Nasazení systému pro správu hesel

Bc. Jakub Pail

Diplomová práca
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jakub Pail**
Osobní číslo:	**A21150**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Prezenční**
Téma práce:	**Nasazení systému pro správu hesel**
Téma práce anglicky:	**Deployment of a Password Management System**

Zásady pro vypracování

1. Proveďte literární rešerší na dané téma.
2. Porovnejte aplikace pro správu hesel.
3. Navrhněte politiky užívání autentizačních faktorů.
4. Navrhněte správce hesel pro použití v Knihovně UTB.
5. Navrhněte automatizovaný systém pro centralizované ukládání hesel.
6. Napište uživatelskou příručku k nasazenému správci hesel.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. BURNETT, Mark a Dave KLEIMAN. Perfect passwords: selection, protection, authentication. Rockland, Mass.: Syngress, 2006, xv, 181 s. ISBN 9781597490412. Dostupné také z: http://www.sciencedirect.com/science/book/9781597490412.
2. BONNETT, Dovell. Making Passwords Secure: Fixing the Weakest Link in Cybersecurity. CreateSpace Independent Publishing Platform, 2016, 170 s. ISBN 9781530164486. Dostupné také z: http://students.aiu.edu/submissions/profiles/resources/onlineBook/F2H2H9_Making%20Passwords%20Secure.pdf.
3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY Advanced Encryption Standard (AES). In NIST FIPS PUB 197. 2001.
4. MCTEER, Dan a Bryan KRAUSEN. Running HashiCorp Vault in Production. Amazon Digital Services LLC – KDP Print US, 2020. ISBN 9798639476969.
5. KARMAKAR, Amiya. Secure Authentication using Advanced Encryption Standard (AES). LAP LAMBERT Academic Publishing, 2021. ISBN 6204728725.
6. JAŠEK, Roman, David MALANÍK a Nicol DAŇKOVÁ. Bezpečnost informačních systémů. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2022. ISBN 9788076780880.
7. SAWANT, Uday R., Oliver PELZ, Jonathan HOBSON a William LEEMANS. Linux: Powerful Server Administration. Birmingham: Packt Publishing Ltd, 2017. ISBN 9781788297424.
8. NEGUS, Chris. Linux bible. Ninth edition. Indianapolis, Indiana: Wiley, 2015, online resource (914 pages). ISBN 9781119209539. Dostupné také z: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119209539.

Vedoucí diplomové práce: **doc. Ing. Zdenka Prokopová, CSc.**
Ústav počítačových a komunikačních systémů

Konzultant diplomové práce: **Ing. Ivan Masár**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **2. prosince 2022**
Termín odevzdání diplomové práce: **1. června 2023**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 8. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 01.06.2023

Jakub Pail v.r.
podpis studenta

ABSTRAKT

Diplomová práca sa zaoberá problematikou správcov hesiel a nástroja na automatizované ukladanie hesiel a ich nasadením v univerzitnom prostredí. Pre výber vhodného správcu hesiel boli použité multi-kriteriálne analýzy. Jedna analýza bola vytvorená na základe súčtu bodov, druhou bolo použitie TOPSIS. Následne po vyhodnotení analýz bol, za použitia prostredia Knižnice UTB, nasadený správca hesiel na systéme Ubuntu. Taktiež bol nasadený systém na automatizované ukladanie hesiel určený pre administrátorov. Výsledkom práce sú dva funkčné systémy nasadené v prostredí Knižnice UTB a návrh bezpečnostnej politiky, z dôvodu, aby boli systémy správne využívané.

Kľúčové slova: správca hesiel, heslo, viacfaktorové overovanie, autentifikácia

ABSTRACT

The diploma thesis deals with the issue of password managers and a tool for automated password storage and their deployment in a university environment. Multi-criteria analyzes were used to select a suitable password manager. One analysis was created based on the sum of points, the other was the use of TOPSIS. Subsequently, after evaluating the analyses, a password manager was deployed on the Ubuntu system using the TBU Library environment. A system for automated password storage designed for administrators was also deployed. The result of the work are two functional systems deployed in the TBU Library environment and a draft security policy, so that the systems are used correctly.

Keywords: Password manager, Password, multifactor authentication, authentification

Poďakovanie

Poďakovanie patrí predovšetkým rodine za podporu počas štúdia či už finančnú alebo aj psychickú. Ďalej konzultantovi Ing. Ivanovi Masárovi za odborné vedenie v rámci diplomovej práce a vedúcej práce doc. Ing. Zdenke Prokopovej, CSc. za vedenie pri písaní diplomovej práce. Poďakovanie patrí tiež Knižnici UTB za umožnenie riešenia diplomovej práce v prostredí Knižnice UTB a za podpory Knižnice UTB a celého personálu.

Prehlasujem, že odovzdaná verzia bakalárskej práce a verzia elektronicky nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

V dnešnej dobe nasadenie správcu hesiel narastá na význame. S narastajúcim výpočtovým výkonom sa neustále zvyšujú požiadavky na silné heslá, čo robí vymýšľanie správneho hesla čoraz zložitejším.

Vytvorenie správneho hesla by samo osebe nebolo príliš zložité, ak by sme si ho nemuseli zapamätať. Preto je dôležité používať nástroj na správu hesiel, ktorý nám umožní bezpečne si ich zapamätať a používať. Papier a pero nie sú vhodné, pretože iné osoby by mohli jednoducho prečítať zaznamenané heslá.

Cieľom tejto práce je vybrať a nasadiť vhodného správcu hesiel na základe požiadaviek Knižnice UTB. Pri výbere a nasadení je dôležité zvážiť nielen samotný výber a nasadenie, ale aj prispôsobenie správcu hesiel prostrediu, v ktorom sa bude používať.

Teoretická časť práce sa zaoberá vysvetlením pojmu "správca hesiel" a všetkým, čo je potrebné vedieť o správnom používaní a nastavení takéhoto nástroja. Práca sa zameriava aj na automatizovaný systém na správu hesiel.

V prvej časti sú popísané základné pojmy k problematike správcov hesiel. Vysvetlené dôvody prečo je nutné sa problematike správcov hesiel venovať. Charakteristické funkcie pre správcov hesiel. Taktiež sú v teoretickej časti stručne popísané typy správcov hesiel. V teoretickej časti sú tiež popísané populárne možnosti, ktoré by sa dali považovať za vhodné varianty. Poslednou časťou prvej kapitoly sú možnosti šifrovania ponúkané správcami hesiel.

Druhá kapitola teoretickej časti práce popisuje základné pojmy potrebné pre pochopenie. Napr. čo to je automatizovaný systém na správu hesiel, ako aj možnosti, ktoré automatizovaný systém na správu hesiel ponúka. V tejto časti sú tiež možnosti s akými autentizačnými nástrojmi dokáže pracovať systém Vault a aké funkcie dokáže vykonávať okrem automatizovaného ukladania a sprístupňovania hesiel.

Diplomová práca v ďalšej kapitole nadväzuje praktickým testovaním správcov hesiel. Konkrétne ukladaním, generovaním a viacfaktorovým overovaním, aby sa zabezpečil výber čo najlepšieho a najvhodnejšieho správcu hesiel na základe požiadavkou Knižnice UTB.

Pre výber vhodného správcu hesiel sa v nasledujúcej kapitole testované funkcie porovnávajú dvomi multi-kriteriálnymi analýzami. Prvá analýza je na základe bodov a druhá na základe bodov s váhami TOPSIS, podľa dôležitosti jednotlivých kritérií pre Knižnicu UTB.

Po určení správcu hesiel na základe analýz je v diplomovej práci ďalej popísané nasadenie správcu hesiel v prostredí Knižnice UTB na základe požiadavkou stanovených Knižnicou UTB. Nasadenie prebiehalo pomocou dostupných nástrojov v prostredí Knižnice UTB. Tiež bol správca hesiel testovaný. V prílohe priložená používateľská príručka je pripravená pre jednoduchší prehľad základných funkcií a jednoduchšiu orientáciu v správcovi hesiel.

Nasadenie prebiehalo v prostredí Linuxu Ubuntu, za použitia príkazov do terminálového rozhrania. Požiadavka nasadenia na Ubuntu bola zvolená kvôli dostupnosti, bezplatnosti a tiež stabilite operačného systému v porovnaní s produktami spoločnosti Microsoft.

Ďalšia kapitola praktickej časti sa venuje nástroju na automatizované a centralizované ukladanie hesiel. Ako nástroj na automatizované a centralizované ukladanie hesiel bol vybraný Vault od spoločnosti HashiCorp. Vault bol tiež testovaný, aby bola overená funkčnosť potrebných základných funkcií na automatizované získanie hesiel.

Poslednou časťou diplomovej práce sú politiky o používaní správcu hesiel s podmienkami pre jednotlivé heslá a tiež na využívanie viacfaktorových autentifikačných mechanizmov. Bez správne nastavenej politiky používania hesiel by využívanie správcov hesiel mohlo strácať zmysel z dôvodu, že by používatelia s veľkou pravdepodobnosťou využívali jedno jednoduché heslo pre množstvo služieb.

I. TEORETICKÁ ČÁSŤ

1 SPRÁVCA HESIEL

Správca hesiel je aplikácia, ktorá funguje ako pomyselná peňaženka, do ktorej sa ukladajú používateľské mená, heslá prípadne tiež údaje k možnej obnove ako overovacia otázka spolu s odpoveďou. U správcov hesiel sa môžeme stretnúť aj s ďalšími možnosťami ako ukladanie rôznych dokladov a tiež dokumentov, závisí to len od možností, daného správcu hesiel. Správca hesiel by sa tiež dal označiť ako aplikácia, ktorá chráni všetky naše tajomstvá a súkromie, ktoré zdieľame s inými ľuďmi pomocou aplikácií tretích strán.

1.1 Dôležité pojmy

Pre plné pochopenie problematiky správy hesiel je potrebné rozumieť pojmom ako používateľské meno, heslo, 2-faktorová a 2-kroková autentifikácia. S týmito pojmami sa stretáme denne, no nie vždy vieme ako ich presne definovať, prípadne aké sú medzi nimi rozdiely.

1.1.1 Používateľské meno

Používateľské meno je text, pomocou ktorého sa pripájame k aplikáciám alebo službám, slúži k identifikácii používateľa poskytovateľom. Ako používateľské meno sa používa aj emailová adresa [1].

1.1.2 Heslo

„Heslo - reťazec znakov, obvykle s dĺžkou 6 - 16 bajtov slúžiaci k overeniu používateľovej identity (niekedy je kratšie heslo napr. „x7Kl2O“ silnejšie, než dlhšie „babicka1“ odhaliteľné slovníkovým útokom) “ [2].

1.1.3 Biometrický údaj

Biometrický údaj je údaj, ktorý je fyzicky spätý s osobou, takzvane nie je možné bez fyzického kontaktu tento údaj získať. Je to napríklad odtlačok prsta, sietnica oka, očná dúhovka, tvár, krvné riečisko a ďalšie. Tieto údaje slúžia k jednoznačnej identifikácii osoby [3].

1.1.4 2-kroková autentifikácia

Spôsob prihlásenia za použitia dvoch krokov, kde oba kroky sú rovnakého druhu napr. prihlásenie pomocou hesla a druhý krok potvrdenie pomocou PIN-kódu, jedná sa v oboch prípadoch o vedomosť [4].

1.1.5 2-faktorová autentifikácia

Prihlásenie použitím dvoch rôznych druhov ako napríklad pomocou hesla a generovaného kódu z aplikácie, kódu z SMS alebo e-mailu taktiež to môže byť pomocou biometrických prvkov ako odtlačok prsta [4].

1.1.6 Viacfaktorová autentifikácia

Viacfaktorová autentifikácia je autentifikácia využívajúca viac ako 1 faktor potrebný k prihláseniu podobne ako pri 2-faktorovej avšak za použitia ďalšieho faktora. Avšak viacnásobné použitie rovnakého faktora neznamená využitie viacerých faktorov [5] .

Viacfaktorová autentifikácia je súhrnom troch otázok. Čo viem ? Čo mám ? Kto som ? ak si zodpovieme tieto tri otázky máme super viacfaktorovú ochranu. Heslo, kľúčenka, biometrický údaj [6].

1.2 Dôvody k používaniu správcov hesiel

Správcovia hesiel slúžia k bezpečnému ukladaniu hesiel, z dôvodu, že je komplikované zapamätať si všetky heslá. Heslá je komplikované si zapamätať primárne z dôvodu, že platné odporúčania ohľadom bezpečnosti stanovujú používať heslo výhradne pre jednu službu. Toto odporúčanie je veľmi dôležité hlavne s ohľadom na množstvo uniknutých databáz s heslami u rôznych spoločností dokonca aj takých, ktoré sa snažia o to, aby boli tieto databázy chránené.

1.2.1 Požiadavky na heslo

Heslo by na základe požiadaviek nemalo mať menej ako 12 znakov v prípade bežných používateľov a má mať najmenej 17 znakov u administrátorov a aplikácií. Jedná sa o požiadavky na základe vyhlášky č. 82/2018Sb. o kybernetické bezpečnosti [7].

Požiadavky na heslo sa väčšinou stanovujú na základe výpočtového výkonu počítačov. Je to spôsobené tým, že čím väčší výkon máme k dispozícii tým väčšie množstvo kombinácií je možné skúsiť za jednotku času. Nie je to tak dávno, čo sa hovorilo o tom, že je vhodné používať heslo o dĺžke 8 znakov, malé veľké písmeno, číslicu a špeciálny znak. Pri výpočtovom výkone, ktorý je dnes bežne dostupný, je toto heslo nepoužiteľné, pretože aj ak by musel útočník použiť všetky možné kombinácie znakov, stačilo by mu na prelomenie „len 5 minút“ [8].

1.2.2 Problémy s ochranou hesiel

Používatelia nevnímajú problém s chránením hesiel ako pre nich závažný. Často je možné stretnúť sa s prípadmi kedy používatelia z dôvodu nemožnosti zapamätať si niekoľko hesiel, používajú stále jedno a to isté. Ešte horšie riešenie, nalepia si papierik s heslom na viditeľné miesto. Prípadne ako je známe z množstva únikov používatelia používajú ľahko uhádnuteľné heslá typu „Meno123“ a podobne, prípadne len po sebe nasledujúce čísla [9].

1.2.3 Zmeny hesiel

Zmeny hesiel sú oveľa jednoduchšie pri používaní správcu hesiel, z dôvodu, že si hesla môžeme jednoducho vygenerovať a nemusíme ich zložito vymýšľať. Meniť heslo je podľa množstva odborníkov vhodné niekoľko krát do roka. Avšak iní si myslia, že je vhodné vykonávať zmeny výhradne v prípade, že viete, prípadne máte podozrenie, na únik hesla. Nové heslo by malo spĺňať požiadavky definované vyššie [10].

1.3 Charakteristika správcu hesiel

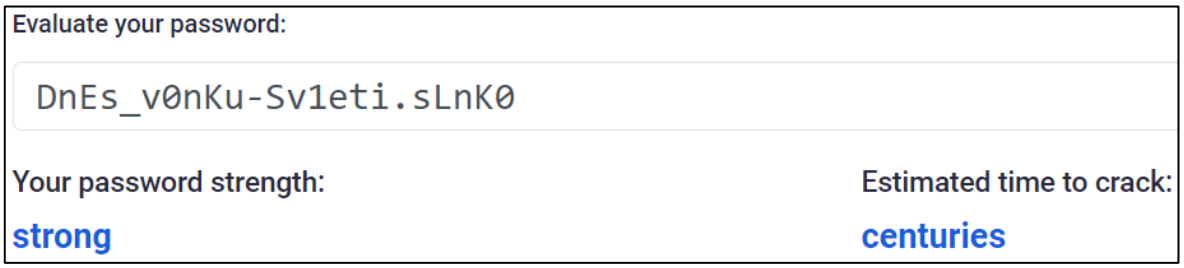
Správca hesiel je zvyčajne aplikácia alebo služba, ktorá slúži k uchovávaniu hesiel k jednotlivým aplikáciám, webom prípadne iným službám. Správcovia hesiel vznikli hlavne z dôvodu, že nie je vhodné používať jedno heslo na viac ako jednu službu a tiež nie je jednoduché pamätať si zložité heslá k desiatkam služieb [11].

1.3.1 Základné funkcie

Medzi základné funkcie správcu hesiel patria generovanie hesla, ukladanie hesiel, zdieľanie hesiel, zobrazenie hesiel, ktoré by sa mali zobraziť po zadaní hlavného hesla k správcovi hesiel [11].

Hlavné heslo

V prípade správcu hesiel je nutné si pamätať jedno heslo, ktoré zabezpečuje prístup ku všetkým ostatným heslám a tiež údajom, ktoré sú ukladané pomocou správcu hesiel. Hlavné heslo musí byť unikátne, rovnako ako bežne používané heslá, ale malo by byť také, aby ste si ho dokázali ľahko zapamätať. V takomto prípade sa odporúča použiť kľudne vetu s rôznymi špeciálnymi znakmi a náhradami za znaky. Napr. „DnEs_v0nKu-Sv1eti.sLnK0“ takto by mohlo vyzerať heslo, ktoré by sa dalo použiť a spĺňalo by všetky požiadavky na bezpečnosť obrázok 1 [12].



Obrázok 1 Hlavné heslo [13]

Generátor hesiel

Program, ktorý na základe zadaných parametrov vygeneruje náhodnú postupnosť náhodne zvolených znakov ako sú veľké, malé písmená, čísla a symboly. V generátoroch hesiel je možné zvoliť si dĺžku hesla, počet špeciálnych znakov, počet čísiel [14].

Ukladanie hesiel

Heslá sa ukladajú do úložiska zabezpečeného hlavným heslom, kde je základom ukladanie šifrovaných súborov. Je to ukladanie s tzv. nulovou znalosťou, čo znamená, že heslá sa šifrujú už na zariadení používateľa a posielajú sa na server len zašifrované dáta [15] [16].

Zdieľanie hesiel

Funkcia zdieľania hesiel funguje tak, že v prípade, že je potrebné aby heslo používalo viac ľudí je nutné, aby bolo synchronizované a mali k nemu prístup všetky oprávnené osoby. Zdieľanie hesiel pomocou správcu hesiel je založené na princípe každý má svoj účet a heslo je prístupné pre konkrétnych používateľov zvolených vlastníkom hesla [17].

1.3.2 Rozšírené funkcie

Jedná sa o funkcie, ktoré ponúkajú správcovia hesiel buď len od niektorých vydavateľov alebo za poplatok. Ide o funkcie automatické dopĺňania, viacfaktorového overovania, ukladanie dokumentov a dokladov a tiež sledovanie dark-webu [11].

Automatické dopĺňanie

Funkcia automatické dopĺňanie hesiel v prehliadačoch a aplikáciách. Niekde aj dopĺňanie platobných údajov. Funguje na princípe, ak správca hesiel pozná webovú stránku automaticky ponúkne v prípade odomknutého trezoru možnosť zadania hesla [11].

Ukladanie dokumentov a dokladov

Rozšírenou funkciou u niektorých správcov hesiel býva možnosť uložiť si bezpečne aj súbory ako napríklad kópiu dokladov totožnosti, platobných kariet a dôležité dokumenty. Dokumenty sú samozrejme tiež ukladané v šifrovanej podobe [11].

Sledovanie dark-webu

Niektorí správcovia hesiel tiež ponúkajú aj rozšírené funkcie nájdenia úniku hesiel na dark-web. Prehľadáva databázy s uniknutými heslami, ktoré sú ponúkané na dark-webe [11].

1.4 Typy správcov hesiel

Existujú tri typy bezpečných správcov hesiel. Správcovia hesiel môžu ukladať heslá lokálne na počítač, na vzdialené úložisko, prípadne možnosť jednotného prihlásenia, kde používate jedno heslo pre množstvo aplikácií [18].

1.4.1 Lokálne na PC

Správca hesiel s ukladaním lokálne na PC je vlastne len šifrovaný trezor. Nevýhoda je, že k heslám sa nedá dostať z iného zariadenia. Naopak je to výhoda pre ľudí, ktorí chcú hesla zabezpečené a uložené len na svojom PC [18].

1.4.2 Na vzdialené úložisko

Ukladanie hesiel na vzdialené úložisko prináša množstvo výhod v podobe jednoduchého prístupu k heslám z rôznych zariadení pripojených k internetu. Správcovia hesiel založený na vzdialenom úložisku môžu byť formou rozšírení prehliadača, počítačových ako aj mobilných aplikácií [18].

1.4.3 Jednotné prihlásenie

Typ správcu pomocou jednotného prihlásenia, jedná sa o prihlásenie, kde sa používajú rovnaké údaje pre množstvo aplikácií. Je to obľúbené u množstva organizácií pre prístup k aplikáciám organizácie, pretože to šetrí čas v prípade zabudnutia hesla sa zmení heslo pre všetky aplikácie využívajúce jednotný prístup v rámci organizácie [18].

1.5 Populárny správcovia hesiel

V tejto časti sa práca zaoberá porovnaním možností, akého správcu hesiel zvoliť s ohľadom na používateľa, bezpečnosť, cenu a dostupnosť služieb. Varianty na porovnanie boli zvolené

spomedzi najpoužívanejších nasledovné: Vaultwarden(Bitwarden_RS), LastPass, Dashlane, KeePass, Keeper.

1.5.1 Vaultwarden (Bitwarden_RS)

Vaultwarden je bezplatný, open-source správca hesiel naprogramovaný v jazyku RUST, ktorý ponúka 256-bitové šifrovanie AES na bezpečné ukladanie hesiel. Ponúka tiež možnosť ukladať dáta lokálne. Vaultwarden má aj funkciu 2-faktorovej autentifikácie, ktorú je možné spárovať s aplikáciami od tretích strán ako Google Authenticator a tiež je možné pristúpiť pomocou kľúča U2F [19] [20].

1.5.2 LastPass

Jeden z najpopulárnejších bezplatných správcov hesiel, ktorý ponúka 256-bitové šifrovanie AES. LastPass je určený prioritne na použitie v prehliadačoch, ale ponúkajú tiež aplikácie pre mobilné telefóny s OS Android, iOS a Windows Phone. LastPass je obľúbený z dôvodu, že ponúka najviac bezplatných funkcií. V prípade LastPass je však bezplatná verzia obmedzená na 1 používateľa a 1 zariadenie z každého typu ako laptop, mobil a pod. Bezplatná verzia ponúka aj základnú MFA [21].

1.5.3 Dashlane

Dashlane je jedným z najbezpečnejších a najpopulárnejších správcov hesiel, ktorý sú na trhu je prehľadný, bezpečný a ponúka množstvo funkcií. V bezplatnej verzii ponúka len 50 hesiel a jedno zariadenie, čo je veľmi málo. Dashlane ponúka 256-bitové šifrovanie AES ako aj MFA a kompatibilitu s U2F kľúčmi. Správca hesiel Dashlane ponúka tiež jednoduché zdieľanie hesiel za použitia emailovej adresy. Ďalšou nezanedbateľnou bezpečnostnou funkciou je sledovanie dark-webu, ktoré zabezpečujú pomocou vlastných databáz, ktoré aktualizujú denne [22] [23].

1.5.4 KeePass

Dôvod výberu KeePass ako jedného z nástrojov, ktoré boli zaradené do porovnania je bezplatnosť. Tiež ako ostatný správcovia hesiel používa 256-bitové šifrovanie AES a dokonca ponúka aj dvojfaktorovú autentifikáciu pomocou kľúčového súboru [24].

1.5.5 Keeper

Správca hesiel od spoločnosti Keeper Security je obľúbený a prehľadný. Na šifrovanie používa 256-bitové šifrovanie AES. Keeper má množstvo možností, čo ukladať, či už osobné údaje, ďalej platobné údaje. Keeper má tiež rýchlo a prehľadne spracovaný aj import údajov. Ďalšou podstatnou a použiteľnou funkciou je BreachWatch, jedná sa o nástroj na monitorovanie dark-webu. BreachWatch môžete použiť v prípade, že chcete vedieť či niekedy unikli vaše dáta na dark-web aj bez toho aby ste boli zákazníkom spoločnosti Keeper, avšak bez detailov o uniknutých dátach. Keeper ako správca hesiel ponúka aj MFA a SSO [25].

1.6 Šifrovanie správcov hesiel

Ako už bolo zmienené vyššie, populárni správcovia hesiel využívajú na šifrovanie prevažne 256-bitovú šifru AES. AES je najrozšírenejší aj z dôvodu, že sa používa na celom svete a je implementovaná v softvéri aj hardvéri. Táto šifra je považovaná za bezpečnú, pretože zatiaľ neexistuje dôkaz o jej prekonaní.

1.6.1 AES 256 bit

AES 256 bit je bloková šifra, ktorá používa bloky o veľkosti 128 bit a kľúče troch rozdielnych dĺžok na základe čoho sa určuje počet kôl. AES šifra sa skladá z týchto krokov:

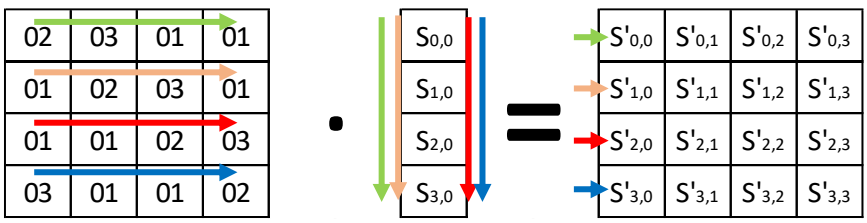
- Pridanie kľúča kola (Add Round Key). Jedná sa o využitie matice 4x4 a kľúča, ktorý sa rozdelí na maticu 4x4, kde každá bunka obsahuje 1 bajt. Na rovnaké bunky z oboch matíc sa aplikuje XOR, na základe čoho vzniká nová matica, ktorá pokračuje do ďalšej fáze. Kľúče kôl sa využívajú v poradí v akom boli generované. Kôl môže byť na základe dĺžky kľúča:
    - 10 u 128 bitového kľúča,
    - 12 u 192 bitového kľúča,
    - 14 u 256 bitového kľúča.
- Nahrádzanie bajtov (Sub-Bytes). Každá bunka z matice obsahuje 2 znaky v hexadecimálnom tvare, ktoré slúžia k vyhľadaniu nahrádzajúcej bunky. Prvý znak zastupuje riadok v substitučnej tabuľke 16x16 a druhý znak stĺpec. Substitučná tabuľka 16x16 je zobrazená na obrázku 2. Bunka v ktorej sa pretnú zastupuje novú hodnotu, ktorá sa zapíše do novej matice [26] [27].

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Obrázok 2 Substitučná tabuľka 16x16 [28]

- Posúvanie v riadku (Shift Rows), funguje na princípe posunutia doľava, podľa toho, o ktorý ide riadok, začína sa 0. To znamená, že nultý riadok sa neposúva, prvý sa posúva o 1 pozíciu, druhý o 2 a tretí o 3 pozície doľava. Žiadne údaje sa nestrácajú, len menia pozíciu [26].
- Mix Columns

  V tomto kroku ide o počítanie pomocou konštantnej matice a matice z predchádzajúceho kroku, kde sa postupne násobia prvky z riadku krát prvky zo stĺpca. Podobne ako je to vyobrazené aj na obrázku 3, kde je zobrazená konštantná matica a prvý stĺpec z pôvodnej matice, na základe čoho dostaneme prvý stĺpec z požadovanej matice [26].



Obrázok 3 Počítanie požadovanej matice

Pri Mix Columns je potrebné ešte na všetky násobené časti použiť XOR, aby sme dostali potrebnú hodnotu. Ako postupovať je zobrazené v nasledujúcej rovnici 1.

$$\{S'_{0,0}\} = \{02.S_{0,0}\} \oplus \{03.S_{1,0}\} \oplus \{01.S_{2,0}\} \oplus \{01.S_{3,0}\} \quad (1)$$

Tento krok sa vykonáva v počte kôl -1 pretože v poslednom sa už len pridáva kľúč.

- Add Round Key
  Pridanie kľúča kola po Mix Columns je závislé od toho, či ide o priebežné kolo alebo posledné, pretože v prípade posledného sa tabuľka prepíše na šifrovaný text bez vykonania Mix Columns [26] [27] [28].

2 HASHICORP VAULT

HashiCorp Vault (ďalej len Vault) je systém, ktorý slúži na uchovávanie a správu šifrovaných tajomstiev, ako sú heslá, identity, API kľúče, certifikáty. Vault je možné používať v rozhraní Vault UI, CLI alebo HTTP API. Vault ponúka dve možnosti buď cloudové služby alebo vlastné hosťovanie [29].

2.1 Dôležité pojmy

Na plné pochopenie problematiky správy kľúčov, TLS certifikátov a ďalších prístupových možností je nutné poznať pojmy, ako Autentifikačný Token, TLS certifikát, JSON Web Token a API kľúč.

2.1.1 Autentifikačný Token

Autentifikačný Token je protokol, ktorý generuje prístupový token. Slúži ako forma zabezpečenia prístupu k webu, aplikáciám, ktorú je možné použiť vždy len do doby odhlásenia alebo vypnutia aplikácie [30].

2.1.2 Metódy overovania

Metódy overenia slúžia k posúdeniu, či sa jedná o používateľa s potvrdením politík a súborov priradených k jeho používateľovi alebo počítaču. Taktiež sa overuje platnosť poverení. Používajú sa tiež rôzne metódy overenia ako napr. Active Directory a Okta [31].

2.1.3 TLS certifikát

Certifikát zabezpečujúci šifrovanú komunikáciu na internete. Zabezpečuje, aby boli dáta posielané súkromne, neboli modifikované, stratené alebo ukradnuté. Predchodcom TLS (Transport Layer Security) je SSL (Secure Sockets Layer) [32].

2.1.4 JSON Web Token

„JSON Web Token (JWT) je otvorený štandard (RFC 7519), ktorý definuje kompaktný a samostatný spôsob bezpečného prenosu informácií medzi stranami vo forme objektu JSON. Tieto informácie môžu byť overené a dôveryhodné, pretože sú digitálne podpísané. JWT môžu byť podpísané pomocou tajomstva (s algoritmom HMAC) alebo páru verejných/súkromných kľúčov pomocou RSA alebo ECDSA“ [33].

2.1.5 API kľúč

Application Programming Interface (API) je unikátny kód, ktorý odovzdávajú počítačové aplikácie a slúži k identifikácii používateľa alebo programu. API kľúč sa často používa ako jedinečný identifikátor a tajný token [34].

2.1.6 Access Management

Access Management je systém riadenia prístupov do systémov a aplikácií prevažne v prostredí IT, kde je potrebné, aby bolo možné zistiť, kto kedy a k akému systému pristupuje preto sa často používa v spojitosti so správou identity a prístupu (IAM) [35].

2.2 Funkcie Vaultu

Základnou funkciou Vaultu je Secret engine, Ďalšími funkciami Vaultu sú možnosti prístupu k účtu, generovanie náhodných bajtov a hashovanie dát.

2.2.1 Secret engine

Jedná sa o základnú funkciu Vaultu, ktorá slúži k rozdeleniu hesiel a celkovo tajomstiev na do jednotlivých častí na základe toho, o aké tajomstvá sa jedná a v akom formáte majú byť ukladané.

Secret engine je možné povoliť, zakázať presunúť a upravovať. Secret engine ponúka ukladanie generovanie a šifrovanie tajností, ktoré sa delia na generické, cloudové a infra [36].

Generické:

- KV – kľúč / hodnota slúži k ukladaniu kľúču a prístupovej hodnoty. Táto možnosť by sa dala popísať tiež ako heslo k službe, kde kľúč popisuje názov služby [37].
- PKI certifikáty – slúži ku generovaniu certifikátov na základe role. Jedná sa o certifikáty X.509, ktoré sú generované automaticky bez nutnosti žiadať o podpis certifikátu [38].
- SSH – slúži k ukladaniu SSH prístupov pomocou certifikačnej autority prípadne jednorazového hesla [39].
- Transit – slúži primárne k prenosu šifrovaných údajov, za podmienky, že údaje zostávajú stále uložené aj v primárnom úložisku [40].

- TOTP – je funkcia, pomocou ktorej je možné buď generovať kódy pre rôzne služby, ktoré ponúkajú možnosť viacfaktorového overovania, prípadne tiež dokáže fungovať ako poskytovateľ, ktorý overuje generované kódy na základe hesla [41].

Cloudové:

- Active Directory – pomocou tejto služby je možné rozšíriť zabezpečenie Active Directory a to na základe toho, že dokáže na základe využívania ďalších častí z ponuky vaultu generovať jednorazové heslá, aby bolo možné zistiť, kto pristupoval k zdieľaným účtom, prípadne je tiež možnosť aby heslá používateľov rotovali na základe navolených požiadaviek [42].
- AliCloud – je funkcia, ktorá generuje prístupové tokeny alebo údaje k AliCloud na základe požiadaviek nastavených v RAM politikách [43].
- AWS – je služba, ktorá dynamicky generuje prístupové údaje k AWS na základe IAM politík [44].
- Azure – je funkcia, ktorá dynamicky generuje objekty služby Azure spolu s priradením rolí a skupín [45].
- Google Cloud – je nástroj na dynamické generovanie kľúčov a OAuth tokenov na základe nastavenia politík IAM [46].
- Google Cloud KMS – je služba určená na šifrovanie a správu kľúčov pomocou služby Google Cloud KMS [47].

Infra:

- Consul – generovanie Consul API na základe Consul ACL politík [48].
- Database - umožňuje vytvárať dynamické poverenia pre širokú škálu podporovaných databáz. Integrácia tohto mechanizmu s obchodnými aplikáciami prináša hlavnú výhodu v podobe jedinečného a krátkodobého prístupu k základnej databáze, v ktorej sú uložené kritické údaje [31].
- Nomad – je súčasť Vaultu, ktorá generuje tokeny na základe existujúcich ACL politík [49].
- RabbitMQ – je funkcia, ktorá automaticky vytvára používateľské oprávnenia na základe nastavených povolení virtuálnych strojov. V dôsledku toho nemusia služby, ktoré potrebujú prístup k virtuálnemu stroju, vopred definovať oprávnenia v kóde [50].

2.2.2 Autentifikačné metódy

Autentifikačné metódy sú v prípade Vaultu rozsiahle, je možné použiť prístupové metódy generické, cloudové a infra. V generických sa nachádzajú napr. aj bežné prístupové metódy pomocou certifikátov, mena a hesla. V cloudových sa jedná o služby ako AWS, Azure. Infra je kategória, ktorá ponúka možnosti prístupu napr. pomocou Kubernetes [51].

Generické autentifikačné metódy:

- AppRole - umožňuje strojom alebo aplikáciám autentifikovať sa pomocou rolí definovaných v systéme Vault. Vďaka otvorenému návrhu AppRole je možné využiť rôzne pracovné postupy a nastavenia pre spracovanie veľkého počtu aplikácií. Tento spôsob autentifikácie je vhodný pre automatizované pracovné toky [31].
- JWT/OIDC - mnohé organizácie dnes využívajú riešenia jednotného prihlásenia SSO pre autentifikáciu v celom ich IT prostredí. S využitím autentifikačnej metódy OIDC v systéme Vault môžu tieto organizácie efektívne využiť svoj existujúci adresár používateľov na detailné riadenie prístupu k službám systému Vault. Na rozdiel od konfigurácie s priamym prepojením s AD ponúka priamu integráciu MFA [31].
- TLS certifikáty - umožňuje použiť certifikáty SSL/TLS klienta, ktoré môžu byť vytvorené samotným klientom alebo podpísané certifikačnou autoritou. Klientské certifikáty SSL/TLS sú s rozšírením ExtKeyUsage, kde je definované, či sa môže používať na autentifikáciu klienta alebo ľubovoľné [52].
- Meno a heslo – bežná základná možnosť prístupu pomocou mena a hesla.

Cloudové autentifikačné metódy:

Pri migrácii práce z privátnych dátových centier do verejného cloudu sa autentifikačné metódy poskytovateľov cloudu stávajú neoddeliteľnou súčasťou každej inštalácie Vaultu. Vault je nezávislý od konkrétnych poskytovateľov cloudu a ponúka jednu alebo viac autentifikačných metód pre najobľúbenejších cloudových poskytovateľov. Tieto integrácie s cloudu poskytujú rôzne spôsoby, ako aplikácie môžu získať prístup k Vaultu, bez použitia dlhodobo platných tokenov alebo AppRole konfigurácií. Týmto spôsobom sa zvyšuje bezpečnosť a umožňuje sa aplikáciám bezpečne pristupovať k službám Vaultu [31].

Podporované cloudové služby:

- AliCloud – cloud od spoločnosti Alibaba,
- AWS – cloud spoločnosti Amazon,

- Azure – cloud spoločnosti Microsoft,
- Google cloud,
- GitHub [53].

Infra autentifikačné metódy:

- Kubernetes – tento spôsob prihlásenia umožňuje použitie tokenu servisného účtu Kubernates,
- LDAP – pripájanie pomocou prístupov k existujúcej infraštruktúre LDAP,
- Okta – slúži k integrácii a používaniu používateľských prístupových údajov využívaných v prostredí Okta,
- Radius – využitie údajov z Radius, ktoré je možné používať, len v prípade používania autentifikačnej schémy PAP [53].

2.2.3 Generovanie náhodných bajtov

Pri generovaní náhodných bajtov sa definuje počet bajtov, ktoré sa vrátia a tiež formát v ktorom sa vrátia jediné možné formáty sú hex alebo base64. Ako zdroj sa nastavuje jedna z 3 hodnôt - „platform“, „seal“ a „all“. Kde „platform“ znamená entropia platformy, „all“ miešanie všetkých dostupných zdrojov a „seal“ zo zväčšujúcej entropie. „Seal“ je však dostupný len pre enterprise verziu [54].

2.2.4 Hashovanie dát

Vault používa na hashovanie algoritmy sha2-224, sha2-256, sha2-384, sha2-512, sha3-224, sha3-256, sha3-384, sha3-512. Na vstupe je nutné zadať dáta vo formáte base64. A zvoliť výstup hex alebo base64 [54].

II. PRAKTICKÁ ČÁSŤ

3 TESTOVANIE FUNKCIÍ SPRÁVCOV HESIEL

Základnou funkciou, ktorú by mal poskytovať každý správca hesiel je generovanie hesiel, kde sa dá predpokladať veľké rozdiely, či už na základe dĺžky, možnosti použitia symbolov, nastavenia minimálneho počtu znakov určitého typu a podobne.

3.1 Ukladanie hesiel

Ukladanie hesiel u správcov hesiel je najdôležitejšou súčasťou, všetci testovaní správcovia hesiel ukladajú heslá tak, aby nebolo možné ich čítanie inou osobou ako ich vlastníkom tzv. zero-knowledge. Väčšina testovaných správcov hesiel používa ukladanie na cloud, kde sa posielajú heslá ako balík údajov na základe používateľa.

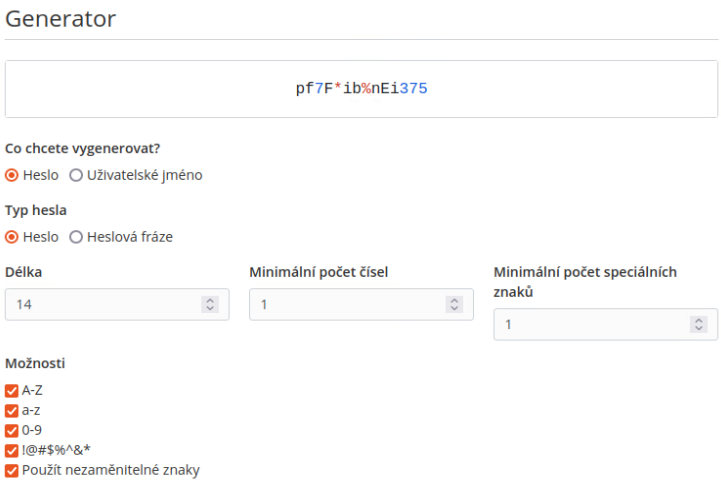
Jediný KeePass je lokálny, kde sa ukladajú samostatne jednotlivé údaje na základe toho, ako si to používateľ nastaví.

3.2 Generovanie hesiel

Generovanie hesiel ja časť ktorou sa jednotliví správcovia hesiel líšia najviac pretože každý generátor je jedinečný či už počtom používaných znakov, výberom symbolov ale tiež zameniteľnosťou znakov.

Vaultwarden

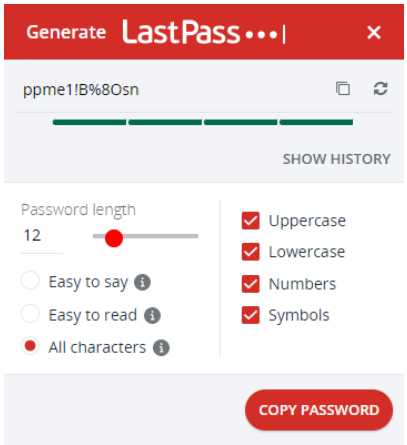
Generovanie hesla s maximálnou dĺžkou 128 znakov s nastavením minimálneho počtu číslic a špeciálnych symbolov od 0 do 9. Ďalej sú tam možnosti ako A-Z, a-z,0-9, “!@#$%^&*“ a vyhnutie sa zameniteľným znakom. Vaultwarden ponúka tiež možnosť generovania hesla ako niekoľko náhodných slov, kde je možnosť si tiež navoliť, či sa má používať aj veľké písmeno na začiatku každého slova, prípadne sa má použiť jedno číslo. Ukážka je tiež na obrázku 4.



Obrázok 4 – Generátor hesiel Vaultwarden

LastPass

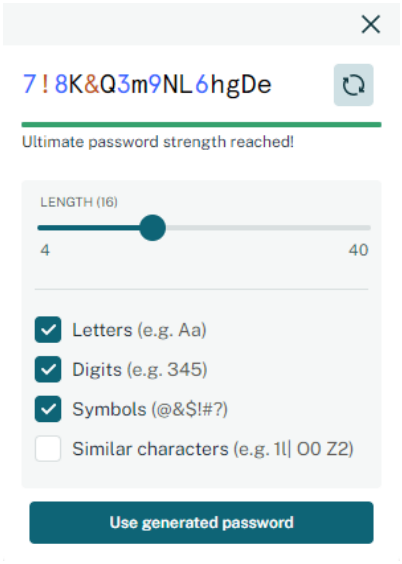
Generovanie hesiel v prípade LastPass minimálne 0 a maximálne 99 znakov, je možnosť navoliť si aké znaky LastPass použije, či má použiť všetky znaky, alebo má použiť len písmená prípadne má použiť znaky, ktoré sa ľahko čítajú, čiže vynechá zameniteľné znaky "!, 7, h, K, I a 1" Ukážka možností, ktoré ponúka LastPass na obrázku 5.



Obrázok 5 – Generátor hesiel LastPass

Dashlane

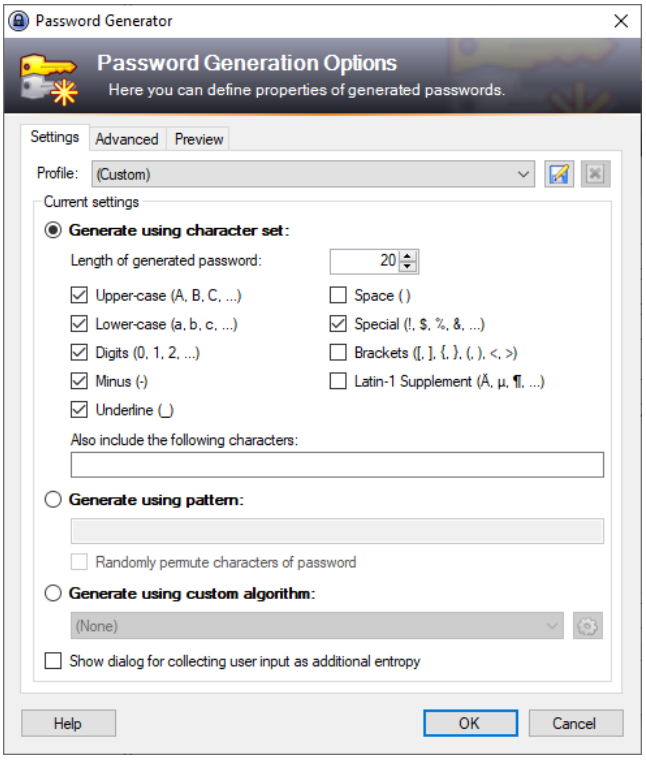
Dashlane generovanie hesiel ponúka heslá s dĺžkou od 4 do 40 znakov. Ďalej ponúka možnosť navoliť si znaky, ktoré sa majú používať písmená, čísla, symboly prípadne aj podobné znaky konkrétne "I,l,1,0,O,Z.2" Dashlane ponúka možnosti generovania vyobrazené na obrázku 6.



Obrázok 6 – Generátor hesiel Dashlane

KeePass

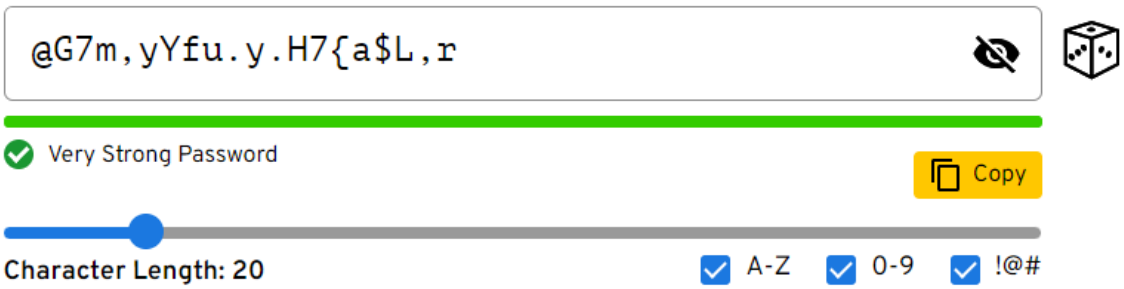
Generátor hesiel má rozsiahle množstvo funkcií, malé písmená, veľké písmená, čísla, mínus, podčiarkovník, medzeru, špeciálne symboly "!,$,%,&" a iné, ďalej ponúka možnosť použitia zátvoriek a latinských znakov. Ďalšou špecialitou u KeePass je možnosť generovania hesla s dĺžkou 0 až 30000 znakov. KeePass generátor ponúka najviac možností obrázok 7.



Obrázok 7 Generátor hesiel KeePass

Keeper

Generovanie hesiel v prípade správcu hesiel Keeper je možné použiť na generovanie hesiel s dĺžkou 8 až 100 znakov, ponúka možnosti použitia písmen, čísiel a špeciálnych znakov. Zaujímavosťou je tiež, že generátor od Keeper security je možné použiť aj bez prihlásenia a ukážka generátoru je na obrázku 8 [55].



Obrázok 8 – Generátor hesiel Keeper

3.3 Viacfaktorové overovanie

Viacfaktorové overovanie je najdôležitejšie často krát pre správcu pre používateľa už menej pretože ho núti aby robil o krok naviac, na základe čoho získa väčšie bezpečie bez nutnosti násobne zvyšovať silu hesla. V tejto časti bude porovnanie možností viacfaktorového overovania.

Vaultwarden

Služba Vaultwarden ponúka množstvo variant dvojstupňového prihlásenia, ako:

- TOTP – generovanie časovo obmedzených kódov,
- YubiKey OTP - ktoré funguje po pripojení k fyzickému zariadeniu,
- Duo Security– funguje buď pomocou duo aplikácie, SMS, telefonátu alebo univerzálneho fyzického kľúču,
- Fido2 WebAuthn – použitie akéhokoľvek bezpečnostného kľúču s podporou WebAutthn,
- Email – overenie pomocou kódu zaslaného na mail.

LastPass

Správca hesiel LastPass ponúka tiež množstvo služieb na viacstupňovú ochranu prihlásenia všetky možnosti, ktoré ponúka:

- LastPass MFA – posiela jednorazovú notifikáciu o vygenerovanom kód pri prihlasovaní,
- TOTP – podpora len pre Google Authenticator a Microsoft Authenticator,
- Toopher – vyskakovacia notifikácie na mobilnom telefóne pre prihlásenie,
- Duo Security – popísané u Vaultwardenu,
- Grid – funguje na princípe, že každý používateľ má tabuľku, v ktorej si navolí kde sú pozície čísiel pre jeho prihlásenie a pri každom ďalšom prihlásení si vyberá tie pozície,
- YubiKey - popísané u Vaultwardenu,
- Fingerprint / Smart Card – podpora pre prihlásenie pomocou odtlačku prstu prípadne čítačky kariet,
- Salesforce Authenticator – posiela vyskakovacie notifikácie určené len pre firemných zákazníkov.

Dashlane

Produkt od spoločnosti Dashlane ponúka výhradne dvoj faktorovú ochranu pomocou vlastnej aplikácia Dashlane authentication.

KeePass

KeePass ako jediný správca hesiel ponúka dvoj krokovú autentifikáciu a to pomocou hesla a súboru, ktorý je treba vložiť pre odomknutie trezora. S viacfaktorovým overovaním dokáže pracovať len s pluginom, ktorý pridá stĺpec na zapísanie kódu pre generovanie jednorazových kódov.

Keeper

Nástroj na správu hesiel Keeper ponúka viacfaktorové overovanie nasledujúcimi spôsobmi:

- SMS – posielanie kódu pomocou textovej správy,
- TOTP – kompatibilné s akýmikoľvek TOTP aplikáciami,
- Chytré hodinky – výhradne s použitím Apple Watch prípade Android Wear a nainštalovanou aplikáciou KeeperDNA,
- RSA SecurityID – vytvára hardvérové a softvérové tokeny pre používateľské zariadenia,
- Duo Security – popísané u Vaultwardenu [56].

4 VOĽBA A HODNOTENIE SPRÁVCOV HESIEL

Voľba správcu hesiel bude na základe multi-kriteriálnej analýzy na základe definovaných požiadaviek organizáciou. Konkrétne budú dve multi-kriteriálne analýzy jedna na základe skóre, kedy budú jednotlivé kritéria s rovnakou váhou a ďalšia, kde budú kritéria naberať váhu podľa podstatnosti pre organizáciu.

4.1 Požiadavky na správcu hesiel organizáciou

Požiadavky na správcu hesiel boli nastavené tak, že by sa malo jednať o bezplatné riešenie, ktoré ponúka neobmedzený počet uložených hesiel minimálne 30 používateľov a tiež možnosť zdieľať heslá medzi jednotlivými používateľmi.

4.2 Hodnotenie správcov hesiel

Hodnotenie správcov hesiel považuje za potrebné spraviť pomocou metódy na hodnotenie kritérií z dôvodu, aby nebolo rozhodnuté subjektívne ale aspoň čiastočne objektívne a na základe faktov.

4.2.1 Hodnotiace kritéria

Hodnotiace kritéria sú pri multi-kriteriálnej analýze nesmierne dôležité a to z toho dôvodu, že len na základe kritérií je možné rozhodnúť o tom, ktorý variant je najvhodnejší. Kritéria je možné použiť s rovnakými alebo rôznymi váhami. Hodnotiace kritéria sú:

- Typ použitej šifry,
- možnosť MFA,
- možnosti generovania hesiel,
- cena,
- uloženie Cloud/Local.

4.3 Multi-kriteriálna analýza s rovnakými váhami

Multi-kriteriálna analýza s rovnakými váhami je dobrá v tom, že ak nie je presne stanové, ktoré kritéria sú pre organizáciu najpodstatnejšie tak dokáže určiť, variantu, ktorá je najvhodnejšia pri porovnaní všetkých kritérií ako celku.

4.3.1 Kritéria

Kritéria použité v analýze s rovnakými váhami sú typ šifry, možnosť viacfaktorového prístupu, generátor hesiel, cena a ukladanie dát či už na PC, vlastný server alebo na verejné cloudové úložisko. Tabuľky 1, 2, 3, 4, 5, 6 vyobrazujú jednotlivé kritéria potrebné k zostaveniu multi-kriteriálnej analýzy. Bodové hodnotenie od 1 do 5 kde 1 je najhoršie a 5 je najlepšie platí pre všetky kritéria.

Tabuľka 1 Bodové hodnotenie

Bodové hodnotenie	Slovné hodnotenie
5	Najlepšie
4	Lepšie
3	Priemerné
2	Horšie
1	Najhoršie

Na základe požiadavkou Knižnice UTB bolo nutné medzi kritéria zaradiť aj cenu, pretože sú možnosti, na základe ktorých je možné spravovať si službu správcu hesiel aj vlastnými silami čo umožňuje použitie aj open-source programu za účelom šetrenia.

Tabuľka 2 Cena u správcov hesiel [19][22][24][25][57]

Názov správcu hesiel	Cena	Body
Vaultwarden	Zadarmo	5
LastPass	3,9€ / osoba mesiac	3
Dashlane	5$ / osoba mesiac	2
KeePass	Zadarmo	5
Keeper	3$ / osoba mesiac	4

Šifrovanie ako kritérium pri správcoch hesiel bolo zvolené aby sa overili a následne porovnali možnosti zabezpečenia jednotlivých správcov.

Tabuľka 3 Šifrovanie u správcov hesiel

Názov správcu hesiel	Šifrovanie	Body
Vaultwarden	AES-256	5
LastPass	AES-256	5
Dashlane	AES-256	5

KeePass	AES-256	5
Keeper	AES-256	5

Kritérium generátoru hesiel je asi najzaujímavejšie rozmanitosťou. Pretože ako už bolo spomínané pri porovnávaní jednotlivých generátorov takmer každý používa iné špeciálne symboly a taktiež považuje iné znaky za zameniteľné.

Tabuľka 4 Generátor hesiel u správcov hesiel

Názov správcu hesiel	Generátor hesiel	Body
Vaultwarden	až 128 znakov	4
LastPass	až 99 znakov	3
Dashlane	až 40 znakov	2
KeePass	až 30 000 znakov	5
Keeper	až 100 znakov	4

Viacfaktorové overovanie je kritérium na základe ktorého nie je nutné tak výrazne dbať na silu hlavného hesla keďže základné heslo stačí maximálne na prihlásenie, na už overenom zariadení. V prípade KeePass to podľa môjho názoru nie je 2 faktorové overenie, ale len 2 krokové. 2 faktorové by to mohlo byť za podmienky uloženia kľúčového súboru na externé úložisko.

Tabuľka 5 MFA u správcov hesiel

Názov správcu hesiel	MFA	Body
Vaultwarden	áno integrované	5
LastPass	áno integrované	5
Dashlane	áno integrované	5
KeePass	nie len 2 kroková	4
Keeper	áno integrované	5

Posledný kritériom u správcov hesiel je ukladanie súborov z dôvodu, aby bolo možné uložiť si aj určité dokumenty, ktoré je nutné aby sa nestratili, ale tiež aby sa k ním nik neoprávnený nedostal.

Tabuľka 6 Ukladanie súborov u správcov hesiel

Názov správcu hesiel	Ukladanie súborov	Body
Vaultwarden	vlastný server / cloud	5

LastPass	cloud	4
Dashlane	cloud	4
KeePass	lokálne na PC	2
Keeper	cloud	4

4.3.2 Výsledné hodnotenie

Hodnotenie multi-kriteriálnej analýzy zo stanovením rovnakých váh je vyobrazené v nasledujúcej tabuľke 7, kde sú vyobrazené hodnoty jednotlivých kritérií a následne celkové skóre jednotlivých správcov hesiel ako aj farebné odlíšenie najlepšej a najhoršej varianty. Celkové skóre bolo získané na základe súčtu všetkých bodov z kritérií.

Tabuľka 7 Výsledná hodnota pri rovnakých váhach kritérií

	Kritéria					
Názov správcu hesiel	**Cena**	**Šifrovanie**	**Generátor hesiel**	**MFA**	**Ukladanie súborov**	**Celkové skóre**
Vaultwarden	5	5	4	5	5	24
LastPass	3	5	3	5	4	20
Dashlane	2	5	2	5	4	18
KeePass	5	5	5	4	2	21
Keeper	4	5	4	5	4	22

Na základe výsledkov porovnania analýzou bez stanovenia váh bolo zistené, že ako najlepšie riešenie je možné považovať Vaultwarden, ktorý získal 24 bodov a stratil len 1 bod za nie najlepší generátor. Najhoršie riešenie na správu hesiel je podľa analýzy Dashlane z dôvodu generátoru hesiel na malý počet znakov a vysokej ceny.

4.4 Multi-kriteriálna analýza TOPSIS

V prípade druhej multi-kriteriálnej analýzy bolo rozhodnuté, že sa použije analýza TOPSIS na základe predchádzajúcich skúseností s touto analýzou. TOPSIS je analýza, ktorá využíva váh u jednotlivých kritérií. Pre vytvorenie analýzy TOPSIS sú využité tabuľky 2, 3, 4, 5, 6 z predchádzajúcej analýzy a rovnice čerpané z literatúry [58].

Váhy

U analýzy TOPSIS je nutné stanoviť váhy podľa priority jednotlivých kritérií tak, aby súčet váh bol rovný 1. Tabuľka 8 s rozdelením váh pre jednotlivé kritéria, ktoré sú rovnaké ako aj v prípade predchádzajúcej analýzy.

Tabuľka 8 Váhy kritérií

Kritérium	Váha
Cena	0,4
Šifrovanie	0,1
Generátor hesiel	0,1
MFA	0,2
Ukladanie súborov	0,2

Pre transformáciu hodnôt sa používa rovnica 2. Hodnoty získané pomocou tohto výpočtu sa následne používajú na vypočítanie ďalších častí. Tieto hodnoty sú vyobrazené v tabuľke 9.

$$r_{ij} = \frac{y_{ij}}{\sqrt{\sum_{i=1}^{n} y_{ij}^2}} \tag{2}$$

Tabuľka 9 Transformované hodnoty

Kritérium	Hodnoty
Cena	8,89
Šifrovanie	11,18
Generátor hesiel	8,37
MFA	10,77
Ukladanie súborov	8,77

Ďalej je potrebné si vypočítať príťažlivosť a následne ju vynásobiť príslušnou váhou kritérií. Príťažlivosť vynásobenú váhami je možné vidieť v tabuľke 10 a pre výpočet sa používa rovnica 3.

$$w_{ij} = v_j r_{ij} \tag{3}$$

Tabuľka 10 Príťažlivosti

Kritérium	Vaultwarden	LastPass	Dashlane	KeePass	Keeper
Cena	0,225	0,135	0,090	0,225	0,180
Šifrovanie	0,045	0,045	0,045	0,045	0,045

Generátor hesiel	0,048	0,036	0,024	0,060	0,048
MFA	0,093	0,093	0,093	0,074	0,093
Ukladanie súborov	0,114	0,091	0,091	0,046	0,091

Ďalším krokom multi-kriteriálnej analýzy TOPSIS je určenie miním a maxím pre jednotlivé kritéria, čo je vyobrazené v tabuľkách 11 a 12. Maximá sú značené zelenou farbou a minimá červenou.

Tabuľka 11 Vyobrazenie maxím

Kritérium	Vaultwarden	LastPass	Dashlane	KeePass	Keeper
Cena	**0,225**	0,135	0,090	**0,225**	0,180
Šifrovanie	**0,045**	**0,045**	**0,045**	**0,045**	**0,045**
Generátor hesiel	0,048	0,036	0,024	**0,060**	0,048
MFA	**0,093**	**0,093**	**0,093**	0,074	**0,093**
Ukladanie súborov	**0,114**	0,091	0,091	0,046	0,091

Tabuľka 12 Vyobrazenie miním

Kritérium	Vaultwarden	LastPass	Dashlane	KeePass	Keeper
Cena	0,225	0,135	**0,090**	0,225	0,180
Šifrovanie	**0,045**	**0,045**	**0,045**	**0,045**	**0,045**
Generátor hesiel	0,048	0,036	**0,024**	0,060	0,048
MFA	0,093	0,093	0,093	**0,074**	0,093
Ukladanie súborov	0,114	0,091	0,091	**0,046**	0,091

Pre vypočítanie výsledných hodnôt je potrebné ešte zistiť vzdialenosť variant od ideálnych a bazálnych variant, ktoré je možné vypočítať pomocou rovníc 4, 5. Vypočítané hodnoty sú vyobrazené v tabuľke 13.

$$d_i^+ = \sqrt{\sum_{j=1}^{k}(w_{ij} - H_j)^2} \quad (4)$$

$$d_i^- = \sqrt{\sum_{j=1}^{k}(w_{ij} - D_j)^2} \quad (5)$$

Tabuľka 13 Ideálne a bazálne hodnoty

	Vaultwarden	LastPass	Dashlane	KeePass	Keeper
Ideálne hodnoty (d_i^+)	0,011952	0,095876	0,141538	0,070853	0,051843
Bazálne hodnoty (d_i^-)	0,154335	0,067756	0,049221	0,139691	0,105335

Výsledné hodnoty sa vypočítajú pomocou rovnice 6 a sú vyobrazené v tabuľke 14, ktorá obsahuje poradie jednotlivých produktov na základe jednotlivých kritérií a váh. Poradie sa určuje od najväčšieho k najmenšiemu.

$$C_i = \frac{d_i^-}{d_i^- + d_i^+} \quad (6)$$

Tabuľka 14 Výsledné hodnoty

	Vaultwarden	LastPass	Dashlane	KeePass	Keeper
c_i	0,928123	0,414077	0,258029	0,663476	0,670165
Poradie	1	4	5	3	2

V analýze TOPSIS vyšiel ako najlepšie riešenie na základe kritérií a váh správca hesiel Vaultwarden. Ako najhoršie riešenie zase vyšiel produkt Dashlane, ktorý je s pomedzi porovnávaných riešení najdrahší. Výsledky sa zhodujú v oboch prípadoch analýz na základe čoho bolo rozhodnuté, že v ďalšej časti práce bude návrh a nasadenie správcu hesiel Vaultwarden.

5 NASADENIE SPRÁVCU HESIEL

Na základe predchádzajúcich analýz vyšiel ako najvhodnejší variant na základe kritérií správca hesiel Vaultwarden. Preto bolo rozhodnuté, že v Knižnici UTB nasadíme práve Vaultwarden, ktorý je tzv. self-hosted, čo znamená na súkromnom serveri a nie ako väčšina iných riešení, ktoré využívajú cloud čiže úložisko ponúkané inou spoločnosťou.

5.1 Prostriedky pre nasadenie

Pre potreby nasadenia správcu hesiel boli vytvorené 2 virtuálne stroje v prostredí VMware vSphere client verzie 7.0.3.1300, ktorá bola v čase prípravy virtuálnych staníc najaktuálnejšou verziou.

Hardvér, na ktorom sa virtualizujú stroje na testovanie a tiež nasadenie nástroja Vaultwarden.

- Chassis Dell PowerEdge VRTX
    - 15x 2,5“ 1.92TB SAS SSD
- Severy 3x PowerEdge M630 (VRTX)
    - 6 x Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz
    - 1280 GB RAM
- R1-2210 VRTX 10Gb Switch

Virtuálne stroje boli vytvorené s operačným systémom Ubuntu 22.04 LTS. Prostriedky vyhradené pre virtuálne stroje:

- 4 jadrá CPU,
- 8 GB RAM,
- 30 GB ROM.

K virtualizovaným strojom bolo zabezpečené pripájanie viacerými spôsobmi, pomocou konzole priamo vo webovom prehliadači a následne pomocou nástroja na pripájanie k virtualizovaným strojom VMware Horizon Client.

5.2 Inštalácia správcu hesiel

Inštalácia nie je veľmi komplikovaná, ale bolo testovaných viac variant keďže je možné inštalovať Vaultwarden pomocou kontajneru a tiež bez. Pri inštalácii s kontajnerom Docker inštalácia prebiehala bez väčších problémov. Pri inštalácii mimo kontajnera sa určité

problémy objavili, aj keď boli odstránené rozhodol som sa použiť verziu s kontajnerom v prípade, že by to chcel niekedy niekto replikovať.

5.2.1 Inštalácia testovacieho prostredia

Inštalácia testovacieho prostredia prebiehala pomocou terminálu, kde sa vkladali jednotlivé príkazy. Tieto príkazy zabezpečili inštaláciu aplikácií potrebných pre stiahnutie, inštaláciu a konfiguráciu správcu hesiel. Pre inštaláciu testovacieho prostredia som sa rozhodol na základe toho, že je nutné najskôr funkcie otestovať a až následne po otestovaní ich nasadiť do prostredia, kde už majú prístup aj používatelia.

Zoznam príkazov potrebných pre inštaláciu testovacieho správcu hesiel Vaultwarden je vyobrazený na obrázkoch 9, 10, 11, 12:

```
# inštalácia závislostí potrebných na inštaláciu
sudo apt install apt-transport-https ca-certificates curl gnupg-agent software-proper-
ties-common
# vytvorenie adresára na uloženie kľúča
sudo mkdir -p /etc/apt/keyrings
# stiahnutie kľúča
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
# pridanie listu Docker do repozitára, aby ich bolo možné inštalovať pomocou apt in-
stall
echo \
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu \
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
# aktualizácia aplikácií
sudo apt update
# inštalácia aplikácií Docker a Containerd
sudo apt install docker-ce docker-ce-cli containerd.io
# pridanie aplikácie Docker na spustení
sudo systemctl enable --now docker
# kontrola statusu aplikácie Docker
```

Obrázok 9 Príkazy na inštaláciu servera Vaultwarden [59]

```
sudo systemctl status docker
# pridanie aktuálne prihláseného používateľa do skupiny Docker
sudo usermod -aG docker $USER
# prepnutie skupiny používateľov na Docker
newgrp docker
# stiahnutie najnovšieho kontajneru Docker s Vaultwardenom
docker pull vaultwarden/server:latest
# vytvorenie zložky vw-data
sudo mkdir /srv/vw-data/
# všetkých okrem vlastníka
sudo chmod go-rwx /srv/vw-data/
# spustenie kontajneru  na pozadí s názvom Vaultwarden zložkami umiestnenými v
/srv/vw-data:/data povolenie používania cez web a nastavenie portov na
localhost:8080 a 3012 a tiež možnosť reštartovania v prípade zlyhania
sudo docker run -d --name vaultwarden -v /srv/vw-data:/data -e
WEBSOCKET_ENABLED=true -p 127.0.0.1:8080:80 -p 127.0.0.1:3012:3012 --res-
tart on-failure vaultwarden/server:latest
# inštalácia kontajnera Caddy
sudo docker pull caddy:latest
# úprava kofiguračného súbora Caddyfile
sudo nano /etc/Caddyfile
# obsah súboru, ktorý je určený na nastavenie proxy pripojenia, ktorý v prípade testo-
vacie-ho prostredia nebol upravovaný hodnoty produkčného riešenia sú odlišné
yourdomain.com {
encode gzip
reverse_proxy /notifications/hub/negotiate 0.0.0.0:80
reverse_proxy /notifications/hub 0.0.0.0:3012
reverse_proxy 0.0.0.0:80
}
# vytvorenie zložky caddy
sudo mkdir /etc/caddy
# odobranie oprávnení všetkým okrem vlastníka
```

Obrázok 10 Príkazy na inštaláciu servera Vaultwarden 2 [59]

```
# spustenie kontajnera Docker Caddy s potrebnými parametrami
sudo docker run -d -p 80:80 -p 443:443 --name caddy -v /etc/Caddy-
file:/etc/caddy/Caddyfile -v /etc/caddy:/root/.local/share/caddy --restart on-failure
caddy:latest
# zobrazenie logov kontajnera Caddy
sudo docker logs caddy
# zastavenie kontajnera Vaultwarden
sudo docker stop vaultwarden
# vymazanie kontajnera Vaultwarden
sudo docker rm vaultwarden
# spustenie kontajnera Vaultwarden s úpravou, aby sa nemohli registrovať noví pou-
žívatelia bez pozvánky
sudo docker run -d --name vaultwarden -v /srv/vw-data:/data -e
WEBSOCKET_ENABLED=true -e SIGNUPS_ALLOWED=false -p
127.0.0.1:8080:80 -p 127.0.0.1:3012:3012 --restart on-failure vaultwar-den/server:la-
test
# inštalácia databáze sqlite3
sudo apt install sqlite3
# vytvorenie adresára pre zálohu inštancie Vaultwarden
sudo mkdir /srv/backup
# odstránenie oprávnení pre všetkých okrem vlastníka
sudo chmod go-rwx /srv/backup
# vytvorenie súboru s nastavením pre zálohovanie
sudo nano /etc/systemd/system/vaultwarden-backup.service
# obsah súboru pre nastavenie zálohovania, ktorý popisuje spustenie zálohovania da-
tabáze
[Unit]
Description=Vault backup

[Service]
Type=oneshot
WorkingDirectory=/srv/backup
ExecStart=/usr/bin/env sh -c 'sqlite3 /srv/vw-data/db.sqlite3 ".backup backup-$(date -
```

Obrázok 11 Príkazy na inštaláciu servera Vaultwarden 3 [59]

```
Is | tr : _).sq3"'
ExecStart=/usr/bin/find . -type f -mtime +30 -name 'backup*' -delete
# nastavenie pri spustení
sudo systemctl start vaultwarden-backup.service
# vytvorenie súboru s nastavením času zálohovania inštancia Vaultwarden
sudo nano /etc/systemd/system/vaultwarden-backup.timer
# obsah súboru časovaču, kde je nastavenie, že sa má spustiť záloha o 4:00
 [Unit]
Description=Vault backup timer

[Timer]
OnCalendar=04:00
Persistent=true

[Install]
WantedBy=multi-user.target
# povolenie spustenia časovača zálohy
sudo systemctl enable --now vaultwarden-backup.timer
# kontrola spustenia časovača
sudo systemctl status vaultwarden-backup.timer
# zastavenie kontajnera s Vaultwardenom
sudo docker stop vaultwarden
# odstránenie kontajnera s Vaultwardenom
sudo docker remove vaultwarden
# príkaz na spustenie služby Vaultwarden s pridaním prístupu k admin rozhraniu
sudo docker run -d --name vaultwarden -v /srv/vw-data:/data -e
WEBSOCKET_ENABLED=true -e ADMIN_TOKEN=HesloKtoreNezverejnimDPJP
-p 127.0.0.1:8080:80 -p 127.0.0.1:3012:3012 --restart on-failure vaultwarden/ser-
ver:latest
# kontrola spustenia Vaultwarden
sudo systemctl status vaultwarden
```

Obrázok 12 Príkazy na inštaláciu servera Vaultwarden 4 [59]

5.2.2 Testovanie inštalácie Vaultwarden

Pri testovaní testovacej inštalácie boli skúšané možnosti zadávania údajov k službám, tiež kompatibilný doplnok pre prehliadač od spoločnosti Bitwarden. Medzi skúšanými možnosťami správcu Vaultwarden bolo tiež ukladanie súborov, dokladov a poznámok.

Testované funkcie v bežnom prostredí

Ukladanie údajov pre prístup k rôznym službám, ukladanie údajov o kartách, dokladoch, poznámky a tiež dokumenty, text, ktoré je potrebné zabezpečiť heslom pred tým, ako ich budeme chcieť odoslať.

Ukladanie súborov je možné len spôsobom uloženia, kde sa vygeneruje odkaz, pomocou ktorého je ich možné aj odoslať inej osobe, ktorá pozná heslo. Taktiež je tam možnosť nastavenia, kedy má odkaz exspirovať prípadne zakázať otvorenie odkazu.

Ďalšia a už vyššie zmienená základná funkcia je generovanie hesiel, pri čom sú ešte možnosti importovania dát aj z rôznych iných správcov hesiel, prípadne exportovanie. Všetky importy a exporty sú možné výhradne vo formátoch .xml, .1pux, .1pif, .fsk, .txt, .csv, .json.

Vaultwarden hlásenia, ktoré sa delia na hlásenia o úniku hesiel, hlásenia o znovu použitých heslách, o slabých heslách, o nebezpečných weboch, o neaktívnom 2FA overovaní a ako posledné hlásenie o úniku dát.

Funkcie pre organizácie

Pre organizácie sú k dispozícii základné prvky a trezor na hesla, karty, identitu a poznámky. U organizácie pribúdajú ďalšie nastavenia ako kto je členom organizácie, kto je pozvaný na vstup do organizácie, kto potrebuje potvrdiť členstvo a kto odmietol. Ďalej sú tam hlásenia o heslách ako aj pri bežnom účte len bez overenia úniku podľa mailu. A teraz sa dostávame k tej najdôležitejšej časti ktorú má nastavenie organizácie naviac a to je nastavenie. Nastavenie v rámci organizáciu umožňuje:

- meniť názov a vlastníka,
- meniť zásady používania ako dvojfaktorové prihlasovanie,
- požiadavky na hlavné heslo,
- nastavenie minimálnych požiadavkou generátora hesiel,
- obmedzenie na členstvo len v 1 organizácii,
- vynútenie uloženia položiek do organizácie zakázaním položky osobné vlastníctvo,
- obmedzenie funkcie odosielania (takže aj ukladania súborov),

- nastavenie možností odosielania.

Nastavenie účtu

V nastavení účtu je množstvo možností ohľadom nastavenia hlavného hesla, prístupových metód 2FA a tiež nastavenie zmeny šifrovacieho kľúču. Tiež je možné zvoliť si KDF algoritmus a množstvo iterácií pre heslo, ktoré slúži k vyššej náročnosti pri útoku hrubou silou. V prípade nastavenia účtu sa tiež nastavujú pravidlá pre chovanie trezora, či sa má zamknúť alebo odhlásiť. Medzi poslednými nastaveniami používateľského účtu sú ešte nastavenia ekvivalentných domén a núdzový prístup.

Administrátorské rozhranie

Taktiež boli skúšané prvky rozhrania administrátora, ktoré ponúka množstvo nastavení, ktoré je inak možné vykonať len pri spustení kontajnera. Nastavenia administrátora fungujú tak, že prepisujú premenné zadávané pri inštalácii podľa toho, čo sa nastaví vo webovom prostredí, niektoré zmeny vyžadujú pre správne fungovanie reštartovanie celého Vaultwarden kontajnera.

Základné nastavenia, ktoré ponúka Vaultwarden admin rozhranie:

- Nastavenie adresy domény,
- API kľúča pre HaveIBeenPwned,
- Limit úložiska pre prílohy na používateľa,
- Limit úložiska pre prílohy organizácie,
- Automatické vymazanie položky po presunutí do koša v dňoch,
- Časový limit pre 2FA overenie,
- Povolenie registrovania nových používateľov,
- Časový limit pre znovu odoslanie overovacieho e-mailu,
- Maximálne množstvo automaticky odoslaných overovacích e-mailov,
- Zoznam povolený e-mailových domén,
- Zoznam používateľov s povolením vytvárať organizácie.
- Povolenie pozývania nových používateľov,
- Povolenie núdzového prístupu,
- Zmena počtu iterácií pre všetkých používateľov (predvolené 60000),
- Povolenie zobrazenia a nastavenia nápovedy k heslám,
- Nastavenie tokenu pre prístup k administrátorskému rozhraniu,
- Natavenie mena pozývajúcej organizácie.

Vaultwarden ponúka tiež množstvo ďalších nastavení, ktoré nie je nutné nastavovať úplne vo všetkých prípadoch. Prípadne nesúvisia tak úplne zo správou správcu hesiel, ale skôr nastavení ďalších služieb, ktoré je možné pripojiť, prípadne všeobecné nastavenia pre webové a databázové služby. Ďalej je možné v admin prostredí nastavovať tieto kategórie:

- 2FA aplikácie (Yubikey, Global Duo, Email 2FA),
- SMTP Email,
- prístup k dátam len na čítanie,
- záloha databáze,
- spravovať zoznam používateľov,
- organizácií,
- sledovať diagnostické údaje.

Doplnok do prehliadača od spoločnosti Bitwarden

Doplnok slúži primárne k automatickému doplňovaniu hesiel, v prípade, že je správne nastavená URL adresa prípadne alternatíva u daného hesla. Sekundárne je možné doplnok používať aj ako náhradu klasického webového rozhrania pretože ponúka základné funkcie ako pridávanie hesiel, generátor hesiel a pridávanie súborov.

5.3 Zmeny pri inštalácii správcu Vaultwarden do produkčného prostredia

Pri inštalácii testovacej verzie správcu Vaultwarden boli použité prevažne základné nastavenia odporúčané vývojármi správcu hesiel. Rozhodnutie použiť na ukážku v diplomovej práci práve tieto nastavenia je dôležité, aby sa zamedzilo šíreniu údajov o nastaveniach internej siete a tým sa zamedzilo poskytnutiu potrebných informácií pre prípadného útočníka.

Hlavnou zmenou pri inštalácii produkčného správcu Vaultwarden do produkčného prostredia je použitie údajov internej siete a tiež certifikátov pre danú službu, aby bola použiteľná pre všetky zariadenia, z ktorých by mohlo byť prospešné k správcovi hesiel pristupovať. Ďalšou podstatnou zmenou je prísnejšie nastavenie pravidiel používania nastavených v administrátorskom rozhraní ako aj následné zakázanie administrátorského rozhrania. Všetky nastavenia reflektujú minimálne požiadavky stanovené v bezpečnostnej politike.

Ďalším podstatným nastavením je nastavenie reverznej proxy keďže využívam nasadenie v kontajneri Docker, u ktorých sa štandardne používa nastavenie adries mimo kontajnera, lebo v rámci kontajnera to často ani nie je možné.

5.4 Používateľská príručka

Používateľská príručka k správcovi hesiel sa nachádza v prílohe P I, pretože je to maličká brožúrka, ktorá má slúžiť používateľom k rýchlemu zorientovaniu sa. V používateľskej príručke sa nachádzajú hlavné body, čo sa kde nachádza, pre jednoduchšiu orientáciu pri začiatku používania. Keďže vývojármi Vaultwardenu nie všetko je pomenované úplne ideálne a u niektorých položiek dokonca úplne chýba preklad, bolo vhodné takúto príručku vytvoriť.

6 NASADANIE SYSTÉMU NA AUTOMATIZOVANÉ UKLADANIE HESIEL

Systém na automatizované ukladanie hesiel je systém, ktorý umožňuje prácu s rozhraním API. Konkrétne sa jedná o systém HashiCorp Vault, pretože umožňuje nasadenie na vlastnom servery a tiež je v tomto prípade bezplatný s obmedzením niektorých funkcií. O použití HashiCorp Vaultu bolo rozhodnuté organizáciou na základe toho, že je to jeden z mála nástrojov, ktoré pracujú s heslami automatizovane a zároveň ponúka možnosť vlastnej správy bez spoplatnenia.

6.1 Prostriedky využívané pre nasadenie

Prostriedky využívané pre nasadenie sú z veľkej miery rovnaké ako pri správcovi hesiel, pretože všetko beží na rovnakom hardvéri, len s iným nastavením siete, vygenerovaním a nastavením certifikátov a databáz.

6.2 Nasadenie testovacieho prostredia

Nasadenie testovacieho prostredia prebiehalo tak, že sa pripravili všetky potrebné dokumenty k nastaveniu servera. Pre nastavenie servera Vaultu sú potrebné certifikáty a tiež config.hcl, ktorý uchováva údaje o konfigurácii či už siete alebo tiež správaní trezora na serveri.

Pri testovacom prostredí Vaultu nie je možné použiť pre testovanie nastavenie adries na lokálne. Lokálne nastavenie nie je vhodné z dôvodu, že je potrebné otestovať funkčnosť s konkrétnym serverom, ktorý by si mal pýtať heslo pomocou API, aby sa zamedzilo úniku na strane používateľa. Taktiež je už pri testovacom prostredí potrebné nastaviť celú sadu certifikátov, aby server fungoval správne a bolo bezpečné naň pristupovať z iných serverov v sieti. Inštalácia Vaultu od HashiCorp prebiehala na základe dokumentácie dostupnej na webových stránkach spoločnosti, kde je možné si tiež zriadiť účty. Účet na webe ponúka všetky možnosti, ktoré ponúka aj vlastná inštalácia dokonca aj viac v prípade, že sa jedná o verziu enterprise.

Zoznam príkazov potrebných na inštaláciu ako testovacej, tak aj produkčnej verzie, pretože sa jedná o kópiu testovacej s úpravou IP adries a certifikátov zobrazený na obrázkoch 13, 14, 15:

```
# update inštalovaných aplikácií
sudo apt-get update
# upgrade inštalovaných aplikácií
sudo apt-get upgrade
# presun do zložky opt
cd /opt/
# stiahnutie súboru s Vaultom
sudo wget https://releases.hashicorp.com/vault/1.12.2/vault_1.12.2_linux_amd64.zip
# rozbalenie súboru s Vaultom
sudo unzip vault_1.12.2_linux_amd64.zip -d
# presun súboru vault do zložky /usr/bin/
cp vault /usr/bin/
# vytvorenie zložky vault a vault-data v časti /etc/
mkdir /etc/vault
mkdir /vault-data
# vytvorenie zložiek /logs/vault súbežne bez nutnosti vytvárať ich postupne
mkdir -p /logs/vault/
# vytvorenie konfiguračného súboru config-vault.hcl
sudo vi /etc/vault/config-vault.hcl
# obsah súboru config-vault.hcl
disable_cache = true //vypnutie cache
disable_mlock = true //vypnutie mlock (len unix distribúcie)

ui = true //povolenie webového rozhrania

listener "tcp" { //tcp komunikácia adresa a port + tls zabezpečenie
    address = "127.0.0.1:1024"
    tls_cert_file      = "/root/DPJP-RootCA/vault.pem"
    tls_key_file       = "/root/DPJP-RootCA/vaultkey.pem"
    tls_client_ca_file = "/root/DPJP-RootCA/DPJP-RootCA.pem"
}
//lokálne úložisko
storage "raft" {
```

Obrázok 13 Príkazy na inštaláciu správcu Vault

```
  node_id = "raft_node_1"
}

cluster_addr = "http://127.0.0.1:8201"
api_addr = "http://127.0.0.1:8200"
//povolenie všetkých dodatočných modulov
sentinel {
    additional_enabled_modules = []
}
max_lease_ttl = "10h"
default_lease_ttl = "10h"
cluster_name = "testcluster"
pid_file = "./pidfile"
raw_storage_endpoint = true
disable_sealwrap = true
disable_printable_check = true
# vytvorenie konfiguračného súboru vault.service
sudo vi /etc/systemd/system/vault.service
# obsah súboru vault service
[Unit]
Description=vault service
Requires=network-online.target
After=network-online.target
ConditionFileNotEmpty=/etc/vault/config-vault.hcl

[Service]
EnvironmentFile=-/etc/sysconfig/vault
Environment=GOMAXPROCS=2
Restart=on-failure
ExecStart=/usr/bin/vault server -config=/etc/vault/config-vault.hcl
StandardOutput=/logs/vault/output.log
StandardError=/logs/vault/error.log
LimitMEMLOCK=infinity
```

Obrázok 14 Príkazy na inštaláciu správcu Vault

```
ExecReload=/bin/kill -HUP $MAINPID
KillSignal=SIGTERM
[Install]
WantedBy=multi-user.target
#spustenie vault.service
sudo systemctl start vault.service
#spustenie vault.service
sudo systemctl start vault.service
# kontrola statusu vault.service
sudo systemctl status vault.service
# povolenie vault.service
sudo systemctl enable vault.service
# nastavenie adresy localhost ako VAULT_ADDR
export VAULT_ADDR=http://127.0.0.1:1024
# aby sa predchádzajúce nastavenie nastavilo pri otvorení terminálu
echo "export VAULT_ADDR=http://127.0.0.1:1024" >> ~/.bashrc
# kontrola statusu Vaultu
vault status
# zapísanie výstupu príkazu vault operator init do /etc/vault/init.file
vault operator init > /etc/vault/init.file
# kontrola obsahu súboru init.file
cat /etc/vault/init.file
# kontrola statusu Vaultu
vault status
# uloženie adresy s portom ako VAULT_ADDR
export VAULT_ADDR=http://127.0.0.1:62666
# uloženie tokenu, aby sa dalo pracovať s funkciami Vaultu v terminále
export VAULT_TOKEN="hvs.nahodneznakyvpocte28znak"
```

Obrázok 15 Príkazy na inštaláciu servera Vault

Vyobrazené príkazy používané v terminále Ubuntu 22.04 LTS, sú nutné na inštaláciu Vaultu, adresy certifikáty a obsah konfiguračných súborov sa v minimálnej miere líšia od skutočnosti, z dôvodu bezpečnosti interných systémov. V zobrazených príkazoch tiež

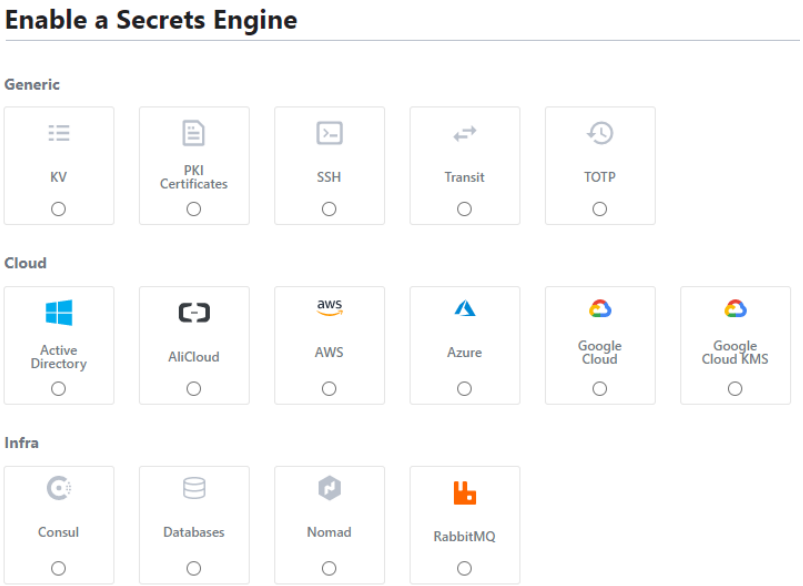
chýbajú kódy k odomknutiu Vaultu, čo prebieha na základe zadania 3 kódov z 5 (threshold cryptography) na odomknutie pri prvotnom prístupe, ktorý sa zadáva pri každom reštarte.

6.3 Testovanie funkcií Vaultu

Testovanie funkcií Vaultu prebiehalo pomocou viacerých rozhraní ako webu tak aj CLI. Vo webovom rozhraní bola testovaná značná časť možností, ktoré by sa dali využiť v prostredí Knižnice UTB. V rozhraní CLI len základné funkcie na prístup a získanie dát z Vaultu.

6.3.1 Testovanie webového prostredia Vault

Webové prostredie aplikácie Vault ponúka množstvo možností ohľadom ukladania dát k rôznym službám čo je možné vidieť aj na obrázku 16. Dokonca aj ku cloudovým službám rôznych poskytovateľov a dokáže pracovať s ich aplikačným prostredím. Na základe toho, že dokáže pracovať aj s ich API ponúka možnosť dynamických tajomstiev.



Obrázok 16 zobrazenie možností na ukladanie tajomstiev

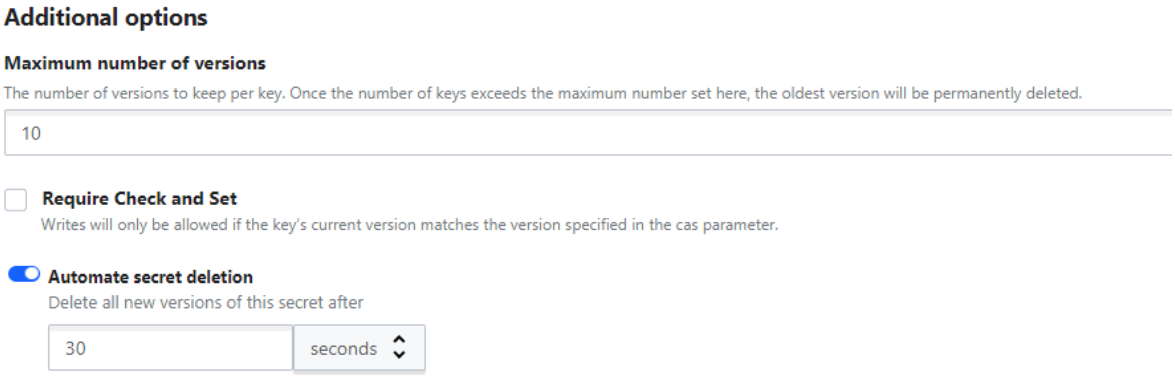
Pre účely danej práce boli využívané výhradne generické mechanizmy a to na základe toho, že Knižnica UTB nepotrebuje aktuálne žiadne ďalšie možnosti, pretože nevyužíva iné ako lokálne cloudové služby a ani aplikácie ako Consul, Nomad a RabbitMQ.

Účelom diplomovej práce bolo navrhnúť automatizovaný systém pre centralizované ukladanie hesiel, k čomu je potrebná len časť KV, pretože to je jediná možnosť ako ukladať štandardné heslá do správcu Vault. Ale keďže je možnosť, že by sa na základe využívaných

prostriedkov v Knižnici UTB dali použiť aj možnosti ako PKI certifikáty a Transit tak boli testované aj tieto možnosti.

Testovanie KV

V prípade testovania KV bolo zistené, že umožňuje množstvo nadštandardných funkcií oproti správcom hesiel a to maximálne uchovávané množstvo verzií hesla, povolenie zápisu len v prípade, že sa aktuálna verzia zhoduje s požiadavkou zaškrtni a nastav a ako posledná špeciálna funkcia automatické zmazanie nových verzií hesla po nastavenom čase. Tieto nastavenia môžete vidieť na obrázku 17.



Obrázok 17 Špeciálne funkcie aplikácie Vault

Testovanie PKI certifikátov

Na základe testovania mechanizmu PKI certifikáty bolo zistené, že Vault pri správnom nastavení dokáže generovať certifikáty X.509 automatizovane v prípade správneho vygenerovania koreňovej CA. Na základe koreňovej CA je možné vytvoriť prechodnú CA. Pomocou CA, údajov o doméne spolu s nastavením povolení pre subdomény a času skončenia je možné požiadať o certifikát. U vydaného certifikátu je tiež možné jednoducho ho zrušiť a tiež vymazať po vypršaní. Pri koreňovej CA je tiež zaujímavá možnosť vygenerovania novej bez zrušenia starej než všetky stroje začnú používať novú. Toto sa zabezpečuje pomocou CA s krížovým podpisom, aby sa dali overiť adresáre podľa starej koreňovej CA. Zrušenie koreňovej CA je možné jednoducho zakázaním vydávať nové certifikáty. V prípade PKI certifikátov je viac možností ako pracovať s CA a certifikátmi ale tento je pre prostredie Knižnice UTB tým najzaujímavejším, pretože umožňuje všetko potrebné.

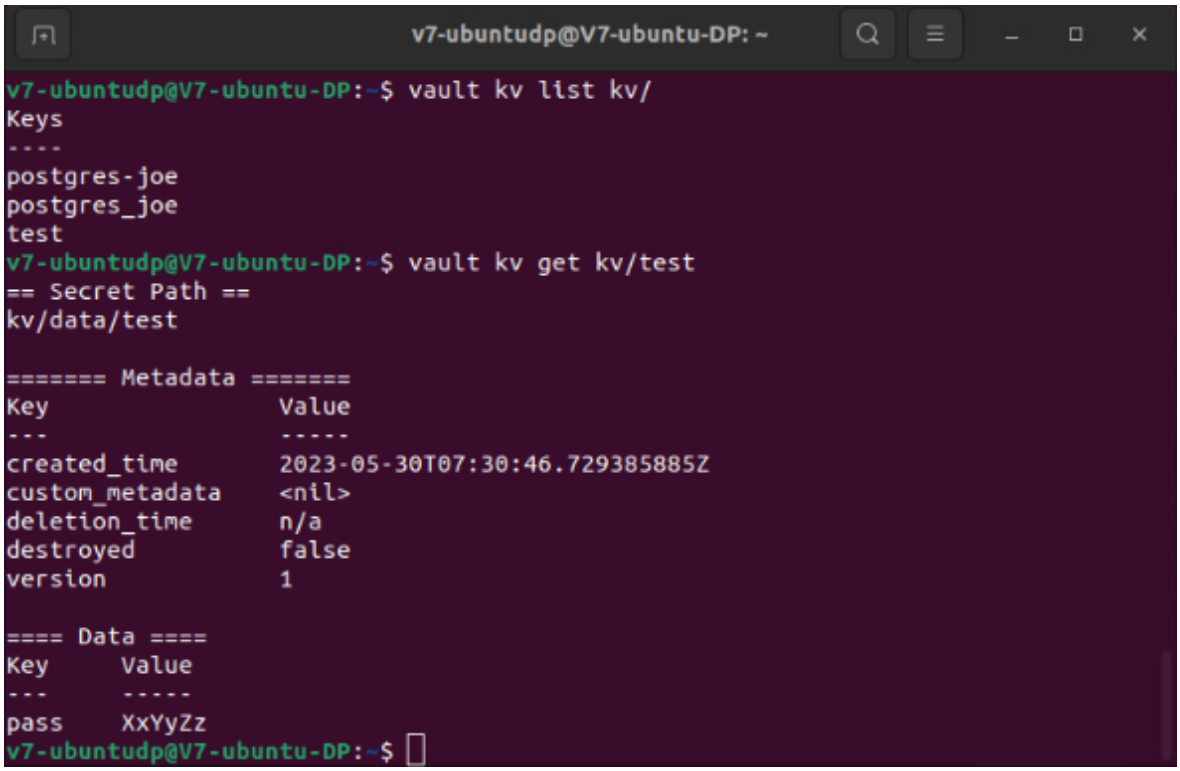
Testovanie Transit

Testovaná funkcia Transit umožňuje pracovanie s vygenerovaným kľúčom, ktorý môže byť generovaný vo variantoch AES, CHACHA, ECDSA a RSA. Následne sa generovaný kľúč

dá použiť na šifrovanie, dešifrovanie, vytvorenie nového šifrovaného kľúča, prebalenie šifrovaného textu, overenie podpisu dát a export kľúča.

6.3.2 Testovanie funkcií správcu Vault pomocou CLI

Na testovanie funkcií Vaultu bolo použité aj CLI, ktoré sa používa pomocou zadávania príkazov do terminálu, kde je nutné poznať adresu a tiež heslo, ktoré sú potrebné na používanie funkcií aplikácie Vault. V prostredí CLI boli testované len základné možnosti ako odomknutie Vaultu, ukladanie hesla a zobrazenie hesla, vytvorenie používateľa, nastavenie politík k používateľovi a prístup zo servera pre možnosť automatizovaného použitia. Ukážka použitia obrázok 18.



Obrázok 18 – Ukážka využitia aplikácie Vault v CLI

6.3.3 Testovanie automatizovaného získania hesiel pomocou API

Pre automatizované získanie hesiel uložených vo Vaulte je potrebné na začiatok správne nastavenie politík používania pre jednotlivých používateľov. Bez správneho nastavenia politík nie je možné používateľom pristupovať k heslám, ktoré uložil ktokoľvek iný a je možné pristupovať len k základným heslám uloženým v cubbyhole. Ukážka ako také politiky vyzerajú spolu s popismi, čo ktorý príkaz v rámci politík rieši sú zobrazené na obrázkoch 19, 20, 21.

```
# povolenie tokenu pozerať na svoje nastavenie
path "auth/token/lookup-self" {
    capabilities = ["read"]
}
# povolenie tokenu aby sa mohol sám obnoviť
path "auth/token/renew-self" {
    capabilities = ["update"]
}
# polenie tokenu aby sa mohol sám zakázať
path "auth/token/revoke-self" {
    capabilities = ["update"]
}
# povolenie tokenu aby videl svoje schopnosti
path "sys/capabilities-self" {
    capabilities = ["update"]
}
# povolenie tokenu aby videl vlastné entity na základe id alebo mena
path "identity/entity/id/{{identity.entity.id}}" {
  capabilities = ["read"]
}
path "identity/entity/name/{{identity.entity.name}}" {
  capabilities = ["read"]
}
# povolenie tokenu aby videl výsledný zoznam svojich práv zo všetkých politík toto je
# užitočné pre používateľské rozhrania, je to interná cesta, pretože formát sa môže
# kedykoľvek zmeniť na základe toho, ako sa menia interné funkcie a možnosti ACL
path "sys/internal/ui/resultant-acl" {
    capabilities = ["read"]
}
# povolenie tokenu obnovu prenájmu prostredníctvom lease_id v tele žiadosti;
# prvá cesta podľa starej dokumentácie, druhá podľa novšej, používajú sa stále obe
path "sys/renew" {
    capabilities = ["update"]
```

Obrázok 19 Politiky správcu Vault

```
}
path "sys/leases/renew" {
    capabilities = ["update"]
}
# povolenie pozerania na nastavenie prenájmov, je vyžadované vopred poznať ID
# prenájmu a neprezrádzať žiadne citlivé údaje
path "sys/leases/lookup" {
    capabilities = ["update"]
}
# povolenie tokenu spravovať vlastnú cubbyhole ( základný trezor bez možnosti zdie-
ľania)
path "cubbyhole/*" {
    capabilities = ["create", "read", "update", "delete", "list"]
}
# povolenie tokenu zabaliť hodnoty do tokenu na obalenie odozvy
path "sys/wrapping/wrap" {
    capabilities = ["update"]
}
# povolenie tokenu vyhľadávať čas vytvorenia a TTL daného tokenu na zabalenie
# odpovede
path "sys/wrapping/lookup" {
capabilities = ["update"]
}
# povolenie tokenu zabaliť token na balenie odpovede a využíva sa preto, aby sa
# zamedzilo zámene tokenov klientov, pretože je tiež súčasťou balenia
path "sys/wrapping/unwrap" {
capabilities = ["update"]
}
# povolenie univerzálnych nástrojov
path "sys/tools/hash" {
capabilities = ["update"]
}
path "sys/tools/hash/*" {
```

Obrázok 20 Politiky správcu Vault 2

```
capabilities = ["update"]
}
# povolenie kontroly stavu požiadavku riadiacej skupiny, ak má používateľ doplnok
path "sys/control-group/request" {
capabilities = ["update"]
}
# povolenie tokenu odosielať požiadavky na autorizačný koncový bod pre
# poskytovateľa OIDC
path "identity/oidc/provider/+/authorize" {
capabilities = ["read", "update"]
}
# povolenie pristupovať ku všetkým cestám ako aj ich vytváranie, čítanie, mazanie a
upravovanie
path "sys/mounts/*" {
capabilities = ["create", "read", "update", "delete", "list"]
}
#povolenie čítať a zobrazovať možnosti na čítanie pre používateľa postgres (testovací
používateľ)
path "postgres/*"{
capabilities = ["read","list"]
}
```

Obrázok 21 politiky správcu Vault 3

Politiky pre nastavenie Vaultu vyobrazené vyššie na obrázkoch 19, 20, 21 sú upravené základné prednastavené politiky tak, aby bolo možné pomocou vytvorených účtov pristupovať, vytvárať, mazať atď. zdieľané tajomstvá. Je to potrebné hlavne na tajomstvá, ktoré sú spravované na úrovni administrátora.

Pri získavaní hesla pomocou účtu priradeného ku konkrétnemu serveru prípadne dokonca službe sa použije príkaz curl, ku ktorému sa pridajú kompletné požiadavky, čo potrebujeme aké tajomstvo, k akej službe a aká je cesta vo Vaulte k danému tajomstvu. Príklad vyobrazený na obrázku 22.

```
# Príkaz slúžiaci k získaniu hesla a načítaniu do premennej vaultpass za použitia to-
kenu a adresy k Vaultu pre tajomstvo postgres_joe
vaultpass=$(SSL_CERT_FILE=/etc/ssl/certs/DPJP-RootCA.pem curl -s -f --header
"X-Vault-Token: $VAULT_TOKEN" -X GET
$VAULT_ADDR/v1/kv/data/postgres_joe | grep -oP '(?<=\"pass\":\")[^\"]*')
```

Obrázok 22 Ukážka získania hesla cez API

6.3.4 Nedostatky zistené pri testovaní

Nedostatky riešenia – v prípade, že chceme používať Vault po tom, čo bol v neaktívnom stave je nutné zadávať kódy na odomknutie. Neaktívny stav je stav, kedy nie je dostupný napr. pri reštarte, vypnutí atď. Zadávanie kódov vyžaduje interakciu s používateľom, prípadne ak by sme chceli prebudenie automatizovať, tak strácame ochranu pre neaktívny stav, pretože by sa kódy nachádzali na zariadení a odomykali Vault automaticky pri spustení serveru. Na základe čoho by sa umožnilo prípadnému útočníkovi dostať sa priamo k prihláseniu, kde by potreboval už len prístupové údaje ako napr. token, meno a heslo.

7 NÁVRH BEZPEČNOSTNEJ POLITIKY NA PRÍSTUP K IS

Bezpečnostná politika na pristupovanie k informačnému systému, je dôležitá na základe toho, že je nutné rozhodnúť ako heslá a všetko v spojitosti s heslami a prístupmi využívať, aby sa zamedzilo zneužitiu čohokoľvek, čo je prístupovými údajmi zabezpečené. Je to z toho dôvodu, aby bolo jasne definované, kto a akým spôsobom má pracovať s akými prístupovými údajmi.

7.1 Cieľ bezpečnostnej politiky

Cieľom bezpečnostnej politiky podniku je zabrániť akémukoľvek neoprávnenému narábaniu s prístupovými údajmi, používaný v súvislosti s Knižnicou UTB a ďalšími súčasťami univerzity. S ďalšími súčasťami z toho dôvodu, že niektoré systémy sú zdieľané a spravované prevažne pracovníkmi univerzitnej Knižnice UTB.

Bezpečnostná politika priamo súvisí s:

- vynútením náročnosti hesiel,
- využívaním správcu hesiel,
- využívaním dvojfaktorovej autentifikácie,
- možnosťami ukladania a zdieľania hesiel,
- zmenami hesiel.

7.2 Účel bezpečnostnej politiky

Účelom bezpečnostnej politiky je oboznámiť zamestnancov zo zásadami, ktoré by mali pochopiť, zaviazať sa k ich dodržiavaniu. Následne by sa bezpečnostná politika mala uplatňovať, k čomu by mal byť oprávnený zamestnanec, ktorý kontroluje dodržiavanie definovaných zásad. Určenie osoby, ktorá zodpovedá za vypracovanie a aktualizáciu bezpečnostnej politiky za účelom zachovania bezpečnosti, ako aj kontrolu dodržiavania (audit).

7.3 Realizácia bezpečnostnej politiky na správu hesiel

Pre realizáciu bezpečnostnej politiky je potrebné si stanoviť, pred akými hrozbami nás má bezpečnostná politika chrániť. V tomto prípade ide o hrozby spojené prevažne s únikom a zneužitím hesiel a s tým spojený prístup k informáciám. Jedná sa konkrétne o únik a zneužitie:

- prístupových údajov k databázam s citlivými údajmi,

- údajov k účtu na správu akéhokoľvek systému,
- údajov k účtu pomocou ktorého by mohlo dôjsť k šíreniu falošných informácií,
- akýchkoľvek údajov, ktoré by mohli ohroziť dobré meno spoločnosti.

7.3.1 Návrh ochrany pomocou hesiel a správcu

Ochrana bezpečnosti hesiel musí byť účelná a tiež dostatočne zrozumiteľná všetkým osobám, ktoré by sa ňou mali riadiť, aby bola užitočná. Pretože ak nebudú všetci rozumieť účelu bezpečnostnej politiky na správu hesiel tak nikdy nebude dostatočná a jej prvky správne využívané.

Konkrétne kroky k ochrane hesiel pomocou bezpečnostnej politiky a správcu hesiel, aby sa zamedzilo nedostatočnej ochrane proti rôznym spôsobom útoku na heslá ako aj zamedzeniu zlyhania ľudského faktoru. Pravidlá stanovené bezpečnostnou politikou:

- Heslo by malo obsahovať veľké, malé písmená, číslice a špeciálne znaky ako napríklad (?:-_/*%!+@&) všade kde je to možné.
- Heslo by malo byť dostatočne dlhé aspoň 12 znakov pre bežných používateľov a 17 znakov pre administrátorov, používateľov s vyššími oprávneniami a aplikácií na základe vyhlášky č. 82/2018Sb. o kybernetickej bezpečnosti[7].
- Heslo neukladať inam ako do služby na správu hesiel Vaultwarden.
- Heslá a kľúče k aplikáciám ukladať do centralizovaného systému Vault, platí pre administrátorov.
- Heslá ani iné prístupové prvky nikdy nezdieľať s inými osobami, ak to nie je nevyhnutné. V prípade, že je nevyhnutné tieto údaje zdieľať, tak len pomocou zdieľania hesla v rámci organizácie v správcovi hesiel Vaultwarden.
- V ojedinelých prípadoch sa môže stať, že je nutné zdieľať heslo aj s externými pracovníkmi. Toto umožniť taktiež len pomocou správcu hesiel Vaultwarden a po ukončení činností, ak nepretrváva dlhodobý zmluvný vzťah ukončiť zdieľanie a heslo zmeniť.
- Zamknutie účtu po zadaní 10 neúspešných pokusov o prihlásenie u bežných používateľov a 5 pokusov u administrátorov.
- U nových používateľov vytvoriť jednorazové heslo v prípade, že je to možné a vynútiť po prvom prihlásení zmenu hesla. V prípade, že by zmena nenastala do 24 hodín heslo deaktivovať.
- Maximálna platnosť hesla je 12 mesiacov.

- Minimálna platnosť hesla je 1 deň.
- Zákaz použitia rovnakého hesla pre viac služieb neplatí v prípade použitia jednotného prihlasovania.
- Na tvorbu hesla je odporúčané využiť generátor hesiel, ktorý je dostupný ako súčasť správcu hesiel Vaultwarden. Je to z dôvodu náhodnosti zoradenia znakov prípadne výberu slov aby nemali priamu súvislosť s osobou ako napr. mená osôb, prípadne domácich maznáčikov a podobne.

7.3.2 Návrh ochrany pomocou MFA

Využívanie viacfaktorového overovania je dôležitou funkciou, pretože na základe tejto funkcie je zabezpečený účet aj v prípade narušenia bezpečnosti únikom hesla. Hlavne preto, že útočník potrebuje na prístup k účtu poznať aj ďalší kód, ktorý je dostupný len v prípade, že sa dostane k inému účtu prípadne zariadeniu. V závislosti od toho v ako zariadení využívate druhú fázu overenia.

- V maximálnej možnej miere využívať aspoň dvojfaktorovú autentifikáciu.
- U účtov, ktoré sú z akéhokoľvek dôvodu významné pre organizáciu využívať v prípade možnosti aspoň trojfaktorovú autentifikáciu.
- Ideálne v kombinácii s biometrickým prvkom ak je to možné.
- Ak je k dispozícii iná možnosť nevyužívať mail a zadanie druhého kódu alebo hesla, ktorý je na princípe, že si ho musíte pamätať.
- Ak nie je iná možnosť využiť aj mail alebo zadanie druhého kódu alebo hesla.

Dvojfaktorové overenie je možné pomocou väčšieho množstva nástrojov a zariadení, je možné ho využívať ako súčasť správcu hesiel v prípade možnosti generovania časovo obmedzeného kódu pre prístup. Ďalšou možnosťou je zvyčajne využitie aplikácie v mobile, na základe ktorej zadávate kód pre prístup, prípadne len potvrdíte, že ste sa o prihlásenie skutočne pokúsili vy.

Troj a viacfaktorové overenie je podstatné preto, že karta môže byť ukradnutá tak isto aj mobil, odtlačky zneužité a heslo prelomené prípadne uniknuté. Preto je vhodné vytvoriť v prípade možnosti čo najviac prekážok.

7.3.3 Školenie ohľadom bezpečnosti prístupových údajov

Školenie ohľadom bezpečnosti hesiel by malo prebiehať v období maximálne 2 roky od predchádzajúceho školenia zamestnanca z dôvodu, aby bolo jasné, že sa oboznámil

s novými podmienkami a tiež s novými hrozbami na základe ktorých sú podmienky nastavované.

Obsahom školenia by mali byť hrozby, ktoré stále trvajú ohľadom zabezpečenia prístupových údajov a tiež ohľadom noviniek, aby mali zamestnanci čo najviac informácií o tom, že dané heslo už by nemuselo plniť svoj účel dostatočne.

Trvanie školenia je veľmi individuálne, ale predpoklad je, že by malo trvať minimálne 2 hodiny aby si zamestnanci zo školenia niečo aj zapamätali. Školenie by tiež malo byť ukončené formou testu, aby sa overilo, čo je vykladané zrozumiteľne a dostatočne zaujímavo. A zasa naopak nie je väčšinou dostatočne zrozumiteľné a chcelo by to pre ďalšie školenia upraviť.

7.3.4 Uplatňovanie bezpečnostnej politiky

Ochranu definovanú v bezpečnostnej politike vynucovať u všetkých zamestnancov bez ohľadu na ich pracovné zaradenie a obmedzenosť prístupu k informačným systémom. Bezpečnostnú politiku vynucovať u všetkých zamestnancov formou potvrdenia podpísaním na základe oboznámenia a upozornenia na všetky aspekty.

Pri akýchkoľvek zmenách informovať zamestnancov o tom, že dané zmeny nastali a pravidelne v 2 ročných intervaloch zamestnancom pripomínať formou povinného školenia postupy, pravidlá a ich povinnosti plynúce z bezpečnostnej politiky.

Kontroly dodržiavania pravidiel stanovených bezpečnostnou politikou by mali prebiehať formou náhodných kontrol. Náhodné kontroly budú prebiehať kontrolou, či nastala zmena hesla v stanovenom intervale keďže nie je možná na základe znalosti formou zero-knowledge akákoľvek kontrola konkrétneho hesla.

ZÁVER

Hlavným výsledkom diplomovej práce sú navrhnuté a nasadené systémy na správu hesiel. Jeden systém je určený pre používateľov, ktorý umožňuje aj zdieľanie v rámci organizácie. Druhý systém je určený pre administrátorov, aby mali čo najlepšie zabezpečené prihlasovanie k serverom prípadne službám. Ďalším prínosom práce je návrh bezpečnostnej politiky, ktorá popisuje ako ich používať, aby sa využili efektívne a boli bezpečné.

Diplomová práca je zložená zo siedmych kapitol. Prvé dve sú venované teoretickej časti práce, kde je popísaná základná problematika. Ďalších päť kapitol sa zaoberá praktickou časťou diplomovej práce, kde už sú popísané konkrétne riešenia.

Na úvod sú v prvej kapitolke popísané základné dôležité pojmy potrebné pre pochopenie celej práce. Ďalej sa práca venuje tomu, čo to je správca hesiel, čo je potrebné vedieť o dôvodoch prečo používať správcov hesiel. Rozdelenie správcov hesiel podľa toho, kam sa ukladajú dáta poskytnuté správcom hesiel a tiež stručný popis populárnych správcov hesiel. Ako posledná časť správcov hesiel je zjednodušene popísaný princíp AES šifry, pretože ju používajú všetci správcovia hesiel.

V druhej kapitole sú definované základné pojmy v spojitosti s automatizovaným systémom na správu hesiel Vault. Ďalej si v tejto kapitole môžete prečítať o tom, čo to Vault je a aké funkcie a hlavne spôsoby ukladania tajomstiev ponúka.

Kapitola tri je zameraná na analýzu, o tom, ktorý zo správcov hesiel je najvhodnejší na použitie na základe požiadaviek a prostredia Knižnice UTB. V tejto kapitole sú vyobrazené všetky kritériá, ktoré sa zohľadňujú pri výbere ako aj analýza na základe súčtu bodov pre jednotlivé varianty správcu hesiel.

Ďalšia, štvrtá kapitola sa zaoberá multi-kriteriálnou analýzou TOPSIS, kde sú popísané postupy a vzorčeky potrebné pre správne výpočty analýzy TOPSIS, ktorá pracuje aj s váhami pre jednotlivé kritéria nie len ich bodmi a tiež záver na základe oboch analýz.

V kapitole päť sa práca zameriava na popísanie prostredia pre nasadenie správcu hesiel Vaultwarden. Tiež popisuje potrebné príkazy pre nasadenie správcu hesiel v testovacom a produkčnom prostredí s ohľadom na bezpečnosť internej siete UTB. V tejto časti práce sú popísané taktiež testované funkcie a drobný popis k používateľskej príručke.

Predposledná kapitolka práce sa zaoberá automatizovaným systémom pre správu hesiel Vault, V tejto kapitole sú ďalej popísané nasadenie testovacieho a produkčného riešenia

Vaultu s ohľadom na bezpečnosť internej siete. Sú tam testované hlavné funkcie, ktoré sa využívajú a tiež také, ktoré by bolo možné využiť na základe používaným nástrojov v prostredí Knižnice UTB.

Posledná časť diplomovej práce sa zaoberá vytvorením návrhu bezpečnostnej politiky používania hesiel a autentizačných faktorov. V tejto časti sú popísané základné náležitosti bezpečnostnej politiky ako aj pravidlá, akým spôsobom a aké heslá využívať v prostredí Knižnice UTB. Taktiež je v tejto časti popísané akým spôsobom by sa malo kontrolovať dodržiavanie podmienok stanovených v bezpečnostnej politike.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Username. *Computerhope* [online]. Computer Hope, © 2023, 31.01.2019 [cit. 2023-05-29]. Dostupné z: https://www.computerhope.com/jargon/u/username.htm

[2] JAŠEK, Roman, David MALANÍK a Nicol DAŇKOVÁ. *Bezpečnost informačních systémů*. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2022, 154 s. ISBN 9788076780880.

[3] Co jsou to biometrické údaje?. *Gdprsolutions* [online]. Praha: AntStudio, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.gdprsolutions.cz/slovnik/biometricke-udaje/

[4] What's the Difference Between 2FA and 2SV?. *Rublon* [online]. Zielona Gora: Rublon, © 2023, 26.08.2021 [cit. 2023-05-29]. Dostupné z: https://rublon.com/blog/2fa-2sv-difference/

[5] BONNETT, Dovell. *Making Passwords Secure: Fixing the Weakest Link in Cybersecurity*. CreateSpace Independent Publishing Platform, 2016, 170 s. ISBN 9781530164486. Dostupné také z: http://students.aiu.edu/submissions/profiles/resources/onlineBook/F2H2H9_Making%20Passwords%20Secure.pdf

[6] BURNETT, Mark a Dave KLEIMAN. *Perfect passwords: selection, protection, authentication*. Rockland, Mass.: Syngress, 2006, xv, 181 s. ISBN 9781597490412. Dostupné také z: http://www.sciencedirect.com/science/book/9781597490412

[7] ČESKO. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. In: *Sbírka zákonů České republiky*. Praha: Tiskárna Ministerstva vnitra, 2018, ročník 2018, číslo 82. Dostupné také z: https://www.nukib.cz/download/publikace/legislativa/vkb_82-2018sb.pdf

[8] Are Your Passwords in the Green?. *Hive Systems* [online]. Richmond: Hive Systems, © 2023, 18.04.2023 [cit. 2023-05-29]. Dostupné z: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

[9] Jak na bezpečné heslo? Nejčastější chyby, které (zřejmě) také děláte. *ÚVT Internet provider* [online]. Jesenice-Zdiměřice: ÚVT Internet, © 2020 [cit. 2023-05-29]. Dostupné z: https://uvtnet.cz/jak-na-bezpecne-heslo-nejcastejsi-chyby-ktere-zrejme-take-delate

[10] How often you should change your passwords, according to cybersecurity experts. *Business Insider* [online]. Insider, © 2023, 26.06.2020 [cit. 2023-05-29]. Dostupné z: https://www.businessinsider.com/guides/tech/how-often-should-i-change-my-password

[11] An Overview Of Password Managers. *Terranova Security* [online]. Fortra, ©, 19.07.2022 [cit. 2023-05-29]. Dostupné z: https://terranovasecurity.com/an-overview-of-password-managers/

[12] Picking the right password for your password manager. *Bitwarden* [online]. Santa Barbara: Bitwarden, © 2023, 09.02.2022 [cit. 2023-05-29]. Dostupné z: https://bitwarden.com/blog/picking-the-right-password-for-your-password-manager/

[13] Password Strength Testing Tool. *Bitwarden* [online]. Santa Barbara: Bitwarden, © 2023 [cit. 2023-05-29]. Dostupné z: https://bitwarden.com/password-strength/

[14] ROUSE, Margaret. Password Generator. *Techopedia* [online]. London: Techopedia, © 2023, 30.08.2015 [cit. 2023-05-29]. Dostupné z: https://www.techopedia.com/definition/31414/password-generator

[15] What is a password vault ?. *Zoho* [online]. Zoho, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.zoho.com/vault/what-is-password-vault.html

[16] Zero-knowledge encryption. *1password* [online]. Toronto: 1Password, © 2023 [cit. 2023-05-29]. Dostupné z: https://1password.com/features/zero-knowledge-encryption/

[17] DUFFY, Jill. How to Share Passwords Safely. *PCMag* [online]. New York: Ziff Davis, © 1996-2023, 02.05.2022 [cit. 2023-05-29]. Dostupné z: https://www.pcmag.com/how-to/share-passwords-safely

[18] What is a password manager?. *Malwarebytes* [online]. Cork, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.malwarebytes.com/what-is-password-manager

[19] GARCÍA, Danie. Unofficial Bitwarden compatible server written in Rust, formerly known as bitwarden_rs. *RustRepo* [online]. RustRepo, 2022, 08.01.2023 [cit. 2023-05-29]. Dostupné z: https://rustrepo.com/repo/dani-garcia-vaultwarden-rust-security-tools

[20] Releases. *GitHub* [online]. GitHub, © 2023 [cit. 2023-05-29]. Dostupné z: https://github.com/dani-garcia/vaultwarden/releases

[21] Best Password Managers. *Investopedia* [online]. 27.02.2023 [cit. 2023-05-29]. Dostupné z: https://www.investopedia.com/best-password-managers-5080381

[22] Secure Business Password Manager. *Dashlane* [online]. Dashlane, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.dashlane.com/business-password-manager

[23] BOYD, Sam. Dashlane recenze: Nejlepší správce hesel roku 2023?. *SafetyDetectives* [online]. SafetyDetectives, © 2023, 24.05.2023 [cit. 2023-05-29]. Dostupné z: https://cs.safetydetectives.com/best-password-managers/dashlane/

[24] WALSH, Conor. KeePass Review 2023: Is It a Good Open-Source Password Manager?. *SafetyDetectives* [online]. SafetyDetectives, © 2023, 23.05.2023 [cit. 2023-05-29]. Dostupné z: https://www.safetydetectives.com/best-password-managers/keepass/

[25] GLAMOSLIJA, Katarina. Keeper Password Manager Review 2023: Is It Any Good?. *SafetyDetectives* [online]. SafetyDetectives, © 2023, 25.05.2023 [cit. 2023-05-29]. Dostupné z: https://www.safetydetectives.com/best-password-managers/keeper/

[26] JENA, Baivab Kumar. What Is AES Encryption and How Does It Work?. *Simplilearn* [online]. San Francisco: Simplilearn Solutions, © 2009-2023, 09.02.2023 [cit. 2023-05-29]. Dostupné z: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

[27] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Advanced Encryption Standard (AES)*. In: NIST FIPS PUB 197. 2001.

[28] AES Encryption 256 Bit. *TowardsDataScience* [online]. Towards Data Science, 20.08.2020 [cit. 2023-05-29]. Dostupné z: https://towardsdatascience.com/aes-encryption-256-bit-a9ae49cde0b6

[29] What is Vault?. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/what-is-vault?optInFrom=vault-

io&_gl=1*1r1t05r*_ga*Nzk5NzkyNzM2LjE2NTMzODU0OTM.*_ga_P7S46ZYEKW*MTY1OTUxNDI2OC4yOS4xLjE2NTk1MTQ0NzAuMA..

[30] What Is Token-Based Authentication?. *Okta* [online]. Okta, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.okta.com/identity-101/what-is-token-based-authentication/

[31] MCTEER, Dan a Bryan KRAUSEN. *Running HashiCorp Vault in Production*. Amazon Digital Services LLC - KDP Print US, 2020. ISBN 9798639476969.

[32] What are tls/ssl certificates?. *Digicert* [online]. DigiCert, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.digicert.com/tls-ssl/tls-ssl-certificates

[33] Introduction to JSON Web Tokens. *JWT* [online]. [cit. 2023-05-29]. Dostupné z: https://jwt.io/introduction

[34] What Is an API Key?. *Fortinet* [online]. Fortinet, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/api-key

[35] What is Access Management?. *CyberArk* [online]. CyberArk Software, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.cyberark.com/what-is/access-management/

[36] Secrets Engines. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets

[37] KV Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/kv

[38] PKI Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/pki

[39] SSH Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/ssh

[40] Transit Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/transit

[41] TOTP Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/totp

[42] Active Directory Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/ad

[43] AliCloud Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/alicloud

[44] AWS Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/aws

[45] Azure Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/azure

[46] Google Cloud Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/gcp

[47] Google Cloud KMS Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/gcpkms

[48] Consul Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/consul

[49] Nomad Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/nomad

[50] RabbitMQ Secrets Engine. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/secrets/rabbitmq

[51] Auth Methods. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/auth

[52] TLS Certificates Auth Method. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/docs/auth/cert

[53] What is Vault. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/tutorials/getting-started/getting-started-intro

[54] /sys/tools. *HashiCorp* [online]. [cit. 2023-05-29]. Dostupné z: https://developer.hashicorp.com/vault/api-docs/system/tools#parameters

[55] Need a super secure password? Try our random password generator. *Keeper Security* [online]. Keeper Security, © 2023 [cit. 2023-05-29]. Dostupné z: https://www.keepersecurity.com/features/password-generator.html

[56] Two-Factor Authentication. *Keeper Security* [online]. Keeper Security, © 2023 [cit. 2023-05-29]. Dostupné z: https://docs.keeper.io/enterprise-guide/two-factor-authentication

[57] Pricing by Plan - LastPass. *LastPass* [online]. LastPass, © 2023 [cit. 2023-05-30]. Dostupné z: https://www.lastpass.com/pricing?pill=business

[58] JABLONSKÝ, Josef. *Modely operačního výzkumu*. Hradec Králové: Gaudeamus, 2002, 235. s. ISBN 8070410299.

[59] MAURYA, Heyan. How to Install Vaultwarden on Ubuntu 22.04 LTS Jammy. *Linux Shout* [online]. Linux Shout, © 2023, 31.05.2022 [cit. 2023-05-29]. Dostupné z: https://linux.how2shout.com/how-to-install-vaultwarden-on-ubuntu-22-04-lts-jammy/

ZOZNAM POUŽITÝCH SYMBOLOV A ZKRATIEK

TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution
PIN	Osobné Identifikačné číslo (Personal Identification Number)
SMS	Krátka správa (Short Message Service)
PC	Osobný počítač (Personal Computer)
AES	Štandard pokročilého šifrovania (Advanced Encryption Standard)
U2F	Universal 2nd Factor
OS	Operačný systém (Operating System)
iOS	iPhone operačný systém (iPhone Operationg System)
MFA	Viacfaktorová autentifikácia (Multi Factor Authentication)
SSO	Jednotné prihlásenie (Single Sign On)
API	Rozhranie pre programovanie aplikácií (Aplication programming interface)
UI	Používateľské rozhranie (User Interface)
CLI	Rozhranie príkazového riadka (Command Line Interface)
HTTP	HyperText Transfer Protocol
TLS	Transport Layer Security
JSON	JavaScript Object Notation
SSL	Secure Sockets Layer
JWT	JSON Web Token
RFC	Request For Comments
HMAC	Hash-based Message Authentication Code
RSA	Rivest-Shamir-Adleman
ECDSA	Elliptic Curve Digital Signature Algorithm
IT	Informačné Technológie
IAM	Identifikačný a prístupový management (Identity and Access Management)

KV	Kľúč hodnota (Key Value)
PKI	Public Key Infrastructure
SSH	Secure Shell
TOTP	Time-based One-Time Password
RAM	Read Access Memory
AWS	Amazon Web Service
KMS	Key Management Service
ACL	Access Control List
OIDC	OpenID Connect
AD	Active Directory
LDAP	Lightweight Directory Access Protocol
PAP	Password Authentication Protocol
SHA	Secure Hash Algorithm
OTP	One Time Password
SAS SSD	Serial-Attached SCSI Solid-State Drive
CPU	Central Processing Unit
LTS	Long-Term Support
ROM	Read-Only Memory
2FA	Two-Factor Authentication
IP	Internet Protocol
CA	Certification Authority

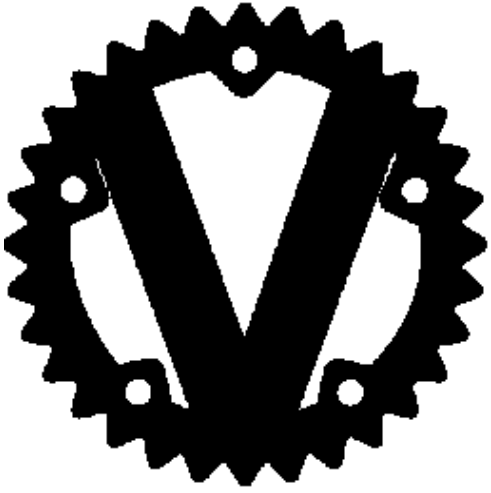
ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

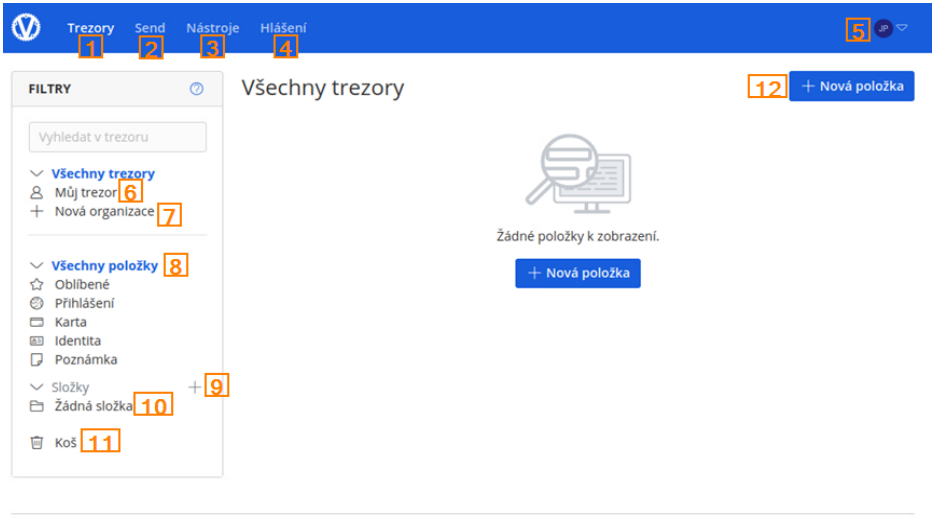
ZOZNAM PRÍLOH

Príloha P I: Používateľská príručka Vaultwarden

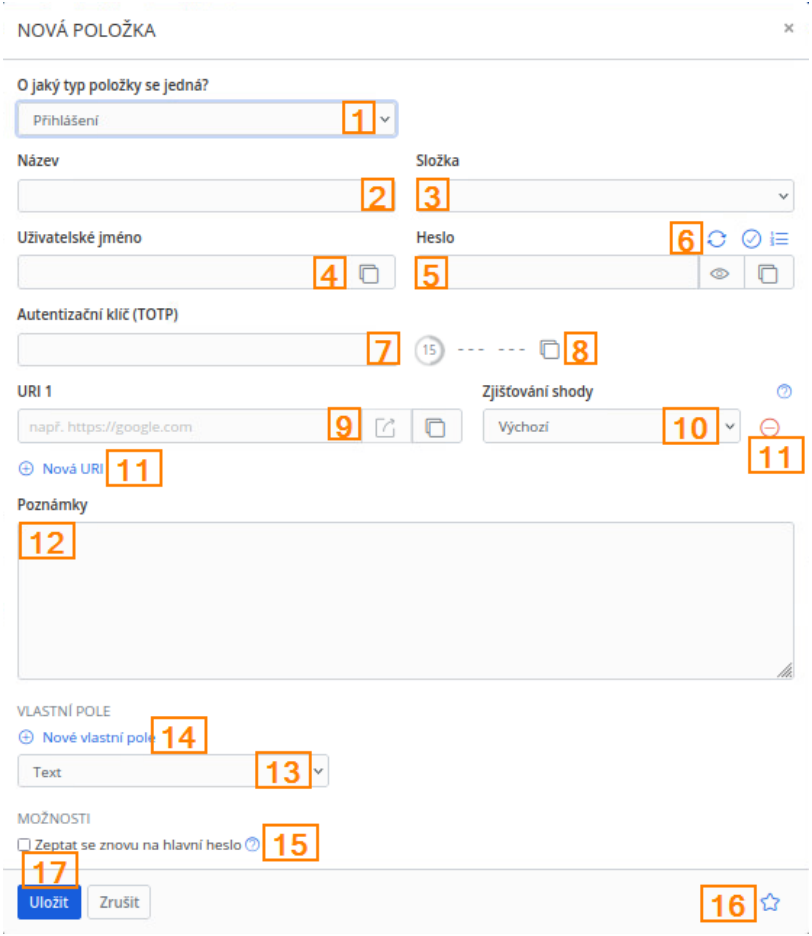
PRÍLOHA P I: POUŽÍVATEĽSKÁ PRÍRUČKA VAULTWARDEN



Vaultwarden

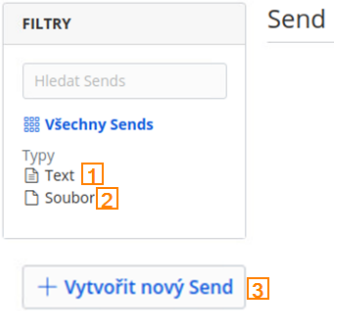


1. Základná pozícia – zobrazenie na obrázku,
2. Odoslanie – časť v ktorej je možné ukladať súbory a texty, kde je umožnené aj odosielanie,
3. Nástroje – pod týmto tlačidlom sú generátor, import a tiež export,
4. Hlásenie – v tejto časti sú hlásenia o problémoch s heslom, o nepoužití 2FA, nebezpečných weboch a únikoch dát,
5. Nastavenie účtu, nápoveda, zamknutie a odhlásenie.
6. Môj trezor – zobrazenie vlastných údajov,
7. Vytvorenie organizácie (na tejto pozícii sa tiež môže nachádzať názov organizácie - zobrazenie zdieľaných údajov organizáciou),
8. Všetky položky podľa typu,
9. Vytvorenie novej zložky,
10. Výpis všetkých zložiek,
11. Kôš,
12. Nová položka – zobrazenia v ďalšej časti.



Nová položka trezoru

1. Typ položky kam sa majú údaje zaradiť,
2. Názov údaju,
3. Priečinok kam to chceme zaradiť,
4. Používateľské meno,
5. Heslo,
6. Generovanie hesla, kontrola hesla a zobrazenie počítadla dĺžky,
7. Kľúč získaný pri vytvorení 2FA s generovaním kódov na krátky čas,
8. Zobrazenie kódu,
9. URL adresa stránky, ku ktorej sú dané údaje,
10. Zisťovanie, či sa zhoduje webová stránky prípadne doména atď.,
11. Pridanie alebo odobranie URL adresy,
12. Poznámky k danému heslu napr. kontrolná otázka ...,
13. Typ nového políčka,
14. Pridanie nového políčka,
15. Prístup k tomuto údaju len po opätovnom zadaní hlavného hesla,
16. Označiť ako obľúbené,
17. Uložiť.

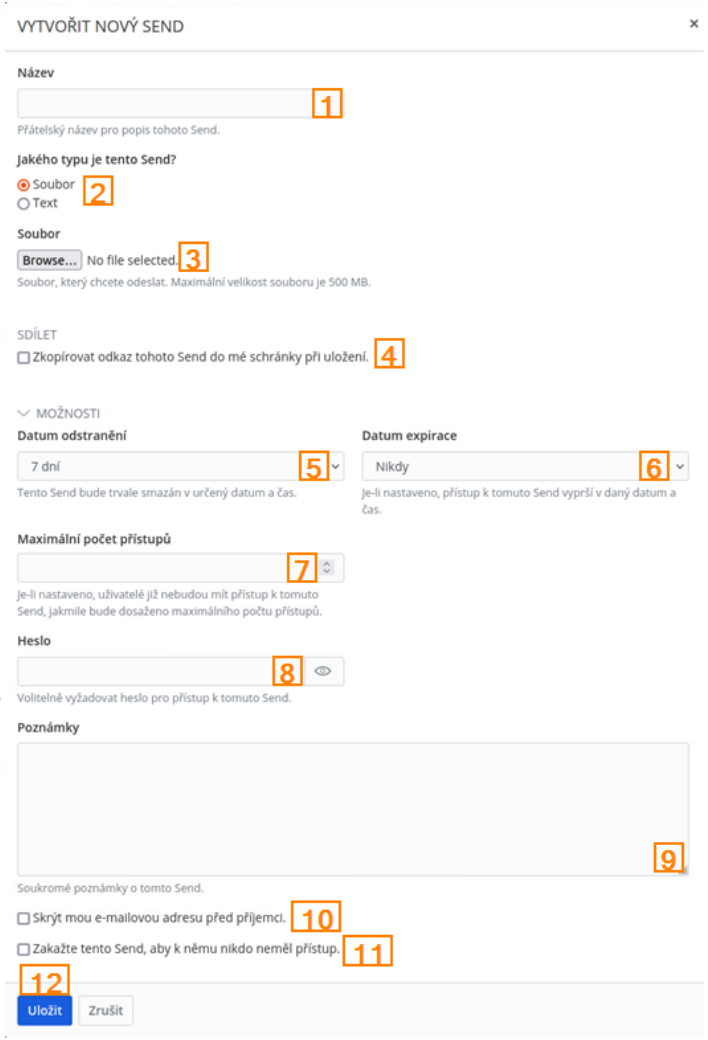


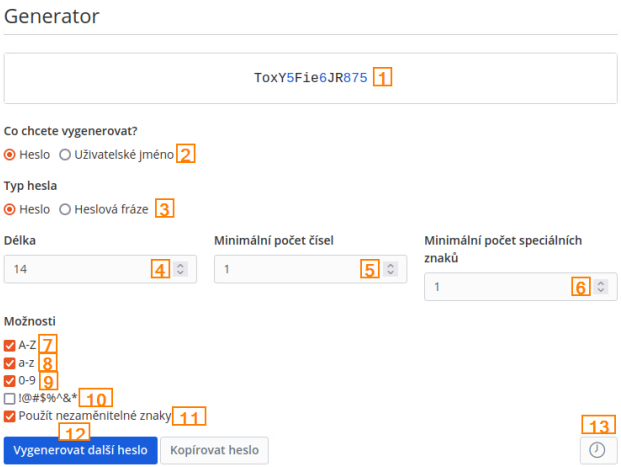
Záložka odoslanie – súbory/text

1. Zobrazenie položiek text,
2. Zobrazenie položiek súbor,
3. Vytvorenie novej položky.

Nová položka odoslanie

1. Názov položky,
2. Typ položky,
3. Vloženie súboru / textové pole,
4. Skopírovanie odkazu po uložení,
5. Nastavenie dátumu vymazania (ľubovoľne),
6. Nastavenie dátumu exspirácie (ľubovoľne),
7. Maximálny počet použití(voliteľné),
8. Heslo (voliteľné),
9. Poznámky,
10. Skryť email pred príjemcom,
11. Zakázanie prístupu k položke,
12. Uložiť.





Generátor hesiel

1. Zobrazenie generovaného hesla,
2. Výber, čo generovať,
3. Typ hesla, náhodné znaky alebo slová,
4. Dĺžka,
5. Minimálny počet čísiel,
6. Minimálny počet špeciálnych znakov,
7. Veľké písmená A-Z,
8. Malé písmená a-z,
9. Číslice,
10. Špeciálne znaky,
11. Len nezameniteľné znaky,
12. Vygenerovanie hesla,
13. História hesiel.

Importovanie dát

1. Formát súboru na importovanie,
2. Vyberte súbor,
3. alebo vložte text do tohto poľa,
4. import dát.

Exportovanie dát

1. Formát pre exportovanie,
2. Potvrdenie formátu, čo spustí aj sťahovanie.