Viry a smrtelník

Igor Hák (Igi), www.viry.cz

PREVENCE

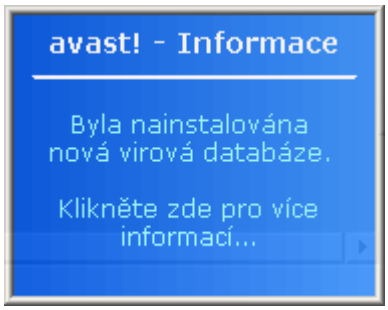
Než abych se rovnou pustil do toho nejhoršího, začnu prevencí :-)

Antivirový systém

by měl být nedílnou součástí každého PC. V tuzemsku se produkují hned dva antiviry – avast! (následující obrázky pocházejí z něho) a AVG. U našich východních bratrů pak jeden - NOD32. Ani zahraničí nespí, výpis všech nejpodstatnějších antivirů je k vidění na závěrečné straně.

Antiviru je potřeba věnovat péči. Uživatel by se měl především ujistit, že:

vlastní aktuální verzi antiviru.



Většina virů (červů) se dnes šíří prostřednictvím e-mailů, takže velice rychle. Rychlost je natolik závratná, že aktualizovat antivirus kupříkladu každou hodinu není dávno luxusem. Pokud je to možné, snažíme se nastavit čas mezi automatickými aktualizacemi na co nejnižší. Antivirus totiž bezpečně detekuje jen ty viry, které zná !

funguje rezidentní štít.

Rezidentní štít (někdy označován jako on-access skener) je součástí všech moderních antivirových systému pro Windows a měl by být neustále v provozu. Zatímco v minulosti bylo nutno každou cizí disketu zkontrolovat ručně, dnes za nás tuto činnost zcela automaticky provede onen zmiňovaný rezidentní štít. Rezidentní štít totiž neustále bdí v paměti a sleduje veškerou činnost uživatele, která by mohla vést k průniku či spuštění počítačového viru.

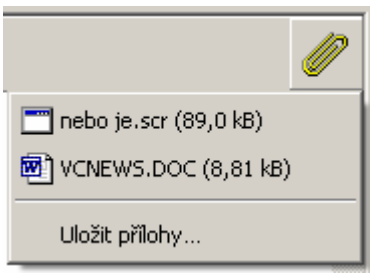
Pokud by snad došlo k nalezení viru, uživatel je na tuto skutečnost upozorněn ještě dříve, než může virus cokoliv provést. Malým příkladem může být následující obrázek,

kde se jeden uživatel pokusil spustit soubor infikovaný virem (červem) Win32:Klez-H. U většiny antivirů platí, ať v tento moment zvolíme cokoliv, nikdy nedojde ke spuštění viru, ale vždycky půjde o jeho likvidaci (formou smazání, vyléčení, přejmenování).

Bezpečnostní záplaty

Antivirus není všechno, je potřeba udržovat i „záplatované“ verze významných produktů, jakými jsou především Internet Explorer spolu s Outlook Expressem.

Bezpečnostní záplaty slouží na „zalepení“ bezpečnostních děr, tedy chyb v programu, které se průběžně objevovaly po jeho vydání. V Internet Exploreru jich je požehnaně a většina virů/červů šířících se e-maily jich využívá. Jedna z nich se třeba postará o to, že příloha e-mailu, tedy případný virus, bude spuštěn zcela automaticky bez rozhodnutí uživatele !



Bezpečnostní chyby jsou pochopitelně odstraňovány v každé nové řadě Internet Exploreru a s ním i spojeným Outlook Expressem, ale nestačí mít pouze poslední verzi (dnes 6.0 SP1). Je potřeba vlastnit i poslední záplaty k bezpečnostním chybám, objevených po vzniku uvedené verze.

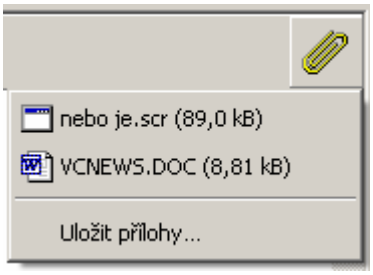
Nejjednodušší formou jejich získání je adresa http://windowsupdate.microsoft.com, kde se průvodce již o každého postará :-)

Dodržování bezpečnostních pravidel

Jedním z nich je „nespouštět všechno, co vidím“. Univerzální návod, jak rozeznat špatnou a dobrou zprávu neexistuje, ale obvykle jen stačí MYSLET !

Zajímavou kategorií e-mailových zpráv jsou pak tzv. HOAXy, tedy poplašné zprávy. Věřte tomu, že e-maily informující o novém, rychle se šířícím viru, kterého nelze žádným antivirem detekovat, jsou nepravdivé. Stejně tak e-maily hovořící o umírajících osobách a o potřebě dodání krve jisté skupiny. To vše jsou nesmyslné zprávy, šířící se rychlostí virů. Bližší informace o této problematice na www.hoax.cz.

VIRY A OSTATNÍ HAVĚŤ



I když se obecně pojmem „virus“ označuje veškerá havěť, není virus jako virus :-) Viry a červi (worms) se narozdíl od trojských koní (trojans) dokážou šířit bez vědomí uživatele i když pouze s jeho pomocí. Virus může do PC přicestovat disketou, ze sítě, z CD/DVD. Takové označujeme jako viry souborové, jelikož cestují spolu s původním programem ve spustitelném souboru. Pak je tu skupina nejrozšířenějších, kterým někdo říká viry, někdo červi. Důležité je, že se šíří e-mailem jako spustitelný soubor v příloze (sponka). Pokud dojde ke spuštění takového souboru (ať už přímo uživatelem, nebo díky bezpečnostní chybě), virus se obvykle natrvalo usadí v PC uživatele, začne vyhledávat co možná největší množství dalších e-mailových adres a na ně pak hromadně odešle svoji kopii – tj. emaily s infikovaným souborem v příloze. A takto se to stále opakuje dokola...

Chce to nervy !!!

S havětí, šířící se e-maily souvisí jedna důležitá a nepříjemná věc. Většina havěti totiž zcela úmyslně falšuje adresu původního odesílatele, což znamená, že adresa na kterou bychom eventuálně odpověděli, nepatří skutečnému odesílateli ! A to je právě kamenem úrazu. I uživatel vyzbrojený poslední verzí antiviru může znejistit, když mu jednou za čas přijde e-mail, oznamující, že právě z jeho adresy přišel virus. Podobný efekt, ale zcela automatizovaný přinášejí některé antivirové systémy na poštovních serverech, které upozorňují na případné infikované e-maily dotyčného odesílatele, v tomto případě bohužel opět nepravého. Proto, nevěřte všemu a mějte nervy !!!

ODKAZY

Následuje přehled některých antivirových systémů spolu s odkazem na českého distributora.

avast! antivirus	***www.avast.cz***
AVG Antivirový Systém	***www.avg.cz***
BitDefender Anti-Virus	***www.clnet.cz***, ***www.net-system.cz***
F-Secure Anti-Virus	***www.aec.cz***
Kaspersky Anti-Virus	***www.pcs.cz***, ***www.aec.cz***
McAfee VirusScan	***www.dns.cz***, ***www.edcz.cz***, ***www.sws.cz***, ***www.aec.cz***, ***www.pcs.cz***
NOD32	***www.esetsoftware.cz***
Norman Virus Control	***www.aec.cz***
Norton Anti-Virus	***www.symantec.cz***, ***www.norton.cz***
Panda Anti-Virus	***www.planetsoftware.cz***
PC-Cillin	***www.dns.cz***
Sophos Anti-Virus	***www.pcs.cz***
VirusBuster	***www.net-system.cz***