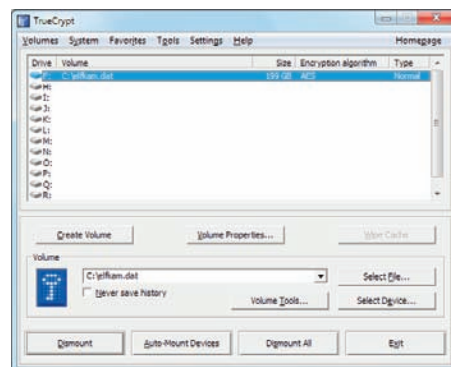


ŠIFROVÁNÍ V KAŽDODENNÍ PRAAXI

Mezi některými uživateli panuje představa, že šifrování dat je těžký kalibr zabezpečení informací, vhodný například pro tajné služby. Opak je však pravda.



NÁSTROJ TRUCCRYPT umí vytvořit celý šifrovaný disk – data jsou dokonale zabezpečena a uživatel musí po zapnutí počítače zadat jen o jedno heslo navíc.

Jedním ze způsobů ochrany na soukromí na internetu je šifrování. Prohlížení běžných webových stránek probíhá skrze nezabezpečený protokol HTTP. Takovou komunikaci lze teoreticky během cesty tzv. odposlouchávat. Například při čtení zpravodajství to není žádný problém. Jiné je to u služeb, kde se pracuje s citlivými, resp. soukromými informacemi. Tam možnost odposlouchávání rozhodně není žádoucí. Nastupuje tedy chráněný protokol HTTPS, který používá stále více služeb, včetně internetového bankovníctví, platebních systémů, e-mailových schránek a v poslední době třeba i sociálních sítí.

BEZDRÁTOVÉ SÍTĚ

Šifrování je také běžnou složkou ochrany bezdrátových sítí, a to i těch domácích. I domácí síť Wi-Fi je totiž vhodné řádně zabezpečit, aby přístup k ní měly jen povolané osoby. K nezabezpečené bezdrátové síti se totiž může připojit kdokoliv, kdo je v jejím dosahu. Bezdrátová

síť vždy přesně nepokrývá jen daný byt, takže přístup k ní může kvůli přesahu signálu reálně získat třeba soused nebo náhodný kolemjdoucí. Šifrováním sice neomezíte dosah sítě (neomezíte nežádoucí přesah), ale zabráníte nepovolaným osobám přihlásit se do ní. Navíc tak ochráníte data v této síti přenášena.

SOUBORY A SLOŽKY

Po šifrování lze sáhnout také při ochraně souborů a složek, k nimž nemá získat přístup nikdo nepovolaný. Hodí se třeba pro ochranu citlivých dat přenášejících na flash disků či paměťové kartě. Tato média lze snadno ztratit.

Nejjednodušším způsobem, jak uložit citlivá data v zašifrované podobě, je zabalit je do komprimovaného archivu, přístup k němuž ochráníte heslem. K souborům a složkám uloženým v archivu pak nelze bez

znalosti hesla získat přístup. Tvorbu šifrovaných archivů zvládne například bezplatný program 7-Zip.

Požadujete-li dokonalejší šifrování souborů a složek, doporučujeme všeobecně respektovaný šifrovací nástroj TrueCrypt. Silnou zbraní programu je šifrování kompletních diskových oddílů včetně těch systémových. TrueCrypt lze tedy použít například k ochraně veškerých dat, která máte ve svém přenosném počítači. Nemusíte se pak bát, že k vašim datům získá přístup nepovolaná osoba. Přenosný počítač (ale i stolní počítač) ochráníte tak, že zašifrujete kompletní obsah pevného disku – pro přístup k němu je pak nutné při nabíhání počítače zadat heslo. Bez hesla se nespustí operační systém a nejsou přístupná data uložená na disku, a to dokonce ani pokud dojde k jeho vyjmutí a připojení k jinému počítači.

■ **JIŘÍ MACICH ml.**, jiri@macich.net

www.7-zip.org

7-Zip

JAZYK: čeština
CENA: zdarma
PPK CD: 16/2011

Komprimační nástroj umožňující zašifrovat archiv.

www.truecrypt.org

TrueCrypt

JAZYK: angličtina
CENA: zdarma
PPK CD: 16/2011

Ucelený nástroj pro šifrování dat i celých disků.

info

JAK TO FUNGUJE?

Šifrováním se pomocí speciálního postupu (tzv. algoritmu) převedou data do nesrozumitelné podoby. Pokud by taková data někdo neoprávněně získal (odcizil, „odposlechl“ během přenosu v síti apod.), musel by znát nejen příslušný algoritmus, kterým byla data zašifrována, ale také unikátní klíč (heslo), potřebný k jejich uvedení zpět do srozumitelné podoby. Šifrovaná data tedy může útočník získat, ale nejsou mu k ničemu dobrá, protože z nich nezíská žádné relevantní informace.

JAK JE TO BEZPEČNĚ?

Většina dnes používaných šifer je dostatečně kvalitních na to, aby dokázaly daná data nebo komunikaci účinně ochránit. Nejslabším místem je tedy lidský faktor, a to hlavně když se šifrovaná data dešifrují zadáním hesla zvoleného uživatelem. S heslem, které se dá snadno uhodnout nebo které zná každý z vašeho okolí, nenadělá nic sebesilnější šifra. Problémové může být také zabezpečení počítače, na němž se s daty pracuje. Škodlivé kódy mohou hesla „odposlechnout“.