Chraňte svá data

Počítače jsou vám bližší, než si možná připouštíte. Svěřujete jim osobní nebo citlivé firemní informace, které by nikdo jiný zhlédnout neměl. Jak efektivně data v počítači ochránit před zvědavci či zloději? [Jiří Kuruc]

Začněme nevesele, ale realisticky: ochrana dat a soukromí v dnešním propojeném světě není nic jednoduchého, jedinou univerzální radu nečekejte. Cílem článku je nastínit možné scénáře úniku vašich dat a co možná nejvíce ztížit zvědavcům, nebo rovnou útočníkům, jejich získání a přečtení. Často navíc úroveň bezpečnosti nezávisí jen na vás, ale i na programátorech a administrátorech vámi využívaných služeb, jejichž

Peníze utracené za programy pro správu hesel jsou investicí, která se rozhodně vyplatí

práci zkrátka neovlivníte. Vy ale vždy můžete pro bezpečnost svých dat učinit maximum. Zároveň vezměte na vědomí zacílení článku: jinou úroveň zabezpečení požaduje tajná služba a jinou majitel počítače s účetnictvím malé firmy.

Heslo jako základ

Bezpečnost stojí a padá s korektní autentizací. Jedná se o proces identifikace uživatele – ověření, že je skutečně tím, za koho se vydává. Způsobů autentizace existuje nepřeberné množství, o těch nejznámějších si přečtete v boxíku na protější straně. Základním způsobem je však již od nepaměti heslo, které zná, nebo by alespoň měl znát, pouze daný uživatel.

Avšak právě při tvorbě hesel uživatelé často velmi chybují. Vyjma administrátorů majících přístup k citlivým datům přitom nelze mít nikomu za zlé, že si nepamatuje třeba velmi silné heslo **Isoer,79d.§rix12.dR!**. Uživatelům ale lze mít za zlé následující:

- Používání krátkých hesel, tzn. s méně než 8 znaky.
- Používání snadno odhadnutelných hesel, viz boxík 25 nejpoužívanějších hesel v roce 2013.
- Používání stejných hesel napříč různými službami.
- Používání zjistitelných správných odpovědí na kontrolní otázky.

Lze jednoznačně stanovit, kolik znaků stačí pro bezpečné heslo? Nelze, vždy totiž záleží na možnostech útoku vedoucího k jeho odhalení. Rozlišujeme dva druhy útoků:

- Útok hrubou silou (Brute Force) – zkoušení všech kombinací hesel. Pomalejší, ale jistý způsob odhalení hesla.
- Slovníkový útok (Dictionary Attack) – výběr a zkoušení pouze nejpoužívanějších hesel. Nezaručuje úspěch, avšak odhalení může být velmi rychlé, jelikož uživatelé hesla jako **aaa**, **ahoj**, **abc**, **heslo**, **123** a jejich obměny v daném jazyce velmi často používají.

Pokud je například nějaká webová služba nastavena tak, že po třech neúspěšných pokusech o zadání hesla zablokuje účet na dalších 10 hodin, výrazně se prodlužuje doba pro úspěšný útoku hrubou silou i u krátkého pětiznakového hesla. Pokud ale administrátor této služby umožní nekonečné a neomezené zkoušení hesla, bude útok dříve nebo později úspěšný. Jde jen o to, kde leží ono „později“. Útok obvykle probíhá kombinovaně, nejprve se zkouší slovníková hesla a po neúspěchu přichází hrubá síla.

Problém nastává ve chvíli, kdy se útočník zmocní celé databáze hesel uživatelů. A že se tak děje, dokazují nedávné útoky na Sony, Adobe nebo Dropbox. Hesla jsou obvykle zašifrovaná, i tak je lze prolomit. Podrobnější popis šifrování hesel a útoku na šifry popisujeme v boxíku **Jak lze prolomit šifrovaná hesla?** na straně 15.

Parametry bezpečného hesla dříve splňovalo heslo s délkou alespoň 8 znaků kombinujících velká a malá písmena, číslice i speciální znaky. Mnoho služeb takové heslo stále vyžaduje a nutno podotknout, že se hůře pamatují. Lze si pomoci berličkou: různá písmena lze nahradit podobnou číslicí, některé písmeno uděláte velké a přidáte speciální znak. Například dobře odhadnutelné heslo **Computer** lze zaměnit za **COmpu!3r**, které bude útoku hrubou silou odolávat výrazně déle. Útočníci však obvyklé záměny o → 0, e → 3, i → ! a podobné znají a přidávají je do svých slovníků.

Právě z tohoto důvodu se v posledních letech od složitého hesla upouští a doporučuje se klidně jednodušší, zato co možná nejdelší heslo. Zatímco **COmpu!3r** je dlouhý 8 znaků, **computerjecasopis** má již 17 znaků. Teoreticky by mohlo heslo rychle podlehnout slovníkovému útoku, ovšem za předpokladu, že by takový slovník byl v češtině, a především obsahoval i logické fráze. Stačí ale mírná modifikace na **COmputerIsCasak!**, a přestože je heslo o znak kratší, vykáže díky nahrazení českého slova **je** za anglické **is** odolnost proti slovníkovému útoku a současně zahrnutím velkých písmen, číslic a speciálních znaků vzroste odolnost proti útoku hrubou silou. Dlouhé frázové heslo navíc obvykle napíšete na klávesnici mnohem rychleji než heslo krátké, z nesmyslně složených znaků. Vyzkoušejte si to.

Druhým velkým prohřeškem je používání stejných hesel napříč různými službami. Použít stejné heslo do diskusního fóra o autech, které vytvořil a spravuje samouk a nadšenec Franta Vonásko, a do internetového bankovnictví je nejlepší cestou, jak o úspory přijít. Řešení je prosté a účinné, pro různé služby si vymyslete příhodná frázová hesla: **radjezdimautem** a **penizevbezpeci**. Zvýšení bezpečnosti těchto hesel máte za domácí úkol.

Tip: Chcete vědět, jak silná jsou vaše hesla? Služba Microsoftu na **jdi.zive.cz/heslo** vám to po jeho zadání prozradí. Jako nejsilnější bude označeno heslo s alespoň 14 znaky, současně obsahující velké písmeno, číslici a speciální znak.

Spousta služeb také stále využívá kontrolní otázky, na které je uživatel dotázán při zapomenutí nebo při špatném zadání hesla. Problém tkví v tom, že spousta uživatelů zde logicky zadává pravdivé informace: **Rodné jméno vaší matky** nebo **Město, kde jste se narodil** jsou informace, které lidé ve vašem okolí znají. Své by o tom mohla vyprávět Paris Hilton, jejíž telefonní seznam a pár lechtivých fotografií uniklo do vln internetu v únoru 2005. Útočník se zde do uživatelské služby T-Zones amerického T-Mobilu dle některých zdrojů dostal poté, co na kontrolní otázku **Jméno vašeho domácího mazlíčka** zadal jméno čivavy, kterou Paris často a ráda vystavovala objektivům fotoaparátů.

Kontrolní otázky nejsou v principu špatnou ochranou, špatné je odpovídat na ně pravdivě. Vymyslete si vlastní odpovědi, zcela nesmyslné a neodhadnutelné, avšak zároveň takové, které si zapamatujete.

V dnešní době používáte často desítky služeb a dle výše uvedených pravidel byste si proto měli pamatovat desítky různých, dlouhých a upravených frázových hesel. To obvykle nelze. Dále poradíme nástroje, které vám s hesly pomohou. Nyní se zaměříme na základní zabezpečení počítače a dat v něm uložených.

Heslo po startu počítače

První, účinnou, avšak přitom málo používanou zdí chránící data ve vašem počítači je prosté heslo vyžadované ihned po startu počítače. Nastavuje se v BIOSu či EFI, který sám by měl být chráněn heslem. Na současných základních deskách se tato hesla rozlišují jako administrátorské (do BIOSu či EFI) a uživatelské, právě to je po startu vyžadováno ještě před tím, než získáte možnost se do BIOSu dostat.

Jde o dobré řešení proti zvědavcům a nezkušeným uživatelům, kteří po sobě nemohou zanechat stopy, typicky kolegové v práci. Dokonce zde stačí použít krátké, avšak neodhadnutelné heslo, které většinu odradí. Avšak pozor, při krádeži celého počítače či notebooku lze heslo jednoduše obejít vyjmutím pevného disku a jeho připojením k jinému počítači. Pokud krádež nehrozí, což nelze nikdy vyloučit, zamkněte si alespoň počítač, aby se útočník k disku nedostal. Avšak upřímně, existují lepší způsoby ochrany.

Heslo k uživatelskému účtu

Uživatelské účty dobře poslouží v běžné rodině s více členy a sdíleným počítačem. V první řadě zde uživatelé často chybují ponecháním aktivního účtu hosta, prostřednictvím kterého se útočník může přihlásit a dostat se tak k datům mimo vaši osobní složku. Všichni uživatelé by proto měli být chráněni heslem. Druhým tradičním prohřeškem je ponechání dalších členů domácnosti jakožto administrátorů. Vinou toho se kdokoli dostane kamkoli na disku, i do osobních složek.

Přihlášení do Windows, OS X i Linuxu obvykle probíhá pomocí klasického hesla. Existují však i jiné možnosti: snímání obličeje vestavěnou kamerou nebo vestavěná nebo připojená čtečka otisku prstů. Standardní možnosti ve Windows 8.1 jsou následující:

Heslo: klasické heslo obsahující písmena, čísla a znaky.

Obrázkové heslo: vyberete si libovolný obrázek na disku a v něm postupně označíte tři místa, přičemž označením může být nejen klepnu-

25 nejpoužívanějších hesel v roce 2013

Server SplashData News (**splashdata.blogspot.cz**) každý rok uvádí Top 25 nejpoužívanějších hesel. Žebříček sestavuje z úniků databází, které hackeři vystavili veřejně na internetu. Ročník 2013 značně ovlivnil únik více než 38 milionů uživatelských účtů společnosti Adobe, to kdybyste se divili, proč je v Top 25 na desátém místě heslo **adobe123** a na patnáctém místě **photoshop**. Hezký příklad toho, že vytvářet hesla relevantní k dané službě není dobrým nápadem.

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123
11. 123123
12. sunshine
13. 1234567890
14. letmein
15. photoshop
16. 1234
17. monkey
18. shadow
19. sunshine
20. 12345
21. password1
22. princess
23. azerty
24. trustno1
25. 000000

Způsoby autentizace

Autentizace je proces ověření identity uživatele, tedy že ten, kdo se vydává za Karla, je skutečně Karel osobně. Existují desítky způsobů autentizace lišící se úrovní bezpečnosti (odolnosti proti útoku) a složitostí, jak pro uživatele, tak pro autentizační proces anebo samotné zařízení. Proces musí být navíc nastaven tak, aby nedovoloval falešné autentizace a současně správně rozpoznal pověřené osoby. Pokud by snímače otisku prstu na iPhonu nebo Samsungu zafungoval vždy až na třetí pokus, uživatelé by jej přestali používat, obtěžoval by je.

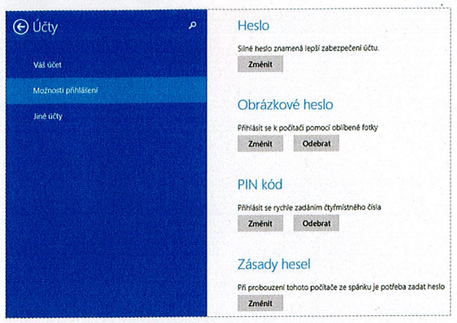
Zdaleka nejrozšířenější autentizací je **heslo**, které zná pouze Karel. Autentizace heslem, ať už v jakékoli podobě (heslo, PIN, obrázková gesta), je jednoduchá z pohledu zařízení, není vyžadován žádný dodatečný hardware. Nejslabší stránkou hesla je samotný uživatel a také způsob ochrany databáze hesel na straně zařízení, aplikace či služby. Za určitou obměnu hesla lze považovat i grafické gesto.

Pro autentizaci se stále častěji využívají jedinečné charakteristiky lidí. Karel má unikátní **otisk prstu**, snímače dnes najdete u byznysových notebooků a stále častěji i v chytrých telefonech. První verze snímačů bylo možné obejít, dnes již legendární je pokus s otiskem na skleničce a rozpuštěnými gumovými medvídky, které posloužily k vytvoření duplikátu. Moderní snímače jsou již odolnější, často snímají krevní řečiště nebo vodivost prstu.

Oční duhovka je jedinečnou vlastností každého člověka, proto se skvěle hodí pro autentizaci. Problém tentokrát tkví v zařízení pro snímání oka, které je v současné době velmi složité. S rostoucím rozlišením a kvalitou i miniaturních kamer se dříve nebo později dočkáme třeba telefonů, které sejmou naši duhovku pomocí přední kamery a tím nás jednoznačně identifikují.

Pro doplnění vzpomeňme i další způsoby: **identifikace hlasu** anebo **celého obličeje**, obojí však skrývá různé problémy: hlas se vám změní při nachlazení, ošálit snímání obličeje často lze prostou fotografií a podobně.

Podle našeho názoru je v současné době nejpříjemnějším a dostatečně bezpečným způsobem autentizace otiskem prstu, avšak v realizaci, jakou nabízí Apple se svým TouchID nebo Huawei Ascend Mate 7, tedy žádné přejíždění prstu, pouhé pohodlné přiložení.



Windows 8.1 nabízí tři různé způsoby přihlášení k účtu: tradiční heslo, obrázkové heslo a PIN kód

tí, ale i zakroužkování či podtržení. Zvolíte například záběr zátoky a vaším heslem bude klepnutí na loď, zakroužkování majáku a podtržení slečny pod slunečníkem. Uhádnout takové heslo je velmi složité.

PIN kód: jednoduchý čtyřmístný číselný PIN.

Druhé dva způsoby jsou velmi efektivní na dotykových zařízeních, nezdržují při zadávání. Rozhodně ponechejte aktivní vyžádání hesla po probuzení zařízení ze spánku.

Výhodou hesla je jednoduchost použití a jde o dobré řešení před zvědavci, kteří nemají čas a klid na překročení tohoto zabezpečení. Opět ale nepomůže při krádeži celého počítače, na internetu lze najít spoustu návodů a programů pro bootování z flashdisku, které odstraní heslo administrátora nebo vytvoří zcela nový účet. Stačí nabootovat některou z Live Linuxových distribucí a přístup k datům na disku je otevřen. Řešením je aktivace hesla do BIOSu a omezení bootování pouze na systémový disk. Toto však neřeší problém odcizení celého počítače a následného vyjmutí disku.

Bezpečnost soukromých dat

V případě běžných uživatelských účtů se všichni dostanou na celý obsah disku vyjma soukromých složek v adresáři Users (Plocha, Dokumenty, Obrázky a další). Administrátor má přístup do složek všech.

Chcete-li určitou složku na disku zpřístupnit pouze sobě, případně jen vybraným uživatelům, klepněte na ni pravým tlačítkem a z nabídky zvolte **Sdílet s** a zde vyberte uživatele. 1 Následně ve stejné nabídce zvolte **Konkrétní lidé...**, 2 kde zvolíte, zda má uživatel právo pouze čtení, nebo má možnost obsah složky i měnit.

Tento způsob ochrany určitých dat se opět hodí spíše jen pro domácí rodinné počítače. Přestože je složka sdílena jen s určitým uživatelem, jiný uživatel s administrátorskými právy se do ní dostane.

Šifrování vybraných dat

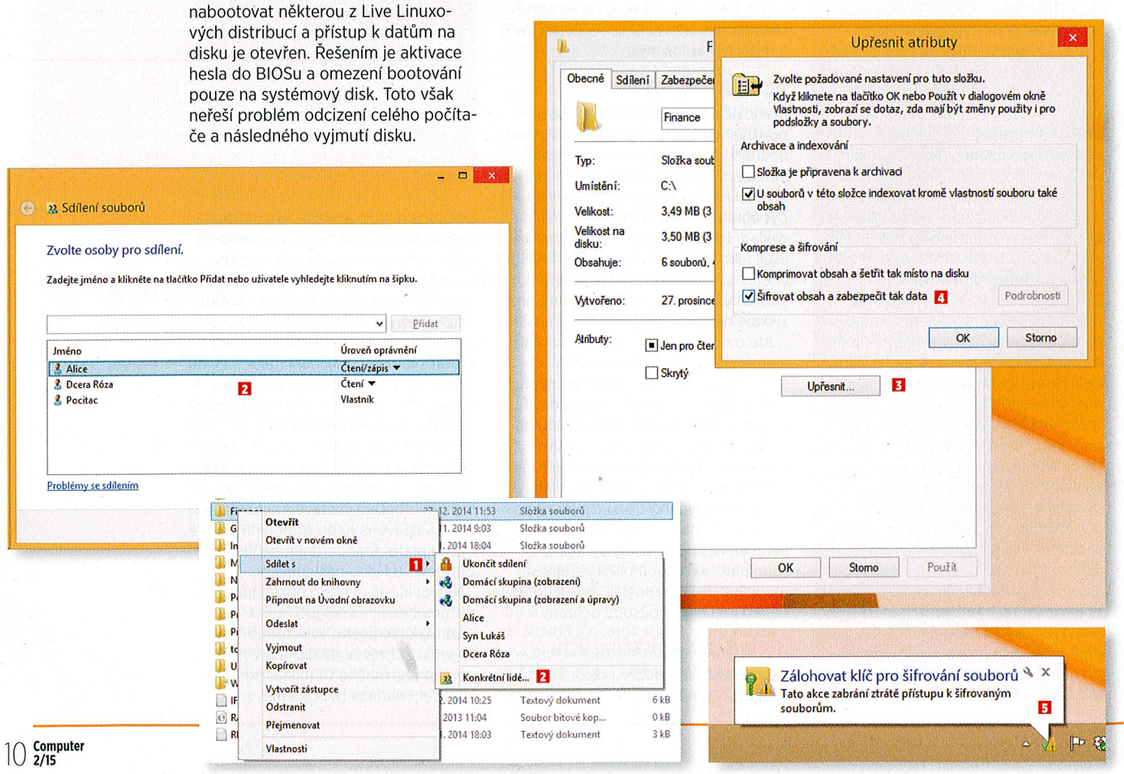
Doposud jsme řešili pouze to, jak zabránit neautentizovaným osobám v přístupu k vašim datům. Nastal čas data skutečně chránit, a to lze jedině šifrováním. Problematika šifrování by vystačila na samostatný článek, poradíme vám však první kroky.

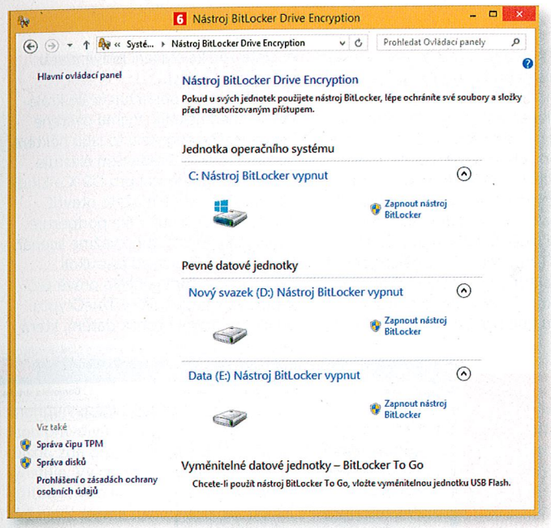
Rozlišujeme základní dva druhy šifrování: synchronní a asynchronní. První způsob hůře odolává útoku hrubou silou, vykazuje však až 1 000× vyšší rychlost než šifrování asynchronní, které naopak nabízí vysokou úroveň zabezpečení. Šifrování proto probíhá následně: pomocí asynchronního šifrování jsou zabezpečeny synchronní klíče, které se používají pro šifrování dat na disku. Jak je patrné, nejslabší místo řetězce představuje bezpečné uložení asynchronních šifrovacích klíčů. To jsme ale v teoretické úrovni, kterou neovlivníte. Podíváme se na praktické postupy zabezpečení dat.

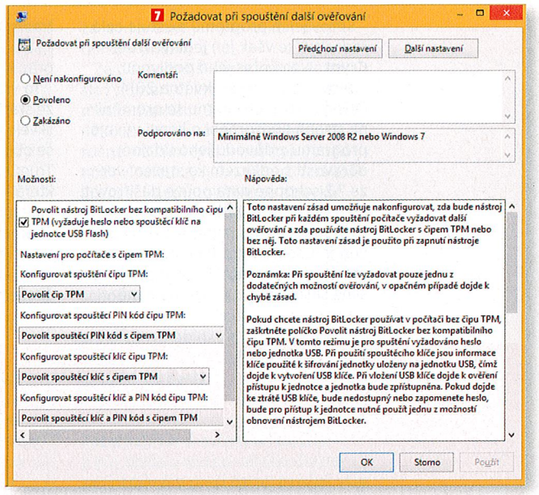
EFS: šifrování adresářů a souborů

Technologie EFS sloužící k šifrování dat je stejně stará jako NTFS, tedy již od Windows 2000. Bohužel avšak ani dnes není podporována ve všech Windows: Vista od Business, 7 od Professional a 8.1 od verze Pro výše. EFS lze použít právě pouze se souborovým systémem NTFS, používáte-li například na flashdisku FAT32 nebo ExFAT, budou sem zkopírované zašifrované soubory dešifrovány. Jelikož se data šifrují vaším osobním certifikátem a klíčem uloženým v počítači, nemůžete bez jejich přenesení data rozšifrovat na jiném počítači.

Výhodou EFS je jednoduchost použití. Vytvořte adresář, do kterého budete ukládat zašifrovaná data. Klepněte na něj pravým tlačítkem myši a zvolte **Vlastnosti**. V první záložce **Obecné** zvolte **Upřesnit** 3 a zcela vespod zatrhněte **Šifrovat obsah a zabezpečit tak data**. 4 Pokud již adresář obsahuje nějaké soubory, budete upozorněni, že dojde k jejich zašifrování. Stačí vše odsouhlasit a od této chvíle získáte k souborům v adresáři přístup pouze vy po úspěšném přihlášení. Zašifrované soubory poznáte snadno, názvy jsou nikoli černé, ale zelené. Šifrovat







celou složku je navíc velmi pohodlné, veškeré sem přesunuté soubory jsou zašifrovány automaticky a při otevírání není heslo vyžadováno.

Po prvním zašifrování se objeví výzva k zálohování certifikátu a klíče, 5 což vřele doporučujeme. Pokud by se například operační systém zhroutil, přijdete o klíče a tím i o svá data. Přístup k datům můžete povolit i dalším uživatelům počítače, avšak již na úrovni konkrétního souboru. Vedle zatržítka pro aktivaci šifrování klepněte na **Podrobnosti** a zde přidejte dalšího uživatele. Pokud v nabídce daný uživatel není, nemá zatím vytvořen vlastní certifikát. Řešení je prosté: tento uživatel musí zašifrovat libovolný, klidně jen dočasný soubor, čímž dojde k vytvoření certifikátu.

Šifrování pevného disku

Heslo do počítače ani heslo do operačního systému neochrání data uložená na disku. Zloděj či útočník může vyjmout disk a připojit jej k počítači jinému, čímž obě zabezpečení obejde. Řešením je standardní šifrování veškerého obsahu disku. Dříve tento proces ukrojil z výkonu procesoru, dnes však zpomalení nezaznamenáte. Zároveň pamatujte: pokud heslo k disku zapomenete, můžete se se svými daty nadobro rozloučit.

Šifrování disku nabízí řada programů, ve Windows Vista a 7 (verze Ultimate a Enterprise) a Windows 8.1 (Pro a výše) však máte k dispozici systémový nástroj BitLocker. Majitelé jablečných počítačů mají již od verze 10.3 Panther takzvaný FileVault, standardní šifrování a dešifrování dat na disku za běhu. První verze uměly šifrovat jen domovskou složku uživatele, od OS X Lion však již lze šifrovat celý disk. Šifrování zapnete v **Předvolby systému – Zabezpečení a soukromí – FileVault**.

V případě Windows je aktivace šifrování mírně složitější. BitLocker totiž standardně vyžaduje základní desku s tzv. TPM (Trusted Platform Module) čipem, který slouží k bezpečnému uchovávání šifrovacích klíčů. Bývá standardem u byznysových notebooků, běžné základní desky ani domácí notebooky jej obvykle neobsahují. BitLocker ale můžete používat i bez TPM a za cenu nižší bezpečnosti. Neprovádí se například kontrola integrity systémových souborů při startu systému, kdy ještě nevládne klasický antivirový program.

1 Otevřete **Ovládací panely – Systém a zabezpečení – Nástroj BitLocker Drive Encryption**. 6 Zde vidíte seznam pevných disků uvnitř počítače i připojené flashdisky. Právě ty by měly být také šifrovány, pokud na nich přenášíte citlivá data.

2 Zapněte nástroj BitLocker u jednotky, kterou chcete šifrovat. Pokud vaše základní deska neobsahuje TPM čip, budete na tuto skutečnost upozorněni. V tomto případě stiskněte **Win+R** a napište **gpedit.msc**. Zde pokračujte přes **Konfigurace počítače – Šablony pro správu – Součásti systému Windows – Šifrování jednotky nástrojem BitLocker – Jednotky operačního systému**. Najděte položku **Požadovat při spouštění další ověřování** 7 a zde zvolte **Povoleno**.

3 Po této úpravě budete moct aktivovat šifrování i na počítači bez TPM čipu. V prvním kroku musíte zvolit, kam se uloží soubor pro případnou obnovu zapomenutého hesla. Můžete jej uložit na USB flashdisk, vytisknout nebo uložit do účtu Microsoftu. V tomto případě však musíte být k počítači připojeni právě prostřednictvím tohoto on-line účtu, a ne účtem lokálním. Doporučujeme uložit klíč na flashdisk a tento bezpečně uložit mimo počítač.

4 Následně zvolíte, zda bude systém pro dešifrování vyžadovat heslo, nebo vložený flashdisk. První případ bude zřejmě obvyklejší. Následně doporučujeme potvrdit, že chcete šifrovat veškerý obsah disku, a nikoli jen aktuálně využitý prostor. Smazaná data by bylo možné pomocí různých programů obnovit. Šifrování sice potrvá déle, jistota je ale jistota.

5 Doba šifrování se odvíjí od míry zaplnění disku. Při přístupu k zašifrovanému disku (při startu) či flashdisku budete následně vždy požádáni o heslo.

Budete-li potřebovat zašifrovaný flashdisk číst i na starších systémech (Vista, XP), budete potřebovat program BitLocker To Go. Stáhnete jej přímo ze stránek Microsoftu na **jdi.zive.cz/bitlocker**.

Šifrování disku je řešením i při krádeži notebooku – k datům se nikdo bez znalosti hesla nedostane ani po vyjmutí disku a jeho připojení k jinému počítači. Nelze jej však považovat za všelék, data jsou v bezpečí ve stavu vypnutí a v hibernaci, avšak po spánku a probuzení heslo vyžadováno není. Údajně však existují postupy, jak lze BitLocker obejít, a dle některých spekulací se špitá i o zadních vrátkách pro americkou Agenturu pro bezpečnost NSA. Pokud ale obchodujete s dětskou výživou, a ne s plutoniem a svá data chcete chránit před zvědavou konkurencí, poslouží šifrování skvěle.

Pamatujte také na skutečnost, že zašifrovaný disk neochrání vaše data před viry a další havětí, která řádí během spuštěného operačního systému, kdy jsou data přístupná. Neochrání proti malwaru, který sleduje úhozy na klávesnici a hledá hesla k vašim službám či k internetovému bankovnictví.

Když nepomohou Windows

Zatím jsme využívali standardní funkce operačních systémů, v případě Windows však jen u těch vyšších verzí. Účinně šifrovat a skrývat data však mohou všichni bez rozdílu verze operačního systému, bez pomoci aplikací třetích stran to však nepůjde.

Šifrovacích programů existuje celá řada, král je však jen jediný: **TrueCrypt**. A to i přes jeho podivnou královraždu dne 28. května 2014. Oficiální web programu se proměnil na strohé upozornění o konci vývoje programu z důvodu jeho údajné děravosti s odkazem ke stažení verze 7.2 schopné data pouze dešifrovat. Bezpečnostní chyba v TrueCryptu rozhodně nebyla, zdrojové kódy jsou veřejně dostupné a bylo provedeno i testování aplikace. Program pro silné šifrování dat je samozřejmě trnem v oku bezpečnostním agenturám a zásah proti programu pochází pravděpodobně právě odsud.

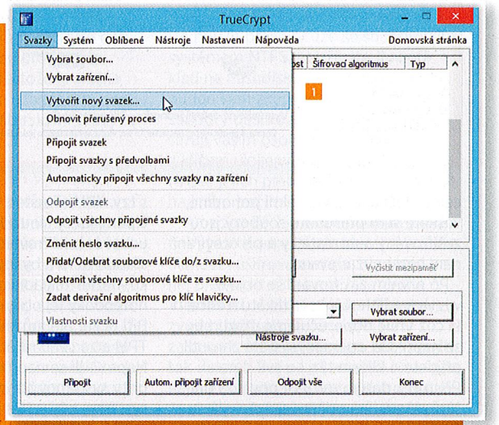
To však nemění nic na skutečnosti, že starší verze programu (7.1a, 7.1) jsou skvěle použitelné a bezpečné. Navíc se objevila iniciativa **TCnext** s mottem TrueCrypt must not die (**truecrypt.ch**), která – jak napovídá doména – sídlí v bezpečnějších vodách Švýcarska. Thomas Bruderer a Jos Doekbrijder již uvolnili alternativu jménem CipherShed jako alfa verzi pro testování širokému publiku. Co je nejdůležitější, najdete zde ke stažení právě starší verze TrueCryptu.

Důvodů, proč ponechat krále kralovat, je hned několik. Vyjma ověřené bezpečnosti programu to jsou některé unikátní funkce. Především existuje vyjma pro Windows i pro OS X a Linux a zašifrovaná data můžete otevřít napříč platformami. Dále podporuje dvojitý skrytý prostor. Zvažme scénář, kdy po vás někdo pod jakoukoli výhrůžkou vyžaduje heslo právě pro dešifrování vašich dat v TrueCryptu. Sdělíte primární heslo k datům, která mohou vypadat důvěryhodně, ale nejsou pravdivá. Útočník nemá možnost zjistit, zda druhý, skrytý oddíl vůbec existuje. Vy se do něj dostanete použitím jiného hesla. Výsledný soubor má navíc pevně danou velikost, neplní se tedy postupně, jak do něj ukládáte citlivá data. Jedná se o účel, útočník nezjistí, kolik dat zkrátka soubor obsahuje a zda jste mu skutečně ukázali vše. První kroky s programem najdete v samostatném boxíku.

Nechcete-li TrueCrypt z jakéhokoli důvodu používat, vyzkoušejte zdarma dostupný **DiskCryptor**. Nabízí stejné šifrovací algoritmy jako TrueCrypt a zvládá šifrovat celé diskové oddíly. Nevýhodou TrueCryptu zůstává jen nemožnost šifrování systémového oddílu na Windows 8.1 (GPT). Tato funkce byla plánována, avšak tvůrci již tuto funkci nestihli implementovat.

Šifrování dat s programem TrueCrypt

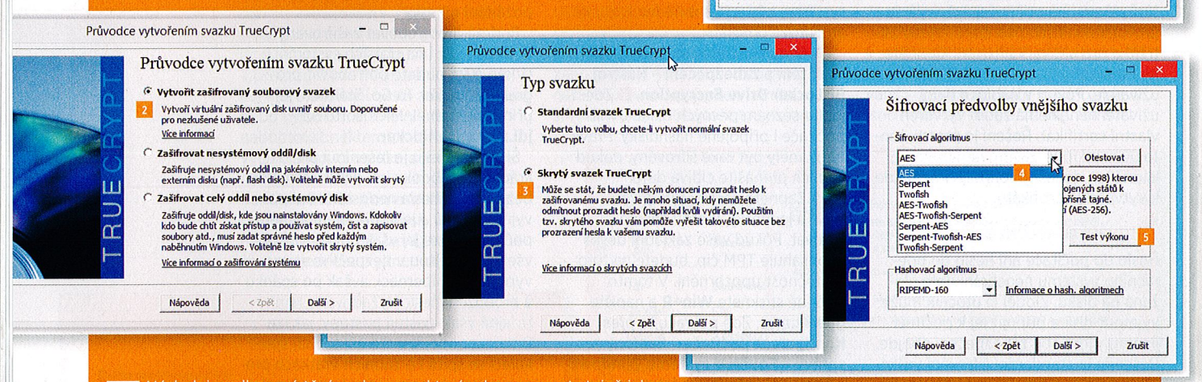
Ověřenou starší verzi programu **TrueCrypt** stáhnete na truecrypt.ch, zde také najdete soubor s českou lokalizací. Po instalaci stačí do adresáře s programem nakopírovat soubor s lokalizací, která se aktivuje automaticky. Ukážeme zde návod na vytvoření důmyslnějšího skrytého svazku.



1 Po spuštění zvolte z hlavní nabídky vlevo nahoře **Svazky – Vytvořit nový svazek**.

2 Následuje volba, zda chcete vytvořit zašifrovaný soubor, který se následně bude připojovat jako další pevný disk, zašifrovat přenosný disk nebo celý diskový oddíl s operačním systémem. TrueCrypt bohužel nepodporuje šifrování disku s Windows 8.1, pro starší systém však poslouží skvěle. Pokračujte první možností.

3 Následuje rozhodnutí, zda chcete vytvořit klasický svazek, nebo skrytý svazek. Zvolte druhou variantu a v dalším kroku zvolte Normální mód. Tím postupně vytvoříte Vnější (falešný) svazek a následně Vnitřní (skutečný) svazek.

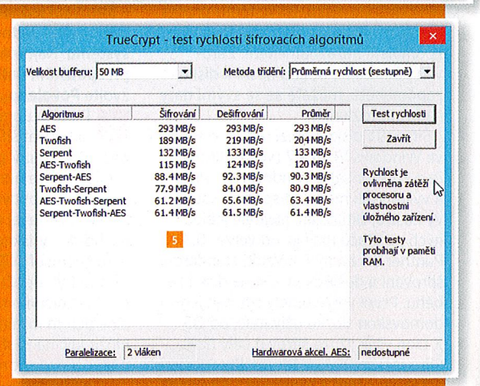


4 Následuje volba umístění souboru, se kterým lze pracovat stejně jako s jakýmkoli jiným souborem – mazat, zálohovat, poslat e-mailem nebo třeba znovu zašifrovat jiným programem. V dalším kroku jste dotázáni na volbu úrovně šifrování. Nabízí se **AES**, **Twofish** a **Serpent**, plus jejich dvojí, či dokonce trojí zřetězení.

5 Se složitostí samozřejmě roste odolnost proti prolomení, avšak současně i rychlost šifrování a dešifrování. Algoritmus AES-Twofish-Serpent je zhruba pětkrát pomalejší než samostatný AES. Ostatně test rychlosti můžete provést stiskem tlačítka **Test výkonu**.

6 Následně jste požádáni o zadání kapacity vnějšího svazku. Pamatujte, že do tohoto svazku musíte vložit důvěryhodná, ale falešná data a ponechat místo pro svazek vnitřní. Po zformátování se proces opakuje, tentokrát vytváříte svazek vnitřní – skrytý. Ten musí mít odlišné, a především velmi silné heslo.

7 Pokud budete po vytvoření vnitřního skrytého svazku zapisovat data do svazku vnějšího, data v tom vnitřním přepíšete. Proto se striktně doporučuje naplnit falešná data předem a již do vnějšího svazku nezapisovat. Tento zdánlivý nesmysl má své opodstatnění: v nouzi můžete zápisem do vnějšího svazku znehodnotit data v tom vnitřním. Vychází se z předpokladu, že je lepší o data přijít, než aby se dostala do nepovolaných rukou.



Hotovo. Chcete-li připojit obsah šifrovaného oddílu, zvolte na hlavní obrazovce **Vybrat soubor** a zadejte heslo ke skrytému svazku. Než začnete program používat, silně doporučujeme nastavit klávesové zkratky, především pro rychlé odpojení připojených disků.

Bezpečnost ve světě internetu

Veškeré otázky bezpečnosti naberou zcela nový směr ve chvíli, kdy se připojíte k internetu a začnete využívat jeho lákadel. Chcete se přihlásit k internetovému bankovnictví, platit, objednávat zboží, komunikovat různými způsoby a pokud možno neodhalit své soukromé údaje. Hrozeb existují stovky, my se podíváme na ty nejobvyklejší a doporučíme maximální možnou ochranu.

CENY VYBRANÝCH ANTIVIROVÝCH PROGRAMŮ

	jeden uživatel	podporovaný operační systém
Avast Free Antivirus	zdarma*	Windows, OS X
Avast Internet Security	1 190 Kč/rok	Windows
AVG AntiVirus Free	zdarma*	Windows, OS X
AVG Internet Security 2015	1 199 Kč/rok	Windows
Avira Free Antivirus 2015	zdarma*	Windows, OS X, Android, iOS
Bitdefender Antivirus Plus 2015	34,95 $/rok	Windows
ESET NOD32 Antivirus	1 209 Kč/rok	Windows, OS X
ESET Family Security Pack (3 stanice)	1 511 Kč/rok	Windows, OS X, Linux, Android
F-Secure Anti-virus 2015	19,95 €/rok	Windows, OS X
Kaspersky Anti-Virus 2015	459 Kč/rok	Windows, OS X
McAfee AntiVirus Plus 2015	49,99 $/rok	Windows
Webroot SecureAnywhere Antivirus	39,99 $/rok	Windows, OS X

* zdarma jen pro domácí a současně nekomerční použití
Pozn.: Většina výrobců nabízí víceleté a víceuživatelské licence za výhodnější cenu

Internet je plný nejrůznější havěti, která se k vám bude chtít dostat všemi možnými způsoby. Jejich tvůrcům přitom již dávno nejde o to, vymazat vám nějaká data, ale spíše o to, jak z vás dostat peníze. Obvyklé jsou programy tvářící se jako skutečné antiviry. Následně falešně hlásí údajné napadení vašeho počítače, k odstranění hrozby však již musíte zaplatit za „plnou" verzi programu. Mnohem nebezpečnější je aktuální hrozba jménem TorrentLocker, který si můžete zanést do počítače obvykle z přílohy e-mailu, jenž se tváří jako důležitá zpráva (nezaplacená faktura, hrozba exekucí a podobně). Virus následně zašifruje vaše data na disku a požaduje dokonce až dvacetitisícové výpalné. A věřte, že po nákaze nepomůže žádný antivirový program.

Můžete se chovat zodpovědně, avšak nástrahy útočníků jsou čím dál protřelejší. Účinnou, avšak samozřejmě ne stoprocentní ochranu nabízí antivirové programy. Ty základní seženete i zdarma, Windows obsahují standardně Defender, ale můžete sáhnout i po Avastu, AVG či Avira. Pamatujte ale, že jsou určeny jen pro nekomerční domácí použití.

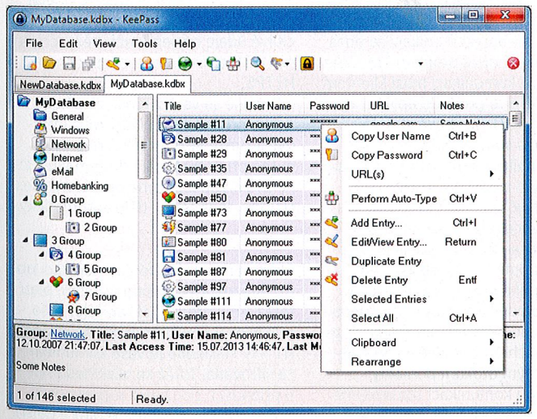
Za důmyslnější verze, obvykle se slovy Smart či Internet v názvu, si již musíte zaplatit. Ceny se pohybují od několika stokorun až jednotek tisíc ročně, všichni tvůrci nabízejí výhodnější víceleté a/nebo víceuživatelské licence. Internetové verze obvykle nabízejí lepší kontrolu e-mailů, přímo kontrolují komunikaci a jsou schopny odhalit hrozby ještě dříve, než se uloží na váš disk. Dodatečné schopnosti se již liší u jednotlivých tvůrců, a pokud chcete platit, určitě si všechny nabídky projděte. Někteří nabízejí například jako bonus praktické správce hesel.

Na hesla zapomeňte

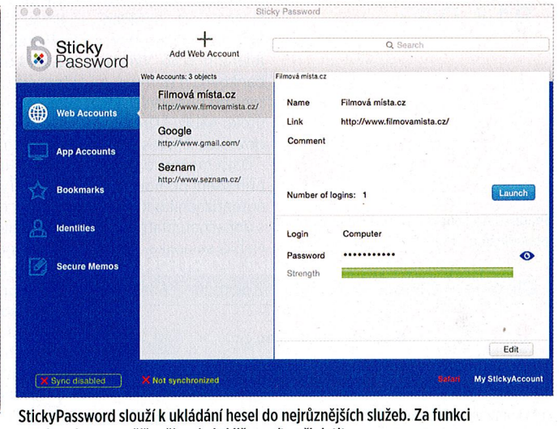
Zapamatovat si extrémně dlouhá a pro každou službu unikátní hesla samozřejmě v praxi nelze. Existují však správci hesel, a to v podobě programů i různých služeb. Myšlenka je prostá: pod jediným, velmi silným heslem se uloží a zašifrují všechny ostatní vaše přístupové údaje. Můžete je členit do kategorií a nechybí praktický generátor silných hesel. Za všechny zmiňme vynikající a zdarma dostupný **KeePass** (**keepass.info**).

Kryptoměnová horečka snížila bezpečnost používaných hesel, 8 znaků již dávno nestačí

V současné době, kdy takřka každý používá více zařízení, se do popředí dostávají multiplatformní aplikace jako **OnePassword**, **LastPass**, **Dashlane** či český **StickyPassword**, které umožňují synchronizaci hesel prostřednictvím cloudu. Navíc díky integraci do webového prohlížeče zpříjemňují obsluhu, nemusíte otevírat peněženku a přihlašovací údaje se vyplňují automaticky. Některé jsou placené, jiné jsou v základu zdarma a teprve za synchronizaci požadují roční poplatek. Vězte ale, že jde o velmi dobře utracené peníze.



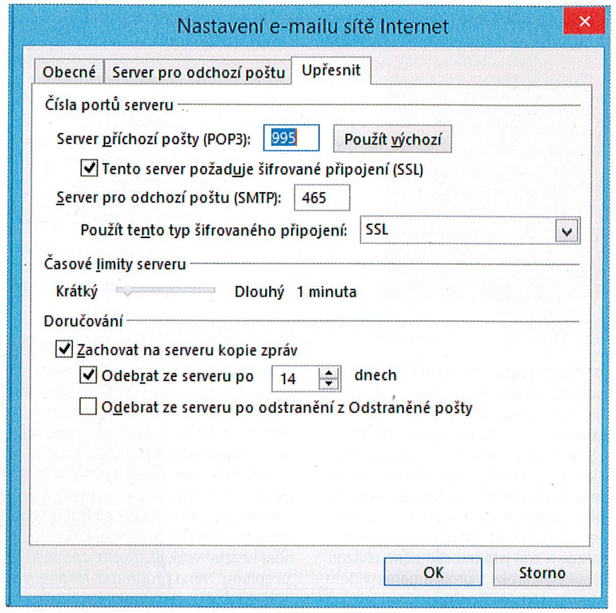
Zdarma dostupný KeePass uloží a zašifruje veškerá vaše hesla pod jediné silné heslo



StickyPassword slouží k ukládání hesel do nejrůznějších služeb. Za funkci synchronizace napříč zařízeními si již musíte připlatit

Rychlé tipy k vyššímu bezpečí

1. Používejte šifrování disku.
2. Aktualizujte operační systém, nainstalujte kvalitní antivirový program.
3. Elektronickou poštu zasílejte výhradně přes zabezpečené připojení.
4. Nepoužívejte stejná hesla pro různé služby, ke službám se připojujte výhradně přes HTTPS.
5. Používejte raději delší fráze než krátká komplikovaná hesla.
6. Nezadávejte pravdivé odpovědi na kontrolní otázky.
7. Nenavštěvujte podezřelé weby, neotvírejte podezřelé přílohy e-mailů.



Zabezpečená komunikace probíhá na jiných portech než komunikace nezabezpečená. Obvykle je třeba ještě nastavit správný typ šifrovaného spojení

Nechcete-li žádné další programy používat, vytvořte si textový soubor a uložte jej do šifrovaného souboru pomocí TrueCryptu. Komfort použití bude sice nižší, avšak data zůstanou v bezpečí.

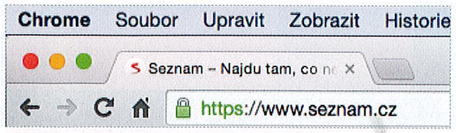
Dvoufázové ověřování

V minulém roce došlo k několikerému úniku databáze hesel uživatelů. Přestože útočník získá většinou jen hashe, může díky používání běžných hesel slovníkovým útokem účty rychle prolomit. Některá internetová bankovnictví již používají takzvané dvoufázové ověřování, které se pomalu, ale jistě dostává i do některých služeb.

Program Authenticator slouží k poměrně pohodlnému dvoufázovému přihlašování

Dvoufázové ověřování vyžaduje vyjma tradičního hesla ještě jeden způsob ověření. Může to být například SMS zaslaná na vaše telefonní číslo. Vyjma bankovních domů toto po posledním útoku nabízí i Dropbox nebo Microsoft.

Další možností je přihlášení pomocí autentizačního klíče s dočasnou platností. Nabízí se aplikace Authenticator od Googlu, která funguje jednoduše: služba (Google, Microsoft, Facebook…) vygeneruje QR kód, který v aplikaci vyfotíte. Při přihlášení do libovolné služby budete požádáni nejen o tradiční heslo, ale i o toto šestimístné číslo, které zjistíte jen z vlastního telefonu. Útočník, který získá vaše primární heslo, se do služby bez současné znalosti ověřovacího kódu, a tedy i vlastnictví telefonu, k vašim datům nedostane. Vhodné je samozřejmě následně ochránit i telefon, například vstupním heslem nebo gestem.



Zda komunikujete se serverem bezpečně, šifrovanou cestou, poznáte pomocí zámečku, případně i zeleného zvýraznění HTTPS

Komunikujte bezpečně

Šifrování a jakékoli zabezpečení vždy požaduje výpočetní výkon navíc. Není tedy divu, že v dobách, kdy nebylo výkonu nazbyt, se šifrování nepoužívalo. Pro šifrovanou komunikaci se dnes používá transportní protokol TLS/SSL, který šifruje komunikaci mezi klientem a serverem, a to pro řadu aplikačních protokolů: HTTP (webové stránky), FTP (přenos souborů), POP3/IMAP/SMTP (e-mailové protokoly) a spousta dalších. Tyto služby však uživatelé využívají nejčastěji.

Komunikace bude vždy fungovat nezabezpečenou cestou, záleží však již jen na administrátorech služeb, zda integrují a povolí i zabezpečený způsob komunikace. Navíc s patřičnou úrovní bezpečnosti, neboť starší verze transportních protokolů (SSL v1, SSL v2) již různým útokům podlehly.

Šifrovanou komunikaci samozřejmě podporují všechny banky a platební systémy, spousta malých internetových obchodů se však s bezpečností příliš nepáře. Mimo jiné také z důvodu, že šifrování vyžaduje certifikát od ověřené certifikační autority, který stojí několik tisíc ročně.

Zabezpečený webový server nebo internetový obchod poznáte jednoduše: na začátku webové adresy není http, ale https. Například Seznam.cz vás i při zadání http automaticky přesměruje na https a vaše přihlašovací údaje do e-mailové služby jsou v bezpečí. Stále však najdete řadu webových e-mailových služeb, které komunikaci zkrátka nešifrují. V takovém případě může administrátor kteréhokoli serveru (či routeru), přes který údaje putují, komunikaci poměrně snadno odposlechnout a heslo získat. Bohužel z vaší strany můžete udělat maximálně to, že nebudete poskytovat citlivé údaje na serverech běžících jen na HTTP, a nikoli na zabezpečeném HTTPS.

Obecně se však situace zlepšuje a jako příklad za všechny můžeme uvést právě **Seznam.cz**. Dříve bylo nutné při přihlašování do e-mailu ručně zvolit zabezpečené přihlášení přes HTTPS, dnes se tak děje automaticky.

Bezpečnost e-mailů

Pokud pro e-mailovou komunikaci používáte webové rozhraní služeb, platí totéž, co v předchozí kapitole: vaše přihlašování musí probíhat na stránce HTTPS. Následně je vaše komunikace šifrována. Totéž se však nedá říci o případech používání e-mailových klientů (Outlook, Thunderbird a další). Poskytovatelé e-mailových schránek totiž povětšinou na prvním místě uvádí návody pro nastavení nezabezpečené komunikace, zabezpečené bývají uvedeny až dále.

Trochu za to mohou i sami uživatelé se svým pohodlím: nezabezpečená komunikace funguje vždy, e-mail nastaví, vše funguje a dál se nestarají. Zabezpečená komunikace fungovat

Používejte raději dlouhá frázová hesla. Byť složitá hesla s délkou méně než 10 znaků lze se současnými stroji odhalit

může, ale i nemusí, záleží na poskytovateli. A následně záleží jen na vás, zda nezabezpečenou komunikaci akceptujete, nebo přejdete jinam.

Z pohledu uživatele je nastavení bezpečného připojení poměrně jednoduché. Běžná a zabezpečená komunikace probíhá na různých portech:

POP3: 110 a 995
IMAP: 143 a 993
SMTP: 25 a 465

První jsou uvedena čísla portů s nezabezpečenou komunikací, druhá čísla znamenají bezpečnou cestu. Běžte do nastavení účtů ve svém e-mailovém programu a zkontrolujte, zda máte nastaveny bezpečné porty. Nastavení bude možná vyžadovat metodu pokusu a omylu – programy umožňují volbu různých metod zabezpečení. Například již zmiňovaný Seznam podporuje SSL, ale již nikoli TLS. V případě zabezpečení odeslané pošty přes SMTP je obvykle třeba ještě zaškrtnout „Server pro odchozí poštu požaduje ověření".

Tímto jednoduchým a rychlým krokem zajistíte, že nikdo, ani váš poskytovatel internetu, neodposlechne přihlašovací údaje do vaší e-mailové schránky.

Chcete-li šifrovat samotný obsah e-mailů a zaručit, že si je přečte jen pověřená osoba, zaměřte se na metody PGP (či GPG). Tento šifrovací proces však vyžaduje vlastnictví certifikátů a pro začátečníky může být vcelku složitý, navíc již byly potvrzeny některé bezpečnostní chyby. Chcete-li zaslat e-mailem skutečně citlivé informace, jděte na to oklikou. Vytvořte si malý soubor v TrueCryptu, uložte do něj vše potřebné a zašlete ho jako přílohu e-mailu. Heslo pro otevření sdělte protějšku bezpečnou cestou.

Zdravý rozum nestačí

Začali jsme nevesele a bohužel ve stejném tónu i skončíme: ačkoli se budete snažit sebevíc svá data ochránit, vždy může zklamat poskytovatel: historie nás poučila o několika případech úniku citlivých dat. A tak již dávno neplatí, že pro bezpečný pohyb po internetu stačí zdravý rozum a neotvírání podezřelých příloh e-mailů.

Byla by ale chyba vzdát se všech výhod, předností a pohodlí, které internet a různé služby nabízejí. Vždy však využívejte nejlepší možnou úroveň zabezpečení, dodržujte pravidla a zajímejte se o bezpečnost. ■

Užitečné české weby o virech a virových hrozbách

Viry.cz
Odstranitvirus.cz
Servis.eset.cz

Jak lze prolomit šifrovaná hesla?

Drtivá většina hesel je dnes ukládána ve formě tzv. hashe. Hashování je jednosměrná funkce, která ze zdrojových dat odvodí řetězec znaků pevně dané délky:

Často používaná, ale bohužel též nejméně bezpečná hashovací funkce MD5 vytvoří z hesla **a** řetězec **0cc175b9c0f1b6a831c399e269772661**

Totéž v případě silného hesla **COmpu!3r,2014**: **0116ad33a4461ef41b0de6886899d2ff**

Klíčové je ono slovíčko „jednosměrná", to znamená, že z hesla **COmpu!3r,2014** lze třeba pomocí na webu dostupných generátorů zjistit hash. Avšak opačná cesta neexistuje, z hashe, pokud by se jej útočník zmocnil, nelze odvodit původní heslo jinak, než hrubou silou: postupným generováním kombinací možných znaků, výpočtem jejich hashe a následným porovnáváním. Je zřejmé, že heslo **a** bude odhaleno rychleji než heslo **COmpu!3r,2014**.

Avšak existuje druhý přístup: všechny kombinace hesel a jejich hashe jsou předem vypočítány a uloženy. Takové databázi se říká „rainbow table" (duhová tabulka), neboť obsahuje všechny možné kombinace hesel do určité délky. Následně stačí získaný hash velmi rychle porovnávat s tabulkou.

Databáze čtyřznakových hesel může zabírat okolo 1 GB (v závislosti na počtu uvažovaných znaků a způsobu uložení v databázi), pro 5 znaků je to již přes 70 GB a 6 znaků zabere 6 TB. Taková paměť je ještě běžně dostupná. Sedm znaků však znamená dalších více než 400 TB a s osmým znakem jde náročnost do desítek PB (petabajtů).

Taková tabulka vznikne jen pro jeden přesně daný druh hashe, takže tabulka pro MD5 není použitelná pro SHA. Administrátor se může bránit proti tomuto útoku poměrně snadno, doplněním hesel o tzv. sůl (salting), která proces hashování upraví. Útočník neví, zda vůbec, případně jak bylo solení použito, což využití tabulek znemožňuje. Bohužel velká část programátorů a administrátorů jsou lajdáci, kteří nepoužívají solení a hesla šifrují nejobvyklejším MD5 nebo SHA. Na druhé straně jsou lajdáci uživatelé se svými krátkými hesly. Není divu, že se útočníkům následně podaří velkou část hesel jednoduše prolomit.

Následující tabulka vyjadřuje dobu nutnou k prolomení hashovaného hesla šifrou MD5. Rychlost generování hashů se především díky kryptoměnám neuvěřitelně zrychlila. Ať už pomocí grafických karet, či pomocí specializovaných zařízení. Nepříjemným důsledkem kryptoměn je tak současné snížení bezpečnosti používaných hashovacích funkcí. V našem výpočtu uvažujeme rychlost generování 1 000 000 000 (miliardu) hashů MD5 za vteřinu. Nejmodernější grafické karty zvládají více než desetkrát tolik, specializovaná zařízení ještě více. Přestože uvažujeme nejslabší šifru, uvažujeme i velmi slabý hardware pro jeho odhalení. Na druhou stranu, pro naši bezpečnost hraje fakt, že zatímco výkon lámacího zařízení lze obvykle zvyšovat lineárně, počet kombinací hesla roste s přibývajícím počtem znaků exponenciálně.

Hashování má jednu velkou výhodu: pokud administrátor nepoužije některý z výše uvedených způsobů prolomení, nezná ani on vaše hesla v databázi. Stále se však najdou služby, které heslo do databáze ukládají v čitelné podobě. Poznáte je snadno: použijete-li funkci zapomenutí hesla, služba vám jej (obvykle navíc nezabezpečenou komunikací) pošle v čitelné podobě e-mailem. Pokud služba používá hashování, obdržíte unikátní odkaz s krátkou časovou platností, kde si musíte vytvořit heslo nové.

ČAS POTŘEBNÝ K PROLOMENÍ HESLA HRUBOU SILOU

Složení hesla:	počet možných znaků	délka hesla: 6	8	10	12	14
jen malá písmena	26	0,3 s	3 min	39 h	3 r	2 045 r
malá a velká písmena	52	20 s	15 h	5 r	12 394 r	33 515 075 r
malá a velká písmena, číslice	62	57 s	61 h	27 r	102 304 r	393 257 529 r
malá a velká písmena, číslice, znaky	95	12 min	77 d	1 898 r	17 134 795 r	154 640 721 tisíciletí

Současná průměrná grafická karta je schopna generovat zhruba miliardu MD5 hashů za vteřinu, nejsilnější grafické karty i více než desetkrát více. Výsledky jsou zaokrouhleny