Vysoká škola ekonomická v Prahe

Fakulta informatiky a štatistiky

Analýza a návrh zavedenia softvéru na správu hesiel pre koncových užívateľov v podnikovej sieti

BAKALÁRSKA PRÁCA

Študijný program: Aplikovaná informatika

Študijný obor: Aplikovaná informatika

Autor: Samuel Koyš

Vedúci bakalárskej práce: Ing. Jiří Sedláček, Ph.D.

Praha, máj 2019

Prehlásenie

Prehlasujem, že som bakalársku prácu *Analýza a návrh zavedenia softvéru na správu hesiel pre koncových užívateľov v podnikovej sieti* vypracoval samostatne za použitia v práci uvedených prameňov a literatúry.

V Prahe dňa 6. mája 2019 .....

Samuel Koyš

Poďakovanie

Chcel by som sa na úvod poďakovať vedúcemu práce pánu Ing. Jiří Sedláčkovi, Ph.D. za venovaný čas pri vedení práce, poskytnuté rady a vecné pripomienky.

Zároveň sa chcem poďakovať pánu Tomášovi Vondráčkovi, ktorý mi pomohol s návrhom témy a za poskytnuté informácie počas vypracovania práce.

Abstrakt

Cieľom tejto bakalárskej práce je poskytnúť vhodný návrh riešenia správy hesiel pracovníkov vo forme špecializovaného softvéru na správu hesiel, ktorý splňuje vopred určené kritéria na základe analýzy v danom podniku. V teoretickej časti sa práca zaoberá heslovou politikou vo firmách, bezpečnostnými požiadavkami na heslo, bežnými chybami užívateľov spojené s užívaním hesiel a hrozbami v podobe lámania hesiel. Nasledujúca časť je venovaná čisto softvérom na správu hesiel, kde sú popísané jej typy, výhody, ktoré znižujú možnosť byť napadnutý a nedostatky spojené s jej užívaním. Posledná kapitola je praktickou časťou, v ktorej je na úvod predstavená spoločnosť a následne prebehne analýza situácie v podniku, určenie kritérií na výber softvéru, popis vybraných potenciálnych produktov a návrh na implementáciu najvhodnejšieho produktu.

Kľúčové slova

Správca hesiel, heslo, heslová únava, útok, dáta

Abstract

The goal of this bachelor's thesis is to suggest a suitable password management solution for employees. This solution should take the form of a specialized password management software that meets predetermined criteria based on an analysis in the specific enterprise. The theoretical part of this thesis discusses password policy in companies, security requirements for a password, common user errors associated with the use of passwords, and threats such as password cracking. The following section is then solely dedicated to password management software, describing its types, benefits that reduce the ability to be attacked, and deficiencies associated with its use. The last chapter is the practical portion, which introduces the company and then analyzes the situation in the company, defining the criteria for selecting the software, describing the selected potential products and proposing the implementation of the most suitable product.

Keywords

Password manager, password, password fatigue, attack, data

Obsah

Úvod

V dnešnom svete má či už bežný užívateľ informačných technológií alebo zamestnanec firmy vytvorené značné množstvo účtov, kde sa vyžaduje autentizácia. Výsledkom toho je chaos v prehľadnosti a ľudia majú preto tendenciu uchovávať tieto informácie na určité média. Najčastejším riešením je vo forme zaznamenania údajov v plaintexte na počítačovom zariadení alebo na fyzickom predmete. Tieto spôsoby uchovávanie hesiel sú veľmi časté, ale z bezpečnostného hľadiska neodporúčané.

Vďaka stále rastúcemu vývoju informačných technológii, vznikli softvéry, ktoré nám túto ťažkosť vedia zjednodušiť. Konkrétne sa jedná o softvéry pre správu hesiel, ktorých využitie sa nájde hlavne na pracoviskách veľkých firiem, ale aj menších podnikov. Dôvod je pomerne jasný. Pracuje sa s viacerými softvérmi vyžadujúce autentizáciu, lenže schopnosť pamätania si všetkých hesiel môže byť pre bežného preživšieho veľmi náročne. Uložením prihlasovacích údajov laickými metódami môže byť riskantné. V tejto práci si preto ukážeme ako môžeme zavedením softvéru na správu hesiel do chodu firiem zmierniť tento problém.

Existuje však veľa firiem, kde sa tento typ softvéru stále nevyužíva. Som zamestnancom jednej takej firmy. A preto som sa rozhodol v spolupráci s IT oddelením spraviť analýzu možnosti zavedenia správcu hesiel na pracovníkov vo firme. Hlavnou činnosťou firmy je poskytovanie zákazníckej podpory pre letecké spoločnosti Air France KLM, jej dcérinu spoločnosť Transavia, China Southern Airlines a ďalšie. Pracuje sa tu s veľkým množstvom objednávok, ktoré zahŕňajú osobné a platobné údaje miliónov ľudí. Ochrana týchto údajov je preto jednou z najväčších priorít. Pri úniku týchto dát do neznámych rúk, by mohol nastať risk straty dôvery ľudí v spoločnosť.

Prvá časť tejto práce bude teoretického rázu. Na začiatok si uvedieme na obecnej úrovni základné princípy heslovej politike vo firmách a rozbor bežných chýb užívateľov pri správe hesiel, ktoré môžu predstavovať potenciálne hrozby. V druhej kapitole analyzujeme softvéry na správu hesiel. Vysvetlíme si v čom spočíva ich využitie, resp. ako dokážu zjednodušiť prácu užívateľa, ale zároveň upozorníme na jej nedostatky.

Následne prejdeme na praktickú časť práce. Budeme riešiť možnosti zavedenia správcu hesiel na základe vopred určených kritérií. Budú zohľadnené hlavne smernice a bezpečnostná politika firmy. Po uskutočnení analýzy bude doporučený softvér, ktorý najbližšie splňuje určené požiadavky.

Dôvod výberu práce

Byť oboznámený o princípy heslovej politiky je kľúčovým elementom k tomu aby sme znížili riziko byť napadnutý útočníkmi a zabránili úniku našich dát. Správcovia hesiel sú momentálne jedným z tých najbezpečnejších riešení. Prihlasovací proces zjednodušujú a urýchľujú. Napriek tomu je ich častosť užívania užívateľmi veľmi zriedkavá.

Návrh na zavedenie softvéru prebehol po diskusii s administrátormi IT oddelenia firmy. Súčasný systém sa nám zdal nedostatočne ošetrený, v ktorom sa nachádzajú potenciálne hrozby. Dúfam, že práca poslúži ako prínosný materiál, ktorej informácie by podnik mohol využiť v praxi.

Cieľ práce

Hlavným cieľom tejto práce je prísť s vhodným návrhom riešenia problému doterajšej správy hesiel pracovníkov vo vybranej spoločnosti. Analýzou niekoľko poskytovateľov správcov hesiel so zohľadnením nenarušenia bezpečnostnej politiky firmy vyberieme najvhodnejšiu alternatívu. Vybraný softvér musí byť aplikovateľný, kompatibilný a nenarúšajúci chod operácií pre spoločnosť. Výsledky a ďalší doporučený postup má slúžiť ako podklad pre realizáciu implementácie.

Druhým cieľom je vykonať rozbor politiky hesiel používanou vo firmách, aké bezpečnostné štandardy sa bežne užívajú a aké hrozby plynú z nedbanlivej práce s heslami zo strany užívateľov. Taktiež chceme pomocou druhej kapitoly uviesť ako môžeme pomocou správcov hesiel zmierniť tieto hrozby.

Použité metódy

Základnou metodikou tejto bakalárskej práce je literárna rešerš, ktorá je použitá v teoretickej časti. Vychádzame z dostupných vedeckých článkov a knižných publikácií. V praktickej časti je použitá metóda komparácie. Na základe vopred určených kritérií porovnávame produkty firiem poskytujúce softvéry na správu hesiel. Potrebné informácie sme získali z oficiálnych stránok výrobcov a emailovou komunikáciou s pracovníkmi zákazníckej podpory firiem.

1 Heslová politika v podnikovej sieti

Heslová politika je súbor pravidiel, ktoré boli vytvorené za účelom zvýšenia počítačovej bezpečnosti podporovaním užívateľa na vytvorenie spoľahlivých a silných hesiel a následne ich poriadne využívať, ukladať a spravovať. (1) Efektívna správa hesiel znižuje risk kompromitovania heslových autentizačných systémov. Organizácie preto musia ochrániť integritu a dostupnosť hesiel tak aby autorizovaní užívatelia a žiadni neautorizovaní užívatelia užívali heslá podľa potrieb. Tieto činitele by mali byť zabezpečené kontrolami bezpečnosti dát, ktoré môžu byť vo forme užívania zoznamov pre riadenie prístupov (z angličtiny Access Control Lists), ktoré zabránia útočníkom aby prepísali heslá. Zabezpečiť diskrétnosť hesiel je náročnou výzvou a zahrňuje množstvo bezpečnostných nástrojov a rozhodnutí o tom, aké majú byť charakteristiky hesiel. Pri určovaní týchto rozhodnutí je hlavné nájsť kompromis v tom, aké majú byť heslá napríklad dlhé a komplexné z dôvodu aby boli ťažšie prelomiteľné pre útočníkov, ale zároveň aby neboli pre užívateľov ťažké na zapamätanie.

Každá organizácia by mala mať takú heslovú politiku, ktorá čo najviac splňuje požiadavky ohľadom správy hesiel. Patria sem požiadavky typu uchovávania hesiel, kompozície hesiel, požiadavky na vydanie a reset hesiel. Zároveň by mali zohľadniť uplatniteľné štandardy (napr. podľa národného inštitútu štandardov, skrátene NIST), regulácie a iné príručky ohľadom hesiel. Heslová politika by mala byť dostatočne flexibilná aby sa prispôsobila rôznym možnostiam hesiel poskytovaná rôznymi operačnými systémami a aplikáciami. Taktiež by sa mala politika pravidelne revidovať z dôvodu možných aktualizácii technológií, ktoré by mohli ovplyvniť správu hesiel.

1.1 Best practices správy hesiel

Následne si ukážeme zoznam najlepších praktík správy hesiel, ktoré sú uvedené v normách inštitútov štandardov NIST/IEC 27002:

- Užívateľský prístup do korporatívnych IT systémov, sietí, aplikácií a informácií musí byť kontrolovaný v súlade s požiadavkami na prístup, ktoré sú špecifikované vlastníkom (Information Asset Owner).
- Využívanie najaktuálnejších informácií pre bezpečnú správu hesiel. Súčasťou je informovanie užívateľov pomocou záučných programov.
- Väčšina organizácií presadzuje tvrdenie nezapisovať heslá. Malá časť tvrdí, že heslá je potrebné zapísať na zapamätanie viacero hesiel, ale len za predpokladu bezpečnej úschovy. Odporúčanou metódou je heslá ukladať v šifrovanom formáte.
- Ku každému novovytvorenému účtu by malo byť pridelené defaultné heslo a užívateľ by mal byť vyzvaný ku zmene po prvotnom prihlásení do účtu.
- Po niekoľko neúspešných prihlasovacích pokusov, bezpečnostné hlásenia musia byť generované a užívateľské účty by mali byť zamknuté. Odporúčaným parametrom je 3 až 5 na možné pokusy prihlásenia.

- História hesiel by mala byť nakonfigurovaná tak aby zabránila užívateľom užitie rovnakého hesla počas určitej doby
- Autentizačné informácie ako sú heslá, bezpečnostné protokoly a bezpečnostné konfigurácie musia byť primerane zabezpečené proti neautorizovaným prístupom, zmenou alebo stratou.
- Často využívanou praktikou na obnovenie zabudnutých hesiel bolo dovoľovať užívateľom reset hesiel v prípade, že uhádnu bezpečnostnú otázku. Tieto otázky nie sú dobre bezpečnostne ošetrené. Slabá entropia v kombinácii s dátami ľudí zdieľanými na sociálnych médiách oslabuje využitie týchto pomôcok. Preto sa odporúča nepoužívať tieto pomocné otázky ako možnosť obnoviť prístup k účtu.
- Ďalšou dlho zaužívanou praktikou bolo nastaviť automatickú expiráciu hesiel. Avšak podľa najnovšej publikácie NIST už je táto metóda neodporúčaná. Dôvodom bolo zistenie, že človek má tendenciu si uľahčiť prácu vytvorenia nového hesla pridaním číslice alebo jedného špeciálneho znaku na koniec pôvodného hesla. Pri ďalšej výzve zmeniť heslo sa proces opakuje. Ľudia buď znak zmenia alebo pridajú ďalší. (2)

Dodržovaním týchto zásad môžu spoločnosti výrazne znížiť zraniteľnosť systému a potenciálne hrozby z vonkajšej alebo internej strany organizácie.

1.2 Požiadavky na heslo a entropia hesla

Kritéria pre nastavenie hesla sa v závislosti na typu softvéru a druhu uchovávaných dát, s ktorými firma pracuje líšia. Nároky kladené na heslo pre účtovnícky program s uloženými číslami bankových účtov a transakčnými operáciami budú výrazne striktnejšie než na účet e-shopu s knihami. Podstatou je aby citlivejšie informácie boli lepšie zabezpečené.

Dlhú dobu bolo odporúčané vytvoriť heslo s minimálnou dĺžkou 8 znakov a vynútenou konfiguráciou. Heslá museli byť dostatočne komplexné, obsahujúce zmes veľkých a malých písmen, čísiel a špeciálnych znakov. Avšak podľa NIST táto algoritmická komplexnosť vedie k výberu hesiel, ktoré síce splňujú požiadavky, ale sú ľahko predvídateľné. Heslá typu „Password1!“ sa s najväčšou pravdepodobnosťou budú nachádzať v slovníku zakázaných hesiel. Takisto to vedie k ťažšej zapamätovateľnosti, ktorá vedie k nedbanlivému správaniu ukladania hesiel. (3) Alternatívou je využitie dlhých heslových fráz, ktoré takisto zabezpečia vysokú entropiu[1] hesla a zároveň sú jednoduchšie na zapamätanie. Pri útokoch hrubou silou výrazne sťažujú prácu útočníka. Avšak nemali by byť moc jednoduché, aby boli hrozbou slovníkových útokov – použitie prostých fráz. Z tohto dôvodu NIST odporúča aby užívatelia zvolené heslá porovnali s heslami v „black liste“ neakceptovateľných hesiel. Účelom je zneškodniť hrozbu v podobe slovníkových útokov (pozri oddiel 1.4.2). Dajú sa takisto využiť online nástroje, napr. https://haveibeenpwned.com/Passwords. Môžeme pozorovať, že niektorí výrobcovia zjednodušujú zavedenie tejto metódy zabudovaním tejto funkcionality do ich produktov. Napríklad firma Microsoft pridala funkciu do aplikácie Azure Active Directory, ktorá upozorní užívateľov, že použili uniknuté heslo. (3)

[1] Miera informácie, ktorá nesie jednotka alebo tiež miera neurčitosti náhodného pokusu

Byť zabezpečený silným heslom znižuje možnosť byť napadnutý útokom hádaním hesiel alebo crackingom[2]. Za predpokladu, že heslá sú vygenerované náhodne sa ich sila určuje dĺžkou a ich komplexnosťou, ktorá je určená jej predvídateľnosťou znakov. Platí, že čím viac znakov je použitých, tým je heslo silnejšie. Zároveň sa sila stupňuje použitím obsiahlejšej znakovej sady. Napríklad, štvorčíselný užívateľom vytvorený PIN môže mať jednu z desiatich hodnôt (0 až 9) pre všetky zo svojich 4 znakov, čo znamená, že keyspace[3] je 10^4. Užívateľom zvolené heslo, ktoré má 8 znakov a pozostáva zo sady 95 znakov, má keyspace 95^8. Čiže čím viac sa zvyšuje keyspace, čas na vykonanie náročného útoku hrubou silou sa zvyšuje. (4)

Z bezpečnostného hľadiska je logické využívať heslá s vysokým keyspacom pokiaľ sú náhodne generované. V skutočnosti to však predstavuje náročnú úlohu pre užívateľa, pre ktorého je nepohodlné vytvárať komplexné heslá a ukladať ich v pamäti. Dôkazom toho je štúdia od Florencio a Herley na analyzovanie hesiel, ktoré užívatelia skutočne využívajú. Na vzorke 544 960 užívateľov zistila, že počas 85 dňovej dobe každý užívateľ sa zalogoval v priemere do 25 odlišných účtov a využil v priemere 6,5 odlišných hesiel, kde sa každé heslo opakovalo na 3,9 účtoch. Priemerná entropia bola 41 bitov, ktorá odpovedá 7 znakom. (5)

Výsledky poukazujú na nezodpovedné správanie užívateľov, čo sa týka ich bezpečnosti. Bližšie si o tom povieme v následnej časti.

1.3 Chyby zo strany užívateľa

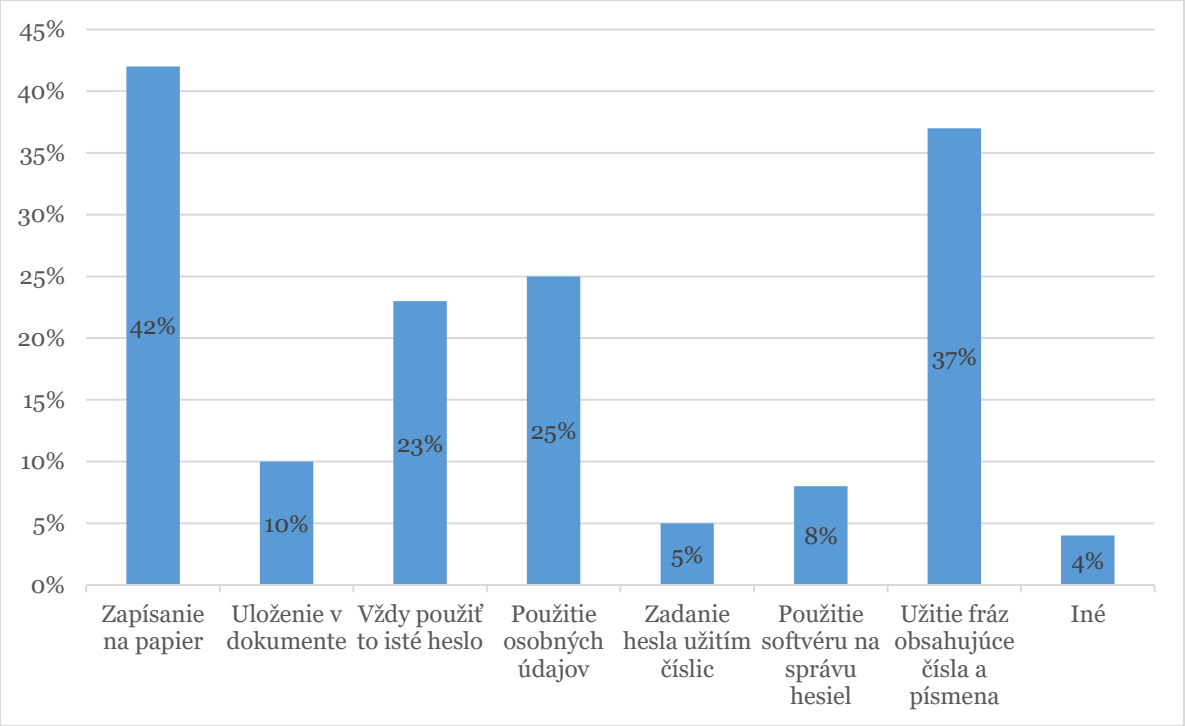
Predtým než prejdeme k samotným chybám užívateľov je relevantné spomenúť, čo je dôsledkom tohto správania. Podľa jednej štúdie z roku 2016 vykonaná Intel Security, bežný užívateľ má v priemere 27 účtov. (6) Rozhodne sa nejedná o malé číslo a preto musí nájsť spôsob ako narábať s týmto počtom loginov. Zároveň sú na užívateľa kladené u vytvorení každého hesla bezpečnostné požiadavky, ktoré ešte viac sťažujú schopnosť zapamätania týchto údajov.

Bežným následkom je heslová únava (z angl. password fatigue). Jedná sa o stav alebo pocit, ktorý má užívateľ v momente, keď si musí zapamätať veľké množstvo hesiel ako časť svojej dennej rutiny. Podporuje to ľudí k osvojeniu si zvykov, ktoré znižujú bezpečnosť svojich informácií.

Ľudský mozog má svoje kapacity v schopnosti pamätania konkrétnych kombinácii znakov. Preto je pochopiteľné, že mnoho užívateľov siaha po rozličných metódach ako najlepšie narábať s problémom heslovej únavy. Lenže väčšina ľudí nepozná, resp. si neuvedomuje bezpečnostné riziká spojené s ich správou. Jedna štúdia od spoločnosti RoboForm (7) z roku 2015 sa pozrela bližšie na túto problematiku. Celkovo sa spýtali 1000 náhodných ľudí zo

[2] Proces spočívajúci v získavaní hesla, ktoré je uložené na úložnom zariadení
[3] Celkový počet možných hodnôt, ktoré „kľúč“ ako je heslo, môže mať

Spojených štátov amerických a Veľkej Británie. Môžeme preto údaje považovať za smerodajné. Otázky boli zamerané na využívané praktiky ohľadom heslovej politiky.



Graf 1 Výsledky odpovedí na otázku aké techniky užívatelia používajú na zapamätanie hesiel (7)

Na otázku: „Aké techniky používate na zapamätanie vašich hesiel?“, kde mohli respondenti zaškrtať viacero možností, odpovedalo 42 %, že si ich ručne zapisujú. Táto metóda úschovy je síce bezpečná proti kyberútokom, ale keďže sa jedná o hmotný predmet, predstavuje to riziko ukradnutia alebo poškodenia inou osobou.

10 % uviedlo, že ukladá heslá v textových dokumentoch. Ako sme si už v úvode práce spomenuli, ukladanie hesiel v plaintexte predstavuje pri nedostatočnom zabezpečení a úspešnom útoku, priamy prístup k loginom užívateľa pre útočníka.

Užívatelia, ktorí využívajú len číslice ako heslá pre účty, kde požiadavky nie sú vysoké, sa vystavujú väčšiemu riziku byť prelomení z dôvodu nižšej entropie hesla.

Bezpečnejším riešením je využitie heslových fráz obsahujúce čísla a písmena, ktorú zaškrtlo 37 % respondentov. Tieto frázy pozostávajú z väčšieho počtu znakov čím sa navyšuje entropia hesla. Možnosť „Použitie softvéru na správu hesiel“ zaškrtlo 8 %.

Vzhľadom k rozsahu sa budeme ďalej konkrétne zaoberať týmto chybám:

1. Znovoupoužívanie hesiel
2. Zdieľanie hesiel
3. Použitie osobných údajov v heslách

1.3.1 Znovupoužívanie hesiel

Správy o úniku dát v ďalšej organizácii sa vyskytujú každoročne. Medzi týmito dátami sa vyskytujú v istých prípadoch aj užívateľské mená a heslá. Tu narážame na častý zvyk užívateľov, ktorým je znovupoužívanie hesiel. Pokiaľ sa medzi kompromitovanými heslami nachádza aj užívateľove heslo, ktorý ho používa do viacero účtov, potom existuje reálna hrozba, že sa útočník dostane do týchto účtov.

Všeobecne neexistuje jednoduchý spôsob ako zistiť znovupoužitie hesiel naprieč systémami. Pokúsiť sa znížiť pravdepodobnosť znovupoužívania hesiel je možné organizáciami, ktoré svojimi pravidlami správy hesiel zakážu to isté alebo podobné heslo konkrétnemu užívateľovi používať. Preto je potrebné zaviesť riadny tréning, ktorý jasne poučí o dôležitosti riadnej správy hesiel a ochrany, ktorá vysvetlí riziká znovupoužívania hesiel. Avšak bez tohto vynucovacieho mechanizmu je málo pravdepodobné, že postupy proti znovuvpoužívaniu hesiel budú veľmi efektívne vzhľadom na počet hesiel, ktoré si užívateľ bude musieť pamätať. (1)

V jednej štúdii na užívateľské názory o heslách od Notoatmodjo (8) sa zistilo, že ľudia zvyknú klasifikovať účty do rozličných kategórií. Na dôležité účty (internetbanking) a málo dôležité účty (čítanie online novinových článkov). Taktiež sa zistilo, že znovupoužívanie hesiel je viac bežné u málo dôležitých účtov. Užívatelia preto majú intuitívne chápanie zvýšeného rizika spojené so znovupoužívaním hesiel, takže sa snažia vyhnúť citlivým aplikáciám ako je online banking. Štúdia prišla k záveru, že vyučenie užívateľov aby zanevreli na znovupoužívanie hesiel je málo pravdepodobná, že by uspela. Aby sa zabezpečila primeraná bezpečnosť a prijateľná užívateľnosť, štúdia odporučila aby užívatelia sa naučili rozpoznať vysoko citlivé aplikácie a zamedziť pri nich znovupoužívanie hesiel.

Rozpoznať vysoko citlivé aplikácie od menej citlivých však nie je riešením zneškodnenia útoku na ostatné účty. Potenciálnym riešením je preto využitie softvéru na správu hesiel, ktorý obsahuje generátor hesiel. Týmto spôsobom sú vytvorené unikátne heslá na každý účet a užívateľ je lepšie zabezpečený na všetky svoje užívané účty.

1.3.2 Zdieľanie hesiel

Ďalším problémom zaobchádzania s heslami je ich zdieľanie iným osobám. Zaujímavým zistením na tento problém je OVUM štúdia zameraná na správu hesiel (9). Až 37 % respondentov, ktorí sú výkonnými IT oddelení, umiestnilo zdieľanie hesiel na papieri ako vysoké riziko a 34 % umiestňujú zdieľanie hesiel cez email na tú istú kategóriu. V niektorých prípadoch zdieľanie hesla je nevyhnutné v určitých oddeleniach podniku, ale musí byť v tom prípade vykonané bezpečne. Na otázku, akým spôsobom riešia zdieľanie hesiel v prípadoch keď sa tomuto riziku dá vyhnúť, 44 % spoločností odpovedalo, že zamestnancov pokračujú ďalej zaúčať, 20 % odpovedalo, že to zakazujú zamestnancom zmluvne.

Na otázku či zdieľajú heslá so spolupracovníkmi odpovedalo 11 % pozitívne. Okrem situácii kedy je zdieľanie hesla ďalšej strane nevyhnutné, je táto praktika obecne považovaná ako zlá a mala by byť zamedzená. Ďalej sa zistilo, že 5 % dotazovaných zdieľalo heslá s osobou

mimo organizácie. To znamená, že v podstate v každej spoločnosti sa nachádza osoba, ktorá predáva ďalej prístupové údaje do systémov. Kľúčovým problémom v tomto prípade je, že stačí zneužitie len jedného zdieľaného údaju na vystavenie riziku organizácie a jeho systému.

Bez správnej kombinácie politiky užívania, vzdelania a technologicky založeného vynútenia, je kladený moc veľký dôraz na zamestnaneckú vlastnú zodpovednosť aby vykonal správne rozhodnutia. V prípade zlyhania zamestnanca pri užívaní podnikových systémov, tak vystavuje sám seba a aj podnik riziku. Môže to vyvrcholiť v náhodné alebo úmyselné poškodenie alebo stratu dát. Lenže pokiaľ firmy nezačnú využívať správu hesiel s monitorovaním systémov potrebné na správu každého prístupu, tak nie sú schopní identifikovať vinníka a odpovedať na spáchanú škodu. Takisto by mohol softvér na správu hesiel vyriešiť tento problém, keďže heslá by boli generované a výsledný reťazec znakov je ťažko zapamätateľný.

1.3.3 Použitie osobných údajov v heslách

23 % respondentov v prieskume uviedlo, že využívajú osobné údaje vo svojich heslách. (7) Užitie mien rodinných príslušníkov, celebrít alebo domácich miláčikov v heslách, nie je odporúčaná metóda. Lámacie techniky ako napríklad slovníkové útoky s veľkou pravdepodobnosťou obsahujú kombinácie typu „Ivan123“. Pridaním špeciálnych znakov nemusíme dosiahnuť požadovaný stupeň bezpečia, keďže útočníci si sú tohto vedomí a skúšajú preto rôzne kombinácie písmen, čísiel a iných znakov.

1.4 Hrozby spojené s heslami z vonkajšej strany

V predošlej kapitole sme si uviedli chyby užívateľov pri narábaní s heslami. Tieto chyby môžu uľahčiť pozíciu útočníka. Pri využívaní informačných a komunikačných technológií v podnikovom prostredí existuje mnoho nástrah v podobe rôznych útokov. Každý z týchto útokov je špecifický a môže potenciálne zraniť internú sieť podniku. Motívy útočníkov bývajú rôzne. Jedná sa buď o hackerov, ktorí si chcú preukázať svoje schopnosti alebo profesionálnych zločincov. Jedným z hlavných cieľov útočníkov býva získať prístup k utajovaným dátam. Dáta bývajú zabezpečené najpoužívanejším autentizačným systémom, ktorým je systém zadania username a hesla. Dôležitú rolu tu hrá bezpečnostná politika, ktorú si organizácia nastaví a následné chovanie zamestnancov.

1.4.1 Spôsoby uchovávania hesiel v systéme

Predtým než sa oboznámime so samotnými útokmi je dôležité si vysvetliť akými spôsobmi sa heslá dajú ukladať v systéme. Pri každej autentizácii musí systém zistiť či osoba má oprávnenie k prístupu. Zadané údaje do prihlasovacieho poľa sa preto musia porovnať s dátami uloženými v databáze.

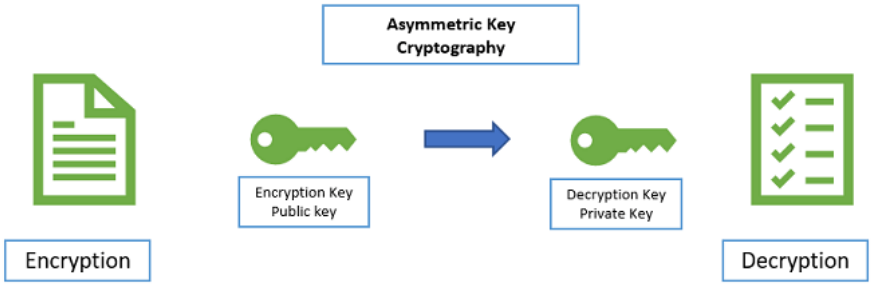
Plaintext – Najjednoduchšou metódou ukladania hesiel je vo forme obyčajného textu, ktorý nie je žiadnym spôsobom kódovaný, šifrovaný alebo inak krytý. Behom autentizácie

porovnáva zadané heslo s kópiou uloženou v databáze. V prípade zhody povolí prístup. Nevýhodou je riziko spojené s užívateľmi alebo útočníkmi, ktorý ak získajú prístup k databáze automaticky môžu nahliadnuť do ktoréhokoľvek účtu. V súčasnej dobe sa plaintext nepovažuje za vhodnú metódu ukladania hesiel. Napriek tomu niektoré stránky ignorujú túto hrozbu. Je náročné zistiť, akým spôsobom stránka ukladá heslá, ale pri niektorých stránkach môžeme použiť nasledujúcu metódu. Stačí stlačiť tlačidlo „Zabudli ste heslo?“ a ak nám zašlú heslo na email, môžeme predpokladať, že heslá sú uložené v plaintexte. Pri hashovaných heslách by táto metóda neuspela.

Hashovanie – Prijateľnejšie riešenie na uchovávanie hesiel je využitie hashe[4]. Hashovacie funkcie sa bežne využívajú pri prihlasovaní, kde sa vyžaduje autentizácia. Pri hashovacích funkciách sa jedná o jednosmerné vzorce, pretože je takmer nemožné vypočítať pôvodne heslo z hashe. Na zistenie hesla, systém prijme požiadavku, spustí rovnakú hashovaciu funkciu a následne porovná výsledok s dátami uloženými v hashovacej databáze. Ak sa zhodujú, systém vyhodnotí heslá ako identické, keďže vytvorili ten istý hash. Využitím hashe, aplikácia alebo webová stránka nikdy neuloží aktuálne heslo. V závislosti na použitej hashe sa odvíja zložitosť dekódovania hashe. Avšak nie sú neprelomiteľné. Útočníkovi stačí vybrať potenciálne heslá a spustiť na nich hashovaciu funkciu a následne porovnať výstupy s hashami v databáze. Pokiaľ sa výstupu rovnajú, útočníkovi sa stačí pozrieť na heslo, ktoré vygenerovalo daný hash. (10) Spôsob ako zosilniť hash je použitie soli. Jedná sa o rovnaký princíp ako pri samotnom hashovaní, len s tým rozdielom, že výsledný hash bude upravený pridanou soľou, čo znamená, že v prípade dvoch identických hesiel nám vzniknú dve rozličné hashe. Vďaka tomu sťažíme prácu útočníka v prípade uskutočnenia hromadného útoku na viacero hesiel, pretože u každého užívateľa bude požadovaný samostatný odhad, ktorý by zabral veľké množstvo času. Ďalšou metódou na zosilnenie hashe je použiť techniku key stretching. Key stretching je metóda využívaná na zosilnenie hesla zvýšením náročnosti (napr. zvýšenie počtu iterácií) na odskúšanie každého možného kľúča.

Šifrovanie – Posledným variantom je prekonvertovať plaintext do šifrovaného tvaru pred uložením do databáze. Poznáme dva typy šifrovania, do ktorých patrí symetrické a asymetrické šifrovanie. Pri symetrickom šifrovaní je kľúč na zašifrovanie a dešifrovanie rovnaký. Druhá metóda je asymetrické šifrovanie, ktorá využíva dva odlišné kľúče. Jeden sa využije na zašifrovanie hodnoty, ktorý sa nazýva aj verejným kľúčom. Druhý kľúč sa využije na dešifrovanie, tzv. súkromný kľúč. (11) Na rozdiel od hashovania, ktoré sa využíva pre ukladanie hesiel v informačných systémoch, sa tieto šifry využívajú v softvéroch na správu hesiel.

[4] Výstup hashovacej funkcie – matematická funkcia – , ktorá mení text do komplexného reťazca znakov. Bez ohľadu na dĺžku vstupu má výstup konštantnú dĺžku pre danú hashovaciu funkciu.



Obrázok 1 Priebeh asymetrického zašifrovania dát (12)

1.4.2 Útoky vykonávané v online a offline režime

Cieľovou skupinou útočníkov pri online útokoch sú heslá, ktoré sú v autentizačnom systéme prístupné online. Typickým príkladom sú webové prihlasovacie formuláre ako napríklad účty emailových schránok, účty na sociálnych médiách alebo internet-bankingu. Tieto účty bývajú lepšie zabezpečené. Autentifikačný systém sleduje pokusy prihlásenia na identifikáciu podvodných akcií. Počet nesprávnych prihlasovacích pokusov je často limitovaný, čo vyvrcholí v zablokovaní účtu alebo zablokovaní IP adresy. Útočníci preto potrebujú VPN na zmeny svojich IP adries.

Offline útoky sú smerované hlavne na súbory alebo systémy, ktoré sú dostupné lokálne. Výnimkou nie sú ani súbory alebo programy stiahnuté z internetu alebo ukradnuté databázy, keďže samotný útok je vykonávaný v offline režime, čo zvýhodňuje pozíciu útočníka. Neexistuje žiaden limit neúspešných pokusov o prihlásenie. Takisto nie sú rýchlostné obmedzenia pri hádaní viacero hesiel. Avšak, niektoré systémy a správcovia hesiel majú zabudovanú metódu key stretching, ktorá spomaľuje proces útoku. V prípade prístupu k vysoko výkonným počítačom alebo niekoľkým počítačom napojených na seba, môžeme vyskúšať množstvo permutácií hesiel. Ako príklad si môžeme uviesť Elektronic Frontier Foundation, ktorá už v roku 1998 vytvorila počítač obsahujúca 1536 čipov a prehľadala 88 miliárd kľúčov za sekundu (13). Odvtedy sa výkon niekoľko násobne zvýšil. Podľa ARS Technica, jeden odborník na lámanie hesiel vytvoril počítačový klaster, ktorý prejde cez 350 miliárd pokusov za sekundu. (14)

Dictionary Attacks – Slovníkové útoky fungujú na princípe systematického výberu a zadávania slov zo slovníkov, ktoré sú skúšané do doby pokým sa nenájde správne heslo. Sú uskutočňované v offline, ale aj v online režime. Avšak slovníkové útoky v online režime môžu byť jednoducho zneškodnené v systéme nastavením limitu povolených nesprávnych pokusov. V offline režime sú tieto útoky stále účinné. Vhodným riešením je využitie správcov hesiel, ktoré obsahujú generátor hesiel. Vygenerované heslá sú kombináciou náhodných znakov, ktoré sa v slovníkoch zvyčajne nevyskytujú.

Brute-Force Attacks – Útoky hrubou silou sú zdĺhavé, keďže proces útoku zahŕňa pokusy miliónov hesiel, ale skúšajú kombinácie všetkých písmen, každého čísla a špeciálnych znakov, pokým sa heslo nenájde. V závislosti na výkonu počítača a entropii lámaného hesla

sa dá určiť celkový možný čas na prelomenie. (10) Použitím vysoko výkonných high-end počítačov môže proces lámania hesiel trvať výrazne kratšie.

Rainbow-tables – Naprostá väčšina hesiel je administrátormi uložená v hashovej forme. Ak útočník chce nájsť text alebo hashovú hodnotu, musí buď vypočítať hashovú hodnotu mnoho kombinácií alebo vopred vypočítať hashe miliárd heslových kombinácií a uložiť ich v dúhovej tabuľke za účelom nájdenia správneho hesla. Vytvorenie takýchto tabuliek trvá veľmi dlhý čas a využíva veľa miesta. Akonáhle má útočník zhotovené tabuľky, umožňuje mu rozlúsknuť heslá s nízkou entropiou v priebehu minút alebo i sekúnd. Podstatou dúhových útokov je využitie reťazcov hashových a redukčných funkcií (reduction funcion). Hashová funkcia zmapuje text do hashov a redukčná funkcia znižuje dĺžku hashových funkcií do fixnej hodnoty. (15)

1.5 Ochrana voči útokom

V súčasnej dobe neexistuje mechanizmus, ktorý by dokázal pokryť všetky požiadavky na ochranu. Preto sa bezpečnostné úrovne dosahujú kombináciou niekoľko nástrojov a metód.

Spomínali sme si využitie soli, ktorá zamedzí útočníkom využitie dúhových tabuliek pri snahe rozlúštenia veľkého množstva hesiel. Tieto útoky sú avšak stále účinné pri útoku na každý samostatný hash. Vysoko výkonné počítače s high-end grafickými kartami dokážu vypočítať miliardy hashov za sekundu, čo robia tieto útoky stále veľmi efektívnymi. Na zníženie efektivity môžeme použiť metódu key stretching, ktorá zvýši pracovnú záťaž útoku a heslo sa stáva viac odolné.

Pri hodnotení útoku alebo zneužitia informácií sa ukazuje, že najslabším článkom v celom systéme ochrany je ľudský faktor. Dá sa povedať, že najrizikovejším faktorom úniku informácií sú vlastní zamestnanci firmy. Odhaduje sa, že až 90 % prípadov porušenia ochrany informácií je spôsobené práve nimi. (16) Môže sa jednať o úmyselné činy alebo nedbanlivé správanie, ktoré zľahčuje prácu útočníka. Nášho názoru je preto dobrá prevencia vo forme nastavenia bezpečnostnej politiky tak aby zamestnanci využívali silné heslá, ktoré sú vo forme ľahšie zapamätateľných heslových fráz alebo, ktoré sú vytvorené spoľahlivým generátorom a uložené v správcovi hesiel. Taktiež systém ukladania hesiel v databáze by mal byť dostatočne bezpečný, tzn. neukladať heslá v plaintexte, ale využiť pomalé šifrovacie funkcie, a ktoré majú veľké pamäťové nároky.

1.6 Možné riešenia pre zjednodušenie správy hesiel v podnikovej sieti

Heslová únava je fenomén súčasnosti, ktorý postihuje zamestnancov vo väčšine firiem. Veľa podnikov má z tohto dôvodu tendenciu využívať nástroje, ktoré dokážu znížiť počet identifikátorov užívateľských účtov a hesiel, ktoré si zamestnanci musia pamätať. Do týchto riešení patria aj špecializované softvéry na správu hesiel, o ktorých si ale povieme v samostatnej kapitole. Následne si ukážeme dve tiež silne preferované metódy.

1.6.1 Heslová synchronizácia

Jedná sa o autentizačný proces, ktorý koordinuje užívateľské heslá naprieč niekoľko počítačových zariadení. Užívateľ sa následne môže pripojiť do zariadení použitím jedného hesla. Povedzme, že máme jeden Mac OS, jeden UNIX a jeden MS-DOS účet. Pomocou synchronizácie hesiel môžeme zmeniť všetky heslá naraz a určiť všetkým tú istú hodnotu. (17)

Využitie tejto platformy síce zjednodušuje proces prihlásenia do viacero zariadení, ale prichádza s ňou aj pár nedostatkov. Ak sa útočníkovi podarí získať prístup do jedného zariadenia, automaticky získa prístup do všetkých ostatných zariadení. Závažné prípady sú pri využití synchronizácie pri odlišných bezpečnostných požiadaviek systémov. Môže sa napríklad stať scenár, že útočník prenikne ľahko do systému s nízkym zabezpečením a následne využil údaje na prístup do vyššie zabezpečeného systému. Z tohto dôvodu je synchronizácie hesiel odporúčaná len v silne zabezpečených systémoch. (1)

1.6.2 Single sign-on technológie

Táto technológia umožňuje užívateľovi sa raz autentizovať a následne pripojiť do všetkých aplikácií, ktoré je užívateľ oprávnený využívať. Rozlišujeme dva užívané typy, ktorú sú Web SSO a Enterprise SSO.

1. **Web Single Sign-On (Web SSO)** – Táto metóda sa špecializuje primárne na webové aplikácie. Umožňuje prístup k webovým serverom, ktoré vyžadujú autentifikáciu. Keď sa užívateľ pokúsi o prístup do webovej aplikácie bežiacej na WebSSO, ten presmeruje prehliadač na autentizačný server, kde užívateľ vyplní loginy. Prehliadač je následne presmerovaný späť do požadovanej aplikácie, ku ktorej má užívateľ už prístup. V prípade, že užívateľ otvorí nové okno a spustí ďalšiu webovú aplikáciu bežiacej na WebSSO, prihlasovacie údaje sa automaticky načítajú. Nie je potreba opätovného zadania loginov. Nevýhodou tejto technológie je, že nie všetky aplikácie (hlavne proprietárny softvér) sa dajú modifikovať k účelu WebSSO prístupu. (18)

2. **Enterprise Single Sign-On (E-SSO)** – Taktiež nazývaný ako hostiteľský SSO je mechanizmus získania prístupu do rôznych nezávislých softvérových systémov použitím jedného loginu. Užívateľ sa prihlási do svojho E-SSO účtu, ktorý overí jeho identitu v centrálnom adresári alebo inej infraštruktúre. Užívateľ následne spustí aplikácie, ktoré sa mu zobrazia v menu E-SSO klientského softvéru. E-SSO načíta užívateľove prihlasovacie údaje z centrálnej databázy, spustí vybrané aplikácie a využije napríklad Windows scripting na zaslanie užívateľského ID a hesla do aplikácie. (19)

SSO sú technológie, ktoré sú momentálne podporované na vyriešenie rastúceho problému heslovej únavy (password fatigue). Umožňujú využívať jeden účet a zodpovedajúce heslo na prístup k jednotlivým účtom vo viac či menej transparentným spôsobom. Avšak, v praxi tieto technológie sú používané len na pripojenie do servisov v rámci domény príbuzných poskytovateľov servisov alebo balíčkov. SSO sú implementované typicky v rámci jednej organizácie alebo v rámci domény úzko spojených organizácií. Z politických, komerčných

a bezpečnostných dôvodov je to nemysliteľné, že všetci poskytovatelia servisov sa zlúčia do jednej domény alebo dokonca pár domén. (20)

Mnoho firiem však stále využíva tento systém na správu interných hesiel. Využívajú SSO od špecializovaných dodávateľov alebo cloudové zabezpečenie na správu prístupu svojich zamestnancov do online servisov. Jednou z najväčších bezpečnostných medzier riešení podnikovej triedy je, že nepokrývajú všetky účty zamestnancov, ktoré používajú k práci.

Za následok podnik necháva užívateľom na starosť aby spravovali svoje heslá na nepodporované zariadenia. Niektorí podstatní zamestnanci, ako napríklad tí zodpovední za administratívu, môžu mať mnoho účtov do niekoľko systémov. Andrew Howard, CTO Kudelski Security vraví, „*Nie je pre nás zvyčajné vidieť klientov kde admini majú 500 alebo 600 rôznych setov osobných údajov. Najhorší možný scenár pre mňa je, že využívajú to isté heslo na všetky aplikácie, a ak jedno heslo je odhalené, všetkých 600 systémov sú v ohrození napadnutia*“. (21)

2 Softvéry na správu hesiel

2.1 História hesiel a ich správa

Od zavedenia elektronických systémov, heslá boli využívané na zabezpečenie prístupu do prístroja len autorizovaným osobám. Jednalo sa o kombináciu písmen a čísiel určené užívateľom, také aké sa využívajú i v dnešnej dobe. Prvý heslový systém bol vytvorený v roku 1960 na MIT (Massachusetts Institute of Technology), keď výskumníci na univerzite vytvorili počítač s názvom CTSS. Každý užívateľ potreboval individuálne heslo na prístup do systému a čas používania bol meraný. Zaujímavým faktom je, že už v tom čase boli uskutočnené prvé útoky na heslo. Výskumník Allan Scheer využíval počítačový systém na MIT pre svoj výskum, ale mohol využiť len 4 hodiny týždenne. Následkom toho našiel spôsob ako vytlačiť listinu hesiel a prihlasoval sa pod inými účtami aby sa vyhol časovým limitom v systéme. (22) Veci sa moc nezmenili, čo sa týka hesiel, napriek zjavným nedostatkom s týmito autentifikačnými metódami. Našťastie sa vyvinula správa hesiel, ktorá lepšie zabezpečuje naše systémy.

Poznámkové bloky sú asi najjednoduchšou formou správy hesiel. Nedostatky hmotných poznámkových blokov sú, že sa môžu ľahko poškodiť, ukradnúť a stratiť. Často využívané Sticky notes umožňujú užívateľom vytvoriť poznámky použitím Post-it okien. Často je využívaný na zaznamenanie hesiel. Je to takisto problematické ako u fyzických poznámkových zošitov. Jak je okno otvorené je viditeľné pre okoloidúcich. Takýmto spôsobom môžu byť údaje pri nedbanlivosti vymazané, editované alebo ukradnuté. Avšak existujú už novšie verzie tohto programu, ktoré umožňujú zamknúť okno a nastaviť autentifikáciu na heslo. Podobnou formou sú súbory s koncovkou docx. a xlsx. Dôvod prečo nie sú odporúčané tieto súbory je vhodné si pripomenúť prípad útoku na Sony, kde útočníci len vyhľadali súbory s názvom passwords.doc. Týmto spôsobom získali cez 3000 rozličných súborov s uloženými heslami. (21) Posledným článkom sú špecializované softvéry na správu hesiel, ktoré prichádzajú popri samotnom spravovaní aj s radou funkcionalít, ktoré zmierňujú hrozby zo strany užívateľa a zo strany útočníka.

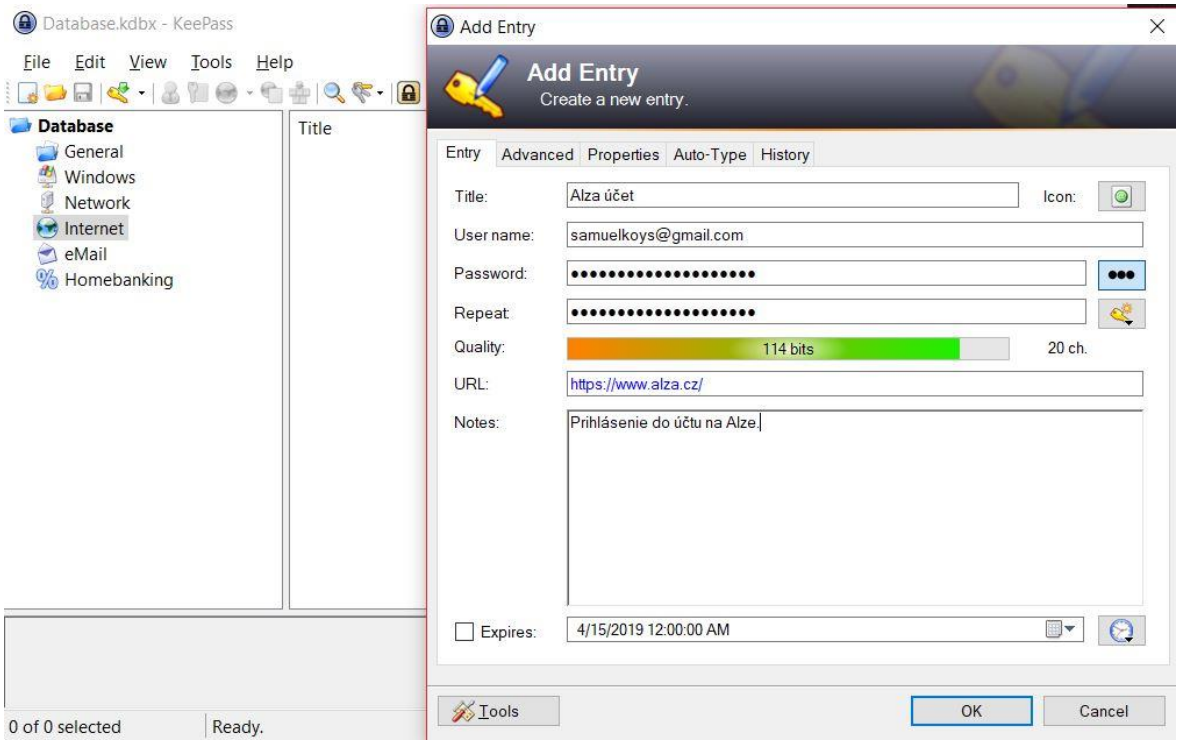
2.2 Typy správcov hesiel

Softvéry na správu hesiel umožňujú uchovávať užívateľské mená, heslá a iné formy citlivých informácii, napr. číslo účtu. Tento typ softvéru môže byť aj jednoduchá funkcia zabudovaná vo webových prehliadačoch na uchovávanie a automatické dopĺňanie uložených hesiel do prihlasovacích stránok. Alebo sa môže jednať o samostatne vyhradený softvérový nástroj na skladovanie a správu hesiel a prihlasovacích informácií. Tento typ softvéru môže poskytnúť užívateľské výhody, ale môže mať za následok vážne vystavenie bezpečnosti. (23)

Password manageri začali ako voľne dostupná nízkonákladová aplikácia pre spotrebiteľov, ktorých úlohou bola monitorovať heslá a prihlasovať do webstránok a aplikácií. Umožňovali

užívateľom vytvárať a spravovať dlhé, ťažko uhádnuteľné a unikátne heslá pre všetky účty. Väčšina funguje šifrovaním zoznamu hesiel jedným masterheslom, ktorý slúži ako ochrana pred neoprávneným prístupom. Existuje mnoho typov tejto technológie. Odlišujú sa spôsobom akým šifrujú informácie, úložným priestorom a doplňujúcimi funkciami typu automatického dopĺňania prihlasovacích údajov do formulára alebo generovaním unikátnych hesiel.

Lokálne inštalovaný softvér – Pri tomto type správy sú heslá ukladané lokálne na počítači. Tento typ softvéru ukladá login údaje v šifrovanom súbore alebo v databáze na hard disku počítača. Tieto aplikácie fungujú v offline režime a databáza hesiel je uložená nezávisle a lokálne na tom istom zariadení. Jedná sa o najstarší typ softvéru pre správu hesiel. Medzi najznámejších výrobcov patrí KeePass a Aurora.



Obrázok 2 Vytvorenie nového kľúča v softvéri Keepass2

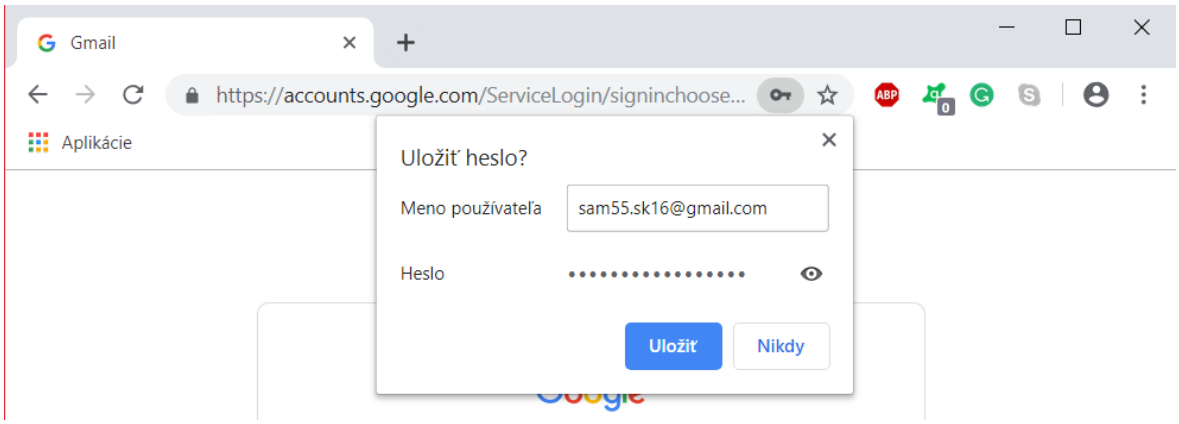
Prenosné zariadenia – Heslá sa uložia v súbore, ktorý je výstup z lokálneho správcu hesiel. Prenosné formy sú v podobe USB flash diskov alebo externých diskov. Ako výhodu môžeme označiť prenosnosť. K heslám je stály prístup pokiaľ je zariadenie u vlastníka. Niektoré typy umožňujú synchronizácia s cloudovou aplikáciou na zálohu hesiel v prípade straty zariadenia.

Obrázok 3 myIDkey USB drive na správu hesiel (24)

Vyššie spomenutý výrobok myIDkey prichádza taktiež s funkcionalitou zvukového vyhľadávania. Užívateľ prejde prstom po skeneri odtlačkov prstov, stlačí tlačidlo na spustenie zvukového vyhľadávania a povie účet, od ktorého chce heslo. (24)

Prehliadače – Fungujú na podobnom princípe ako desktop verzia, ale sú zabudované vo webovom prehliadači. Weboví správcovia umožňujú nenáročné spravovanie loginov, ale chýba im funkcionalita generovania náhodných a unikátnych hesiel pre každý účet, čo je prípadom u Edge, Firefox, Safari a Chrome prehliadačoch. Väčšina prehliadačov šifruje heslá, ktoré sú k dispozícii k nahliadnutiu po dodatočnej autentifikácii (napr. prihlásenie do Google účtu). Firefox je jedným z prehliadačov, ktorý zabezpečuje heslá v šifrovanom formáte ešte masterheslom, ktorý pridáva ďalšiu vrstvu ochrany. Google sa k tomuto vyjadril, prečo Chrome nezabezpečuje heslá masterheslom. Považuje túto praktiku ako falošný spôsob bezpečnosti, keďže nechráni pred rizikom neoprávneného prístupu k počítaču, ktorý útočník potrebuje aby prelomil masterheslo. (25)

Heslá sa dajú pridať do zoznamu pri otvorení stránky, zadania prihlasovacích údajov a následne po zobrazení vyskakovacieho okna môžeme potvrdením tlačidla uložiť prihlasovacie údaje do nášho správcu.



Obrázok 4 Vyskakovacie okno na uloženie hesla v prehliadači Google Chrome

Uloženie na cloude – V jednoduchosti môžeme tento typ pomenovať online password manager. Umožňuje prístup z ľubovoľného prehliadača, keďže heslá sú ukladané na cloude. Výhodou je prenosnosť a prístupnosť k heslám z ľubovoľného zariadenia. Nevýhodou je, že nemáme kontrolu nad ukladanými dátami. Spoliehame sa na bezpečnosť serveru a systému organizácie, keďže nemáme informácie o spôsobe šifrovania alebo hashovania hesiel v databáze. Najlepšie využitie má spomedzi užívateľov, ktorí majú viacero počítačových a mobilných zariadení s rozličnými operačnými systémami.

Zariadenia založené na tokenoch – Bezpečnostné tokeny sú formou správcov hesiel, pri ktorom lokálne prístupné hardvérové zariadenie (napr. smart karty, USB kľúč) sa použije na dodatočnú autentifikáciu užívateľa. Dáta v tokene bývajú väčšinou šifrované na zabránenie voľného čítania z neho. Táto forma správy je jedna z bezpečnejších variant, ale zároveň finančne náročnejšia. (26)

2.3 Výhody správcov hesiel

Účel a hlavné funkcie password managerov sme si už spomenuli. Následne si uvedieme výhody, ktoré zjednodušujú prácu užívateľa alebo sú iným spôsobom prínosné.

2.3.1 Náklady

Máme teraz na mysli časové náklady. Mnoho firiem čelí problému zaťaženosti IT oddelení, ktoré riešia na dennej báze množstvo incidentov vytvorenými zamestnancami. Častým prípadom sú incidenty typu zabudnutého hesla alebo neúspešnej autentizácie. Pomocou správcov hesiel sa tento problém dá zmierniť. Z dôvodu nižšieho čísla incidentov sa zníži zaťaženosť pracovníkov helpdesku.

Z finančného hľadiska je výška nákladov na password manageroch rôzna. Cena sa odvíja v závislosti na potrebách užívateľa alebo firmy. Výrobcovia ponúkajú licencie samostatným užívateľom, ale aj balíčky, ktoré preferujú skôr firmy. Taktiež mnoho z nich poskytujú trial verziu, ktorá je zdarma. Potenciálnym zákazníkom to dáva možnosť otestovať jednotlivé produkty a vybrať najvhodnejšie riešenie.

2.3.2 Zmiernenie heslovej únavy

Ako sme si spomenuli v prvej kapitole, kvôli veľkému počtu využívaných hesiel dostávajú užívatelia tzv. heslovú únavu. Majú tendenciu uľahčovať si proces vytvárania hesiel. Pomocou password managerov nie je potreba pamätať si prihlasovacie údaje. Nemôžeme to síce zovšeobecniť na všetky typy správcov hesiel, ale väčšina správcov má nástroj, ktorý umožňuje vygenerovať náhodné heslá, ktoré sú unikátne a dostatočne silné v závislosti na nastavených kritériách. Užívateľ preto nemusí strácať čas vymýšľaním hesla splňujúce všetky náležitosti. Mnoho kritérií na vygenerovanie sú customizovateľné (dĺžka hesla, komplexnosť). Častokrát býva zabudovaná i funkcia na meranie sily hesla.

2.3.3 Automatické doplňovanie

Správcovia hesiel majú funkcionalitu, ktorou dokážu automaticky vyplniť heslá do prihlasovacieho poľa. V závislosti na typu softvéru môžu byť údaje doplnené už pri otvorení stránky alebo privolaním okna, kde zadáme príkaz na doplnenie prihlasovacích údajov. Automatické doplňovanie do login formulára minimalizuje chybné zadanie údajov užívateľom a taktiež ochraňuje systém pred útočníckou metódou keylogging[5]. Nakoľko tu môžeme z užívateľského hľadiska vravieť o výhode, existujú spôsoby, pomocou ktorých môže byť automatické doplňovanie pri otvorení stránky zneužité útočníkmi (pozri oddiel 2.4.2).

2.3.4 Úschova dôverných dát

Popri správe hesiel umožňuje softvér uschovať dôverne informácie. Môže sa jednať o čísla kreditných kariet a ich PIN kódy, heslá na pripojenie do Wi-Fi siete, bezpečnostné otázky s odpoveďami pre rôzne účty, atď.

2.4 Nedostatky správcov hesiel

U password manageroch môžeme vravieť o užitočnom softvéri, ktorý zjednodušuje prácu užívateľa a zmierňuje mnoho hrozieb. Lenže ani táto aplikácia nie je bezchybná. Následne si uvedieme možné prípady, ktoré sú spojené s užívaním password managerov.

2.4.1 Strata masterpasswordu

V prípade straty hesla na prístup do password manageru, stratíme zároveň prístup ku všetkým heslám na využívané účty. Masterheslo nie je prenášané cez internet, neukladá sa lokálne a nie je známe ani samotnému výrobcovi softvéru. Mnohí výrobcovia neukladajú masterheslo z bezpečnostných dôvodov. Niektorí výrobcovia ale umožňujú obnovu použitím Touch ID alebo Face ID.

[5] Softvér, ktorý sníma stisky jednotlivých kláves. Vyskytuje sa taktiež v hardwarovej forme.

Existujú verzie password managerov, ktoré poskytujú funkcionalitu obnovy hesla. Všeobecne sa ale neodporúča tento krok v prípade straty masterhesla vykonať. Útočník môže byť schopný pomocou nástroja na obnovu hesla zistiť skutočné masterheslo.

2.4.2 Opatrnosť pri autologine

Existuje veľa typov správcov hesiel, ale všetky majú ten istý účel použitia. Najskôr užívateľ navštívi stránku a manuálne zadá prihlasovacie údaje a rozhodne sa uložiť ich v správcovi hesiel. Pri ďalšej návšteve stránky password manager môže automaticky vyplniť prihlasovacie údaje vo formulári, čo môže v niektorých prípadoch predstavovať hrozbu.

Automatické dopĺňanie môže prebehnúť v dvomi rozličnými spôsobmi:

1. Manuálne dopĺňanie – prihlasovací formulár je prázdny keď je stránka načítaná. Užívateľ musí uskutočniť nejakú formu interakcie, ktorá vyplní formulár. Môže sa jednať o kliknutie myšou alebo o klávesovú skratku. Podstatnou vecou je, že užívateľ musí uskutočniť akciu na vyplnenie formulára.

2. Automatické dopĺňanie – na rozdiel od manuálneho dopĺňania formulár je vyplnený akonáhle sa stránka načíta. Žiadna interakcia užívateľa nie je potrebná. Jedná sa o bežný spôsob používaný v mnohých správcoch hesiel.

Nevýhody automatického dopĺňania

- Prípad, keď JavaScript zmení form action po vyplnení formulára. Nie je bezpečné vyplniť formulár. Avšak mnoho ďalších správcov hesiel v tomto prípade povolí vyplnenie (Firefox, Chrome, Lastpass 2.0) i keď sa zmenil form action. Odzrkadľuje to viac obecný trend medzi správcami hesiel, že sa prestanú zaujímať o bezpečie formulára v momente keď je vyplnený.

- Varovanie pred nedôveryhodnou stránkou – Užívateľ dostane chybové hlásenie, že certifikát nie je dôveryhodný. Možnosťou je pokračovať napriek tomu alebo ísť naspäť do bezpečného módu. V žiadnom prípade nie je bezpečné v tomto prípade nechať správcu hesiel vyplniť takéto pole, pretože to vystavuje formulár škodlivému JavaScriptu.

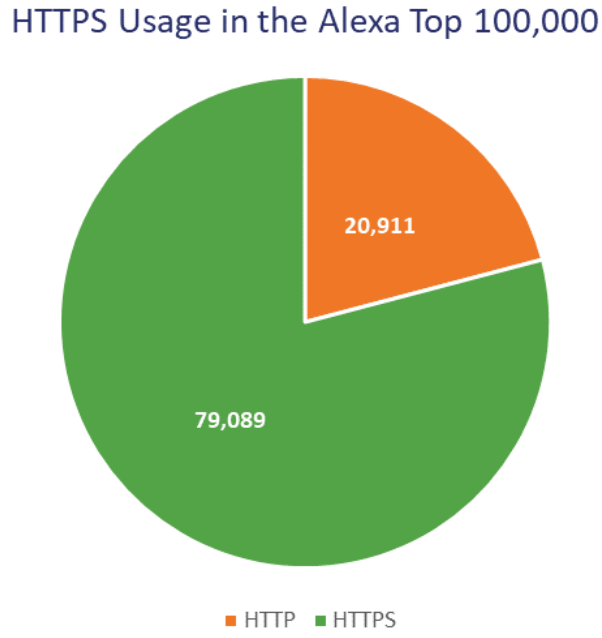
2.4.3 Sweep attacks

Druh útoku, ktorý môže zneužiť automatické dopĺňanie hesiel ukradnutím hesiel bez interakcie užívateľa. Lepšie si to ukážeme na nasledujúcom príklade.

Nachádzame sa v kaviarni a dostaneme chuť si objednať jedlo. Rozhodneme sa využiť WiFi sieť kaviarne a pripojíme sa na papajohns.com, kde objednáme jedlo aby dorazilo na našu adresu. Avšak, WiFi sieť je kontrolovaná útočníkom, ktorý chce ukradnúť užívateľovi heslo do AT&T účtu. Jedná sa o presmerovaný sweep attack. Funguje následovne:

Náš prehliadač zašle GET žiadosť na stránku papajohns.com. Stránka papajohns.com je bežná HTTP stránka, čo umožňuje útočníkovi zachytiť žiadosť a odpovie presmerovaním na att.com. Náš prehliadač následne načíta att.com, server odpovie a tu narážame na prvý problém. Prihlasovacia stránka AT&T sa zobrazuje ako bežná HTTP stránka tiež. To znamená, že to je triviálne pre útočníka vložiť škodlivý JavaScript do odpovede, ktorý má niekoľko vlastností. Môže interpretovať stránku ako neviditeľnú, takže užívateľovi sa zobrazí prázdna stránka. Ale nášmu správcovi hesiel to posiela správu, že sa nachádzame na prihlasovacej stránke att.com. Škodlivý JavaScript môže následne ukradnúť formulár jeho prečítaním a následne ho zaslať útočníkovi. Akonáhle je heslo ukradnuté môže útočník presmerovať prehliadač späť na originálnu stránku, ktorá je papajohns.com. Celý útok zabral pár sekúnd a užívateľ si je nevedomý, že mu bolo ukradnuté heslo.

Tento určitý typ útoku využíva fakt, že niektoré stránky s prihlasovacím formulárom bežia na bežnom HTTP. Vykonáva to napriek faktu, že potvrdzuje prihlasovací formulár cez HTTPS. Z vrchných 100 000 stránok za tretí štvrťrok 2018 podľa portálu Alexa, až 20,9 % využíva HTTP pre načítanie prihlasovacej stránky. Medzi známe mená na tomto zozname patria bbc.com, alibaba.com a wikia.com. (27)



Graf 2 Využitie HTTPS u vrchných 100 000 stránok (27)

Ochrana proti Sweep attacks

1. Manuálne dopĺňanie – Pri automatickom dopĺňaní je problém, keďže zadáva údaje bez interakcie užívateľa. To znamená, že vystavuje heslo v čistom texte. Preto sa odporúča využívať manuálne dopĺňanie v prípade, keď užívateľ explicitne interaguje so stránkou. K tomuto pristupuje pár password managerov (1Password, KeePass a Keeper). Môže sa zdať, že manuálne vypĺňanie je menej pohodlné ako automatické. Avšak, aj pri automatickom vypĺňaní užívateľ musí stále interagovať so stránkou.

2. Bezpečné dopĺňanie (Secure filling) – zabezpečujú správcov hesiel viac ako manuálne dopĺňanie hesla. Funguje na dvoch základnych princípoch: nechce nechať JavaScript čítať automaticky doplnené heslá. Akonáhle password manager doplní heslo je nečitateľné pre JavaScript. Ďalším princípom je nenechať správcu hesiel potvrdiť formulár bez potvrdenia, že akcia je zhodná s akcia v momente keď heslo bolo uložené. To zabraňuje útočníkovi ukradnúť heslo zmenou form action v HTML kóde. Samozrejme aby tento krok bol účinný, stránka musí potvrdiť prihlasovací formulár použitím HTTPS, aby útočník nemohol prečítať heslo priamo zo siete.

Obmedzenia

Secure filling nie je kompatibilný so stránkami, ktoré využívajú AJAX na potvrdenie prihlasovacieho formulára. Nepredstavuje to ale veľký problém, pretože sa tomu dá predísť. Prihlasovacie formuláre sa môžu vložiť do iFrame-ov. Prehliadače môžu implementovať SendPwd API, ktoré dovoľuje JavaScriptu zadať heslo bez toho aby sa samotné heslo prečítalo. (28)

2.4.4 Odhalené heslá v pamäti počítača

Táto chyba bola nájdená bezpečnostným poradenstvom ISE (Independent Security Evaluators). ISE vyspovedala popredných poskytovateľov softvérov na správu hesiel. Konkrétne sa jedná o výrobcov 1Password, Dashlane, KeePass a LastPass. Problém spočíva v nefunkčnosti „lock“ tlačidla softvérov. Niektoré heslá boli vystavené v pamäti počítača napriek tomu, že aplikácie boli v „zamknutom“ móde. 1Password mal dokonca chybu, ktorá pri určitých krokoch užívateľa môže nechať masterheslo v pamäti počítača uložené v plaintexte. Šéf ochrany proti útokom pre 1Password Jeffrey Goldberg sa k tomu vyjadril: „Aby mohol útočník nahliadnuť do pamäti počítača musel by útočník fyzicky sedieť za počítačom alebo donútiť užívateľa stiahnuť škodlivý softvér. Preto je reálna hrozba limitovaná. Útočník, ktorý je v pozícii ťažiť z informácie v pamäti počítača sa nachádza už v mocnej pozícii. Žiaden password manager nemôže bežať bezpečne na kompromitovanom zariadení“. Spoločnosti a výskumníci sa zhodli na tom, že problém s únikom informácii v pamäti sa nedá vyriešiť bez zásadných zmien v operačných systémoch. (29)

2.5 Prípad kybernetického útoku na správcu hesiel

Ani najlepší password manageri sa nevyhnú „faux pas“ ak dáta miliónov užívateľov sa stanú kompromitované. Za posledné roky bolo zaznamenaných pár útokov na dáta poskytovateľov správcov hesiel. Asi najviac diskutovaným útokom je nasledujúci prípad.

OneLogin je podobný bežnému správcovi hesiel, ale taktiež spravuje identity a prihlasovacie údaje mnohých podnikových a korporátnych užívateľov (napr. nemocníc, právnických firiem a redakcií). Funguje ako centrálny bod, ktorý umožňuje svojim zákazníkom prístup do svojich účtov. 31. mája 2017 správca identít OneLogin Alvaro Hoyos upozornil svojich

užívateľov na svojom blogu, že sa vyskytol neautorizovaný prístup do databázy v ich regióne. Útočník získal a použil AWS (Amazon Web Services) kľúče od jedného hostiteľa aby sa dostal do rozhrania AWS. Skrz užívateľské rozhranie AWS, útočník vytvoril niekoľko inštancií, ktorými získaval informácie z infraštruktúry. Útočníkovi sa podarilo získať databázové tabuľky, ktoré obsahovali informácie užívateľov, aplikácií a rôznych kľúčov. Nakoľko OneLogin šifrovala určité dáta, nemohli vylúčiť možnosť, že vzhľadom k veľkému počtu dát mohol útočník získal spôsob ako dešifrovať dáta. (30)

3 Návrh zavedenia správy hesiel vo firme Bluelink International CZ

Bluelink je medzinárodná korporátna spoločnosť patriaca skupine Air France – KLM group. Medzi hlavné činnosti firmy patria služby poskytovania zákazníckej podpory. Špecializuje sa primárne na transportný sektor, zdravie, turizmus, kultúru a voľný čas. Bluelink ponúka multimediálne služby v 18 jazykoch, medzi ktoré patria služby typu consultingu, vedenia, správa sťažností, webová podpora, rezervácií a predaj. Firma bola založená v roku 2003, kde začínalo 40 zamestnancov. Momentálne firma zamestnáva okolo 500 ľudí z 50 rôznych krajín sveta.

3.1 Aktuálna situácia v podniku

Politika hesiel je nastavená podľa požiadaviek certifikácie PCI-DSS[6]. Pre všetky využívané softvéry je potrebné dodržovať tieto štandardy. Novovytvorené heslo musí byť aspoň 8 znakov dlhé a musí spĺňať aspoň tri zo štyroch požiadaviek. Medzi požiadavky patrí veľké písmeno, malé písmeno, číslica a špeciálny znak. Heslá je potrebné každé tri mesiace meniť. Staré alebo obmenené heslá sú uložené v archíve, ktoré porovnaním s novým zadaným heslom, slúžia k zabráneniu užívateľovi zadať heslo, ktoré už jedenkrát použil. U softvéru, ktorý uchováva citlivé dáta sú požiadavky na nastavenie hesla komplexnejšie. Ako príklad si môžeme uviesť softvér NICE, ktorý slúži na zaznamenanie a správu interakčných dát so zákazníkmi z rôznych kanálov na jednom mieste.

Kde to okolnosti dovoľujú, sa firma snaží napojiť aplikácie na SSO. Momentálne je technológia SSO zavedená u 70 % aplikácií, napríklad aj na prístup do Office 365 – balík služieb a kancelárskeho softwaru. Pri ostatných aplikáciách už firma necháva zodpovednosť na zamestnancoch spravovať heslá. Následkom toho je už často spomínaná heslová únava. Častým prípadom je zabudnuté heslo do Windows účtu zamestnancov. V priemere 15 krát do mesiaca rieši helpdesk reset týchto hesiel. U väčšiny aplikácií v prípade zabudnutého hesla existuje možnosť zaslať žiadosť o obnovenie hesla prostredníctvom emailu. U softvéroch, kde táto možnosť nie je alebo aktivácia neprebehla úspešne, zamestnanec musí vytvoriť tiket cez tiketovací systém SysAid.

Ku konci tejto časti chceme zdôrazniť, že PCI-DSS platí pre všetky organizácie, ktoré prijímajú, spravujú a ukladajú informácie kreditných kariet. Čiže naša sledovaná firma je povinná dodržovať tieto štandardy napriek tomu, že v niektorých ohľadoch nie je v súlade s normami NIST.

[6] Payment Card Industry Data Security Standard je metodika navrhnutá skupinou Visa, MasterCard a American Express. Framework vychádza z noriem rady ISO 27000.

3.2 Podnety k zavedeniu

Pomerne často počujeme ako ďalšia spoločnosť alebo organizácia sa stala obeťou kybernetického útoku. Vieme, že kyberzločinci sú viac vytrvalí a my musíme byť viac obozretní, čo sa týka ochrany našich informácií. V osobnom živote zodpovedáme len za vlastnú bezpečnosť, ale na pracovisku za bezpečnosť celej firmy.

Faktom je, že zamestnanci predstavujú dôležitú rolu, čo sa týka ochrany firemných dát. Nedbanlivosťou alebo nepozornosťou môže zamestnanec spôsobiť nemalú škodu. Nedávna štúdia globálneho poradenstva Willis Towers Watson zistila, že 90 percent incidentov sú výsledkom ľudskej chyby alebo ľudského správania. Následkom týchto zistení bol spustený tzv. Prieskum kyberkultúry (Cyber Risk Culture Survey). Tento nástroj má odhaliť najrizikovejšie miesta vo firme, ako napr. sledovanie rozsahu rizika prítomná v správaní ľudí, určiť metódy ako zmierniť tento faktor a vytvoriť kompetentnú pracovnú silu. Anthony Dagostino, vedúci Willis Towers Watson poznamenal, *„Nakoľko technológia hrá dôležitú úlohu, musí byť prepojená so schopnosťami ľudského chápania. Pravdou je, že únik dát bude skôr zavinený zamestnancom, ktorý nechá prenosný počítač vo vlaku ako by ho zavinil škodlivý kriminálny útok. Veríme, že zamestnanci a spoločnosti so silnou politikou a uvedomelou pracovnou silou sú prvou líniou ochrany proti kyberútokom.“* (31)

Na základe vykonaného rozboru situácie v sledovanej firme, môžeme pozorovať, že sa podnik snaží vytvoriť, čo najvhodnejšie pracovné podmienky pre zamestnanca. Avšak keďže za daných okolností nie je možné SSO napojiť na všetky aplikácie, je zamestnancom prenechaná zodpovednosť spravovať zvyšné využívané heslá. Z tohto dôvodu je implementácia špecializovaného softvéru na správu hesiel opodstatnená.

3.3 Predpoklady k zavedeniu softvéru

V nasledujúcej časti si popíšeme akými procesmi je potrebné prejsť k úspešnému zavedeniu. Prvým krokom je vytvoriť návrh obsahujúci náležité informácie, ktoré splňujú požiadavky. Zohľadní sa či je nový systém užitočnejší než súčasný systém. Chceme zistiť či implementácia bude vyhodnotená ako výhodná investícia.

Software prechádza interným schvaľovacím procesom cez ticketing system a odsúhlasením poverenými osobami podľa IT Charteru. Pokiaľ sú zúčastnené strany s návrhom spokojní, môžeme sa presunúť k samotnému testovaniu produktu. Počas modelovej situácie je potrebné otestovať funkcionality – vytvorenie účtov, generovanie hesiel, atď. Následne sa spíšu manuály, ktoré obsahujú náležitosti k správnej funkčnosti softvéru. Samotné zavedenie je vykonané administrátormi.

Dôležitým procesom je oboznámiť zamestnancov o správnom užívaní aplikácie. Po konzultácii s administrátorom sme dospeli k záveru, že vzhľadom k náročnosti užívania softvéru by samotné školenie pracovníkov nebolo potrebné. Postačilo by vytvorenie inštruktážneho manuálu alebo videa, v ktorom by sa ukázali najhlavnejšie funkcie softwaru – ako zmeniť súčasné heslá a vygenerovať nové heslá, ako pridať nové údaje do zoznamu.

3.4 Kritéria pre výber softvéru

V nasledujúcej časti si uvedieme kritéria, ktoré budeme zohľadňovať pri výbere softvéru. Navrhnutý súbor kritérií sme vytvorili na základe teoretických poznatkov o správe hesiel a po zhodnotení niekoľko vyjadrení systémových administrátorov.

Prístup k účtu možný len z firemného prostredia

Vo firemnom prostredí sa nachádzajú všetky aplikácie, systémy a podporné systémy, ktoré pracovníci využívajú na vykonania podnikových procesov. Prístup do tohto prostredia je obmedzený len autorizovaným osobám. Výnimka nesmie byť ani v prípade zavedenia nového softvéru. Preto musí softvér, ktorý hľadáme, umožniť nastavenie prístupu.

Jedno masterheslo

U tohto kritéria chceme určiť či bude správca hesiel voľne prístupný po prihlásení do pracovného účtu alebo sa vyžaduje dodatočná autentizácia. Jednou možnosťou je synchronizovať Windows heslo s heslom pre lokálneho alebo cloudového správcu hesiel, aby sa zabránilo využitie masterhesla. Menším nedostatkom tohto riešenia je fakt, že kto získa prístup k Windows účtu automaticky získa prístup ku všetkému využívanému softvéru. Práve preto hľadáme produkt, ktorý je zabezpečený masterheslom.

Nenáročná údržba

Týmto kritériom je myslená jednoduchosť obsluhy užívateľského rozhrania . Vo firme je častá fluktuácia zamestnancov (približne 10 ľudí mesačne). Preto by mali byť funkcie vytvorenia nového záznamu v prípade prijatia nového zamestnanca do firmy a funkcia zmazania záznamu, nenáročné na uskutočnenie. Možnosť odstránenia záznamu – v prípade ak zamestnanec opustí firmu – zo systému je nevyhnutná.

Logovanie aktivít

Pokiaľ sa jedná o databázu, kde sú uložené dáta viacero ľudí, sú tieto auditné záznamy nevyhnutnou potrebou. Účelom tejto funkcionality je umožniť administrátorom lepšie merať narábanie s heslami zamestnancov a detailne sledovať aktivity naprieč celou organizáciou. Tieto reporty môžu byť užitočné, ktoré pomôžu administrátorom spozorovať potenciálne problémy. Napríklad spozorujeme podozrivú históriu prihlasovania do systému alebo sa nájdu slabé heslá, ktoré potrebujú byť nahradené.

Šifrovanie

Chceme sa ubezpečiť aby password manager uložené heslá v databáze šifroval dostatočne silnou šifrou. Ak by sa útočníkovi podarilo ukradnúť databázu, mala by byť doba prelomenia šifry, čo najdlhšia. Šifrovacia metóda by mala vytvoriť kľúče dostatočne dlhé, ale zároveň to nemôže výrazne spomaľovať rýchlosť procesu.

Lokalita serverov

Nezanedbateľným bodom je aj zistiť dôveryhodnosť organizácie, ktorá poskytuje služby správy hesiel. Zaujíma nás kde uchovávajú dáta a či servery vlastnia alebo zverujú ich tretím stranám. Ak má spoločnosť prenajaté dátové centrum, stávajú sa naše informácie viac zraniteľné. Takisto treba zohľadniť sídlo krajiny, keďže rôzne krajiny majú iné zákony. Ideálne by bolo vybrať krajinu, kde zákony nie sú príliš obmedzujúce. Krajiny so striktnými zákonmi sú USA, Veľká Británia, Kanada, Austrália a Nový Zéland, kde dovoľujú zákonodarcom vydať záruky na získanie užívateľových informácií od spoločností na správu hesiel alebo poskytovanie VPN.

Aktualizácie

Zaujíma nás v akých intervaloch sú poskytované aktualizácie produktu. Takisto chceme vedieť či ich môžeme manuálne potvrdiť alebo budú automaticky prevedené.

Podpora platformy

Týmto kritériom sa chceme ubezpečiť, že daný softvér je kompatibilný na využívaných zariadeniach. Vo firme sa prevažne využívajú operačné systémy Windows 7 a Windows 10.

Nastavenie vlastnej politiky na heslá

Produkt musí umožniť nastavenie kritérií na heslá užívateľov.

Cena

Pri tomto kritériu nás zaujímajú licenčné podmienky firmy, ktorá produkt ponúka. To znamená, na základe čoho sa odvíja cena produktu. Pre našu sledovanú firmu sme pred analýzou trhu produktov nedokázali určiť, v akej výške by sa mali náklady pohybovať. Toto kritérium by sa následne riešilo v schvaľovacom procese. Momentálne sú terajšie náklady nulové. Firma preto posúdi či investovaná čiastka bude mať dostatočne vysokú pridanú hodnotu.

3.5 Analýza trhu

V tejto časti sme uskutočnili analýzu dostupných produktov na trhu, ktoré poskytujú služby správy hesiel pre firemné prostredie. Informácie o produktoch boli nájdené na oficiálnych stránkach poskytovateľov a emailovou komunikáciou s pracovníkmi daných firiem.

Na začiatok sme vyčlenili produkty podľa typu softwarovej licencie. Prvým typom je voľne dostupný softvér (napr. všeobecná verejná licencia GNU) a druhým typom je proprietárny softvér[7]. Open Source produkty sa ukázali byť nevhodným typom na porovnávanie, keďže

[7] Softvér, ktorý je licenciou alebo iným spôsobom upravený k jeho používaniu. Má obmedzenia používania a kopírovania. Zdrojové kódy spravidla nie sú k dispozícii.

nesplňovali väčšinu požiadaviek (podpora platformy, audit log). Preto sme zamietli produkty ako je napríklad KeePass a jeho verzie (KeePassX a KeePassXC), ktorý je určený pre single users a nedisponuje napríklad nastaveniami práv alebo audit logom. Medzi voľne dostupné produkty, ktoré sa dostali do ďalšieho kola patrí Bitwarden, Zoho Vault a Psono. U týchto produktoch je avšak Enterprise verzia spoplatnená.

Množstvo ďalších produktov sme vopred museli zamietnuť z dôvodu nenájdenia dostatočných informácií o produktoch na webstránke poskytovateľa či neúspešnej komunikácie so zamestnancami spoločností. Do tejto skupiny patria nasledovné spoločnosti: TeamID, Hypervault, Pleasant Solutions, Password Manager Pro, Thycotic, LastPass, Splikity a Keeper Security.

Do užšieho zoznamu sme vybrali nasledovných 6 produktov, ku ktorým si bližšie popíšeme sledované kritéria v samostatných sekciách:

1. Produkt 1Password
2. Zoho Vault
3. Psono
4. Dashlane
5. Passwork
6. Bitwarden

U všetkých vybraných produktoch je pre vstup do aplikácie povinné zadať masterheslo, preto nebudeme toto kritérium ďalej bližšie popisovať. Takisto funkcionalita vytvorenia nového záznamu a vymazania starého záznamu je zabudovaná v každom produkte. Prehľad ostatných funkcionalít vybraných produktov je k dispozícii v prílohe A.

3.5.1 Produkt 1Password

Prístup k účtu len z firemného prostredia – 1Password má funkcionalitu zamedziť určité skupiny účtov k určitým zariadeniam. Napríklad, môžeme skupine s názvom „HR“ nastaviť prístup užívateľom len pomocou desktopových zariadení, ale zamedziť prístup pomocou telefónov. Táto vlastnosť sa volá App Access. Po kontakte s pracovníkom obchodného tímu mi bolo povedané, že firma zvažuje implementáciu vlastnosti, ktorá umožní nainštalovať 1Password na zariadenia s určitou IP adresou alebo rozpätie adries.

Šifrovanie – Využíva sa tu model End-to-end šifrovania. Dáta sú ukladané 256 bitovou šifrou AES-GCM-256. PBKDF2 využívajú na odvodenie šifrovacieho kľúča z masterhesla. Masterheslo šifrované touto metódou môže trvať dekády na dešifrovanie.

Logovanie aktivít – Softvér má možnosť vytvoriť reporty administrátorom. Report aktivít umožňuje sledovať všetky zmeny, ktoré sa vyskytli v jednotlivých účtoch. Táto funkcionalita je dostupná len v balíčku 1Password Business.

Aktualizácie – Na pravidelnej báze vychádzajú aktualizácie, ktoré sa dajú stiahnuť z App Storu pri použití iOS alebo z Google Play pre Android. Podstatné zmeny sa uskutočňujú raz ročne.

Lokalita serveru – Momentálne majú 3 lokality serverov. Všetky 1Password.com účty majú servery v Amerike. 1Password.ca má servery v Kanade a 1Password.eu účty má servery v Európe.

Podpora platformy – Aplikácia je podporovaná na zariadeniach Windows, macOS, iOS a Android. Taktiež je možnosť využiť 1Password X pre užívateľov Linuxu.

Možnosť nastavenia požiadaviek na heslo – Aplikácia neumožňuje nastavenie vlastných požiadaviek sily hesla.

Cena – Predajca ponúka dve možnosti licencovania produktu pre väčšie firmy.

1. 1Password Teams – poplatok 3,99 USD mesačne na užívateľa
2. 1Password Business – poplatok 7,99 USD mesačne na užívateľa

V závislosti na počte užívateľov sú poskytované zľavy. Pre 500 členný tím môže predajca ponúknuť zľavu vo výške 10 % pre možnosť 1Password Teams a zľavu vo výške 25 % pre možnosť 1Password Business. (32)

3.5.2 Zoho Vault

Prístup k účtu len z firemného prostredia – Je možné nastaviť obmedzenie užívania na konkrétnu IP adresu. Táto vlastnosť umožňuje užívateľom pristupovať k správcovi hesiel len z podnikovej siete. Možnosť zakázania prístupu na určité zariadenie nie je zabudovaná.

Šifrovanie – Produkt využíva funkciu PBKDF2 na odvodenie kľúča z masterhesla a AES 256 bitové šifrovanie na zabezpečenie dát. Všetky dáta sú zašifrované na strane klienta a iba šifrované dáta sú uložené na serverovej strane.

Logovanie aktivít – Všetky aktivity vykonané v Zoho Vault sú sledované a ukladané ako audit trail. Tento report obsahuje detaily v akom čase sa prihlásila osoba na konkrétny účet.

Aktualizácie – Keďže sa jedná o online poskytovateľa správy hesiel, všetky aktualizácie sú automaticky vsunuté, ktoré nemajú dopad na službu.

Lokalita serveru – Predajca má niekoľko dátových centier. V závislosti na doméne, na ktorú využijeme na prihlásenie sa uložia naše dáta k určitému regiónu. Zoho.com má servery v USA, zoho.eu má servery v Európe a zoho.in ich má v Indii.

Podpora platformy – Jedná sa o online password manager. Užívatelia sa môžu pripojiť na ktorékoľvek zariadenie pri použití prehliadaču ako je Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, atď.

Možnosť nastavenia požiadaviek na heslo – Produkt umožňuje definovať požiadavky na heslo a vynútiť ich pre všetkých užívateľov.

Cena – Náklady na produkt sa odvíjajú v závislosti na vybranom balíčku. Z nájdených balíčkov, ktoré splňujú kritéria sme našli nasledovné verzie:

1. Professional – poplatok 3,6 EUR mesačne na užívateľa.
2. Enterprise – poplatok 6,3 EUR mesačne na užívateľa. Ponúka SSO pre cloudové aplikácie, integráciu s Active Directory a ďalšie. (33)

3.5.3 Psono

Prístup k účtu len z firemného prostredia – Úložisko serverov by bolo v podnikovej sieti, v ktorej môžeme nastaviť obmedzenia. Prístup sa dá obmedziť nastavením na konkrétnu IP adresu.

Šifrovanie – Dáta sú ukladané niekoľkými vrstvami šifrovania a hashovania. Na strane klienta sa na autentizačné šifrovanie využíva šifra Salsa20[8], funkcia Poly1305[9] a eliptická krivka Curve25519[10].

Logovanie aktivít – Audit log je súčasťou Enterprise verzie.

Aktualizácie – Produkt poskytuje aktualizácie na mesačnej báze. Väčšinou sa jedná o úpravu rozhrania bez väčšieho narušenia služby.

Lokalita serveru – Celá infraštruktúra firmy je umiestnená vo Frankfurte nad Mohanom v datacentrách Googlu.

Podpora platformy – Jedná sa o online aplikáciu, čiže produkt nie je závislý na platforme. Je podporovaná na všetkých operačných systémoch, na ktorých beží Chrome alebo Firefox.

Možnosť nastavenia požiadaviek na heslo – Firma Bluelink, pre ktorú hľadáme softvér využíva LDAP[11], ktorú môžeme napojiť na Psono. LDAP poskytovateľ umožní nastaviť vlastnú politiku, napr. entropiu hesla, komplexnosť a životnosť.

Cena – Enterprise edícia pre väčšie spoločnosti (min. 25 užívateľov) stojí 2 EUR na užívateľa mesačne. (34)

---

[8] Prúdová šifra, ktorej základom je pseudonáhodna funkcia, ktorá prijíma na vstupu kľúč s veľkosťou 256 bitov a jednorazovú hodnotu s veľkosťou 64 bitov.
[9] MAC (message authentication code) funkcia určená k overeniu integrity dát a autentizácii správy.
[10] Eliptická krivka pre Diffieho-Hellmanovú výmenu kľúčov nad eliptickou krivkou v prostredí internetu. Jedná sa o šifrovací protokol, ktorý umožňuje dvom stranám, ktoré sa nikdy nestretli, zdieľať informácie na nechránenom komunikačnom kanáli.
[11] Lightweight Directory Access Protocol – definovaný protokol pre ukladanie a prístup k dátam na adresárovom serveri. Jednotlivé položky sú na serveri ukladané formou záznamov.

3.5.4 Dashlane

Prístup k účtu len z firemného prostredia – Produkt neponúka možnosť nastavenia tejto vlastnosti.

Šifrovanie – Predtým ako sa dáta uložia lokálne alebo na servery Dashlanu, všetky dáta sú zašifrované pomocou unikátneho kľúča, ktorý je odvodený z užívateľovho masterhesla. Dashlane šifruje všetky dáta použitím AES-256 šifry a poskytuje rôzne možnosti funkcií pre odvodenia kľúča, z ktorých je odporúčané využiť Argon2d.

Logovanie aktivít – Administrátori majú prístup k uloženým heslám všetkých užívateľov v ich prostredí, ale nemajú možnosť vidieť detailné informácie v akom čase a kde konkrétny užívateľ využil určité heslo.

Aktualizácie – Vychádzajú v závislosti na platforme. Sú nasadené automaticky na mobilné zariadenia a doplnky prehliadača, ale pre desktopové aplikácie musia byť manuálne potvrdené.

Lokalita serveru – Nepodarilo sa zistiť ani po konzultácii so zástupcom firmy, ktorá ponúka tento produkt.

Podpora platformy – Na aplikačnej úrovni sú poskytované pre Windows, Mac, iOS a Android. Ako rozšírenie prehliadača sú podporované pre Google Chrome, Firefox a Edge, ktoré môžu byť použité v desktop móde alebo v Standalone móde. Podpora je poskytovaná aj pre Linuxové systémy.

Možnosť nastavenia požiadaviek na heslo – Dashlane má zabudovaný generátor hesiel, ktorý umožňuje definovať požiadavky na heslo.

Cena – Pre podniky poskytuje výrobca verziu Dashlane Business, ktorá stojí 4 USD na užívateľa mesačne. (35)

3.5.5 Passwork

Prístup k účtu len z firemného prostredia – Passwork má možnosť nastavenia prístupu. Podporuje LDAP, čo umožní prihlásenie do aplikácie po zalogovaní do Windowsu.

Šifrovanie – Všetky dáta sú šifrované AES-256 algoritmom. Je možná konfigurácia šifrovania v prehliadači.

Logovanie aktivít – Produkt poskytuje pre všetky svoje verzie možnosť audit logu. Administrátor má možnosť monitorovať všetky akcie a zmeny užívateľov.

Aktualizácie – Dajú sa stiahnuť z repozitára. Táto činnosť môže byť vykonaná manuálne alebo nastavená na automatické aktualizácie. Doba trvania je väčšinou 10 minút.

Lokalita serveru – Jedná sa o spoločnosť sídliaca vo Fínsku a takisto všetky jej servery sú uložené v Helsinkách. Dodržujú zákony podľa EÚ.

Podpora platformy – Passwork je dostupný ako online password manager pre všetky moderné prehliadače. Pre mobilné zariadenia je k dispozícii aplikácia na stiahnutie. A ako rozšírenie prehliadača je dostupný pre Google Chrome a Firefox.

Možnosť nastavenia požiadaviek na heslo – Táto vlastnosť je zabudovaná v produkte.

Cena – Náklady na produkt sa vyvíjajú v závislosti na počte užívateľov. Keďže hľadáme produkt pre firmu s približne 500 zamestnancami pripadá na nás možnosť Premium bez limitu, ktorá stojí 4900 EUR. Po komunikácii so zamestnancom firmy mi bolo oznámené, že sú poskytované množstevné zľavy. V našom prípade by sa jednalo o zľavu vo výške 10 % z celkovej sumy. (36)

3.5.6 Bitwarden

Prístup k účtu len z firemného prostredia – Výrobca ponúka produkt s on-premise riešením, ktorý umožňuje kompletnú kontrolu prístupu.

Šifrovanie – Bitwarden využíva 256 bitovú AES šifru na zabezpečenie dát. PBKDF2 sa využíva na odvodenie šifrovacieho kľúča z masterhesla. Kľúč je následne osolený a zahashovaný. Počet použitých iterácií je 100 001 na strane klienta a ďalších 100 000 iterácií je použitých pre uloženie na serverovej strane.

Logovanie aktivít – Táto vlastnosť bude zabudovaná v produkte. V čase písania práce mi bolo oznámené, že pracujú na auditu klientov.

Aktualizácie – Sú vykonávané automaticky v nepravidelných intervaloch.

Lokalita serveru – Cloudové servery sa nachádzajú v USA.

Podpora platformy – Funguje na všetkých hlavných operačných systémoch, ktoré podporujú Docker a Docker Compose, čiže Windows 7, 8 a 10. Je kompatibilný aj s macOS a Linux.

Možnosť nastavenia požiadaviek na heslo – Vynútenie heslových nastavení nie je zatiaľ v produkte dostupná.

Cena – Jediná verzia obsahujúca všetky požadované funkcionality je Enterprise. Licenčné podmienky sa zakladajú na počte užívateľov. Mesačný poplatok na užívateľa je vo výške 3 USD. Sú poskytované množstevné zľavy začínajúce od 300 užívateľov. Pre firmu s 500 užívateľmi by bola zľava vo výške 25 % z celkovej sumy. (37)

3.6 Výber najvhodnejšieho produktu

Zamietnuté produkty

Polovicu z porovnávaných produktov sme museli zamietnuť z dôvodu nesplnenia kľúčových požiadaviek. Pre firmu je dôležité nastavenie prístupu k účtu správcu hesiel len z firemného prostredia, čo nesplňujú produkty 1Password a Dashlane. Firma 1Password síce umožňuje zamedzenie prístupu k účtom na určitý typ zariadení, ale nemá možnosť limitovania prístupu len na podnikovú sieť, i keď do budúcna túto funkcionalitu zvažuje. Ďalším podstatným kritériom je nastavenie požiadaviek na heslo. Keďže sa firma bude naďalej riadiť podľa štandardov PCI-DSS, bude dodržovať taktiež danú dĺžku a komplexnosť hesiel. Táto funkcionalita nie je zabudovaná v produktoch 1Password a Bitwarden, preto sme ich museli zamietnuť.

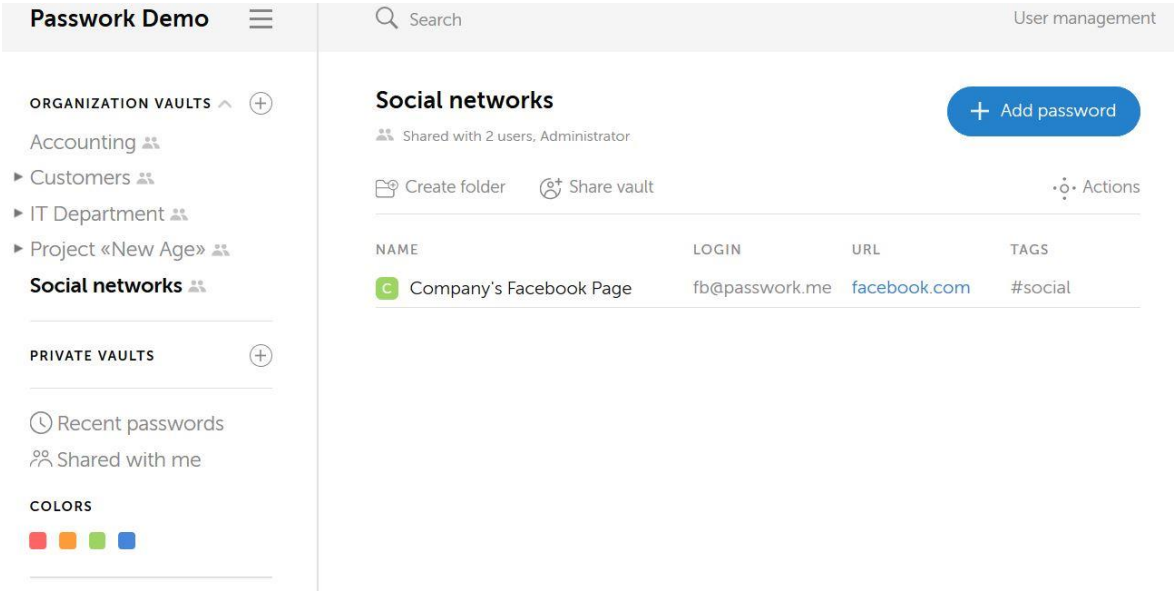
Zhodnotenie vybraných produktov

Na základe vykonanej analýzy splňujú len 3 produkty všetky vopred určené kritéria, ktorými sú Zoho Vault, Psono a Passwork. Funkcionality týchto programov sú zrovnateľné. Jedná sa o online password manageroch, ktorí majú úložisko dát na cloude. Avšak spoločnosť Passwork ponúka i self-hosted verziu. Všetky produkty poskytujú dostatočne silné šifrovanie a sú nezávisle na platforme.

Produkt, ktorý sme určili ako najvhodnejší pre implementáciu je od firmy Passwork. Jedným z rozhodujúcich kritérií je cena, ktorá je najvýhodnejšia práve pri tomto produkte. U vyššie spomenutých dvoch kandidátoch sa účtuje ročný poplatok. Avšak za služby od tohto poskytovateľa by bolo potrebné zaplatiť len jednorazový poplatok, ktorý je vo výške 4900 Euro (suma je pred upravením o zľavu).

Ďalším dôvodom výberu je užívateľská prívetivosť rozhrania aplikácie, ktorá nám prišla jednoduchšia a intuitívnejšia v porovnaní s produktom Psono alebo Zoho Vault. Pod administrátorským účtom sa dajú jednoducho vytvoriť organizačné skupiny (vo firme sa bude jednať o konkrétne oddelenia firmy) a určiť im práva prístupu. Táto funkcionalita sa dá dobre využiť pre zdieľané účty. Samostatnú kategóriu predstavuje súkromná zložka, do ktorej si pracovníci môžu pridať a následne meniť svoje prihlasovacie údaje do aplikácií k výkonu svojej práce.

Ďalšou výhodou tohto softvéru je, že má podporu LDAP, ktorá umožňuje prístup do aplikácie na adresárovom serveri. Je možné preto nastaviť užívateľské loginy do Passworku na tie isté loginy, ktoré užívatelia používajú do Windowsu. Pomocou LDAP môžeme taktiež vynútiť vlastnú politiku hesiel, napr. komplexnosť a entropiu.



Obrázok 4 Užívateľské prostredie demo verzie aplikácie Passwork

3.7 Dopady implementácie na podnikové procesy

Počas procesu implementácie nového softvéru do chodu podniku sa musí vopred zohľadniť, ktoré časti podniku by boli touto zmenou zasiahnuté. V tejto sekcii rozoberieme hlavné dopady na procesy v podniku.

1. Infraštruktúra – Veľký dopad môžeme očakávať v predkonfigurovanej infraštruktúre IT oddelenia. Zmeny môžeme čakať v tímovej štruktúre a musia sa spraviť úpravy v rolách zamestnancov. Napríklad bude potrebné určiť administrátora na správu a vedenie softvéru.
2. Poučenie zúčastnených strán – Dôležitým krokom je vytvorenie inštruktážneho manuálu alebo videa pre užívateľov. Takisto musíme zaučiť helpdesk ako riešiť prípadné poruchy softvéru.
3. Súlad s používanými štandardmi – Firma sa riadi štandardom PCI-DSS, ktorý by po implementácii naďalej aplikovala. Uvedieme si jeden príklad. Podľa najnovších best practices NIST je pravidelná žiadosť o zmenu hesla praktikou neodporúčanou. Keďže sa spoločnosť naďalej bude riadiť doteraz používaným štandardom, ktorá k tomu pristupuje inak, budú zamestnanci stále žiadaní o zmenu hesla každé tri mesiace.

3.8 Hrozby implementácie

Implementovaním tohto softvéru do chodu firmy musíme však počítať s možnými vedľajšími následkami. Prvým prípadom je strata masterhesla, o ktorom sme si spomenuli už v druhej kapitole. Obnova hesla by musela prebehnúť buď zaslaním žiadosti na email alebo vytvorením tiketu, ktorý je zaslaný na helpdesk. Môže nastať aj scenár, že pracovníci uložia

masterheslo v plaintexte. Tak sa môžu neautorizovaní zamestnanci dostať ku všetkým účtom druhých zamestnancov.

Druhou hrozbou je náročnosť obsluhy softvéru. Za zmienku stojí informácia, že priemerný vek pracovníkov vo firme je 27 rokov, čiže môžeme predpokladať, že by táto veková skupina nemala mať väčšie problémy s užívaním softvéru. Avšak určitá časť zamestnancov môže byť technicky menej zdatná, u ktorej môžu nastať problémy s obsluhou. Preto je dôležité vytvoriť inštruktážny materiál na užívanie softvéru, čo najjasnejšie a najpresnejšie.

Hrozbou môže byť taktiež prípad spadnutých serverov poskytovateľa. Užívatelia budú používať vysoko komplexné heslá a keďže nebudú mať alternatívny prístup ku svojím heslám, nemôžu sa potom prihlásiť do užívaných softvérov. Môže to viesť k vysokým finančným stratám podniku. Jeden takýto prípad bol zaznamenaný 26. novembra 2018. Servery password managera LastPass boli offline po dobu šiestich hodín. Outage bola spôsobená poškodenými sieťovými paketmi. (38)

3.9 Prínosy implementácie

Najväčším prínosom tejto implementácie považujeme väčšiu bezpečnosť uloženia užívateľských hesiel. Zamedzíme využívanie menej bezpečných metód ako je napríklad ukladanie hesiel v Sticky notes alebo zapísanie hesiel do zošitu. Vďaka správcu hesiel budú heslá uložené v šifrovanom formáte. Obzvlášť keď sa využije silný šifrovací štandard ako je napríklad AES-256.

Ďalším plusom je zvýšenie komfortu užívateľov. Pracovníci počas procesu autentizácie ušetria čas zadávaním správnych loginov do formulára. Zamedzia sa tým počty neúspešných pokusov prihlásenia sa do aplikácie, čiže sa zníži chybovosť užívateľov. Celkovo znížime heslovú únavu pracovníkov, čím zamedzíme chyby typu znovupoužívania hesiel, zdieľania hesiel, atp.

Pracovníkov takisto inšpirujeme k využitiu softvéru pre ich osobné účty. Avšak to by mohli učiniť len vytvorením nového účtu na správu hesiel. V pracovnom účte sa nemôžu vyskytovať prihlasovacie údaje nesúvisiace s náplňou práce.

Záver

Zhrnutie praktickej časti

Práca sa primárne venovala analýze softvérov na správu hesiel, ktorej cieľom bolo nájsť produkt, ktorý by nahradil súčasnú správu hesiel v sledovanej firme. Na začiatok sme rozobrali súčasnú situáciu vo firme, kde sme dospeli k záveru, že technológiou SSO nepokryjeme všetky účty zamestnancov a preto je implementácia špecializovaného softvéru na správu hesiel vhodným a praktickým riešením. Následne sme určili kritéria, ktoré produkt musí spĺňať. Na základe toho sme vyselektovali, ktoré produkty budú zamietnuté, a ktoré budú vybrané do hlbšej analýzy. Výsledkom toho bol zúžený zoznam, v ktorom sme detailne popisovali kritéria jednotlivých produktov. Porovnaním jednotlivých softvérov sme vybrali finálny produkt, ktorý sme navrhli firme pre implementáciu, čím sme splnili hlavný cieľ práce. Či implementácia produktu bude uskutočnená, mi počas písania práce nebolo možné potvrdiť, keďže návrh je v stave schvaľovania. Posúdi sa či investované náklady do produktu budú odpovedať pridanej hodnote pre spoločnosť.

Chceme poznamenať, že sme vybrali produkt, ktorý sme usúdili za najvhodnejší porovnaním s poskytovateľmi, pri ktorých sme našli dostatočné množstvo informácii. Pri mnoho produktoch nie je dostatok verejne dostupných informácií a preto sme kontaktovali zástupcov firiem alebo ich pracovníkov zákazníckej podpory. Odozvu sme však nedostali v skoro polovici prípadov. Napriek tomu sme dokázali poskytnúť porovnanie niekoľko produktov.

Došli sme taktiež k záveru, že trh poskytovateľov služieb správy hesiel je dokonalou konkurenciou. Vyskytuje sa tu veľký počet firiem, ktorý ponúka takmer identický produkt. Mnoho z týchto ponúkaných nástrojov sa ponúkajú za nízke alebo dokonca nulové náklady. Pri výbere tohto softvéru pre väčšie spoločnosti sú však kladené väčšie nároky na splnenie určitých funkcionalít, ktoré sú dostupné vo väčšine prípadov v enterprise alebo business edíciách produktu. Častým problémom je preto nájsť cenovo dostupný a požiadavkami spĺňujúci password manager, ktorý je možný zaviesť do politiky firmy. Takisto musia firmy posúdiť či prínosy softvéru prevyšujú možné hrozby.

Odporúčania a využitie výsledkov práce

V tejto práci obsiahnuté informácie môžu byť využité bežnými užívateľmi informačných technológii, ktorých to môže podnietiť k zavedeniu tohto softvéru do ich rutinnej práce s počítačom či mobilom. Pre menšie či väčšie spoločnosti práca môže poslúžiť ako podkladový materiál pri výbere vlastného softvéru na správu hesiel.

Hlavne v organizáciách je dôležitou súčasťou ochrany správa hesiel. Bezpečnosť sa dá čiastočne dosiahnuť dodržovaním inštitútmi navrhovanými štandardmi, ale nemôžeme zabudnúť na ľudský článok, ktorý hrá tiež podstatnú rolu v celkovej bezpečnosti dát v podniku. Pri zaúčaní nových zamestnancov nie je venovaný dostatočný čas bezpečnostnej politike hesiel a pracovníci si následne uľahčujú ukladanie hesiel laickými metódami. Množstvo

hesiel, ktoré je pracovník povinný si pamätať v kombinácii s prísnou politikou hesiel vedie pracovníkov k heslovej únave.

Mnoho firiem preferuje využitie SSO technológií na zmiernenie problému heslovej únavy napriek tomu, že nepokrývajú všetky využívané aplikácie. Naším odporúčaním je preto vykonať analýzu obdobnú tejto práci a zistiť na koľko by implementácia špecializovaného softvéru na správu hesiel bola prínosná.

Upozornili sme na množstvo nedostatkov a hrozieb, ktoré sú spojené so softvérmi na správu hesiel. Napriek tomu považujeme password managerov za najbezpečnejší spôsob uchovávanie hesiel v súčasnosti. Negatíva tohto softvéru sú minimálne v porovnaní s ostatnými metódami správy hesiel, ktoré predstavujú pre užívateľov väčšie riziko. Posledný cieľ, a to analýza ako môžu softvéry na správu hesiel zmierniť chybovosť užívateľov, bol úspešne splnený.

Použitá literatúra

1. Karen Scarfone; Murugiah Souppaya. *Guide to Enterprise Password Management (Draft)*. [Online] 2009. https://csrc.nist.gov/csrc/media/publications/sp/800-118/archive/2009-04-21/documents/draft-sp800-118.pdf.

2. Tipton, Harold F. a Krause, Micki. *Information Security Management Handbook*. Boca Raton : Auerbach Publications, 2006. stránky 60–62. ISBN 978-1-4200-6045-4.

3. Harpur, Richard. Pluralsight. *New normal: Today's best practices for passwords*. [Online] 2018. https://www.pluralsight.com/blog/security-professional/modern-password-guidelines.

4. National Institute of Standards and Technology. *Recommendations of the National Institute of Standards and technology*. [Online] 2009. https://csrc.nist.gov/csrc/media/publications/sp/800-118/archive/2009-04-21/documents/draft-sp800-118.pdf.

5. Herley, Cormac a Florencio, Dinei. *A Large-Scale Study of Web Password Habits*. New York : s.n., 2007. stránky 657–665. ISBN 978-1-59593-654-7.

6. Beal, Vangie. Webopedia. *65 Password Security Tips: How to Create and Secure Accounts*. [Online] 27. 3. 2017. https://www.webopedia.com/DidYouKnow/Internet/password-security-tips.html.

7. Couillard, Kaitlin. Roboform. *Password Security Survey Results- Part 1*. [Online] 6. 3. 2015. https://roboform-blog.siber.com/2015/03/06/password-security-survey-results-part-1/.

8. Notoatmodjo, Gilbert a Thomborson, Clark. Information Security Volume – 98 . *Passwords and perceptions*. 2009. ISBN 978-1-920682-79-8.

9. Kellet, Andrew a Turner, Rik. *Close the password security gap: convenience for employees and control for IT*. [Online] 2017. https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/ovum-lastpass-whitepaper.pdf.

10. Burnett, Mark a Kleiman, Dave. *Perfect passwords*. Rockland : Syngress Publishing, Inc., 2006. ISBN 1-59749-041-5.

11. Bell, Steve. *Websites storing clear text passwords*. [Online] 10. 1. 2018. https://www.bullguard.com/blog/2018/01/websites-storing-clear-text-passwords.

12. Cheap SSL Security. *What is Asymmetric Encryption? Understand with Simple Examples*. [Online] 2019. https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/.

13. Stinson, Douglas Robert a Paterson, Maura. *Cryptography: Theory and Practice*. Boca Raton : CRC Press, 2019. ISBN 9781138197015.

14. Samborski, John. *Hi-Tech Guessing Game: 350 Billion Passwords a Second* . [Online] 16. 12. 2015. https://www.rdmag.com/blog/2015/12/hi-tech-guessing-game-350-billion-passwords-second.

15. Towhidi, Farnaz, a iní. *The Knowledge Based Authentication Attacks*. [Online] 2011. [Dátum: 17. 3. 2019.] http://ezproxy.techlib.cz/login?url=https://search-proquest-com.ezproxy.techlib.cz/docview/1272092762?accountid=119841.

16. Požár, Josef. *Informační bezpečnost*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

17. Rouse, Margaret. Search Security. *Password synchronization*. [Online] 2006. https://searchsecurity.techtarget.com/definition/password-synchronization.

18. Hitachi ID Systems, Inc. *Definition of Web Single Sign-On (WebSSO)*. [Online] 2019. https://hitachi-id.com/resource/itsec-concepts/websso.html.

19. Hitachi ID. *Definition of Enterprise Single Sign-On (E-SSO)*. [Online] 2019. https://hitachi-id.com/resource/itsec-concepts/esso.html.

20. Jøsang, Audun, AlZomai, Mohammed a Suriadi, Suriadi. *Usability and Privacy in Identity Management Architectures*. [Online] 2007. https://eprints.qut.edu.au/7289/1/JAS2007-AISW.pdf.

21. Korolov, Maria. CSO Online. *Password managers grow up, target business users*. [Online] 4. 1. 2018. https://www.csoonline.com/article/3244137/password-managers-grow-up-target-business-users.html.

22. McMillan, Robert. Wired. *The World's First Computer Password? It Was Useless Too*. [Online] 27. 1. 2012. https://www.wired.com/2012/01/computer-password/.

23. AlFayyadh, Bander, a iní. *Improving Usability of Password Management with Standardized Password Policies*. [Online] 18. 10. 2011. http://folk.uio.no/josang/papers/ATJK2012-SARSSI.pdf.

24. LeClair, Dave. New Atlas. *myIDkey voice-searchable USB drive makes password management portable*. [Online] 27. 6. 2013. https://newatlas.com/myidkey-voice-searchable-usb/28073/.

25. Stokes, Natasha. Techlicious. *Is it Safe to Use a Password Manager?* [Online] 30. 7. 2018. https://www.techlicious.com/tip/are-password-managers-browser-stored-passwords-safe/.

26. MakeUseOf. *Password Management Guide.* [Online] 2013. https://www.makeuseof.com/tag/the-password-management-guide-fulltext/.

27. WatchGuard. *Internet Security Report - Q3 2018.* [Online] 2018. https://www.watchguard.com/wgrd-resource-center/security-report-q3-2018.

28. Silver, David, Jana, Suman a Boneh, Dan. *Password Managers: Attacks and Defenses.* [Online] 20. 8. 2014. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-silver.pdf.

29. Fowler, Geoffrey. Washington Post. *Password managers have a security flaw. But you should still use one.* [Online] 19. 2. 2019. https://www.washingtonpost.com/technology/2019/02/19/password-managers-have-security-flaw-you-should-still-use-one/?utm_term=.77db649634cb.

30. Hoyos, Alvaro. OneLogin. *May 31, 2017 Security Incident.* [Online] 31. 5. 2017. https://www.onelogin.com/blog/may-31-2017-security-incident.

31. Willis Towers Watson. *When it comes to cyber risk, businesses are missing the human touch.* [Online] 1. 3. 2017. https://www.willistowerswatson.com/en-US/press/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch.

32. 1Password. *Meet and exceed your security compliance needs.* [Online] 2019. https://1password.com/business/.

33. Zoho. *Frequently asked questions.* [Online] 2019. https://www.zoho.com/vault/help/faq.html#.

34. Psono. *Psono documentation.* [Online] 2019. https://doc.psono.com/user_overview_supported_features.html.

35. Dashlane. *All the tools you need for a simpler, safer life online.* [Online] 2019. https://www.dashlane.com/features.

36. Passwork. *FAQ.* [Online] [Dátum: 12. 4. 2019.] https://passwork.pro/#faq.

37. Bitwarden. *Help/FAQs.* [Online] 2019. https://help.bitwarden.com/.

38. Wagenseil, Paul. *LastPass Knocked Offline, Freezing Out Password Users*. [Online] 26. 11. 2018. https://www.tomsguide.com/us/lastpass-password-manager-offline,news-28592.html.

Prílohy

Príloha A: Prehľad vybraných produktov

	1Password	Zoho Vault	Psono	Dashlane	Passwork	Bitwarden
Prístup k účtu z firemného prostredia	Nie (len na určitý typ zariadenia)	Áno	Áno	Nie	Áno (podpora LDAP)	Áno
Šifrovanie	AES-GCM-256	AES-256	Curve25519, Salsa20 a Poly1305	AES-256	AES-256	AES-256
Logovanie aktivít	Áno	Áno	Áno	Nie	Áno	Áno
Aktualizácie	Manuálne	Automaticky	Automaticky (mesačne)	Automaticky	Možnosť manuálne alebo automaticky	Automaticky (nepravidelné intervaly)
Lokalita serveru	Európa (pre 1Password.eu účty)	Európa (pre zoho.eu účty)	Frankfurt	-	Helsinky	USA
Podpora platformy	Windows/macOS/ iOS /Android	Nezávislosť na platforme	Nezávislosť na platforme	Windows/Mac/ iOS /Android	Nezávislosť na platforme	Windows 7, 8 a 10/macOS/ Linux
Možnosť nastavenia požiadaviek na heslo	Nie	Áno	Áno	Áno	Áno	Nie
Cena	Business verzia - 7,99 $ na užívateľa mesačne	Professional verzia - 3,6 € na užívateľa mesačne	Enterprise verzia - 2 € na užívateľa mesačne	Business verzia - 4 $ na užívateľa mesačne	4 900 € - jednorazová platba	Enterprise verzia - 3 $ na užívateľa mesačne