JAK BEZPEČNĚ POUŽÍVAT E-MAIL

Klasik by asi pravil, že „největší chybou uživatelů e-mailu je to, že používají e-mail“. To je ale rada k nezaplacení, protože s používáním „nebezpečného“ média jménem elektronická pošta se v současném světě zkrátka musíme naučit žít. Jak?

Stejně jako jsou mezi námi řidiči a „řidiči“ či umělci a „umělci“, také v případě počítačů jsou mezi námi uživatelé a „uživatelé“. A v případě e-mailu to platí dvojnásob. Zatímco někdo na „počítačovou hygienu“ velmi dbá, a viry mu tudíž problémy nepůsobí, počítač někoho jiného je pravým rájem pro všemožnou elektronickou havěť. Oba uživatelé (či spíše uživatel a „uživatel“) se přitom pohybují ve stejném prostředí.

ANTIVIROVÝ PROGRAM JE ZÁKLAD

Základem bezpečného používání elektronické pošty je prevence. Nikdy totiž nedokážeme zajistit, aby k nějakému problému (např. k napadení virem) nedošlo. Na problémy se však můžeme připravit. Právě nepřipravit se na možné potíže a spoléhat se na přízeň osudu je nejčastější chybou uživatelů elektronické pošty.

Součástí preventivní ochrany je antivirový program. Který? Na tuto otázku se nedá jednoznačně odpovědět. Každý uživatel počítače totiž vyžaduje něco jiného: někdo preferuje cenu, jiný přidané služby, další četnost aktualizací a někdo třeba grafické rozhraní. V otázce výběru antivirového programu tak existuje jediné doporučení: sami si vyzkoušejte, co vám – lidově řečeno – sedí. Je dobré přihlédnout též k doporučením druhých. Jak už ale bylo uvedeno výše, každý uživatel má jiné požadavky. Každý počítač je navíc unikátní kombinací hardwaru, softwaru, jejich verzí a nastavení, takže to, co funguje u souseda, nás může v práci spíše omezovat.

Antivirový program je samozřejmě nutné správně používat – především mít jej stále zapnutý a aktualizovaný. A jak často aktualizovat? Co nejčastěji. Žádné univerzální pravidlo ohledně četnosti aktualizací není, neboť každý uživatel má trochu jiné potřeby a požadavky. Ale pracujete-li s internetem denně, měli byste antivirový program aktualizovat každý den.

Antivirový program je nesmírně důležitý právě v souvislosti s elektronickou poštou, protože vysoké procento infiltrací přichází v současné době právě e-mailem.

VŽDY POUŽÍVEJTE AKTUALIZOVANÝ ANTIVIROVÝ PROGRAM. PRAVIDELNĚ ZÁPLATUJTE OPERAČNÍ SYSTÉM. PŘÍLOHY NEJPRVE ULOŽTE NA DISK A OTEVÍREJTE JEN TY, KTERÉ OPRAVDU POTŘEBUJETE.

Jako další chybu při využívání elektronické pošty je s trochou nadsázky možné uvést používání aplikace Outlook nebo Outlook Express. Jelikož jsou to nejrozšířenější klientské poštovní programy na světě, drtivá většina soudobých škodlivých kódů je samozřejmě „šita na míru“ právě jim. Proto se mnohdy doporučuje přejít k používání alternativních programů, což však není vždy možné nebo žádoucí.

PROSTÝ TEXT JE BEZPEČNÝ

Poměrně velkou chybou (nebo spíše neštěstí) některých uživatelů je, že při vytváření e-mailové zprávy používají HTML formátování. Místo toho se doporučuje používat prostý text (plain text). Ten sice neumožňuje používat různé velikosti písma, jeho různé typy či barvy, vkládat obrázky, zvuky nebo další objekty, ale – je bezpečný! A to je nezanedbatelná výhoda. Sami se však musíte rozhodnout, zda dáte přednost bezpečí, nebo pozlátku.

NÁHLED JE RISKANTNÍ

Stejně tak si dejte pozor na další „pohodlnou“ a často používanou věc – zapnutý náhled (preview) v poštovním klientském programu. Jeho použití sice umožňuje příchozí poštu si okamžitě přečíst, ale pokud zpráva obsahuje virus schopný sám sebe aktivovat bez zásahu lidské ruky, pak máte ve zlomku sekundy počítač zavirovaný, aniž byste mohli vy (nebo antivirový program) reagovat. Jak je možné, že v některých případech antivirový program není schopen virus zachytit? Je to tehdy, když dochází ke spuštění škodlivého kódu přímo z e-mailu, bez předchozího uložení na disk.

POZOR NA PŘÍLOHY

Největší nebezpečí z hlediska elektronické pošty však představují přílohy. Předně si musíme uvědomit, že nebezpečné jsou všechny typy příloh bez výjimky. Ve skutečnosti to není tak docela pravda, ale nebezpečné přílohy se s oblibou „maskují“ za ty bezpečné. To je třeba případ tzv. dvojitých přípon. Soubor s virem má název SMLOUVA.DOC.VBS a třeba i falešnou wordovskou ikonku. Jenomže některé počítače mají nastavenu volbu „nezobrazovat známé přípony“, a známou příponu VBS (Visual Basic Script) tedy nezobrazí. Vinou toho se virus může uživateli jevit jako wordovský dokument.

Také proto (a kvůli pohodlnějšímu zpracování antivirovými programy) se doporučuje každou přílohu před jejím zpracováním/otevřením uložit na pevný disk.

Pro úplnost upozorňujeme, že žádný soubor nemá dvě přípony, ale jen jednu jedinou. Jakákoliv další část názvu souboru, tvářící se jako přípona, je opravdu jen jeho názvem.

Tomáš Přibyl

ZÁPLATUJTE

Každopádně je nutné operační systém a používané programy záplatovat. Softwarové firmy chyby ze svých programů postupně odstraňují a programy upravují, aby byly stabilnější a bezpečnější.

Aby si uživatelé po každé vydané opravě nemuseli celý program, nebo rovnou operační systém znovu instalovat, vznikly tzv. patche – záplaty. Jedná se o menší programy, které mají za cíl instalovaný program a jeho konfiguraci upravit tak, aby se odstranily známé problémy (kolize s jiným programem, v některých případech špatná funkce, nechtěná vlastnost, kterou mohou využít hackeři nebo viry apod.).

Záplatování se v případě operačního systému Windows provádí prostřednictvím webové stránky *www.windowsupdate.com* nebo *windowsupdate.microsoft.com*. Pozor, některé záplaty mohou být poměrně obsáhlé (až desítky MB), ale jejich instalace se rozhodně vyplatí.