AKO PREDCHÁZAŤ NAPADNUTIU POČÍTAČA VÍRUSMI

Peter Kováč
Ústav súdneho lekárstva LF UK Bratislava

V súčasnosti existuje viac ako 60 tisíc rozličných druhov počítačových vírusov, červov, trójskych koní a iných nebezpečných programov. Je teda dôležité, aby každý používateľ počítača nebral túto potenciálnu hrozbu na ľahkú váhu. Takmer každý je už dnes pripojený do internetu, takmer každý používa elektronickú poštu. Pritom sú to dnes najčastejšie brány, ktorými sa do počítača môže dostať vírus, či iná podobná infiltrácia. Škody, ktoré môžu vzniknúť v dôsledku sekundovej nepozornosti za počítačom môžu dosiahnuť neuveriteľné výšky. Pri ochrane počítača proti infiltráciám a hrozbám nielen z internetu je veľmi dôležité dodržiavať určité zásady. Tieto jednoduché a ľahko zapamätateľné zásady bezpečného používania počítača by mal ovládať každý používateľ počítača.

1. Používajte antivírusový program

Najčastejším, najjednoduchším a najspoľahlivejším spôsobom ochrany počítača je inštalácia antivírusového programu. Všetky dnešné antivírusové programy majú rezidentný skener, ktorý kontroluje každý jeden súbor, ktorý sa sťahuje z internetu, ukladá na pevný disk či disketu alebo sa má spustiť. Výber antivírusového programu je jedným z najdôležitejších rozhodnutí, ktoré pre ochranu svojich dát môžete urobiť. Istú informáciu vám môžu poskytnúť nezávislé testy, napríklad testy odborného časopisu Virus Bulletin (www.virusbtn.com). Ale pozor, nie každý test, ktorý nájdete je testom, ktorý vám má pomôcť. Niektoré sú skôr maskovaným marketingom. Pokiaľ už máte antivírusový program nainštalovaný, pravidelne ho používajte, najmä jeho rezidentý skener. Správnu činnosť antivírusového programu si môžete bezpečným spôsobom overiť pomocou neškodného EICAR testovacieho súboru, ktorý každý antivírusový program deteguje. (www.eicar.com). Každý antivírusový program postupom času zostarne a prestane poskytovať dostatočnú ochranu. Preto je nanajvýš potrebné pravidelne aktualizovať databázy vzoriek antivírusových programov priamo zo stránok výrobcu alebo distribútora. Dnes už nie je zvláštnosťou ani nastavenie pokusov o aktualizáciu na jeden krát za hodinu. Veľkým plusom pre ochranu vašich dát je antivírusový program s účinnou heuristickou analýzou. Takýto program má obrovskú výhodu oproti konkurencii v najkritickejšou časovom úseku vírusovej epidémie – od okamihu začiatku šírenia sa vírusu či červa do vydania aktualizácie databáz antivírusových programov. Aj keď antivírusový program je dôležitou súčasťou ochrany počítača, musíte si uvedomiť, že žiaden antivírusový program nikdy nebude detekovať všetky existujúce vírusy. Antivírusový program nie je skrátka všeliekom.

2. Inštalujte všetky opravy chýb v programoch a v operačnom systéme

Množstvo počítačových infiltrácii dokáže využívať známe bezpečnostné chyby v operačnom systéme (či už Windows alebo inom) alebo programoch. Každá takáto chyba predstavuje možné ohrozenie vašich dát. Preto pravidelne navštevujte stránky výrobcov vášho operačného systému a programov, ktoré máte nainštalované. Aktívne pátrajte po aktualizáciách a bezpečnostných záplatách. Pokiaľ nemáte dostatočné skúsenosti, prenechajte túto činnosť odborníkom alebo použite automatické nástroje určené na vyhľadávanie, sťahovanie a aktualizáciu operačného systému či programov. V prípade operačného systému Microsoft Windows je to služba Windows Update, pre Microsoft Office existuje Office Update. Pokiaľ je možné v operačnom systéme alebo programoch nastaviť zabezpečenie, voľte skôr vyššie úrovne, pretože poskytujú lepšiu ochranu proti infiltráciám.

3. Majte odloženú bootovaciu disketu

V prípade problémov s operačným systémom nie je často možné iné riešenie než len použitie bootovacej diskety. Preto ju majte vždy pripravenú a uloženú na bezpečnom mieste. Je síce veľmi pravdepodobné, že ju nebudete potrebovať, ale v prípade potreby by ste mali byť pripravený. Pokiaľ takúto možnosť ponúka pri inštalácii váš operačný systém alebo antivírusový program, vždy ju využite!

4. Nastavte počítač na bootovanie z pevného disku

Aj keď boot vírusy takmer vymizli spolu s DOSom, riziko, že na diskete zabudnutej v mechanike môže byť práve takýto vírus nie je nulové. Dnešné operačné systémy môžu reagovať na infekciu boot vírusom veľmi nepredvídateľne. Zmeňte preto radšej nastavenie poradia médií, z ktorých sa počítač bude snažiť o zavedenie operačného systému v BIOSe tak, aby sa operačný systém zavádzal najprv z pevného disku.

5. Pouvažujte o používaní alternatívnych programov

Jedným z predpokladov pre úspešné šírenie počítačových infiltrácii je ich zameranie sa na najčastejšie používaný softvér. Dnešné červy často využívajú špecifiká najrozšírenejších poštových klientov Microsoft Outlook/Outlook Express, chyby v Microsoft Internet Exploreri či možnosti robustného makrojazyka implementovaného v Microsoft Office. Oplatí sa preto pouvažovať nad alternatívami ku uvedeným programom. Zdá sa totiž, že tieto alternatívne programy sú menej často cieľovou platformou pre autorov počítačových infiltrácii. Možno tiež konštatovať, že alternatívy majú menšiu náchylnosť obsahovať chyby, ktoré možno zneužiť. Mozilla (www.mozilla.org), Opera (www.opera.com) sú vhodnou náhradou za Internet Explorer, The Bat!, Pegassus Mail (www.pmail.com) a už spomínaná Mozilla bez problémov nahradia poštových klientov spoločnosti Microsoft. Ako náhradu kancelárskeho balíka môžete skúsiť napríklad OpenOffice. Napriek všetkým uvedeným výhodám však aj tieto alternatívne programy môžu obsahovať bezpečnostné chyby, preto je nevyhnutne potrebné ich pravidelne aktualizovať.

6. Windows scripting host – potrebujete ho vôbec ?

Windows Scripting Host je štandardnou súčasťou operačného systému, avšak v skutočnosti je veľmi málo používaný. Windows Scripting Host umožnuje spúšťanie Visual Basic Scriptu (súbory s príponou VBS) a JavaScriptu (súbory s príponou JS). Asi najčastejšie využívajú Windows Scripting Host rozličné červy. Je veľmi rozumné túto peknú, ale zbytočne rizikovú súčasť operačného systému deaktivovať alebo pri inštalácii vôbec neinštalovať. Rozumným riešením pri inštalovanom Windows Scripting Hoste môže byť aj nastavenie štandardnej akcie pre súbory s príponami VBS/VBE a JS/JSE na úpravu v Notepade (Edit) namiesto prednastaveného otvorenia. Tak si budete môcť prezrieť obsah súboru a v prípade potreby zostane zachovaná možnosť tieto súbory spustiť.

7. Pozor na zdieľanie zdrojov v sieti

Veľmi peknou a zároveň nebezpečnou vlastnosťou operačných systémov je možnosť

MUDr. JUDr. Peter Kováč
Ústav súdneho lekárstva LFUK, Sasinkova 1
813 72 Bratislava

zdieľať po sieti adresáre, disky či tlačiarne. Ak nie ste pripojený do lokálnej siete, zakážte zdieľanie súborov a tlačiarní. A pokiaľ ste pripojený do siete, zdieľajte skutočne len to, čo nevyhnutne musíte. Rozhodne nie je rozumné poskytnúť na zdieľanie celý disk a najmä nikdy, naozaj nikdy nezdieľajte dôležité adresáre (napríklad adresár Windows). Prístup na zapisovanie pre zdieľané zdroje by ste mali poskytnúť naozaj len vtedy, pokiaľ je to nevyhnutne potrebné. Každý zdieľaný zdroj by ste mali chrániť heslom, pokiaľ možno ťažko uhádnuteľným. Nepoužívajte nikdy heslá ako „qwert“ či „abcdef“. Treba si uvedomiť, že adresáre a disky zdieľané v prostredí siete červy a vírusy veľmi často využívajú na svoje šírenie.

8. Nastavte zobrazovanie prípon súborov

V časoch, keď bol DOS kráľom, každý vedel, že názov programu sa skladá z mena súboru a prípony. Dnešné okienkovo a ikonovo orientované operačné systémy umožnili užívateľom zabudnúť na túto skutočnosť. To v sebe nesie riziko, že používateľ nebude schopný zistiť, či je program spustiteľný alebo nie. Nastavte preto operačný systém a tiež aj všetky programy (prinajmenšom svojho poštového klienta) tak, aby sa vždy zobrazoval úplný názov súboru, vrátene jeho prípony. Takýmto spôsobom sa vám tiež nestane, že naletíte na známy trik s dvoma príponami.

9. Pozor na prílohy správ elektronickej pošty

Súbory v prílohe správ elektronickej pošty sú dnes najčastejším spôsobom, ako sa môže počítačová infiltrácie dostať do počítača. Nikdy, skutočne nikdy by ste nemali robiť ani jednu z nasledovných rizikových činností:

- nikdy neotvárajte prílohy správ elektronickej pošty od niekoho, koho vôbec nepoznáte
- nikdy neotvárajte prílohy správ elektronickej pošty aj pokiaľ ste ju dostali od známeho, avšak nevyžiadali ste si ju
- nikdy a to naozaj nikdy bezhlavo nespúšťajte súbory, ktoré dostanete elektronickou poštou bez ohľadu na to, kto ich posiela
- nikdy neverte upozorneniam na „nebezpečný vírus“ či „zákerný červ“ s odporúčaním na vymazanie určitých súborov pokiaľ ich dostanete bez vyžiadania. Nikdy neposielajte takéto správy ďalej
- neotvárajte prílohy správ elektronickej pošty, ktorých jazyk nezodpovedá jazyku v ktorom s vami komunikuje osoba, ktorá je odosielateľom správy.

Niektoré klientské poštové programy umožňujú zobrazenie náhľadu správy. Už len takéto zobrazenie môže v niektorých prípadoch viesť k aktivácii červa či vírusu. Je nanajvýš rozumné túto funkciu vypnúť, prípadne ak je známe, že existuje bezpečnostná záplata riešiaca spomenutý problém s vírusmi, nainštalujte si ju. Uvedomte si, že červy a vírusy veľmi často používajú na svoje ďalšie šírenie záznamy v adresároch elektronickej pošty. Z uvedeného dôvodu preto vírus prichádza najčastejšie ako správa od niekoho, koho veľmi dobre poznáte. Vírusy a červy navyše veľmi často sfalšujú údaje o odosielateľovi infikovanej správy.

10. Používajte len softvér zo spoľahlivých zdrojov

V minulosti boli najčastejším vektorom šírenia vírusov počítačové programy a hry prenášané na disketách. To síce už patrí minulosti, ale je to nové nebezpečenstvo v podobe rozličných peer-to-peer systémov na zdieľanie súborov. KaZaA, Morpheus, Grokster ale aj IRC či ICQ umožňujú výmenu spustiteľných programov. Tie sú často pochybného pôvodu. Aj keď väčšina z týchto programov môže naozaj robiť to, čo tvrdí ich názov, niektoré z nich môžu obsahovať rozličné zadné dvierka, skryté nástroje pre vzdialenú správu či vírusy. Používajte preto len originálny softvér, pochádzajúci zo spoľahlivého zdroja. Každý crack či keygen ktorý stiahnete z internetu v sebe nesie riziko.

11. Pozor na súbory s dvoma príponami

Vírusy a červy veľmi často využívajú známy a osvedčený trik – súbor, v ktorom sú uložené, má dve alebo dokonca tri prípony – napríklad let_it_be.mp3.exe. Skutočne dôležitá býva najčastejšie práve tá na poslednom mieste. Uvedený súbor preto neobsahuje skladbu od Beatles ale je normálnym spustiteľným súborom.

12. Nebezpečné typy súborov

Ak používate Microsoft Word, mali by ste si zvyknúť používať pre vaše dokumenty namiesto formátu DOC čistý Rich Text Format (RTF). Formát RTF na rozdiel od formátu DOC neobsahuje makrá a je preto bezpečnejší. Ale aj v tomto je onen príslovečný háčik. Niektoré vírusy pri pokuse uložiť súbor vo formáte RTF uložia v skutočnosti dokument vo formáte DOC a dajú mu príponu RTF. Takéto dokumenty obsahujú makrá a teda môžu obsahovať aj makrovírusy. Word navyše rozpozná pri otváraní súboru jeho skutočný formát a aktivuje prípadné makrá. Dokonca aj samotný formát RTF nie je až tak dokonale bezpečný ako si mnohí myslia – formát totiž umožňuje vkladanie objektov... Pokiaľ potrebujete súbor len čítať, stojí za úvahu použitie formátu PDF, ktorého prehliadače sú k dispozícii zadarmo.

Podľa možnosti je vhodné vyhnúť sa z presne rovnakých dôvodov aj používaniu formátu XLS a nahradiť ho radšej formátom CSV (Comma Separated Variable). Upozornite svojich známych, že uprednostňujete posielanie dokumentov vo formáte RTF a údajov vo formáte CSV.

13. Diskety a iné výmenné médiá

Aj keď sú v dnešných časoch diskety tesne pred vyhynutím, takmer v každom počítači nájdete disketovú jednotku. Občas sa diskety aj dnes používajú na prenášanie kratších súborov. Pokiaľ používate disketu, alebo vôbec akékoľvek prenosné médium na prenášanie súborov z vášho počítača na iný, zabezpečte každé takého médium proti zápisu. Ak naopak prenášate prostredníctvom výmenných médií súbory z iných počítačov na váš, nezabudnite takéto súbory najskôr skontrolovať antivírusovým programom.

14. Zálohovať, zálohovať, zálohovať

Cena počítača v porovnaní s cenou údajov ktoré sú na ňom uložené predstavuje často len zanedbateľnú položku. Z uvedeného dôvodu je priam životne dôležité cenné údaje viacnásobne zálohovať. Ak sa náhodou stane niečo nepríjemné, záloha bude zárukou, že škoda nebude nezvratná.

15. Nepodliehajte panike

Napriek všetkému ani dodržiavanie uvedených zásad nie je stopercentnou zárukou, že sa vášmu počítaču nič nemôže stať. Ak máte podozrenie, že vás napadol vírus, obráťte sa na odborníkov. Najdôležitejšie je nepodľahnúť panike. Hlavne sa nepokúšajte problém s vírusmi a červami vyriešiť na vlastnú päsť, môžete spôsobiť viac škody ako osohu. Nestrašte a neplašte svojich spolupracovníkov. Pokiaľ vám došlo nejaké upozornenie o víruse, informujte sa u odborníkov.

Pokiaľ budete dodržiavať tu uvedené zásady, nebudete pred vírusmi a červami úplne bezpečný, ale svojim prístupom zabezpečíte, že riziko infekcie vášho počítača klesne na najnižšiu možnú mieru. Uvedomte si ale, že tieto zásady, ak majú byť účinné, musíte dodržiavať na všetkých počítačoch, s ktorými pracujete. Teda nielen v práci, ale aj doma či na vašom notebooku.

Uverejnené so súhlasom redakcie PC Revue