Prečo je ukladanie hesiel do prehliadača nebezpečné?

S rastúcim počtom webových služieb a online účtov sa zvyšuje aj počet hesiel, ktoré si musí človek pamätať. Ako reakciu na túto potrebu si mnohí používatelia zvolili ukladanie hesiel do svojich internetových prehliadačov a používanie automatického vypĺňania. Je to pohodlné riešenie, ale webové prehliadače sú **primárne navrhnuté na zobrazovanie webového obsahu** a nie na zabezpečené ukladanie hesiel. V tomto článku sa dočítate prečo je nebezpečné ukladať svoje heslá v prehliadači a o odporúčaniach ako si ich ochrániť.

Heslá sú jedným z mála spôsobov, ako dokážeme zabezpečiť svoje účty. Odborníci z oblasti IT pravidelne vyzývajú používateľov, aby si tvorili bezpečné heslá – v súlade so špecifickými požiadavkami. Bližšie podrobnosti o bezpečnosti a vytváraní hesiel sme si pre Vás pripravili začiatkom septembra.

Obrázok 1 Bezpečné heslá Zdroj: CSIRT

Nech sú vaše heslá akokoľvek bezpečné, v momente ich uloženia vo webovom prehliadači čelíte viacerým rizikám.

Riziká ukladania hesiel v prehliadačoch

1. Prvé nebezpečenstvo predstavuje **fyzický prístup** k odomknutým zariadeniam obete, kedy útočník dokáže uložené heslá **zneužiť na neoprávnený prístup** do ,,zapamätaných" systémov a následné **vykonanie úkonov** podľa úrovne oprávnenia účtu. Útočník dokonca môže heslá **extrahovať na ďalšie použitie**.

2. Správca hesiel vo webových prehliadačoch ukladá heslá do šifrovaných databáz, avšak pre **konkrétne prehliadače** sú verejne **známe presné umiestnenia súborov** na disku, ktoré **obsahujú históriu prehliadania, databázu hesiel a dokonca aj hlavné heslo** k šifrovaným databázam. **Túto skutočnosť zneužívajú rôzne rodiny malvérov**, ktoré zbierajú základné informácie o kompromitovanom zariadení, históriu prehliadačov a komunikačných platforiem, uložené heslá prehliadačov, obsah schránky operačného systému (eng. clipboard) alebo iných zvolených súborov a tieto údaje rôznymi metódami zasielajú útočníkovi. Medzi najznámejšie malvéry zamerané na získavanie citlivých dát možno zaradiť napr. Redline, Racoon, Lumma, SnakeKeylogger, Agent Tesla a ďalšie. Znalosť umiestnenia kľúčových súborov je **taktiež využívaná aj v rámci riešenia kybernetických bezpečnostných incidentov** a vyšetrovania trestných činov počítačovej kriminality.

3. Mimoriadne riziko predstavuje možnosť **previazania prehliadača s kontom používateľa** (napr. konto na službe MICROSOFT alebo GOOGLE), ktoré umožňuje **pokročilé funkcie práce na viacerých zariadeniach**, ako sú napr. zdieľanie histórie webového prehliadania, záložiek a synchronizácie uložených hesiel. **Synchronizácia hesiel** na jednej strane **zvyšuje komfort používateľa**, na druhej strane však predstavuje **dodatočné riziko**, kedy sa k heslám možno dostať **kompromitáciou ľubovoľného zariadenia** asociovaného s daným kontom.

Ako **odstrašujúci príklad** zneužitia tejto funkcionality možno použiť kybernetický bezpečnostný incident, ktorý spoločnosť CISCO riešila v roku 2022. Jeden z interných **zamestnancov mal webový prehliadač na pracovnom zariadení previazaný so súkromným GOOGLE účtom a využíval synchronizáciu hesiel**, vrátane prihlasovacích údajov do podnikovej VPN siete. Tento používateľ sa stal **obeťou phishingového útoku**, počas ktorého **útočník získal prístup k jeho GOOGLE účtu** a tým aj ku **všetkým heslám**. **Prihlasovanie do VPN** síce bolo **chránené** prostredníctvom **viacfaktorovej autentifikácie**, ale **útočníkovi sa tento bezpečnostný prvok podarilo obísť prostredníctvom techník sociálneho inžinierstva**, ktoré sú bližšie popísané na tomto odkaze v článku.

4. Ukladanie údajov v prehliadači zvyšuje aj úspešnosť phishingových kampaní, kedy prehliadač pri rozpoznaní **formulára** na zadanie osobných alebo kartových údajov ponúkne používateľovi možnosť **automatického vypĺňania**. Táto funkcia je mimoriadne riziková dokonca aj v prípade, že si obeť uvedomí, že sa stala obeťou phishingu ešte pred odoslaním formulára, pretože **pokročilé phishingové frameworky priebežne zasielajú zadávané údaje útočníkovi**.

5. Okrem funkcií zabudovaných priamo v prehliadači je na ukladanie hesiel možné použiť aj **externé doplnky, zásuvné moduly a pluginy**, ktoré majú rôznu kvalitatívnu úroveň. Útočníci rôzne rozšírenia dokonca používajú ako **mechanizmus šírenia škodlivého kódu**, nakoľko

používateľ medzi veľkým množstvom dostupných možností často nedokáže rozlíšiť legitímne aplikácie od tých škodlivých.

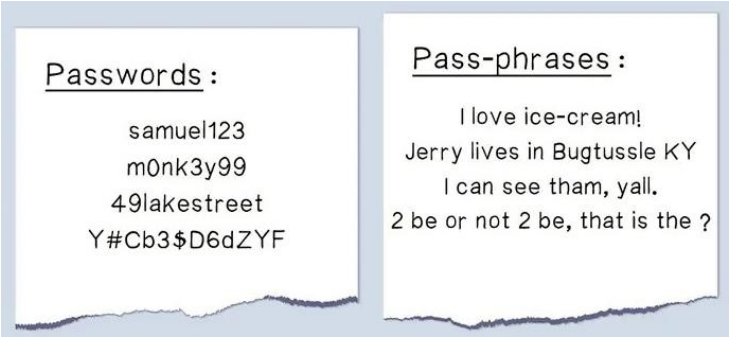
6. Vyššie uvedené **rozšírenia** rovnako ako samotné **prehliadače** môžu obsahovať **bezpečnostné zraniteľnosti**, ktoré možno zneužiť na naplnenie rôznych cieľov, od získania neoprávneného prístupu k citlivým údajom až po vzdialené vykonanie škodlivého kódu. Tie najzávažnejšie zraniteľnosti je možné zneužiť vzdialene a bez interakcie obete. Preto je dôležité všetky používané zariadenia a aplikácie **pravidelne aktualizovať**.

Výhody používania aplikácií na správu hesiel

Na ukladanie hesiel sa odporúča používať výhradne špecializované nástroje, tzv. **aplikácie na správu hesiel** (eng. password manager), ktoré boli navrhnuté s primárnym dôrazom na **zabezpečenie dát, robustné šifrovanie a ochranu pred rôznymi scenármi odcudzenia** prihlasovacích údajov. Tieto aplikácie umožňujú heslá prehľadne **organizovať** do kategórií a dokonca vykonávajú **analýzy nad heslami**, aby používateľov upozornili na recykláciu hesiel alebo skryté a predvídateľné vzory pri generovaní hesiel, vrátane jednoduchých úprav pri pravidelných zmenách hesiel. Niektoré služby dokonca heslá **overujú voči online databázam uniknutých hesiel**, čím umožňujú reagovať na prípadné úniky dát. Jednou z najznámejších služieb umožňujúcich preverenie, či došlo k úniku Vašich prihlasovacích údajov, je **HAVEIBEENPWNED**, s ktorou **CSIRT.SK v roku 2021 uzatvoril spoluprácu**. Okrem hesiel umožňujú aj **ukladanie súborov** – napr. obrázkov a iného kryptografického materiálu (certifikáty, SSH kľúče a pod). Heslá skopírované do schránky operačného systému v nej udržujú len po obmedzený čas, čím znižujú riziko ich krádeže. V prípade využívania online služieb na manažment hesiel je treba brať do úvahy aj riziko, že bezpečnostné zraniteľnosti a incidenty u Vášho poskytovateľa môžu priamo ohroziť aj Vaše heslá.

Odporúčania ako sa chrániť

1. **Používajte silné heslá**: Používajte silné heslá, ktoré obsahujú kombináciu veľkých a malých písmen, číslic a špeciálnych znakov. Odporúčame používať passphrase, frázy, ktoré si používateľ dokáže ľahšie zapamätať. ***NEPOUŽÍVAJTE*** však verše pesničiek, odseky z kníh, populárne citáty, osobné údaje alebo heslá, ktoré ste niekde videli (napr. slogany, reklamy....). VJ CSIRT odporúča používať diakritiku pri vytváraní frázy, kde je to možné.



Obrázok 2 Bezpečné heslá Zdroj: CyberHoot

2. **Nepoužívajte funkciu automatického ukladania hesiel a dopĺňania** vo webových prehliadačoch. Namiesto toho si zapamätajte svoje heslá alebo použite aplikácie na správcu hesiel, ako napríklad KeePass, LastPass, 1Password alebo Bitwarden.

3. **Striktne oddeľujte** súkromné a pracovné zariadenia.

4. Na všetkých službách, kde je to možné, **majte aktivované viacfaktorové overovanie** prístupu. Môžete si nastaviť overenie biometriou, odosielanie SMS správ, telefonický rozhovor alebo používať generátor tokenov pre vytvorenie jednorazového kódu či push notifikácie pre autentifikáciu do účtu (Duo Mobile, Authy, Google Authentificator). **Svojich zamestnancov a známych vzdelajte aj o aktívne zneužívaných metódach obchádzania viacfaktorovej autentifikácie**.

5. **Pravidelne aktualizujte** operačný systém, používané aplikácie a ich rozšírenia, nakoľko môžu obsahovať ľahko zneužiteľné bezpečnostné zraniteľnosti.

6. **Používané aplikácie,** externé doplnky, zásuvné moduly a pluginy **vždy inštalujte z overených a dôveryhodných zdrojov**.

7. **Hardening prehliadačov.** Cieľom hardeningu prehliadačov je znížiť možný dopad zraniteľností a zvýšiť odolnosť prehliadača pred útokmi. Slúži nám na to najmä vhodná konfigurácia, ktorá zahŕňa blokovanie cookies, blokovanie načítavania obsahu z neznámych alebo nebezpečných zdrojov, aktiváciu dodatočných bezpečnostných funkcií ako blokovanie reklám, vypnutie telemetrie a mnoho ďalších nastaveníOdolnosť svojho prehliadača si môžete overiť prostredníctvom online testu.

8. **Používateľské konto.** Pri práci s prehliadačmi na operačnom systéme by ste mali vždy používať používateľské konto s nízkymi oprávneniami (user account) a nie administrátorské konto (administrator account).

V tomto článku sme si ukázali riziká spojené s ukladaním hesiel vo webových prehliadačoch, popísali výhody používania aplikácií na správu hesiel a odporúčania ako svoje heslá chrániť. Pri práci s heslami je potrebné dodržiavať základné zásady kybernetickej hygieny a držať sa vyššie uvedených odporúčaní VJ CSIRT.

Sledujte nás na sociálnych sieťach:
https://www.linkedin.com/company/csirt-sk
https://www.facebook.com/VJCSIRT
https://twitter.com/CSIRT_SK

Zdroje:

https://blog.talosintelligence.com/recent-cyber-attack/
https://www.kaspersky.com/blog/how-to-store-passwords-securely/48784/
https://www.tomsguide.com/news/dont-let-web-browsers-save-passwords
https://news.trendmicro.com/2023/11/27/is-it-safe-to-save-passwords-in-your-browser/
https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
https://coveryourtracks.eff.org/