

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informatiky



Teze diplomové práce

Komplexní zabezpečení domácího PC

Bc. Martin Kočí

© 2015 ČZU v Praze

Souhrn

Tato diplomová práce charakterizuje různé hrozby, kterým jsou vystaveny domácí počítače. Uživatelům poskytuje rady a návody, jak se proti takovým hrozbám bránit, případně, jak minimalizovat jejich dopad.

V teoretické části práce jsou vysvětleny pojmy důležité pro pochopení možných hrozeb, uvedeny principy útoků a také popis jednotlivých řešení, které mají počítač chránit.

Praktická část je vypracována pomocí dotazníku. Po vyhodnocení bylo zjištěno, že většina uživatelů má dobré znalosti v oblasti ochrany dat na domácím počítači, ale nejsou vždy využívány všechny potřebné metody.

V poslední části práce uvádí doporučení, která by měla pomoci uživatelům domácích počítačů výrazně zvýšit ochranu jejich dat před ztrátou. Zároveň tato část obsahuje ekonomické náklady jednotlivých řešení.

Klíčová slova

Antispyware, antivirový program, domácí PC, firewall, infiltrace, malware, ochrana, útočník, zálohování.

Úvod

V současné době jsou osobní počítače rozšířeny do téměř každé domácnosti. Z tohoto důvodu padla volba při výběru tématu na „komplexní zabezpečení domácího PC“. Dalším důvodem bylo to, že jsem od roku 1992 nejen aktivním uživatelem osobního počítače, ale i technikem a poradcem při sestavování, konfiguraci a provozu desítek osobních počítačů převážně v domácím použití. Přicházím proto poměrně často do kontaktu s různě vzdělanými uživateli v oblasti počítačů a rozhodl jsem se zaměřit na oblast zabezpečení.

V dnešní době, kdy je možnost infiltrace uživateli mnohem blíže než dřív, je toto téma velmi aktuální. Práce se zaměřuje na zlepšení informovanosti uživatelů a také bude vodítkem pro zvýšení bezpečnosti jejich počítače, potažmo dat. Také bude navrženo řešení, jak lze počítač ochránit, včetně cenové kalkulace.

Cíl práce a metodika

Cílem této diplomové práce je:

- charakterizovat a zhodnotit současný stav zabezpečení domácích PC;
- poskytnout informace o možnostech ztráty dat a jejich dopad;
- poskytnout běžným domácím uživatelům informace a návody, jak si zabezpečit svůj domácí PC proti uvedeným nebezpečím.

Metodika:

Diplomová práce se skládá z teoretické části, která je tvořena z rešerše odborné literatury a vlastních názorů a zkušeností autora, a dále z praktické části, která je založena na dotazníkovém výzkumu úrovně znalostí uživatelů domácího PC.

Doporučení

1. Uživatelé by si nejprve měli doplnit znalosti zejména v kritických oblastech, jako je používání elektronické pošty a internetového bankovníctví;
2. měli by zlepšit své znalosti v možnostech ochrany počítače, především u spywaru a originality softwaru;
3. měli by používat software na ochranu před infiltrací, protože povědomí o něm mají a navíc je možno používat i velmi kvalitní software zdarma;
4. v každém případě by měli uživatelé zálohovat svoje uživatelská data, v optimálním případě pravidelně;
5. nakonec by uživatelé měli také používat alespoň základní ochranu proti přepětí v rozvodné síti, pokud vlastní stolní počítač.

Závěr

Diplomová práce se zabývala komplexním zabezpečením domácího PC. Jsou v ní charakterizovány vnitřní a vnější hrozby, na které by uživatelé měli být připraveni a také metody a programy, které takovým hrozbám umí čelit.

Pro vypracování byly využity dlouholeté znalosti a zkušenosti autora z oblasti osobních počítačů, především pro domácí použití. V praktické části byla použita metoda dotazníkového výzkumu znalostí domácích uživatelů.

Z výzkumu vyplynulo, že v oblasti ochrany proti vnějším hrozbám mají uživatelé velmi dobré povědomí o programech, které je mohou ochránit, ale ne všichni uživatelé takové programy používají. Dále bylo výzkumem zjištěno, že se stále najde určitá část uživatelů, kteří si nejsou vědomi následků svého jednání při používání počítače. V neposlední řadě výzkum ukázal, že zálohování a ochrana proti výpadku el. energie nebo přepětí není na dobré úrovni.

Práce proto uvádí konkrétní doporučení, jak si svůj počítač ochránit proti vnitřním i vnějším hrozbám, včetně rozpočtu jednotlivých druhů ochran.

Na závěr tedy lze konstatovat, že zabezpečení domácích PC je na dobré úrovni, stále je však co zlepšovat, zejména v oblasti osvěty uživatelů.

Diplomová práce by měla být vodítkem a zdrojem informací pro běžné uživatele domácího počítače. Měla by pomoci omezit škody, ke kterým dochází při ztrátě dat, ať už osobního charakteru, nebo souborů uložených v počítači.

Hlavní použité zdroje

BITTO, Ondřej. *Jak zabezpečit domácí a malou síť Windows XP*. Brno: Computer Press, 2006, 216 s., ISBN: 80-251-1098-2.

ENDORF Carl, CHULTZ Eugene, MELLANDER Jim. *Detekce a prevence počítačového útoku*. Praha: Grada, 2005, 356 s., ISBN 80-247-1035-8.

HALBICH Čestmír, BRECHLEROVÁ Dagmar. *Bezpečnost informačních systémů – vybrané kapitoly*. Praha: Česká zemědělská univerzita v Praze, 2003, 104s., ISBN: 80-213-1090-1.

HANÁČEK Petr, STAUDEK Jan. *Bezpečnost informačních systémů*. Praha: Úřad pro státní informační systém, 2000, 128s., ISBN: 80-238-5400-3

JIROVSKÝ Václav. *Kybernetická kriminalita*. Praha: Grada, 2007, 288 s., ISBN: 978-80-247-1561-2

KRÁL, Mojmír. *Bezpečnost domácího počítače - prakticky a názorně*. Praha: Grada, 2006, 336 s., ISBN: 80-247-1408-6.

Český statistický úřad. *Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci 2014* [online]. [cit. 2015-01-10]. Dostupné na www: <<http://www.czso.cz/csu/2014edicniplan.nsf/p/062004-14>>

Svět hardware. *Počítačová havěť – vývoj a rozdělení malware* [online]. [cit. 2015-01-10]. Dostupné na www: <<http://www.svethardware.cz/pocitacova-havet-vyvoj-a-rozdeleni-malware/25680>>

Viry.cz. *Rozsáhlé DDoS útoky ochromily služby řady institucí* [online]. 2013-03-07 [cit. 2015-01-10]. Dostupné na www: <<http://www.viry.cz/rozsahle-ddos-utoky-ochromily-sluzby-rady-instituci/>>