HESLO12341

Připomíná vám tento text něco? Podle studie společnosti NordPass vytvořené v roce 2023 je toto nejoblíbenější heslo uživatelů internetu v České republice. Pokud podobně vypadají i vaše hesla, jste na tom stejně jako já. Musím se přiznat, že hesla nesnáším, stále je zapomínám a mám v nich naprostý chaos.

Zbyněk Pavienský

V mnoha firmách, kde jsou pravidla na tvorbu hesel mimořádně přísná, musí mít heslo do internetové sítě minimální délku 12 znaků, neobejde se bez velkých a malých písmenek, čísel a speciálních znaků. A navíc musí uživatelé počítačových systémů každý rok vymýšlet heslo nové. Bavil jsem se s jedním kamarádem pracujícím ve velké nadnárodní firmě, který si na začátku říkal, že si prostě vytvoří dvě hesla, a ta bude pravidelně střídat. Jaké bylo jeho zklamání, když zjistil, že v řadě dvanácti za sebou jdoucích hesel se nesmí ani jedno opakovat. Tedy, že první heslo může použít až za třináct let! Naprosto jsem rozuměl jeho rozčilení, a tak udělal to, co dělá většina běžných uživatelů v podobné situaci – vytvořil si základ hesla a k němu každý rok přidal drobnou změnu. To je stav, o kterém naprostá většina odborníků tvrdí, že je velice špatný, a takto vzniklá hesla jsou snadněji prolomitelná. Snahy IT oddělení o bezpečnější systémy vedou paradoxně k menší bezpečnosti.

Spíš horší, než lepší

Typické heslo, které uživatel musí každý rok měnit, vypadá zhruba podobně jako to v nadpisu článku. Tedy nějaké základní slovo a k tomu se každý rok přidá jedno číslo. Útočníkovi pak už stačí jen zjistit ono základní slovo a výsledné heslo si sám odvodí. Možná i právě proto připravil americký Národní institut standardů a technologií (NIST) nová pravidla zabezpečení, ve kterých už odpadají nesmyslné požadavky, jako například výše zmiňovaná povinnost každoroční změny hesel, která ve výsledku stupeň zabezpečení spíše zhoršují, než zlepšují. Pravidla společnosti NIST platí pouze pro americké federální úřady, ale mnoho firem, včetně soukromých, se jimi řídí.

Americká pravidla

NIST mimo jiné navrhuje, že hesla musí mít alespoň 8 znaků a nesmí být povinná kombinace běžných znaků, číslic a zvláštních symbolů. Heslo s čísly a zvláštními symboly vyžaduje většina poskytovatelů internetových služeb a jak je vidět, na bezpečnost má spíše negativní vliv. Dále se nesmí vynucovat pravidelná změna hesel. (Doufám, že si to přečtou i lidé zodpovědní za bezpečnost ve firmách.) Hesla se musí měnit, jen pokud došlo k jejich prolomení a kompromitaci. Dále se nesmí používat autentizace založená na znalostech, jako například: „Jak se jmenoval váš první mazlíček?“

Babiččiny buchty

Jak je vidět, NIST vnímá bezpečnost hesel naprosto jinak a běžná intuitivní představa, že čím komplikovanější heslo, tím bezpečnější, není úplně pravdivá. Americká organizace navrhuje vytvářet spíše dlouhá hesla složená ze slov a vět. Heslo „mojebabičkapečenejlepšíbuchty“ je tedy bezpečnější než něco podobného jako „x5.y-;§@9xz.“ Navíc informaci, že moje babička peče nejlepší buchty, si pamatuji celý život, ačkoliv je už delší dobu peče v nebeském království. (Tedy aspoň doufám.)

Bez hesel

Celé moje povídání o heslech, bez kterých se nikdo neobejde, ale směřuje k blízké budoucnosti, ve kterých hesla údajně nebudou vůbec potřeba. Místo nich budeme používat tzv. přístupové klíče, pomocí kterých se budeme přihlašovat. Těmi přístupovými klíči jsou myšleny naše mobily, které disponují možností biometrického přihlášení, a to buď otiskem prstu, nebo vlastním obličejem. Už dnes po mně banka vyžaduje, abych se přihlašoval pomocí tohoto ověření. Moc se těším, až veškerá hesla skončí a bude se o nich vyučovat maximálně tak v hodinách dějepisu.

Foto: pathdoc, Vitalii Vodolazskyi, Mongta Studio - Adobe stock

Sebevražda

Napsal a nafotil: Zbyněk Pavienský