Deset rad pro zabezpečení MS Windows 2000/XP

Lukáš Rychnovský, Radim Peša,ÚVT MU

V poslední době narůstá do nepříjemných rozměrů agenda spojená s řešením následků napadení počítačů na MU *počítačovými červy*. Podobně jako počítačové viry představují i počítačoví červi škodlivý software, který se však nešíří prostřednictvím infikovaných souborů, nýbrž přímo prostřednictvím síťových paketů. Stanice se spuštěným červem náhodně nebo podle nějakého klíče kontaktuje jiné stanice připojené k internetu a při nalezení nezabezpečeného počítače se jej pokusí infikovat. Na rozdíl od počítačových virů není tedy pro spuštění zapotřebí přímá interakce červa s uživatelem. Zatímco výskyt počítačových virů šířících se elektronickou poštou se podařilo na MU dostat do únosných mezí, počítačů napadených červy se vyskytuje relativně velké množství. Cílem tohoto krátkého článečku je dát návod, jak se problémů s počítačovými červy vyvarovat, případně jak je řešit.

Drtivá většina řešených případů se týká počítačů s operačním systémem Microsoft Windows verzí 2000/2003 a XP. Proto se v rámci tohoto návodu omezíme na řešení problémů těchto operačních systémů.

Protože uvedené zásady jsou společné pro ochranu před počítačovými viry, červy i jinými druhy škodlivého softwaru, budeme dále mluvit pouze o společné kategorii „škodlivý software“. Podrobná definice a popis vlastností jednotlivých druhů škodlivého softwaru je k nalezení například v publikaci Moderní počítačové viry [1].

1 Jak zabezpečit svůj počítač

Jak tedy zabezpečit Microsoft Windows 2000/XP? Celý proces se v zásadě rozpadá na 5 částí. Každá z nich chrání váš počítač před jiným typem nebezpečí a každá je také jinak náročná na znalosti uživatele. Některé popsané metody vyžadují spíše pokročilou znalost systému MS Windows, nicméně základní kroky může podniknout i úplný začátečník.

1.1 Aktualizace zabezpečení operačního systému

[složitost: ★ důležitost: ★★★★]

Operační systém jako takový se skládá z mnoha programů, které zajišťují jeho běh. Může se však stát, že tyto programy obsahují chybu, kterou lze zneužít například k získání dat z vašeho počítače, vytvoření nového uživatelského účtu, nebo třeba rozesílání spamu. Když je nějaká taková chyba objevena a nahlášena, Microsoft v krátkém čase reaguje a vydá tzv. záplatu (angl. patch), která tuto chybu opraví. *Aktualizace zabezpečení* znamená stáhnout a nainstalovat tyto záplaty.

Postup je v tomto případě velice jednoduchý. Spusťte webový prohlížeč Internet Explorer a v menu *Nástroje* zvolte volbu *Windows Update*. Přímý link je `http://www.windowsupdate.com`. Je rovněž možné (a doporučené) nastavit si automatické stahování a instalaci aktualizací. Toto nastavení se nachází v „Ovládacích panelech“ nabídky START operačního systému. Pro aktualizace v rámci MU je rovněž možné používat univerzitní aktualizační server. Informace o službách, které poskytuje, jsou k nalezení na www stránkách ÚVT MU [2].

1.2 Aktualizace ostatních aplikací

[složitost: ★★ důležitost: ★★★]

Stejným způsobem je třeba dbát také o aktuálnost aplikací nainstalovaných na počítači. Mezi nejrozšířenější patří sada kancelářských programů Microsoft Office, ke které lze aktualizace nainstalovat z `http://www.officeupdate.com`. Informace o bezpečnostních problémech dalších aplikací je třeba sledovat přímo na stránkách výrobců. Některé kritické software automaticky upozorňují, je-li k dispozici jejich nová verze. Mezi nejkritičtější patří FTP-Servery, HTTP-Servery, Peer-2-peer klienti atp.

1.3 Antivir a jeho pravidelná aktualizace

[složitost: ★ důležitost: ★★★★]

Na každý počítač patří antivirový program. Hlavním posláním antiviru je bránit počítač před spuštěním škodlivého softwaru uloženého v emailových přílohách, webových stránkách a

spustitelných programech. Princip ochrany je ve velké většině založen na tom, že antivir již o existenci dané varianty škodlivého softwaru musí vědět a pak teprve je schopen před ním počítač chránit. Objeví-li se nový vir, musí příslušná antivirová firma pružně reagovat a vydat aktualizaci virových definic, kterou je pak třeba stáhnout a nainstalovat. Až poté je antivir připraven počítač před tímto virem ochránit. Proto je tedy velice důležité udržovat databázi virových definic aktuální. Rozumné je aktualizovat virové databáze jednou za den, u centrálně udržovaných antivirů je to možné i častěji. Většina antivirů umožňuje nastavit na počítači uživatele automatické periodické stahování aktualizací bez zásahu uživatele.

1.4 Firewall

[složitost: ★★★★ důležitost: ★★★]

Ihned po připojení počítače do sítě Internet, během krátké chvíle (řádově desítky minut), lze pozorovat pokusy z vnějšku o síťová připojení, které se snaží zjistit nedostatky v zabezpečení počítače popsaných v bodech 1. a 2. Při nalezení nedostatků v zabezpečení přejdou většinou tyto aktivity během krátké chvíle k přímému útoku, což v případě úspěchu může mít opět za následek přístup cizí osoby k vašim datům, či jiné bezpečnostní problémy spojené s vaším počítačem. Firewall (zvaný též osobní nebo personální firewall) je program sloužící k tomu, aby se tyto aktivity vašeho počítače nedotkly. Správná konfigurace firewallu je však obtížnější věc a měl by ji dělat člověk, který dané problematice rozumí. V opačném případě se může stát, že firewall počítač chrání nedostatečně či vůbec ne. Windows XP (na rozdíl od Windows 2000) již obsahují firewall, jehož pouhé zapnutí výrazně zvýší ochranu operačního systému před útoky, ke kterým dochází při připojení k internetu. Bohužel řada uživatelů o této možnosti vůbec neví a ve výrobcem nešťastně nastaveném výchozím stavu je firewall vypnut. Naštěstí od aktualizace Service pack 2 dostupné od srpna 2004 je ve výchozím nastavení firewall zapnut a jsou výrazně zlepšeny jeho možnosti [1].

[1] Nastavení firewallu ve Windows XP SP2 se mění v Ovládacích panelech, Brána firewall systému Windows.

1.5 Správná konfigurace systému Windows

[složitost: ★★★★★ důležitost: ★★]

Některá bezpečnostní opatření lze podniknout již na bázi konfigurace systému MS Windows. Jedná se například o nespouštění služeb, které nejsou využívány, změny ve výchozím chování a autentizaci, přejmenování administrátorského účtu a mnoho dalšího. Do těchto úprav by se však měl pouštět jen ten, kdo opravdu ví, co dělá.

2 Jak poznat, že je počítač napaden, a co v takovém případě dělat

I přes výše popsané zásady se může stát, že je počítač škodlivým softwarem napaden. To se nejčastěji projevuje „zpomalením“ chodu počítače, zvýšeným zobrazováním reklam, pády aplikací i celého operačního systému, případně další viditelnou či neviditelnou aktivitou. Při podezření na napadení počítače virem doporučujeme provést následující kroky:

2.1 Odpojení od počítačové sítě

[složitost: ★ důležitost: ★★★★]

Napadený počítač je nutné co nejdříve odpojit od počítačové sítě, aby se zamezilo dalšímu šíření škodlivého softwaru na ostatní počítače v síti. Mimo ochrany ostatních počítačů je odpojení nezbytné i pro úspěšné odvirování. U neodpojeného počítače se snadno může stát, že během odstraňování jednoho viru je počítač znovu napaden další nákazou. Odpojení počítače od počítačové sítě sice ztěžuje získání potřebných nástrojů a aktualizací k zabezpečení počítače (nelze je stáhnout ze sítě), ale ty je možné přenést i na jiných médiích.

2.2 Záloha dat

[složitost: ★ důležitost: ★★★★]

I když současné viry většinou nepoškozují soubory na disku, je velmi vhodné vytvořit si při podezření na přítomnost škodlivého softwaru záložní kopii dat, která je potřeba zachovat. (Vřele doporučujeme vytvářet si periodické zálohy dat i za normálního chodu počítače – a to nejen kvůli virům; hardwarová poškození disku či krádež počítače nejsou bohužel události tak výjimečné,

jak by se mohlo zdát!) Operační systém i aplikace je možné obnovit během několika hodin. Obnovit nezálohovaná uživatelská data většinou není možné vůbec!

2.3 Kontrola antivirovým programem

[složitost: ★ důležitost: ★★★★]

Po odpojení počítače od sítě a provedení zálohy dat je vhodné ověřit aktuálnost virových definic lokálního antivirového programu, provést jejich případnou aktualizaci a následně spustit kontrolu všech souborů na disku počítače.

2.4 Kontrola na přítomnost „ad-waru“

[složitost: ★ důležitost: ★★★]

Mimo klasických virů existuje také třída programků, jejichž přítomnost na počítači je nežádoucí, nicméně většina antivirů je nedetekuje; jde o tzv. *ad-ware*[2]. Jejich chování balancuje na hraně legality a antivirové firmy se je kvůli možným soudním sporům obávají detekovat. Jejich přítomnost však ohrožuje stabilitu operačního systému i bezpečnost dat. Naštěstí existují softwary, které se specializují na detekci a odstranění podobného obsahu. Při podivném chování počítače je vhodné zkontrolovat soubory na disku například nástrojem Lavasoft Ad-aware [3] nebo Spybot-S&D [4].

2.5 Kontrola spouštěných procesů

[složitost: ★★★★ důležitost: ★★★]

Přes usilovnou snahu antivirových firem existuje škodlivý software, který antivirové programy nedokáží detekovat. Proto je i při použití antivirového softwaru vhodné provést kontrolu spouštěných a běžících procesů.

Běžící procesy zobrazuje například nástroj Správce úloh (zobrazí se klávesovou zkratkou CTRL+SHIFT+ESC – záložka *Procesy*). Mnohem lepší je však použít například nastroj Process Explorer, který je zdarma ke stažení ze stránek firmy Sysinternals [5]. Tento nastroj, obdobně jako Správce úloh, zobrazuje běžící procesy v systému, ale poskytuje o procesech celou řadu dalších užitečných informací.

Pokud je některý z běžících procesů podezřelý, je dobré zadat jeho jméno do vyhledávače Google a pokusit se ověřit, co je zač, a případně spouštěný soubor z počítače odstranit nebo přejmenovat. Tento postup však již vyžaduje jisté znalosti a není vhodný pro uživatele bez znalosti o fungování operačního systému. Ideální je znát všechny procesy, které mají ve „zdravém“ systému běžet. Jistým vodítkem muže být, že podezřelé jsou například všechny procesy u nichž nejsou vyplněna pole Company Name a Description nebo jejichž jméno je tvořeno nahodilou kombinací písmen a čísel.

Dalším vodítkem při hledaní škodlivého kódu může být seznam programů spouštěných při startu systému nebo přihlášení uživatele. Protože kontrola všech míst v registrech, které umožňují automatické spouštění, je velmi pracná, je vhodné opět použít další nástroj od firmy Sysinternals jménem Autoruns. Ten zobrazí všechny programy spouštěné při startu systému nebo přihlášení uživatele.

Zjištěné procesy škodlivého softwaru je třeba ukončit a odstranit z disku soubor, který obsahuje jejich kód. Pokud se soubor po vymazání znovu vytváří, je třeba dohledat rodičovský proces, který jej vytváří a spouští. K tomu je opět možné využít nástroj Process Explorer, případně Pstools, obojí z dílny již zmíněných Sysinternals.

Toto je samozřejmě jen velice zevrubný návod, nicméně už vědomí toho, že není něco v pořádku, může být potřebným prvním krokem k odstranění i závažnějšího problému. V takovém případě je pak třeba vyhledat odborníka – například ve fakultní Laboratoři výpočetní techniky. Problematiku virů a počítačové bezpečnosti není radno podceňovat, přece jen v sázce jsou vaše data…

[2] Programy označované termínem ad-ware se obvykle zabývají zobrazováním reklamy a sledováním aktivit uživatele využitelných k marketingovým účelům. Instalují se často jako součást freewarových programů nebo při prohlížení www stránek, jejichž autoři se snaží tímto způsobem financovat své aktivity.

Literatura

[1] Igor Hák. Moderní počítačové viry. http://www.viry.cz/go.php?id=kniha/index

[2] http://www.ics.muni.cz/services/sus/
[3] Lavasoft Ad-aware. http://www.lavasoft.de/
[4] Spybot-S&D. http://www.safer-networking.org/en/download/index.html
[5] Sysinternals. http://www.sysinternals.com □