28. 4. 2017

ID: 105836

Heslovitě o správném nastavení hesel

Má vaše heslo 16 znaků včetně těch speciálních? Máte pro každou online službu jiné unikátní heslo, jak to radí odborníci na kybernetickou bezpečnost? Pakliže tyto podmínky nesplňujete, jste na tom stejně jako valná většina lidí pracující v online prostředí. Na druhou stranu, tam, kde obyčejný smrtelník ohrožuje své osobní informace nebo nejhůře peníze, je odpovědnost advokáta mnohem větší.

Jan Drozd

Jan Drozd je odborníkem na počítačovou bezpečnost a u nás v SingleCase hlídá, aby všechny zabezpečovací prvky fungovaly tak, jak mají. Dali jsme společně s ním dohromady seznam doporučení, která v případě převedení do praxe radikálně snižují riziko krádeže vašich online účtů a dat.

U všech Honzových značně rigidních bezpečnostních pravidel jsme hledali jejich vnitřní princip, vlastně jsme si u každého udělali takový malý teleologický výklad. V 4. bodě na konci článku pak nabízíme konkrétní systém správy hesel, který mohou aplikovat i právníci či jakýkoliv jiní lidé, které neživí počítačová bezpečnost.

1) Jak má vypadat bezpečné heslo

Honza: “Doporučená délka hesla je 32 znaků, obsahuje malá, velká písmena, číslice a speciální znaky.”

My sami máme někdy problém vzpomenout si na PIN ke kartě nebo jaký paragraf má v novém OZ veřejná soutěž (§ 1772, pro ty, kterým by nedalo to hledat), takže 32 znaků je stoprocentně nad naše možnosti. Důležité je si uvědomit, že každý znak navíc pomáhá síle hesla. Na rozluštění hesla od 1 do 9 potřebujete maximálně 9 pokusů, pokud ale přidáme znak navíc, je to už 99 pokusů. Složitost roste řádově. Kombinatorika nám totiž říká, že na rozluštění jedné pozice ze znaků a čísel nepotřebujeme 9, ale až 36 (9+27) pokusů. A ještě více je to se speciálními znaky, proto je také Honza doporučuje používat.

2) Jak mám vytvořit bezpečné heslo

Honza: “Heslo by nemělo obsahovat nezměněná jednoduchá slova, jméno a přezdívku uživatele, jeho rodiny, firmy nebo domácích mazlíčků, data narození, výročí svatby a podobně. V ideálním případě nedává smysl, nedá se nijak dovodit.”

32 znaků nedávajících žádný smysl připomíná do značné míry učení se na zkoušku z práva životního prostředí. Jde ale o obranu vůči nejčastějšímu způsobu útoku, o tzv. brute force, v překladu hrubou sílu. Hackerský software automaticky dosazuje kombinace nejčastěji v heslech používaných výrazů a slov. Jak víme ze zkoumání databází hesel zveřejněných hackery, tak nejpoužívanější heslo na světě je "heslo" (resp. "password"). Na druhém místě je "123456". V první stovce pak najdeme křestní jména, čísla typu 121212, několik sprostých slov, ale také "starwars". Software je automaticky vyzkouší, protože mají největší pravděpodobnost úspěchu.

Hacker zvyšuje úspěšnost tím, že softwaru poradí několik klíčových slov, jmen a datumů dohledatelných právě ze sociálních sítí, diskuzních fór a veřejných registrů. Proto libovolné Lence narozené v roce 81 nepomůže při profesionálním útoku zkomolit jméno na heslo Leniczka81, hackerský software se nejspíš zkomolení Lenka na Leniczka už dávno naučil a s velkou pravděpodobností kombinaci s rokem narození zkusí.

3) Kolik mám mít hesel

Honza: "Na každém účtu mějte jiné unikátní heslo."

Nejspíš už je vám jasné, že Honzova doporučení jsou nesplnitelná nejen pro běžného uživatele. Zapamatovat si desítky hesel o 32 znacích je nesplnitelné pro kohokoliv, kdo nemá zvláštní dar a zákaz vstupu do kasína. Prozradíme, že řešením je správce hesel, více o něm v dalším bodě. Nyní se však podívejme zase na pozadí Honzovy rady. Asi nejhorší případy hackerského útoku jsou v kompletní krádeži v podstatě celé online identity uživatele.
Dochází k tomu typicky ve dvou scénářích. Prvním je právě jednotné heslo. Zloděj ukradne vaše heslo na nějaké službě (v poslední době proběhl velký únik hesel ze sítě LinkedIn) a vyzkouší to samé heslo nebo jeho variace ve službách ostatních. Druhým scénářem ztráty více služeb během jednoho útoku jsou případy prolomení ochrany účtu, kterým se autorizujete do jiných služeb, typicky osobní mail nebo účet na Facebooku. Ve starých mailech hacker najde vaše přihlašovací údaje nebo další data potřebná k prolomení jiného účtu.

4) Jak se vůbec dá tato doporučení následovat

Honza: "Je mi jasné, že si nemůžete zapamatovat 20 různých hesel s délkou 32 znaků. Neukládejte hesla do prohlížeče, jsou často napadané. Pořiďte si správce hesel, ideálně takový, který v prohlížeči neuchovává ani data."

I my musíme doporučit správce hesel, z celé plejády možností vychází nejlépe poměrem starosti o řešení a jeho bezpečnosti. Pokud se pro něj rozhodnete, použijte KeePass, LastPass a 1Password. Honzovi žádná s výše zmíněných aplikací nevyhovovala, a vyvinul svou, ještě bezpečnější variantu.

Pokud správci hesel nedůvěřujete nebo ho nechcete z jiného důvodu používat, doporučujeme rozdělit vaše služby na tři kategorie podle důležitosti:

1. Do té první dejte ty nejcitlivější - internetové bankovnictví, SingleCase či jiný online přístup ke spisu, e-mailovou schránku, Facebook. Těmto službám vymyslete unikátní a složitá hesla. Pokud to povolují, aktivujte u nich dvoufázové ověřování přes telefon.

2. Druhá skupina hesel jsou služby, které používáte a jsou zneužitelné, ale případná škoda při jejich ztrátě by nebyla tak vysoká. Sociální sítě jako Twitter, Instragram, LinkedIn, služby s kreditem: Košík.cz, kreditová jízdenka Student Agency apod. U nich můžete vymyslet variaci hesla, například "muj ucet @ foto koccek a 2 psu" pro Instagram a "muj ucet @ zivotopis a pr0 chlubeni" pro

LinkedIn. Pokud to s bezpečností myslíte opravdu vážně, můžete si přečíst odborný článek o tvorbě silných hesel od Michala Špačka.

3. Třetí kategorie jsou služby, na jejichž ztrátě vám nezáleží. Typicky je to povinné vyplňování profilu u soutěží, anket, her, kde musíte vymýšlet přihlašovací údaje, ale nejspíš je už nikdy nepoužijete. Je s podivem kolik lidí dá neznámé službě svůj mail a vyplní k němu shodné heslo. U těchto služeb mějte jedno heslo na všechny.

Svá hesla si rozhodně nepište na papírek k monitoru nebo je nenoste v peněžence. Také se vyhněte používání tzv. bezpečnostních otázek, získat rodné jméno vaší matky nebo vaši přezdívku z mládí je totiž ještě snažší než prolomení nedobrého hesla.

Heslovitě

- Nemějte všude stejné heslo.
- Vytvořte si silná hesla.
- Používejte správce hesel nebo alespoň rozdělte služby podle důležitosti a přiřaďte jim adekvátní hesla.
- Používejte dvoufázové ověřování a nepoužívejte bezpečnostní otázky.
- Nechť vás provází síla (hesla).

Jak se kradou hesla?

V tuto chvíli musíme vysvětlit, že krádež databáze hesel z nějaké služby dnes většinou automaticky neznamená, že zloděj má vaše heslo. To totiž u dobrých služeb nemá ani její provozovatel, jeho databáze obsahuje jen šifry, které odemknete právě svým heslem. Ne každá internetová stránka s uživatelským přístupem ale databázi šifruje, nešvar je to třeba u starých e-shopů. Šifrování je výrazné znesnadnění práce pro internetové zloděje, problémem ale je, že velká část služeb stále šifruje starou šifrovací metodou známou jako MD5, kterou lze bez problému prolomit.

V praxi to znamená, že jednou rozšifrované heslo se dostane do tzv. rainbow tables. To jsou databáze rozšifrovaných hesel, které si hackeři sdílí a prodávají. Běžně používaná hesla, o kterých jsme mluvili v předchozím bodě, jsou o to nebezpečnější, hlavně to ale znamená, že postupem času ubývá hesel, které šifrování při úniku databáze hesel ochrání. Samo o sobě vás tedy silné heslo neochrání, pokud ho už v minulosti někdo použil a hacker rozšifroval. SingleCase a jiné dobře zabezpečené služby používají na ochranu proti rainbow tables techniku tzv. solení - před zašifrováním hesla k němu přidají "sůl" - řetězec znaků unikátní pro danou službu.
BOX

Další články:

- Prémiový rezidenční komplex Bakers Court přináší na realitní trh komfortní bydlení s 5* službami

- ESG Simple jako praktická opora pro ESG reporting malých a středních podniků
- Digitální důkazy z webu v soudním řízení: jak doložit, co bylo online zveřejněno?
- V lednu přišel šok. Ze seznamu zmizely tisíce soudních překladatelů
- Koupě nemovitosti v Rakousku: vedlejší náklady v praxi
- Legal Innovation Day 2026: Praktické využití umělé inteligence v právní praxi
- Prémiový rezidenční komplex Bakers Court přináší na realitní trh komfortní bydlení s 5* službami
- Festival jako prestižní teambuilding
- Spojení Generali České a Právní ochrany D.A.S. přináší první výhodu: navýšení pojistného limitu na 5 milionů
- Kultura jako prestižní benefit: Proč by právní firmy měly sázet na „inteligentní zážitky“? Rozhovor s JUDr. Martinou Jankovskou
- Wolters Kluwer uvádí na český trh AI právní pracovní prostor Libra s integrovaným obsahem ASPI