Prolomte každé heslo!

Sada rad a doporučení pro případy, kdy zapomenete heslo (CD)

DAVID ČEPIČKA, DANIEL BEHRENS

Ochrana před neoprávněným přístupem pomocí hesel je bezesporu věc velmi užitečná. Má snad jen jedinou vadu na kráse – pokud správné heslo zapomenete, rázem se dostanete do prakticky neřešitelných problémů.

Co například dělat, když si přes internet zakoupíte program a nemůžete za nic na světě najít e-mail, v němž byly všechny informace potřebné pro jeho odblokování? Naštěstí vám v tomto článku právě pro takové či podobné situace přinášíme řešení.

Jak nepříjemný asi musí být pocit, když znovu instalujete Windows a najednou nemůžete najít licenční čísla ke všem programům, které jste si poctivě zakoupili. U programů, které jste si pořídili v klasickém obchodě v krabici, jsou licenční čísla většinou napsána na papírovém obalu CD nebo na kartičce. Obojí lze ztratit velmi jednoduše. U softwaru kupovaného prostřednictvím internetu se pak podobný problém objeví tehdy, když se nepodaří nalézt e-mail, v němž byly uvedeny všechny informace potřebné pro aktivaci programu. Taková situace může kupříkladu nastat tehdy, když se vám najednou poškodí pevný disk.

V první části našeho článku vám poradíme, jak se zachovat právě v takových situacích. Dozvíte se nejen, kde na internetu nalézt licenční čísla, nýbrž i to, jaká právní či bezpečnostní opatření byste měli brát v úvahu.

V další části se budeme zabývat problémem, pokud ztratíte přístupová data k některé z placených internetových služeb. Poradíme vám, jak budete schopni tyto služby zase využívat. Mnohé internetové stránky jsou totiž chráněny tak chabě, že se řada platících zákazníků může cítit poněkud zklamána tím, jak snadné je dostat se k obsahu, za který oni vydávají peníze.

Každý, kdo všechny dokumenty s důvěrnými informacemi opatřuje přístupovým heslem, jedná bezpochyby velmi obezřetně. Jenže pokud heslo zapomene, stojí najednou před zavřenými dveřmi. Budeme se zabývat i řešením tohoto problému.

V článku také zjistíte, jak je snadné zobrazit všechna hesla uložená v počítači. Z tohoto důvodu je nanejvýš vhodné svému operačnímu systému nedůvěřovat. Podrobnější vysvětlení opět uvedeme vzápětí. Nakonec se budeme zabývat zabezpečením bezdrátových sítí, kde uvidíte, jak snadno se do nich dá proniknout, pokud jsou nesprávně nakonfigurovány.

Sériová čísla

Při ztrátě sériového čísla zakoupeného programu byste rozhodně měli nejprve kontaktovat jeho prodejce, popřípadě výrobce. Pokud máte alespoň doklad o zakoupení zboží, pak by získání nového sériového čísla nemělo být problémem. Nárok na nové sériové číslo však nemáte, záleží na dobré vůli toho, kdo vám produkt prodal či kdo jej vyrábí. Často se také stává, že výrobce programu již neexistuje, například proto, že zbankrotoval.

1. Nouzové řešení: sériová čísla z internetu

Pokud se vám nepodařilo získat licenční číslo způsobem uvedeným v úvodu nebo pokud chcete program do doby, než toto sériové číslo dostanete, používat, můžete se zkusit na internetu podívat na některé ze specializovaných stránek. Na nich získáte přístupové kódy k celé řadě programů. V mnoha případech se jedná o tzv. *KeyGenerator*, jenž dokáže vypočítat prakticky libovolné množství sériových čísel.

Rozhodně vám při tomto způsobu získávání sériových čísel nedoporučujeme do internetových vyhledávačů typu Googlu zadávat výrazy typu *Serials* či *Cracks* a následně přecházet na libovolný z nalezených odkazů. Jakmile se totiž dostanete na některou ze stránek slibujících sériové číslo, můžete si z ní nepozorovaně odnést nepříjemný dáreček ve formě trojského koně, spywaru či dialeru.

Připravili jsme pro vás několik internetových adres, které slouží jako vyhledávače pro získávání sériových čísel. Odkazují zpravidla pouze na stránky, které dodržují to, co slibují – samozřejmě i ony mohou do velké míry sloužit k rozšiřování spywaru.

2. Právní stránka věci: je takové počínání legální nebo ne?

Z právního hlediska je stahování a používání sériových čísel či jejich generátorů záležitostí, která kupodivu není tak jednoznačná, jak by se mohlo na první pohled zdát. Někteří výrobci programů dávají do svých licenčních ujednání větičku, že program smí být používán pouze s registračním číslem, které bylo získáno přímo od nich. Na druhou stranu v případě ztráty sériového čísla však generátor či číslo stažené z internetu používáte vlastně pouze proto, abyste zboží, které jste řádně získali, mohli používat k účelu, pro který bylo vytvořeno. Zkrátka byste nikdy neměli používat takové sériové číslo, které by vám umožnilo využívat funkce programu, k nimž nemáte ve vámi získané licenci k programu oprávnění. Zakoupíte-li si kupříkladu standardní nebo OEM verzi programu pro vypalování, pak rozhodně nesmíte použít žádný softwarový klíč, který by vám umožnil využívat funkce programu v takovém rozsahu, jako je například možné ve verzi Professional. Stejně tak nesmíte pomocí nového sériového čísla prodlužovat období, v němž máte oprávnění stahovat aktualizace daného programu.

Sériová čísla na internetu

V následujícím seznamu jsou uvedeny internetové stránky, přes něž se dostanete k sériovým číslům pro celou řadu programů. Nezapomínejte na právní a bezpečnostní rizika spojená s prohlížením podobných stránek a popřípadě se stahováním souborů z těchto stránek.

www.allseek.info
www.astalavista.box.sk
www.astalavista.com
www.freeserials.com
www.serials.ws
www.serialsite.com
www.t1000.net

3. Pět důležitých tipů pro vaši bezpečnost

Při vyhledávání sériových čísel byste se měli mít na pozoru. Vzhledem k tomu, že stránky poskytující sériová čísla nebo jejich generátory jsou velmi intenzivně navštěvované, nelze se divit, že jejich provozovatelé z nich chtějí mít také nějaký užitek. Například se vám pokouší vnutit spyware ve formě různých panelů nástrojů pro snadné vyhledávání či podobné nástroje. V lepším případě se objeví tzv. upozornění zabezpečení, které nabízí zablokování instalace podezřelého prvku. V horším případě pak spyware využívá bezpečnostních trhlin v Internet Exploreru, aby se mohl nainstalovat, aniž bychom si toho všimli. Pokud se chcete před všemi druhy malwaru účinně chránit, pak dodržujte následující doporučení:

1. Používejte jiný prohlížeč než Internet Explorer, například **Firefox 1.0.6** (naleznete jej i NA NAŠEM CD), a to zvláště pro prohlížení podezřelých stránek. Tento prohlížeč je totiž o něco bezpečnější než Internet Explorer a navíc má v sobě zabudovanou funkci blokování pop-up oken, což je zvláště u stránek pochybného charakteru k nezaplacení. Internet Explorer tuto funkci nabízí pouze ve verzi Windows XP s nainstalovaným Service Packem 2.

2. Nainstalujte antivirový program, který dokáže rozpoznat a zablokovat kromě virů i spyware. Pokud chcete řešení, které vás nebude stát ani korunu, pak vám doporučujeme zdarma dostupný **Antivir Personal Edition Classic 6.31**, který rovněž naleznete NA NAŠEM CD. Po instalaci programu a restartu počítače aktivujte ochranu proti spywaru. To provedete tak, že poklepáním na ikonku v pravé části Hlavního panelu otevřete konfiguraci rezidentní ochrany (*Antivir Guard*) a v následujícím okně klepnete do menu *Options/Configuration*. Na záložce *Unwanted Programs* pak umístěte zatržítka před všechny položky kromě položky *Games*. Tato možnost je k dispozici pouze ve Windows 2000 a XP.

3. Pokud používáte Internet Explorer, pak je nutné jej a ostatně celá Windows udržovat vždy v tom nejaktuálnějším stavu, nejlépe povolením funkce automatických aktualizací Windows 2000 a XP, popřípadě pravidelným stahováním a instalací aktualizací z internetové stránky ***www.windowsupdate.com***.

4. Je naprosto nezbytné věnovat při surfování na internetu pozornost dialogovým oknům

▶ **Pozor při vyhledávání sériových čísel: tato internetová stránka zkouší instalovat panel nástrojů. V takovém případě vždy klepněte na tlačítko Ne.**

Minitipy

Použití cracku modifikuje software

Při hledání sériových čísel na internetu pravděpodobně narazíte i na tzv. **cracky**. Mnohé z nich modifikují program takovým způsobem, že se po jeho spuštění přestane zobrazovat výzva pro zadání sériového čísla – programy fungují stejně dobře i bez něho. Jiné druhy cracků zase slouží k tomu, aby obešly časově omezené používání demoverzí, popřípadě aby umožnily používat některé v demoverzích nedostupné funkce. Někteří právní experti jsou toho názoru, že jakákoliv modifikace softwaru je vždy nezákonná, a to i tehdy, když jste daný program řádně zakoupili a crack jste použili jenom proto, že jste ztratili licenční číslo nebo instalační CD s plnou verzí. Proto vám jednoznačně doporučujeme se používání cracků vyhnout. V opačném případě byste se snadno mohli dostat do konfliktu se zákonem.

Buďte neviditelní

Pokud máte špatný pocit, když navštěvujete více či méně pochybné internetové stránky se sériovými čísly – ostatně člověk nikdy neví, jaké informace o vás se dostanou k někomu nepovolanému – pak byste raději měli surfovat anonymně. K tomu účelu vám poslouží utilita **JAP**, kterou naleznete i NA NAŠEM CD. Provozovatelé této služby se zavazují, že u žádného uživatele nepovedou záznamy o jeho aktivitách.

Přístupové údaje na dotaz

V *Usenetu*, což je centrální diskusní fórum, existuje řada diskusních skupin (newsgroups), v nichž lze získat a měnit hesla k různým internetovým službám. Nejjednodušeji se do Usenetu dostanete, pokud použijete vyhledávač Google, kde klepnete na odkaz Skupiny (***www.google.com/grphp?hl=cs&tab=wg&q=***).

Zobrazení hesel v Internet Exploreru

Asterisk Logger bohužel nefunguje u hesel, která jsou uložena v Internet Exploreru. Z tohoto důvodu stejný autor vytvořil utilitu **Protected Storage Passview**, kterou naleznete rovněž NA NAŠEM CD. Ta dokáže zobrazit nejen hesla uložená v Internet Exploreru, nýbrž i hesla zadávaná pro přístup k e-mailovým schránkám přes protokol POP3 v programech MS Outlook či Outlook Express. Podobně jako u Asterisk Loggeru lze jednotlivé položky označit a uložit do textového souboru.

Více anonymity

Pokud se chcete ukrýt v anonymitě nejen při surfování na internetu, nýbrž i při jiných internetových aktivitách, kupříkladu při posílání s názvem *Upozornění zabezpečení* (v Internet Exploreru), popřípadě *Upozornění – Bezpečnost* (Firefox). Vždy je třeba stisknout tlačítko *Ne*, popřípadě *Neinstalovat*.

5. Pro lepší zabezpečení je vhodné do počítače nainstalovat také antispywarový program, který dokáže pracovat na pozadí, např. **Ad-Aware SE Plus**.

3. Utility zabraňující povinné registraci programu

Řada programů, které jsou v obchodech běžně k dostání, vyžaduje při instalaci pokud možno ihned nebo nejpozději do několika dnů provedení tzv. aktivace. Pouze po úspěšném aktivování programu je možné jej dále používat. Nejvýraznějším propagátorem tohoto způsobu registrace programů je firma Microsoft, zvláště její operační systém Windows XP. Tuto politiku nyní používá i Symantec se svými produkty Norton.

Zájem výrobce, který se snaží v co největší míře zabránit pirátskému šíření svých produktů, je zcela v protikladu vůči zájmu zákazníka, který oprávněně chce svoje zakoupené zboží používat okamžitě a bez jakýchkoliv omezení – aniž by musel telefonovat na aktivační telefonní linku nebo produkt aktivovat přes internet, zvláště když vůbec netuší, jaká data se při tomto způsobu aktivace z jeho počítače vůbec odesílají.

Na internetu lze nalézt řadu návodů a utilit, jak tuto aktivaci obejít. Z právního hlediska je tento postup přinejmenším sporný, neboť aktivace produktu je součástí licenčního ujednání mezi výrobcem a uživatelem. V následném sporu by pak rozhodnutí, do jaké míry jsou ustanovení v licenční smlouvě platná, náleželo zřejmě pouze soudcům.

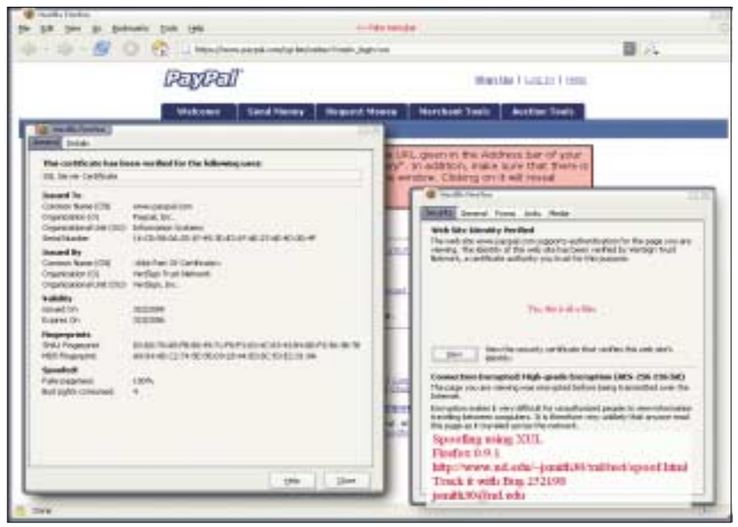
Přístup zdarma na placené stránky

Zapomenete-li heslo pro přístup na internetové stránky s placeným obsahem, pak zpravidla existuje možnost jeho zaslání e-mailem. Pokud však tento způsob možný není, nezbývá nic jiného, než kontaktovat provozovatele stránek a doufat, že nějakým způsobem rychle zareaguje. Mezitím můžete vyzkoušet několik triků, pomocí nichž se lze na takové stránky dostat.

5. Deep Link: přístup prostřednictvím URL

Některé internetové stránky s placeným obsahem disponují pouze velmi chatrnou ochranou proti neoprávněnému přístupu. Skrývají totiž placený obsah ve složce, na kterou není nikde možné najít odkaz. Jedinou možností, jak se na takovou stránku dostat, je ze stránky, na které uživatel zadává svoje uživatelské jméno a přístupové heslo. Pak je do této složky po ověření přístupových údajů přímo přesměrován.

Pokud se tedy jednou dozví jméno složky s placeným obsahem, pak si může při dalších návštěvách zadávání jména a hesla ušetřit a dostat se do složky s placeným obsahem přímo. Stačí do internetového prohlížeče pouze zadat adresu ve tvaru ***www.placenastranka.test/tajnaslozka***.



▲ **Podvedený webový server: pokud je kontrola oprávněnosti přístupu na stránky sledována pouze prostřednictvím Referreru, může s pomocí spoofingu na jinak nepřístupné stránky každý trochu zkušenější uživatel.**

Zmíněnou adresu by si rovněž měl uživatel pro jistotu uložit mezi své oblíbené položky. Pokud to neudělá a heslo ztratí, stále ještě zůstává možnost podívat se v prohlížeči do historie, kde se ukládá seznam všech navštívených stránek za posledních 10 až 20 dnů. Další možností je navštívit některou z diskusních skupin na internetu.

6. Spoofing: oklamaný webový server

Když provádíte *spoofing*, znamená to, že se někomu, v tomto případě webovému serveru, snažíte něco namluvit. Mnohé špatně zabezpečené internetové servery poznají správně přihlášeného uživatele jen podle toho, že se na placené stránky dostal z určité internetové stránky. Informace o tom, z jaké stránky se uživatel na danou stránku dostal, se nachází v parametru *Refferer* v hlavičce (*Header*) protokolu HTTP. Pokud uživatel adresu stránky s placeným obsahem zadá přímo, chybí v hlavičce protokolu parametr *Refferer* a webový server v takovém případě přístup odmítne. Pomocí zdarma dostupných rozšíření prohlížeče se však parametr *Refferer* dá libovolně měnit, čímž se uživateli otevírá možnost přístupu k placenému obsahu chráněnému právě tímto způsobem. Pokud má uživatel adresy placených stránek v historii prohlížeče, může kteroukoliv z nich zadat jako parametr *Refferer* a tím se dostane na stránky s placeným obsahem. Ve speciálních diskusních fórech na internetu je možné nalézt řadu adres, které můžete zadat jako parametr *Refferer*, abyste získali přístup k nejrůznějším placeným stránkám.

7. Přihlašovací údaje pro zdarma přístupné stránky

Služba **BugMeNot** (česky „Nerozčiluj mě“) na internetové adrese **www.bugmenot.com** nabízí přístupové údaje pro řadu internetových stránek. Jedná se ovšem o přihlašovací údaje ke stránkám, které svůj obsah poskytují zdarma, pouze vyžadují registraci. Vzhledem k tomu, že se jedná o otevřenou databázi, do níž může přispívat skutečně každý, objevují se zde i údaje pro přístup ke stránkám s placeným obsahem.

Služba *BugMeNot* rovněž nabízí tzv. *bookmarklet*, tedy jakýsi miniskript pro Internet Explorer. Ten se zabuduje do oblíbených položek. Tato integrace se provede tak, že klepnete na bookmarklet pravým tlačítkem myši a z kontextového menu vyberete příkaz *Přidat k oblíbeným položkám*. Pokud se při surfování dostanete na stránky vyžadující přihlašovací údaje, klepnete na tento odkaz v menu *Oblíbené*. Otevře se pop-up okno, které zobrazí potřebné údaje, samozřejmě pokud budou v databázi služby *Bug-*

Minitipy

e-mailů, pak je vám k dispozici služba na stránkách ***www.findnot.com***. Jedná se o placenou službu v ceně 9,95 USD za měsíc. Ta spolehlivě utají jak váš prohlížeč, tak celé internetové připojení. Přitom je daleko rychlejší než JAP.

BugMeNot pro Firefox

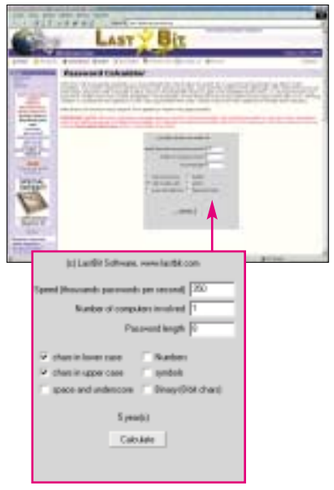
Rychlejší přístup ke službě *BugMeNot* nabízí stejnojmenný doplněk pro Firefox do verze 1.0 a vyšších. Klepněte pravým tlačítkem myši do políčka, kam chcete zadat uživatelské jméno, a z kontextového menu vyberte příkaz *BugMeNot*. Doplněk se dotáže databáze služby a patřičná políčka pro přihlášení vyplní.

Brute Force jako hra pro dospělé

Chcete-li získat představu o tom, jak dlouho může trvat uhádnutí hesla pomocí metody *Brute Force*, pak se určitě podívejte na internetové stránky ***www.lastbit.com/pswcalc.asp***, kde najdete **Password Calculator**. Vycházejme z toho, že vlastníme počítače s procesorem Pentium 4 taktovaným na 2,5 GHz, který dokáže za sekundu prověřit 350 000 až 400 000 kombinací. Pak může lá-

Minitipy

mání hesla trvat dlouhého osm znaků trvat přibližně 7 dnů, ovšem pouze za předpokladu, že heslo obsahuje pouze malá písmena. Jakmile určíme, že heslo může obsahovat i velká písmena, pak se doba potřebná na rozluštění hesla protáhne až na 5 let. Pokud heslo bude dále obsahovat číslice či speciální znaky, pak může uhádnutí hesla trvat několik set let. Heslo z pěti znaků se dá uhodnout už za šest hodin. Tady je názorně vidět, o kolik bezpečnější je používání dlouhých hesel.



Prolomení hesel na zakázku

Ten, kdo na prolomení dokumentu s heslem spěchá, si může nechat otevřít chráněný dokument takříkajíc na zakázku. Služba na internetových stránkách ***www.passwordnow.com*** slibuje, že dokáže odstranit ochranu heslem pomocí speciálních algoritmů řádově v minutách. Každý úspěšně prolomený dokument vás však bude stát 35 USD.

IEEE 802.11i/WPA2

Standard IEEE 802.11i pro bezdrátové sítě WLAN, který je také označován jako **WPA2**, má nahradit stávající metodu zabezpečení WEP (*Wired Equivalent Privacy*) a rozšířit možnosti nyní používaného způsobu zabezpečení prostřednictvím standardu WPA (*Wi-Fi Protected Access*) o metodu šifrování AES (*Advanced Encryption Standard*). V současnosti podporuje standard 802.11i celá řada WLAN-routerů a WLAN-adaptérů, jiná zařízení podporují WPA se šifrováním AES, aniž by byla označena jako zařízení WPA2. Především starší routery a adaptéry však budou mít s tímto standardem problémy. U některých existuje ještě možnost updatu firmwaru. Zda je to i případ vašeho zařízení, nejlépe zjistíte na internetových stránkách jeho výrobce.

▲ **Úspora času: i když mnohé stránky poskytují svůj obsah zdarma, přesto vyžadují registraci. BugMeNot je veřejně přístupná služba, poskytující potřebné přihlašovací údaje.**

MeNot k dispozici. Pokud se přihlášení pomocí zobrazených údajů nepodaří, klepněte na položku *THIS LOGIN DIDN'T WORK*. Pokud má *BugMeNot* v databázi další variantu pro přihlášení, nabídne další přihlašovací údaje, které následně můžete použít. Pro Firefox je k dispozici plug-in, jenž přihlašovací údaje do příslušných políček automaticky vyplní.

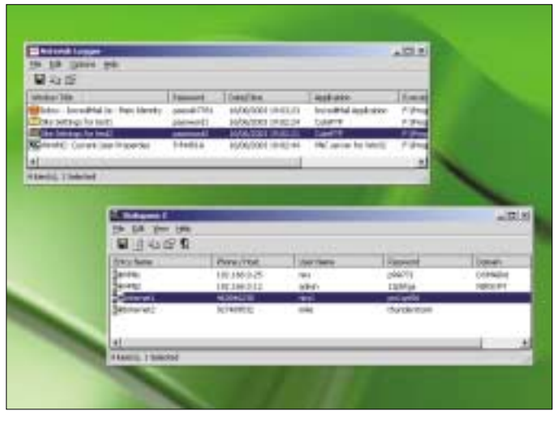
Prolamování hesel

Pomocí hesel chráníte svoje data před neoprávněným přístupem, ale také sami před sebou, pokud správné heslo zapomenete. V takové situaci vám jistě přijdou vhod následující tipy.

9. Zobrazení uložených hesel

Z bezpečnostních důvodů byste ve svém počítači nikdy neměli ukládat žádná hesla. Pokud to však přesto děláte, pak vám to samozřejmě pomůže, pokud některá z nich zapomenete. Předpokládejme, že musíte znovu instalovat Windows – pak potřebujete hesla kupříkladu k tomu, abyste mohli používat internet, chat či elektronickou poštu.

Pokud si na žádné z hesel nedokážete vzpomenout, měli byste si před novou instalací Windows nejprve zobrazit ve stávajících Windows všechna hesla, která jste v tomto systému používali. Pomůže vám k tomu řada freewarových utilit. Například **Asterisk Logger**, který naleznete i NA NAŠEM CD, se používá obzvláště snadno. Spusťte jej a následně otevírejte postupně všechny programy, v nichž používáte nějaké heslo. V každé aplikaci klepněte do políčka, v němž je heslo napsáno – nyní v podobě teček nebo hvězdiček. Asterisk Logger se automaticky postará o zobrazení hesla a místo hvězdiček či teček ho zobrazí pomocí písmenek. Tato možnost funguje téměř u všech aplikací, ale ne úplně u všech. Dále tato utilita zaznamenává ve svém aplikačním okně všechny otevřené programy včetně zobrazených přístupových hesel.



◀ **Zobrazení uložených hesel: existuje řada zdarma dostupných utilit, které vám pomohou osvěžit si paměť.**

Pomocí klávesy <Ctrl> pak můžete označit několik položek současně a pomocí menu *File/Save Selected Items* je exportovat do textového souboru. Všechny položky můžete označit pomocí klávesové zkratky <Ctrl><A>. Vygenerovaný textový soubor pak uložte na bezpečném místě, aby se k němu nikdo nepovolaný nemohl dostat. Pro zobrazení hesel uložených v Internet Exploreru potřebujete program **Protected Storage Passview**. K programu existuje i český jazykový modul. Po rozbalení archivu stačí umístit soubor PSPV_LNG.INI do složky, kam byla utilita nainstalována. Oba soubory naleznete NA NAŠEM CD.

Přístupová hesla pro připojení k internetu v okně *Telefonické připojení sítě* se dají zobrazit pomocí Asterisk Loggeru pouze ve Windows 95/98/ME. Windows 2000 a XP totiž používají vylepšenou formu skrývání přístupových údajů. V tomto případě musíte použít utilitu **Dialupass**, kterou opět naleznete NA NAŠEM CD. Ta rovněž dokáže uložit všechna hesla do textového souboru. Dialupass však korektně pracuje pouze tehdy, pokud jste v systému přihlášeni jako administrátor.

Vzhledem k tomu, že se zmiňované utility často zneužívají pro krádež dat v jiných počítačích, chápou jejich přítomnost některé antivirové programy jako virové nebezpečí a upozorňují na ně.

10. Otevření dokumentů chráněných heslem

Některé programy nabízejí možnost chránit vytvořené dokumenty přístupovým heslem. Nejznámějšími průkopníky tohoto trendu jsou Word a Excel od Microsoftu. Ve verzi 10 (Microsoft Office XP) například naleznete u obou aplikací tuto možnost v menu *Soubor/Uložit jako/*tlačítko *Nástroje/Možnosti zabezpečení*. Pokud přístupové heslo k dokumentu zapomenete, můžete pro tento účel použít speciální utility. Často je ale jejich použití možné pouze tehdy, pokud heslo není příliš dlouhé a složité.

11. Další způsoby otevření dokumentů s heslem

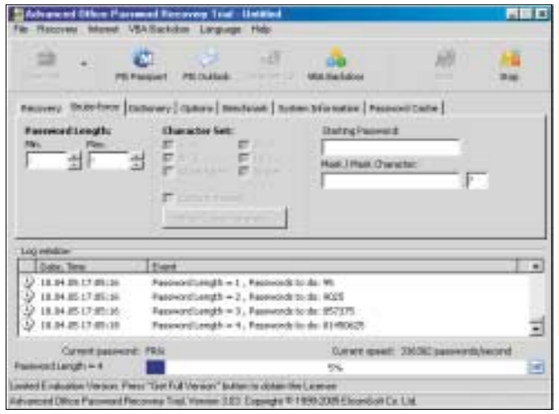
Nejdůkladnější metodu pro rozluštění hesla představuje **Brute Force**. Je to však také metoda nejdlouhavější. Zkouší totiž všechny možné kombinace písmen až do zadané délky hesla, například od „*a*“ až po „*zzzzzzz*“. Pokud předpokládáte, že se v hesle objevují číslice, velká pís-

Jak jednoduše získat přístup do sítě WLAN

Hackerům se ještě stále daří snadno pronikat do bezdrátových sítí. Základem pro získání přístupu jsou záznamy veškerého právě probíhajícího síťového provozu. Pokud tedy používáte síť WLAN, měli byste si dávat pozor zejména na následující:

1. **Ochrana SSID:** Je-li v Access Pointu povolena možnost *Skrýt SSID*, mohou se k této síti připojit pouze uživatelé, kteří znají tento údaj, jenž daný Access Point identifikuje. Provedením analýzy síťového provozu WLAN útočník může zjistit SSID při komunikaci libovolného počítače s Access Pointem – SSID je při této komunikaci přenášeno nezašifrované.
2. **Filtrování MAC adres:** Každá síťová karta a každý WLAN-adaptér má svoji adresu, která jej jednoznačně charakterizuje. Této adrese se říká *MAC-adresa* (*Media Access Control*). Access Point se dá nakonfigurovat tak, aby povolil připojení pouze od těch zařízení, která mají určitou MAC-adresu. Útočník může opět na základě analýzy síťového provozu tyto MAC-adresy zachytit, neboť jsou posílány nezašifrované. Pomocí speciálních utilit, jako je například **Smac 1.2**, pak může útočník odpovídajícím způsobem změnit MAC-adresu svého adaptéru WLAN na takovou, aby mu byl přístup k dané bezdrátové síti povolen.
3. **Šifrování WEP:** U celé řady routerů WLAN je standardně toto šifrování vypnuto. Bohužel toto šifrování vás chrání pouze před těmi hackery, kteří příliš spěchají. Trpělivější hacker, který bude zaznamenávat provoz na takové bezdrátové síti po několik dní, dokáže z těchto záznamů pomocí speciálních utilit jako například **Airsnort** či **Wepcrack** klíč WEP spočítat. Pak může bez problémů číst všechna přenášená data a rovněž není problém do takové sítě proniknout.

Na snadnosti takového průniku se ve velké míře podílí použitý šifrovací algoritmus, který má svoje slabá místa. Dalším šifrovacím algoritmem je algoritmus WPA, jehož prolomení je daleko těžší. V současnosti používají šifrování WPA prakticky všechny novější WLAN-routery. Bohužel šifrování WPA nepodporují starší systémy Windows, pouze Windows XP se Service Packem 1 nebo 2. Nejvyšší stupeň zabezpečení nabídne až nový standard pro sítě WLAN s názvem 802.11i.



Zdlouhavé prohledávání: při použití metody Brute Force se zkoušejí všechny možné kombinace písmen a znaků, což může trvat pěkně dlouho.

mena, znaky s diakritikou či speciální znaky, je nutné program patřičně konfigurovat, aby zkoušel i kombinace s těmito znaky. V závislosti na délce a složitosti hesla může proces dešifrování hesla trvat až extrémně dlouho.

Daleko rychlejší je prolomení hesla pomocí tzv. **slovníkové metody**. Vychází z toho, že heslo je pravděpodobně nějaké obvyklé slovo, neobsahující ani číslice, ani žádné speciální znaky. Pro prolomení hesla jsou tudíž testovány pouze výrazy ve slovníku. Doporučuje se vždy nejprve vyzkoušet tuto metodu prolomení hesla a teprve až selže, použít metodu Brute Force.

12. Balíčky programů pro prolomení hesla

Firma *Lastbit Software* nabízí celou řadu programů pro prolomení hesel, které se dají pořídit buď jednotlivě, nebo jako celý balíček. Moduly **Word Password** a **Excel Password** například stojí každý 39 USD, v jednom balíčku nazvaném **Office Password** pak 59 USD. Pro archivy ZIP chráněné heslem rovněž existují odpovídající utility. Bohužel nepodporují nový způsob šifrování metodou AES, která se používá ve Winzipu 9.0. V balíčku **Password Recovery Tools**, jenž naleznete NA NAŠEM CD, umístila firma Lastbit Software demoverze všech svých programů pro lámání hesel. Tyto aplikace však dokáží rozluštit heslo v maximální délce tří znaků.

Dalším výrobcem programů pro prolamování hesel je firma *Elcomsoft*. Pro Word a Excel nabízí dva balíčky: **Advanced Office Password Recovery** (v ceně od 30 USD, demoverzi schopnou prolomit heslo v maximální délce čtyř znaků naleznete NA NAŠEM CD) a **Advanced Office Password Breaker** (v ceně od 99 USD, demoverzi, která pouze vyhledá šifrovací klíč, naleznete NA NAŠEM CD). Advanced Office Password Recovery pracuje klasickými metodami Brute Force a slovníkovou metodou. Advanced Office Password Breaker používá novou metodu prolamování hesel, při níž se netestují všechny možné kombinace, nýbrž pouze kombinace z vygenerovaného šifrovacího klíče. Pak je možné na průměrném počítači prolomit heslo pro jeden dokument maximálně za 10 dní, nezávisle na jeho délce či složitosti.

Advanced PDF Password Recovery (v ceně od 30 USD, omezenou demoverzi naleznete i NA NAŠEM CD) prolamuje heslo u dokumentů PDF chráněných heslem například proti jejich modifikaci, kopírování a tisku. Pokud se jedná o dokument PDF chráněný heslem proti neoprávněnému otevření, pak je nutné použít program ve verzi Professional Edition (v ceně od 60 USD).

Firma *Elcomsoft* dále nabízí programy pro prolomení hesel i pro archivy ZIP či RAR, pro dokumenty vytvořené v programech Corel Wordperfect Office, Lotus Smartsuite či pro soubory šifrované v souborových systémech Windows 2000 či XP. 5 0544/OK ❑

Pomocník v nouzi: Word Password je placená utilita, která dokáže zpřístupnit dokumenty zajištěné ve Wordu heslem.

Prolomte každé heslo: přehled softwaru

Program	Cena	Operační systém	Internetová adresa	Název a velikost souboru	Jazyk
Ad-Aware SE Plus	599 Kč	Windows 98/ME, NT4, 2000, XP	***www.lavasoftusa.com/software/adawareplus***	–	anglický
Advanced Office Password Breaker 1.40	99 USD	Windows 95/98/ME, NT4, 2000, XP	***www.elcomsoft.com*** a NA NAŠEM CD	AOPB.ZIP (633 KB)	anglický
Advanced Office Password Recovery 3.03	30 USD	Windows 95/98/ME, NT4, 2000, XP	***www.elcomsoft.com*** a NA NAŠEM CD	AOPR.ZIP (3,05 MB)	anglický
Advanced PDF Password Recovery 1.50	30 USD	Windows 95/98/ME, NT4, 2000, XP	***www.elcomsoft.com*** a NA NAŠEM CD	APDFPR.ZIP (1,17 MB)	anglický
Antivir Personal Edition Classic 6.31	zdarma pro soukromé použití	Windows 98/ME, NT4, 2000, XP	***www.free-av.com*** a NA NAŠEM CD	AVWINSFX.EXE (6,8 MB)	anglický
Asterisk Logger 1.02	zdarma pro soukromé použití	Windows 95/98/ME, NT4, 2000, XP	***www.nirsoft.net*** a NA NAŠEM CD	ASTLOG.ZIP (24,4 KB)	anglický
Dialupass 2.43	zdarma pro soukromé použití	Windows 95/98/ME, NT4, 2000, XP	***www.nirsoft.net*** a NA NAŠEM CD	DIALUPASS2.ZIP (41,6 KB)	anglický
Firefox 1.06	zdarma	Windows 98/ME, NT4, 2000, XP	***firefox.czilla.cz*** a NA NAŠEM CD	FIREFOX SETUP 1.0.6.EXE (4,8 MB)	anglický
JAP 5.019	zdarma	Windows 95/98/ME, NT4, 2000, XP	***anon.inf.tu-dresden.de/win/download_en.html*** a NA NAŠEM CD	JAPSETUP.EXE (12,5 MB)	anglický
Password Recovery Tools 8.1.4523	59 USD	Windows 95/98/ME, NT4, 2000, XP	***www.lastbit.com*** a NA NAŠEM CD	MSODEMOSETUP.EXE (1,36 MB)	anglický
Protected Storage Passview 1.62	zdarma pro soukromé použití	Windows 95/98/ME, NT4, 2000, XP	***www.nirsoft.net*** a NA NAŠEM CD	PSPV.ZIP (30,8 KB), český jazykový modul PSPV_CZECH.ZIP (1,03 KB)	český