Používate bezpečné heslo?

Skúste sa na chvíľu zamyslieť na tým, koľko hesiel ste dnes zadali. Prvým heslom asi bude PIN vášho mobilného telefónu. Nasleduje prihlásenie sa do počítača v zamestnaní, heslo na firemný server, heslo na e-mail, heslo na súkromný e-mail, heslo na internet banking, heslo na prihlásenie na chat... Ešte šťastie, že starý dobrý Windows si pamätá väčšinu z týchto hesiel. Heslo do Windows býva teda obyčajne akýmsi kľúčom všetkých kľúčov. Po odomknutí jediných dverí máme prístup nielen ku všetkému, čo sme na počítači kedy vytvorili, ale navyše aj k mnohým ďalším službám, ktorých heslá si už ani nepamätáme. Je preto veľmi dôležité vedieť si správne vybrať heslo.

Stačí si pozrieť niektorý z mnohých zoznamov hesiel užívateľov, ktorý bol zverejnený na internete „vďaka“ niektorému hackerovi. Prevládajú heslá veľmi jednoduché, máloktoré má viac ako 5 znakov. Existuje množstvo programov, ktoré dokážu zistiť prístupové heslo do Windows. Všetky majú spoločné jedno...

ROZLÚSKNUTIE HESLA JE OTÁZKOU ČASU

Ten, kto má fyzický prístup k vášmu počítaču, dokáže veľmi jednoducho (najmä ak používate operačný systém Windows 95/98) nainštalovať do vášho počítača program, ktorý hľadá heslá. Ak je vaše heslo napríklad slovo „leto“, útočník ho zistí na priemerne rýchlom počítači za menej ako minútu. Originálne slovo ako „cukrik“ zabaví útočníka sotva na hodinu. Pozrite si tabuľku, ktorá znázorňuje, ako dlho trvá rozlúsknutie rôznych hesiel tou najjednoduchšou metódou – brute force, teda brutálnou silou pomocou bežne dostupných nástrojov, ktoré nájdete napríklad aj na ***www.lastbit.com***:

Počet znakov	Bežná abeceda – 26 znakov (nerozlišuje veľké a malé písmená)	36 znakov (len písmená a čísla)	52 znakov (veľké aj malé písmená)	96 (všetky znaky)
4	0	0	1 minúta	13 minút
5	0	10 minút	1 hodina	22 hodín
6	50 minút	6 hodín	2,2 dní	3 mesiace
7	22 hodín	9 dní	4 mesiace	23 rokov
8	24 dní	10,5 mesiaca	17 rokov	2287 rokov
9	21 mesiacov	32,6 roka	881 rokov	219 000 rokov
10	45 rokov	1159 rokov	45 838 rokov	21 milión rokov

Zdroj: www.lastbit.com

Z tabuľky je zrejmé, že väčšinu našich hesiel zistí útočník do hodiny. Nehovoriac o tom, že niektoré programy dokážu pracovať na pozadí a potichu vyhľadávať heslo. Brániť sa môžeme len jediným účinným spôsobom – zvoliť si heslo, ktoré má minimálne 8 znakov a obsahuje aj veľké, aj malé písmená a číslice. Ak sa vám podarí zapamätať si ešte aj niekoľko znakov, ako napríklad „!&^#$%“, útočník s takýmto programom v podstate nemôže uspieť.

Hacker teda s vami zvádza nerovný boj – kým vy zadáte o jeden znak viac, on musí zrýchliť svoje výpočty minimálne 26-násobne – v ideálnom prípade. V tom „najhoršom“ prípade takmer 100-násobne. Preto je zrejmé, že ak si vy dobre zvolíte heslo, útočník používajúci jednoduché metódy zisťovania hesla nemá prakticky nijakú šancu.

Šance útočníkov však zďaleka nie sú také malé, ako by sa mohlo zdať. Sofistikované programy, používajúce napr. tzv. Smart brute force, dokážu aj 10-znakové heslo prelomiť aj za menej ako hodinu. Je to možné vďaka ľudskej vlastnosti zadávať skôr slová ako znaky. Málokto si totiž chce zapamätať heslo ako „Da&3*?b“. Preto vyspelejšie programy vyhľadávajú napríklad priamo slovné spojenia.

Nedávno sa objavili správy o metóde, pomocou ktorej dokázali vedci odhaliť až hrozivých 99,9 % alfanumerických hesiel za neuveriteľných 14 sekúnd! Metóda je postavená na nedokonalosti šifrovania Windows. Tento najpoužívanejší operačný systém totiž dve rovnaké heslá zašifruje

Slovník terminológie

■ **Enkryptovanie**
Transformovanie dát do takej podoby, ktorá je nečitateľná. Enkryptovať môžete rôznymi spôsobmi. Najjednoduchšími metódami sú napríklad vymenenie písmen za číslice alebo rotovanie znakov. Zložitejšie metódy používajú prakticky nezistiteľné algoritmy pomocou využitia výpočtovej techniky.

■ **Dekryptovanie**
Proces dešifrovania enkryptovaných dát. Jednoducho to znamená odstránenie enkrypcie pomocou správneho kľúča.

■ **Hash**
Hashing je metóda vytvorenia jedinečných znakov pre daný záznam. Teoreticky útočník nemôže získať zo zahashovanej verzie heslo. Táto nezvratná metóda (nie je možné dekryptovať hash) sa používa najmä pri ochrane hesla. Systém teda nepozná vaše heslo – len jeho zašifrovanú podobu.

rovnako. Preto vám stačí veľký súbor hesiel, resp. ich zašifrovanej podoby, nahrať do pamäte RAM počítača a nechať počítač pracovať... pár sekúnd. Tým, že zadáte špeciálne znaky, odhalenie hesla síce spomalíte, ale nezastavíte. Útočník si jednoducho „posedí“ pri počítači o niekoľko sekúnd dlhšie alebo si zoženie väčší súbor dát. Vaše heslo však musí existovať v danej databáze. Databáz používaných hesiel je však aj na internete veľa. Ochrana? Použiť zložité heslo, nie slovo ani súbor slov!

AKO JE TO V KONKURENČNÝCH OPERAČNÝCH SYSTÉMOCH?

Spomeňme si aspoň Linux. Vďaka svojej povahe otvoreného systému Linux umožňuje modulárne spôsoby šifrovania alebo „vlastnú tvorbu“ – teda môžete si naprogramovať alebo nahrať taký modul hashovania, ktorý vám vyhovuje. Bežne sa používa napríklad metóda MD5 so seedom, ktorá zabráni tomu, aby boli dve heslá zahashované rovnako, ako je to napríklad vo operačných systémoch Windows. Úroveň bezpečnosti je teda vyššia ako v systéme Windows. Samozrejme, platí to, čo v operačných systémoch Windows – ak si zvolíte štvormiestny kód, odhalenie bude s najväčšou pravdepodobnosťou otázkou niekoľkých minút.

Ak potrebujete skutočne profesionálnu ochranu prístupu k počítaču, riešením zrejme nebude prejsť na iný operačný systém. Ponúka sa jednoduché riešenie – zašifrovať obsah pevného disku niektorým zo špeciálnych programov. Počítač spustí operačný systém až po tom, čo správne zadáte heslo. Keby aj útočník vybral pevný disk a vložil ho do iného počítača, kde by sa pokúsil dostať k jeho obsahu, neuvidel by nič. Takéto zašifrovanie dát však znamená spomalenie práce s pevným diskom (približne o 30 – 50 %), ako aj riziko, že ak heslo zabudnete, prídete o všetky dáta na disku...

TAKŽE ČO PORADIŤ NA ZÁVER?

1 Najdôležitejšie: Heslo do Windows si vyberte starostlivo. Malo by mať minimálne 8 znakov, malo by obsahovať číslice aj špeciálne znaky. Mohlo by vyzerať napríklad takto: „4K;-ah@J“

2 Používajte organizéry hesiel. Ide o program, ktorý starostlivo zakryptuje vaše heslá. Stačí vám teda vedieť jediné heslo (samozrejme, iné ako to, ktoré ste použili na vstup do operačného systému), ktorým sa dostanete ku všetkým. Toto heslo však musí stáť za to!

3 Pokúste sa heslo vybrať náhodne, nie slovo.

4 Pamätajte, že prelomenie hesla závisí od toho najslabšieho článku. Ak si hoci aj 15-miestnym heslom „zaheslujete“ Word 7.0, útočník ho zistí takmer okamžite! Pozor na nezabezpečené internetové servery! Váš provider emailových služieb pravdepodobne pozná aj vaše heslo do POP schránky! Ak ste pripojení na internet prostredníctvom mikrovlnného pripojenia, ktoré je navyše nešifrované, prakticky všetky vaše dáta, ktoré posielate cez internet, môžu byť veľmi jednoducho prečítané nepovolanou osobou.

5 Heslo si nezapisujte, pamätajte si ho!

6 Pri zadávaní hesla sledujte svoje okolie a uistite sa, že heslo píšete do správnej kolónky.

7 Heslo si z času na čas meňte (optimum je každé dva týždne).

8 Ak má niekto fyzický prístup k vášmu počítaču alebo má priamo na ňom konto, šanca na „úspech“ je oveľa vyššia.

Na záver tip pre tých najostražitejších:
Keďže úroveň ochrany prístupového hesla vo Windows nie je vysoká, nehovoriac o množstve ďalších ciest, ako sa dostať k heslu (napríklad útočník môže sledovať, aké klávesy ste stláčali), mám pre vás radu:

1 Z internetu si zadarmo stiahnite niektorý z početných freeware programov na šifrovanie a vytváranie kľúčov.

2 Stiahnite si program šifrovania dát v reálnom čase (napr. BestCrypt – nie je dostupný ako freeware).

3 Nechajte si vygenerovať kľúč – heslo pozostávajúce napr. zo 128 znakov.

4 Tento kľúč si uložte napríklad na disk USB, ktorý nosíte stále so sebou.

5 Zašifrujte si napríklad Moje dokumenty jedným z ponúkaných algoritmov, ako heslo si zvoľte to, ktoré máte na disku USB.

6 Všetky dôležité údaje si ukladajte výlučne do zašifrovaného adresára Moje dokumenty.

7 Nastavte si bezpečnostnú politiku tak, že sa adresár automaticky zašifruje napríklad po 1 hodine nečinnosti.

8 Pokiaľ vám nikto nezoberie kľúč USB, má len veľmi teoretickú šancu, že sa dostane k vašim dokumentom.

Daniel Keder