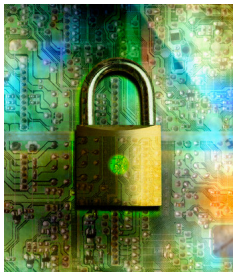

Bezpečné heslo uživatele je dnes základem bezpečnosti firemních dat, ale i těch vašich soukromých. Své o tom ostatně ví i UniCredit Bank, jejíž administrátor webových stránek měl údajně jedno z nejhloupějších hesel vůbec – Banka123. Pojďme se podívat na to, jaká hesla nejsou bezpečná a proč, jak nakládat se svými hesly a jak bezpečná hesla tvořit.

Jak se prolamují hesla

Než se pustíme do podrobnějšího povídání o tvorbě hesel, pojďme se podívat na to, jakým způsobem se dají prolamovat hesla.

Znalost majitele hesla je jednou ze základních technik, jak doslova „uhádnout“ vaše heslo. Data narození vás a vašich nejbližších, jejich jména a příjmení, jména vašich domácích mazlíčků, to vše patří mezi nejčastěji používaná hesla. Je dobré si také uvědomit, že data narození už zdaleka nejsou nějakým těžko dosažitelným údajem. Ministerstvo spravedlnosti je běžně dává do Obchodního rejstříku (včetně rodných čísel, která, pravda, teď musíte už někdy dohledávat až ve Sbírce listin) a spousta lidí je má uvedená na Facebooku a LinkedInu (proč by také ne, když je Ministerstvo spravedlnosti stejně u statutárních orgánů a vlastníků právnických osob masivně zveřejňuje).

Použití slovníků pro prolomení hesel je další z technik, která číhá zejména na ty, kteří rádi místo hesla používají nějaké slovo, a to i sofistikovanější než třeba „heslo“ nebo „password,“ což jsou jedny z nejčastěji používaných hesel. Programy pro prolamování hesel běžně umějí pracovat se slovníky jednotlivých jazyků. Během pár sekund pak dokáží prostřednictvím specializovaného programu, který je obvykle volně ke stažení, vyzkoušet stovky tisíc slov – ta se většinou zkouší na nějakém souboru s vaším uloženým klíčem (kdysi to šlo zejména ve Windows XP velice jednoduše). Při přihlašování např. do vaší e-mailové schránky nebo internetového bankovnictví už to zas tak jednoduché není. Přesto, i když si zvolíte jako heslo

nejdelší české slovo: „nejneobhospodařovávatelnějšího," nebude to bezpečné heslo.

Použití kombinace čísel a slov je další technikou prolamování hesel. Ta byla pravděpodobně použita i v případě UniCredit Bank. Programy na prolamování hesel přitom běžně umožňují nastavit zkoušení kombinací slov a čísel před anebo za slovem ze slovníku. Použití čísel prolomení hesla značně zpomaluje (z jednotek minut jsou to najednou desítky až stovky), ale pořád se bavíme o velice rychlém prolomení hesla. Navíc některé programy umožňují zkoušet třeba jen oblíbené kombinace jako právě „123" anebo případně zadat nějaké konkrétní číslo (např. rok vašeho narození).

Útok hrubou silou neboli brute-force attack je poslední a nejméně šikovnou možností, kterou lze pro prolomení hesla použít. Program na prolomení hesla pak zkouší postupně všechny kombinace velkých a malých písmen, číslic i zbylých znaků na klávesnici na všech pozicích. Doba potřebná k prolomení hesla pak roste exponenciálně v závislosti na jeho délce. Proto se dnes požaduje délka hesla aspoň 8 znaků, aby jeho prolomení hrubou silou z jednoho počítače trvalo řádově dny až týdny.

Jak se zjišťují hesla

Útok hrubou silou, ale koneckonců i zkoušení slov ze slovníku, může být někdy časově poměrně náročnou činností. Mnohem elegantnější je proto zkusit si vaše heslo zjistit. Tím se zároveň obejde problém s bezpečnými hesly (viz dále). A jak se hesla zjišťují?

Okoukání z klávesnice je jedním z nejstarších a nejelegantnějších způsobů, jak zjistit heslo, případně PIN k vaší platební kartě. Tím, že budete své heslo zadávat před útočníkem, nebo v dnešní době spíše před nějakou kamerou, která například v kavárně vidí na vaše prsty na klávesnici na vašem notebooku, můžete snadno sdělit útočníkovi vaše heslo.

Přečtení si hesla na papírku, kam jste si ho napsali je jedním z nejhloupějších a přesto velice častých příkladů, jak zjistit vašeho heslo. Legendární jsou zejména historky, kdy si zaměstnanci své přihlašovací údaje napíší na post-it papírek, který si nalepí na svůj monitor. A dlužno dodat, že na rozdíl od jiných legend je tohle bohužel popis běžné reality. Řada lidí si také píše hesla na papírky v peněženkách, do mobilu anebo do nešifrovaných souborů. Je přitom zřejmé, že pokud někdo získá k těmto věcem přístup, získá přístup i k vašim heslům a přihlašovacím údajům.

Odesílání přihlašovacích údajů prostřednictvím nešifrovaných protokolů a přenosů je další z častých neduhů. Tento způsob získávání hesel pomocí tzv. sniffingu byl v jednu dobu populární zejména u uživatelů Facebooku, kteří nepoužívali k přihlašování HTTPS (S jako Secure) protokol. K zjišťování takto odesílaných hesel se používá analyzátor paketů. Ten buď zachytává pakety na nezabezpečené WiFi např. v kavárně či restauraci, anebo může zachytávat pakety na trase mezi vaším počítačem a serverem, ke kterému na internetu přistupujete. Pokud se přihlašujete prostřednictvím nešifrovaného protokolu HTTP nebo FTP, přenáší se všechny vaše přihlašovací údaje nešifrovaně od vašeho počítače až k příslušnému serveru a kdokoliv vybavený příslušným volně dostupným software si je může přečíst. Totéž se týká i nešifrovaného přihlašování k poštovnímu serveru prostřednictvím protokolů POP3 a SMTP anebo odesílání přihlašovacích údajů v nešifrovaném e-mailu. Pokud své přihlašovací údaje zkrátka vyšlete do internetu prostřednictvím libovolného komunikačního protokolu a kanálu je to stejné, jako kdybyste uprostřed náměstí plného lidí křičeli své přihlašovací údaje do megafonu. Spoustu lidí to absolutně nebude zajímat, spousta lidí ani nepostřehne, že jste je tam říkali, ale někdo si je může zapamatovat a později využít.

Získání vašich přihlašovacích údajů k jiné službě je dalším způsobem, jak jednoduše získat vašeho heslo. Řada provozovatelů internetových služeb bohužel ukládá vaše heslo v textové podobě a nikoliv ve formě kontrolního součtu, ze kterého je nadmíru těžké až nemožné původní heslo získat. Pokud je vaše heslo uložené jen jako text, může si ho provozovatel dané služby kdykoliv přečíst. Pokud pak stejné přihlašovací údaje využíváte i k jiným službám, není pro něj problém získat k nim přístup.

Využití keyloggerů na počítači, ze kterého se přihlašujete je další možností, jak zjistit vaše heslo. Keylogger je škodlivý software, který zaznamenává všechny stisky klávesnice. Ty pak nechává v souboru na disku, kde si je útočník vyzvedne (např. u počítače v internetové kavárně) anebo je útočníkovi odesílá prostřednictvím internetu (v případě infikováni vašeho vlastního počítače).

Jak zvolit bezpečné heslo

Bezpečné heslo by mělo splňovat několik základních zásad:

- Neobsahovat slova ze slovníku libovolného jazyka
- Obsahovat kombinaci velkých a malých písmen
- Obsahovat číslice, a to nikoliv v obvyklé posloupnosti „123“ ani z vašeho data narození nebo data narození vašich blízkých. Číslice je dobré kombinovat s písmeny.

- Obsahovat speciální znaky jako např. zavináč, tečka apod.
- Být aspoň 8 znaků dlouhé
- Vyvarovat se posloupností znaků z klávesnice (např. qweASD)

Nejčastěji uváděným příkladem bezpečného hesla je např. „P@$$w0rd," což je zároveň ideální příklad hesla, které nikdy nepoužívejte, protože je modelovým příkladem, který najdete všude. Jen na Googlu má 280 000 výskytů.

Jak je zřejmé z výše uvedeného popisu, tak nároky na heslo jsou poměrně velké a pro řadu lidí může být komplikované si takové heslo zapamatovat. Tím spíš, pokud si má takových hesel zapamatovat více. Existuje proto několik způsobů, jak taková bezpečná hesla vytvářet. Jedním z nich je samozřejmě použít běžné slovo a nahradit některé jeho písmena různými znaky. Např. „Bu$inessV1z€". Dalším způsobem je použít nějakou dobře zapamatovatelnou větu, buď třeba oblíbený citát, anebo větu popisující vaši každodenní činnost. Třeba z věty „Každý den vstanu v 8, dám si šálek čaje" lze vytvořit heslo: „Kdvv8,d$sc."

Jak nakládat s bezpečným heslem

Když už bezpečná hesla používáte, je potřeba s nimi také bezpečně nakládat. Uveďme si proto několik zásad, jak nakládat s bezpečnými hesly:

- Nepřihlašovat se z cizích počítačů/telefonů/tabletů (nebezpečí keyloggerů)
- Chránit svůj počítač/telefon/tablet před škodlivým software (nebezpečí keyloggerů)
- Nikdy si nepsat heslo na papírek ani do nešifrovaného souboru
- Nikdy si heslo nikam nepsat, nesdělovat ho nikomu a neposílat ho nikomu e-mailem
- Nikdy se nepřihlašovat nešifrovaným protokolem
- Nezadávat heslo v přítomnosti třetí osoby anebo v místě, kde kamera může zabírat vaše ruce na klávesnici (jde vyřešit pomocí
- Pravidelně heslo měnit (např. jednou za 3 měsíce), a to i proto, že výše uvedeného se ani při vší opatrnosti ne vždy vyvarujete
- Používat různá hesla pro různé služby
- Změnit heslo pokaždé, když se domníváte, že mohlo být prozrazeno.

Použité zdroje a literatura

1. Keystroke logging. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-06-12]. Dostupné z: http://en.wikipedia.org/wiki/Keylogger
2. Packet analyzer. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA):

Wikimedia Foundation, 2001- [cit. 2013-06-12]. Dostupné z: http://en.wikipedia.org/wiki/Packet_analyzer

3. Brute-force attack. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-06-12]. Dostupné z: http://en.wikipedia.org/wiki/Brute-force_attack