiste ”/auth/userpass/users/”) tai kirjautuminen sisään käyttäjätunnusta ja salasanaa käyttäen (kosketuspiste ” /auth/userpass/login/{username}”). Pyyntötiedot ja vastaustiedot Vaultiin ja Vaultista ovat JSON-muodossa. Kuvassa 7 on esimerkki API:n toiminnasta eli sisäänkirjautumisesta käyttäjätunnuksella ja salasanalla.



Kuva 7. REST API:n pyynnön esimerkki. JSON-tiedosto ja vastauksen status

4.3.2 Bitwarden

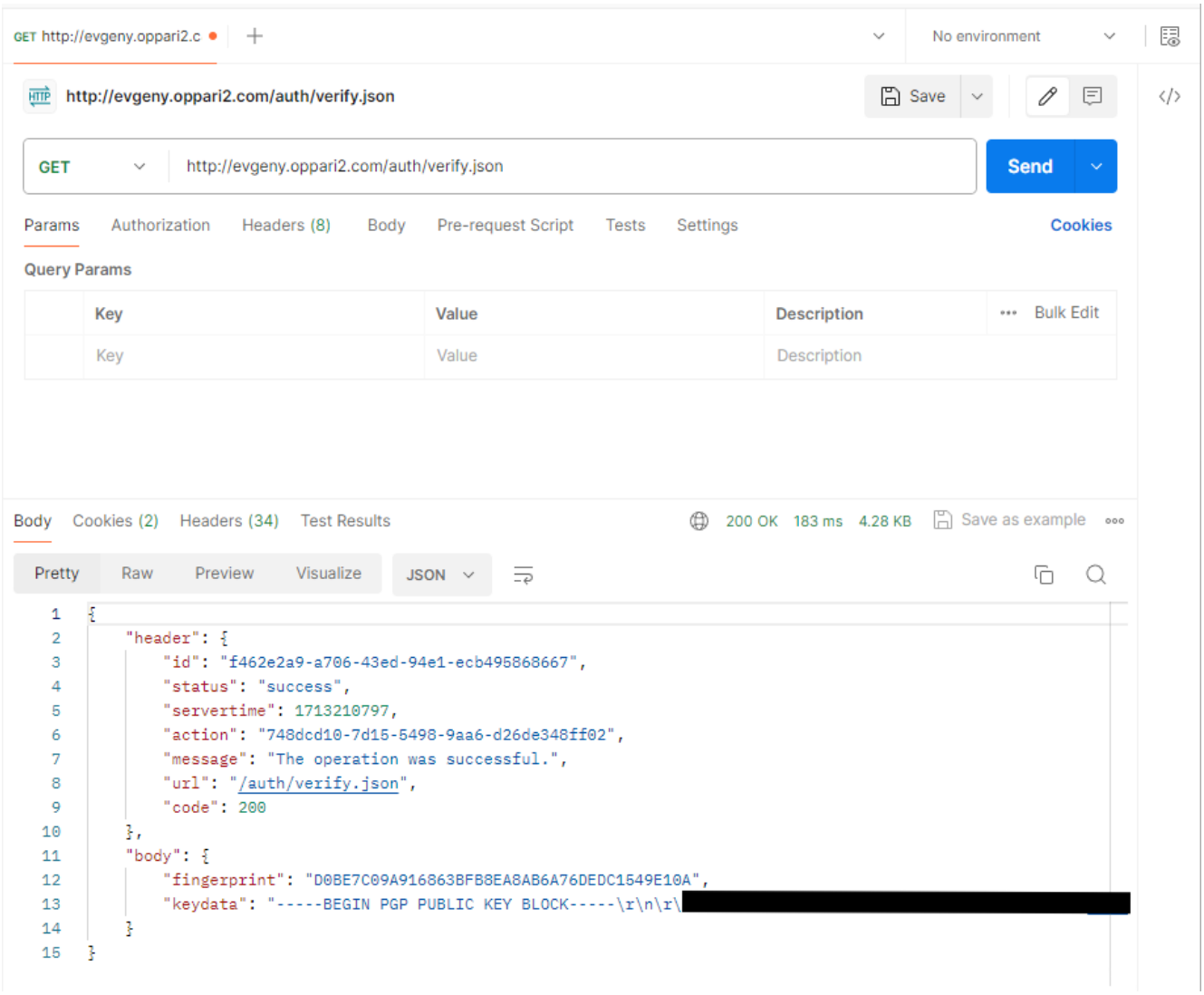
Dokumentaation mukaan Bitwardenilla on kaksi API:a, joilla on erilaiset toiminnot (Bitwarden, i.a. -b). Toinen on Public API, joka on saatavilla organisaatioille ja toinen, nimellä Vault Management API, on saatavilla yksityisille käyttäjille. Bitwardenin versio, jota käytetään tässä työssä, on yksityisille tarkoitettu salasanahallintaohjelma, sen takia harkitaan vain toista API:a. Vault Manager API:n toiminta vaatii Bitwarden CLI -komentorivikäyttöliittymän asentamista. Sen asentamisen jälkeen käyttäjällä on pääsy bw-komentoon. Sen avulla voidaan työskennellä Vault Manager API:n kanssa komentorivillä. Kuvassa 8 nähdään esimerkki, miten voidaan kirjautua sisään sähköpostia ja master-salasanaa käyttämällä.

```
evgeny@evserver:~$ bw login
? Email address: evgeny.baranov@seamk.fi
? Master password: [hidden]
? Two-step login code: 212293
You are logged in!
```

Kuva 8. Bw-komennon käyttäminen

Dokumentaatiossa on suuri määrä komentoja, esimerkiksi ”bw unlock”, joka luo purkuavaimen, jota käytetään vuorovaikutuksessa tietojen kanssa, tai ”bw create item”, joka luo uuden objektiin holviin, mutta joidenkin käyttö edellyttää organisaation lisenssiä.

Aivan kuten kahdessa muussa ohjelmassa, Passboltilla on oma REST API, jota asiakkaat voivat käyttää kehitystyössä (Passbolt, i.a. -b). Tietojen käsittelyn helpottamiseksi vastaus palvelimelle lähetettyihin pyyntöihin palautetaan JSON-muodossa, kuten Hashicort Vaultissa ja Bitwardenissa. REST API:n toiminnan tarkistamiseen käytettiin Postman-ohjelmaa. Sen avulla käyttäjä voi olla vuorovaikutuksessa API:n kanssa graafisen käyttöliittymän avulla. Ohjelman avulla lähetetään erilaisia pyyntöjä (GET, POST, PUT, DELETE ja muut) ja analysoidaan vastauksia. Kuva 9 näyttää, että GET-pyyntö lähetetään endpointille (kosketuspisteeseen) "/auth/verify.json", josta sitten saadaan JSON-vastaus.



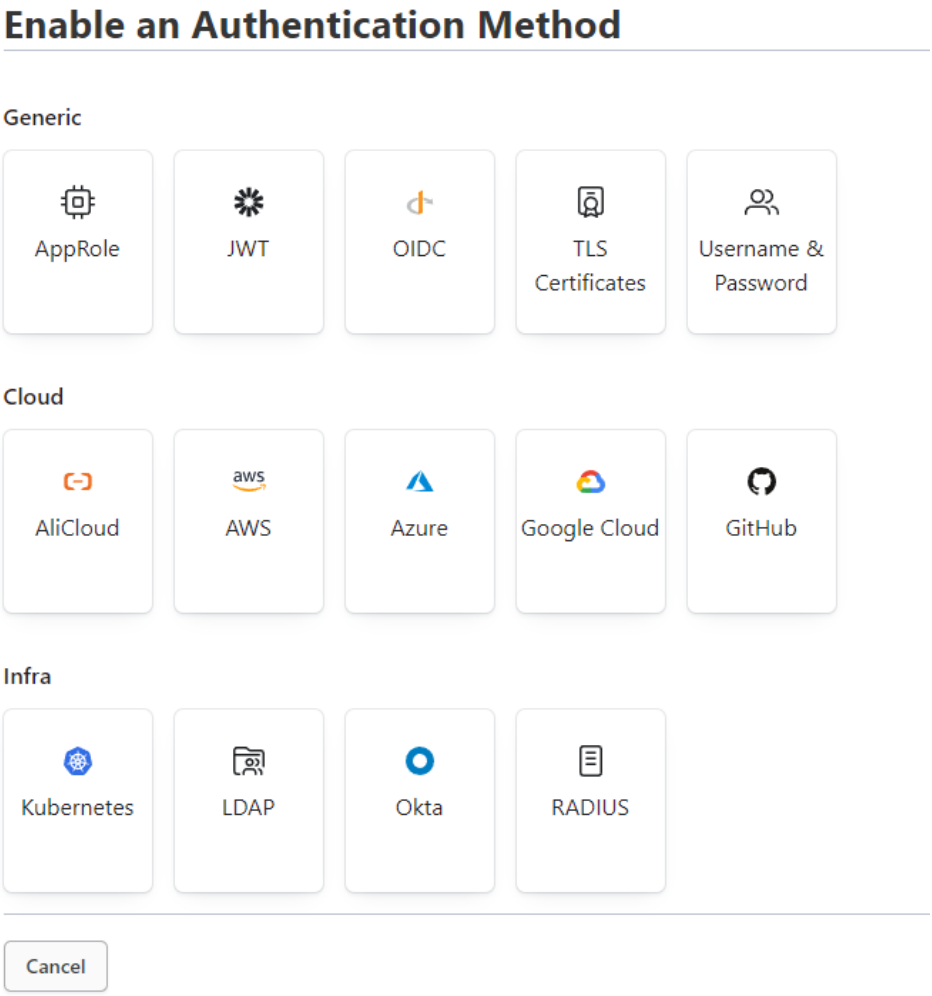
Kuva 9. Passboltin API:n testaus Postman-ohjelman avulla

4.4 Monivaiheisen tunnistautumisen saatavuus.

Tässä alaluvussa kerrotaan monivaiheisen tunnistautumisen saatavuudesta.

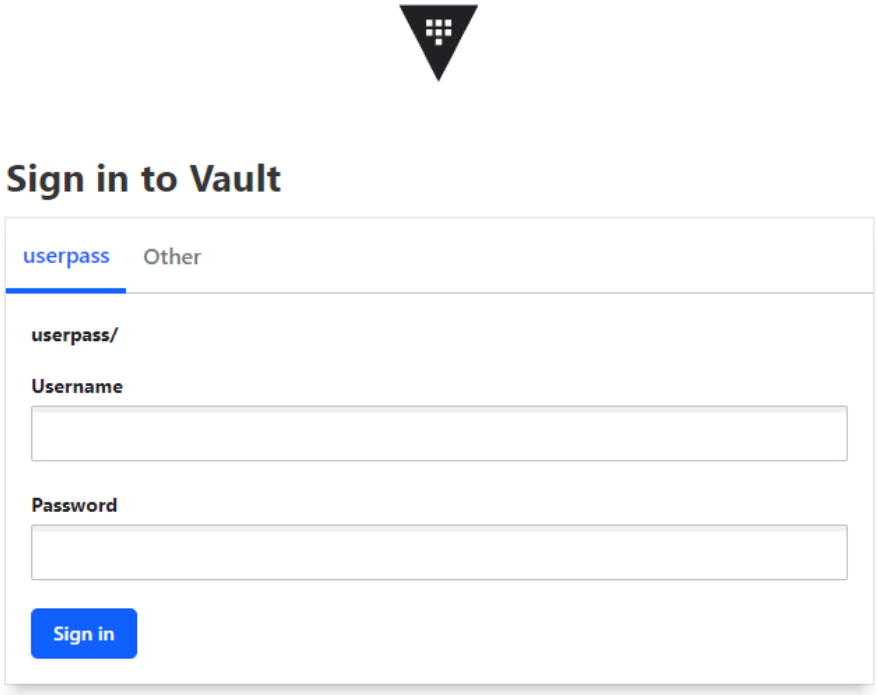
4.4.1 Hashicorp

Hashicorp Vaultin asennetun version avulla voidaan valita erilaisia todennusmenetelmiä. Kuva 10 esittelee kaikkia saatavilla olevia todennusmenetelmiä Hashicorp Vaultissa.



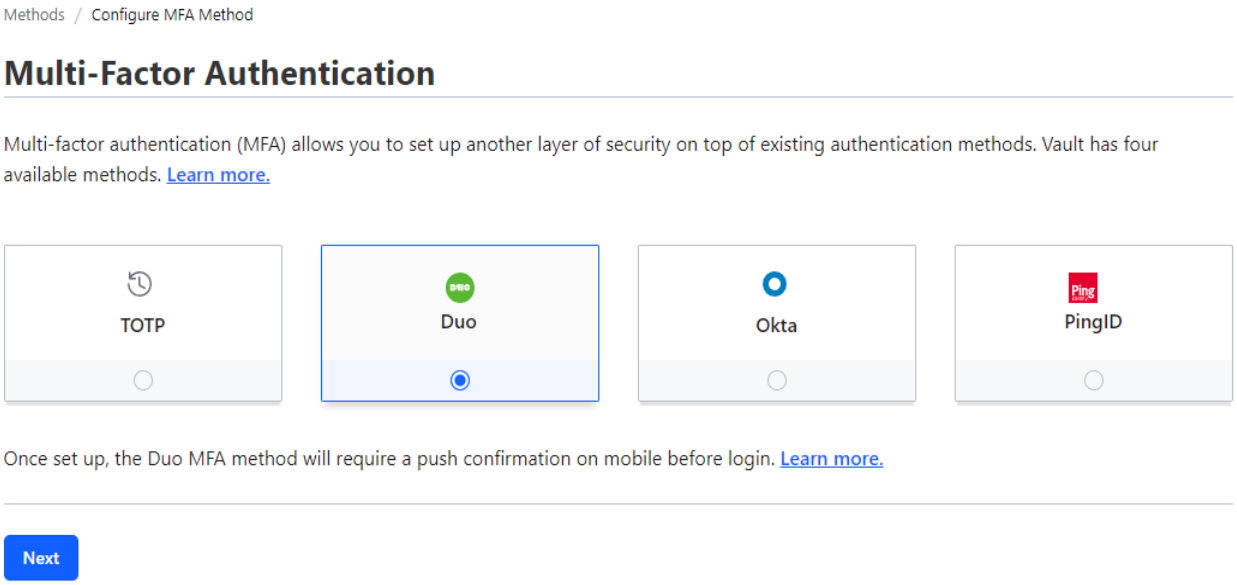
Kuva 10. Hashicorp Vaultin kirjautumismenetelmät

Työssä käytettiin käyttäjätunnus/salasana-todennusta, jolla pääsee käyttäjän sivulle. Tätä varten luotiin uusi käyttäjä järjestelmänvalvojan puolelle ja tehtiin asetukset Hashicorp-dokumentaation mukaisesti. Kuvassa 11 nähdään kirjautumissivu, missä valitaan käyttäjätunnus/salasana-todennus.



Kuva 11. Hashicorp Vaultin kirjautumissivu

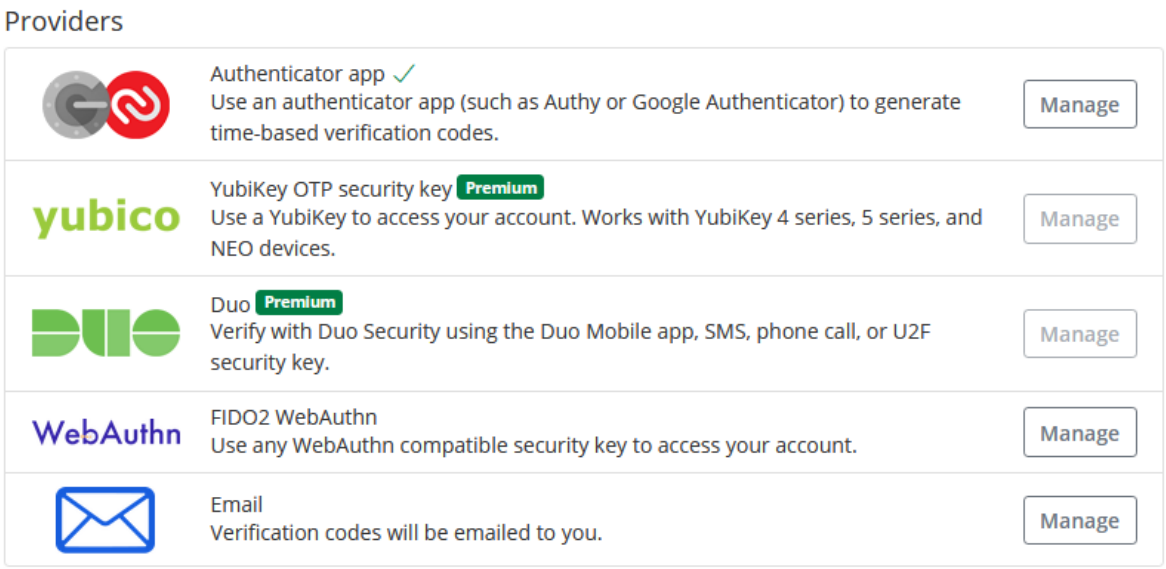
Lisäksi Hashicorp Vaultin avulla voidaan määrittää monivaiheinen todennus olemassa olevan todennuksen päälle. Kuten kuva 12 näyttää, Vaultilla on käytettävissä neljä menetelmä: TOTP, Duo, Okta, PingID. TOTP on kaksivaiheinen todennusmenetelmä, joka käyttää kertaluonteisia salasanoja, jotka on luotu nykyisen ajan perusteella (Time-Based One-Time Password). Duo, Okta ja PingID ovat tunnistautumisen ja pääsyhallinnan alustoja, jotka tarjoavat monivaiheisen todennuksen. Esimerkiksi salasanan syöttämisen lisäksi käyttäjää voidaan pyytää syöttämään kertaluonteinen koodi, joka lähetetään hänen mobiililaitteeseensa.



Kuva 12. Saatavilla olevat monivaiheiset todennusmenetelmät Hashicorp Vaultissa

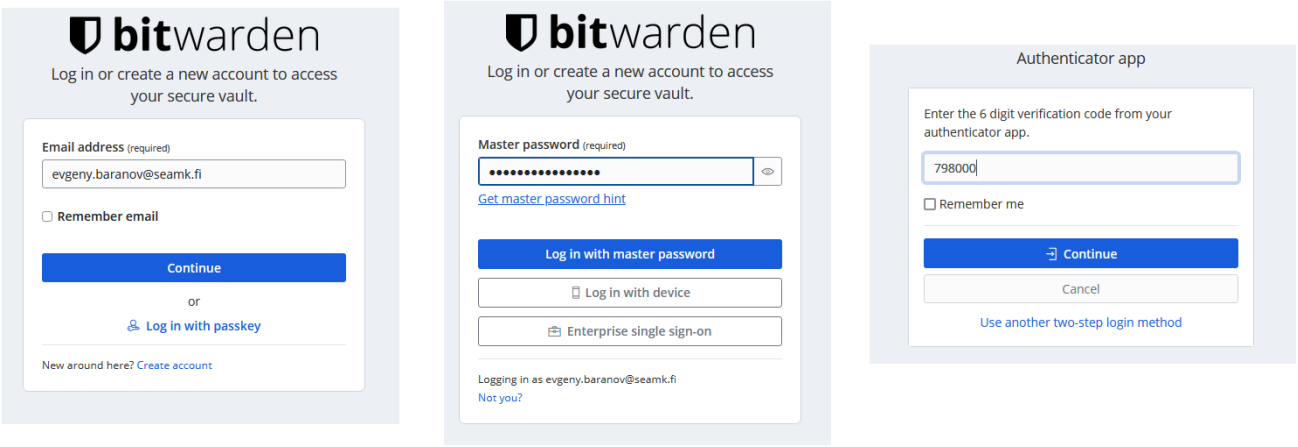
4.4.2 Bitwarden

Bitwarden, samoin kuin Hashicorp Vault, tarjoaa mahdollisuuden määrittää monivaiheinen tunnistautuminen. Kuvassa 13 näkyy, että Bitwardenin asennetussa versiossa on 5 erilaista todennusmenetelmää, joista kaksi vaatii maksullisen lisenssin.



Kuva 13. Saatavilla olevat monivaiheiset todennusmenetelmät Bitwardenissa

Tässä käytetään Authenticator App -menetelmä, joka vaatii sovelluksen, kuten ”Authy” Androidille. Sen avulla saadaan vahvistuskoodi, joka päivitetään joka minuutti, ja jota tarvitaan Bitwarden-sivulle kirjautumiseen pääsalasanan lisäksi. Kuvassa 14 on Bitwardenin kirjautumisvaiheet monivaiheista tunnistautumista käyttäen.



Kuva 14. Bitwardenin kirjautumisvaiheet monivaiheista tunnistautumista käyttäen

Passbolt, niin kuin muut ohjelmat, tarjoaa monivaiheista tunnistautumista. Siihen kuuluu TOTP-menetelmä, DUO- ja Yubikey-alustat. Kuten alaluvussa 4.2.3 mainittiin, SSL-avaimen puuttumisen vuoksi tämän palvelun toimintaa oli työssä mahdotonta varmistaa. Kehittäjäsivulla on kuitenkin ohjeet kunkin menetelmän määrittämiseen.

4.5 Ominaisuustaulukko

Tässä taulukossa vertaillaan salasanahallintaohjelmia ominaisuuksien perusteella.

Taulukko 1. Ominaisuustaulukko

	Hashicorp Vault	Bitwarden	Passbolt
Valmistusmaa	US	US	Luxemburg
Avoin lähdekoodi	kyllä	kyllä	kyllä
API	kyllä	kyllä	kyllä
Hinta (yrityksille, enterprise)	käsitellään erikseen asiakkaan kanssa	$6/käyttäjä/kk	käsitellään erikseen asiakkaan kanssa
MFA	kyllä	kyllä	kyllä
Mobiilisovellus	ei	kyllä	kyllä
Selaimen lisäys	kyllä	kyllä	kyllä

5 TULOKSET JA POHDINTA

Opinnäytetyön tavoitteena oli vertailla salasanahallintaohjelmia. Vaikka markkinoilla on tällä hetkellä valtava valikoima ohjelmia, otetiin vertailuun tuotteet, jotka tarjoavat pilviratkaisujen lisäksi itseisännöityjä versioita. Jokaista salasanahallintaohjelmaa varten virtuaalikoneeseen oli asennettu erilliset palvelimet.

Asennusvaiheessa ilmeni vaikeuksia, koska kaksi ohjelmaa vaati verkkotunnuksen osoitteen. Tämän ongelman ratkaisemiseksi oli tarpeen määrittää virtuaalikoneen verkko siten, että palvelimet voivat ottaa yhteyttä toisiinsa ilman ulkopuolista verkkoa. Onnistuneen asennuksen jälkeen määritettiin kriteerit, joilla ohjelmia voitiin verrata. Koska ohjelmat ol asennettu ilman SSL-avainta, joitain ominaisuuksia, kuten monivaiheinen tunnistautuminen, ei voitu tarkistaa. Lisäksi, koska asennetut ohjelmat ovat ilmaisia, jotkin ominaisuudet eivät ole käytettävissä, kuten käyttäjäryhmän luominen.

Samalla tutustuttiin ohjelmien REST API -saatavuuteen. Suuri määrä kosketuspisteitä (endpointeja) voi tarjota lisämahdollisuuksia käyttöön ja kehittämiseen.

Yksiselitteisesti on vaikea sanoa, mikä salasanahallintaohjelma on paras, koska jokaisella ohjelmalla on toiminnot, jotka olivat vertailukriteereissä. Kaikissa niissä on avoin lähdekoodi, mahdollisuus monivaiheiseen tunnistautumiseen ja REST API:n saatavuus. Bitwardenin ja Passboltin mobiilisovelluksen saatavuus on positiivinen tekijä. Ehkä ratkaiseva tekijä on hinta, joka veloitetaan yritysversiosta.

Tulevaisuudessa opinnäytetyön tutkimus voi olla hyvänä alkuna toimeksiantajalle uuden salasanahallintaohjelman valinnassa. Samaan aikaan salasanojen hallinta on melko laaja ja tärkeä aihe, joka vaatii lisäkoulutusta ja tutkimusta jatkokäyttöön.

Työ onnistui hyvin, vaikka asentamisen osuudessa tuli vastaan vaikeuksia. Töitä tehdessä joutui tutustumaan verkon asetuksiin, palvelimiin ja DNS-palvelujen asentamiseen, mikä toimi hyvänä käytäntönä ja uutena kokemuksena. Jatkossa olisi mielenkiintoista osallistua asennukseen, perehtyä salasanahallintaohjelman toimintaan ja käyttöön.

LÄHTEET

1Password. (28.10.2022). *What is a dictionary attack, and how do you protect yourself from it?* https://blog.1password.com/what-is-dictionary-attack/

Arnon. (i.a.). *ABOUT US.* https://arnon.fi/company/about-us

Beaver, K. (2010). *Hacking for Dummies* (3. p.). Wiley Publishing

Beyond Identity. (i.a.). *Rainbow Table Attack*. https://www.beyondidentity.com/glossary/rainbow-table-attack

Bitwarden. (i.a. -a). *How Bitwarden works.* Bitwarden. https://bitwarden.com/products/

Bitwarden. (i.a. -b). *Password Manager APIs*. Bitwarden. https://bitwarden.com/help/bitwarden-apis/

Buckler, C. (24.8.2022). *What Is a REST API?* Sitepoint. https://www.sitepoint.com/rest-api

Containerize. (i.a.). *Free, Open Source & Self-hosted Password Manager.* Containerize. https://products.containerize.com/password-management/passbolt/

Docker.docs. (i.a.). *Docker overview.* Docker.docs. https://docs.docker.com/get-started/overview

Erickson, K. (2019). *Hacking: 4 Books in 1- Hacking for Beginners, Hacker Basic Security, Networking Hacking, Kali Linux for Hackers.* CODING HOOD

HashiCorp Developer. (i.a. -a). *What is Vault?* HashiCorp Developer. https://developer.hashicorp.com/vault/docs/what-is-vault

HashiCorp Developer. (i.a. -b). *Install Vault*. HashiCorp Developer. https://developer.hashicorp.com/vault/tutorials/getting-started/getting-started-install

Irwin, L. (11.4.2023). *What is a MITM Attack? Definition, Prevention & Examples.* IT Governance European Blog. https://www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-middle-attacks

Istvan, F., & Micaela, A. (22.12.2023). *Which Password Managers Have Been Hacked?* Best Reviews. https://password-managers.bestreviews.net/faq/which-password-managers-have-been-hacked

Kiser, Q. (2020). *Cybersecurity: A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering* (lukija: I. Busenius). [Äänikirja]. Quinn Kiser.

McAfee. (i.a.). *What Is a Password Manager?* https://www.mcafee.com/learn/what-is-a-password-manager

Passbolt. (i.a. -a). *Install Passbolt on Ubuntu 22.04.* Passbolt. https://www.passbolt.com/docs/hosting/install/ce/ubuntu/

Passbolt. (i.a. -b). *Passbolt API Documentation*. Passbolt. https://help.passbolt.com/api

Psono. (i.a.). *What is a self hosted password manager?* Psono. https://psono.com/

Secret Double Octopus. (i.a.). *Password Spraying.* https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying

Stytch. (10.7.2023). *The top 10 password cracking techniques – and how to outmaneuver them*. https://stytch.com/blog/top-10-password-cracking-techniques/

The College of New Jersey (TCNJ). (i.a.). *Passwords.* https://security.tcnj.edu/security-guidelines/passwords

Yasar, K. (2023). *What is multifactor authentication?* TechTarget. https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

Zawalnyski, A. (13.11.2023). *What Are The Different Types Of Password Manager?* Expert Insights. https://expertinsights.com/insights/what-are-the-different-types-of-password-manager