ZAMOŘENÝ INTERNET

Jak praví studie provedená specialisty z Washingtonské univerzity, každá šedesátá sedmá WWW stránka na internetu obsahuje nějaký virus nebo škodlivý kód. Statistika je to neradostná, ale bohužel pravdivá.

Aby výzkumníky nikdo nemohl napadnout za neobjektivitu nebo za nedostatečně reprezentativní statistický vzorek, založili svá konstatování na kontrole celkem osmnácti milionů WWW stránek. Je to přitom jen jedno z mnoha varování – internet začíná být v poslední době škodlivými kódy skutečně přeplněn.

ZCELA BEZPEČNÉ STRÁNKY NEEXISTUJÍ

Lze se setkat i s názorem, že pokud nenavštěvuji pochybné stránky (pornografické stránky, nelegální soubory apod.), mohu zůstat klidný. To je pravda jen částečně. Jistě, důsledně se vyhýbat rizikovým místům je alfou a omegou bezpečného chování.

NEOTEVÍREJTE NEVYŽÁDANOU POŠTU. NESPOLÉHEJTE NA ANTIVIROVÝ PROGRAM ANI NA ALTERNATIVNÍ PROHLÍŽEČ. PŘISTUPUJTE K INTERNETU JAKO K NEBEZPEČNÉMU PROSTŘEDÍ, NIC VÁS PAK NEMŮŽE PŘEKVAPIT.

Ty se do počítačů dostávají různými způsoby. Třeba tak, že využívají bezpečnostních nedostatků v prohlížečích, takže uživatel vůbec nemusí pojmout podezření, že se mu do počítače instaluje něco nežádoucího nebo že se někdo snaží pod nějakou záminkou získat souhlas s instalací...

Opravdu mimořádnou pozornost věnujte tomu, s čím na internetu souhlasíte nebo co do počítače instalujete. Mnohé WWW stránky nabízejí k volnému stažení celé filmy, plné hry nebo další atraktivní komodity – ale pod podmínkou, že si do počítače nainstalujete příslušnou „klientskou“ aplikaci. Pochopitelně že ta může obsahovat mnoho nepěkných vlastností, o kterých vás její tvůrci (jistě z pouhého opomenutí) pozapomněli informovat.

ANTIVIRUS VÁS NEZACHRÁNÍ POKAŽDÉ

Pozor, nespoléhejte v této chvíli na antivirový nebo jiný bezpečnostní program, protože ty si nemusí se všemi škodlivými kódy poradit. Třeba proto, že si dotyčnou aplikaci do počítače instalujete zcela dobrovolně. Nebo třeba proto, že antivirové firmy jsou schopné detekovat kódy, které se ŠÍŘÍ – nikoliv kódy, které jsou pevně vložené do nějakých stránek, a které tedy není možné pomocí nastražených pastí odchytávat (následně analyzovat apod.). To pochopitelně není důvod k tomu, abyste nepoužívali antivirový program, ale považujte ho raději jen za poslední záchrannou brzdu v případě mimořádné situace. Filozofie „mám antivirový program, můžu se chovat, jak se mi zlíbí“ je totiž sebevražedná.

Na druhé straně si však musíme uvědomit, že žádná pevná hranice mezi bezpečným a nebezpečným internetem neexistuje. A že i v uplynulém roce bylo zaznamenáno několik případů, kdy se hackerům podařilo do stránek jinak korektních a seriózních provozovatelů (např. šlo o hojně navštěvované zpravodajské servery) „propašovat“ škodlivé kódy. Ty zde sice měly životnost nanejvýš několik desítek minut, ale i tak byly jasným příkladem toho, že se na „bezpečný internet“ spoléhat nelze.

POZOR NA NEVYŽÁDANOU POŠTU

Často se také podceňuje nebezpečí plynoucí z otevírání nevyžádané elektronické pošty, spamu. Málokdo si uvědomuje, že pokud je spam zaslán v HTML formátování, nemusí e-mail veškerá data nést s sebou, ale může je de facto stahovat z nějakého předdefinovaného serveru. Takováto zpráva se pak chová v podstatě jako malé okno prohlížeče. Nebezpečí je přitom několikeré, třeba takové, že odesílatel spamu může snadno zjistit, kdo zprávu otevřel – a kde tedy sedí člověk, k němuž spam přes všechny filtry projde, a který je dokonce ochoten spam otevírat!

Dalším nebezpečím je fakt, že právě tímto způsobem se do počítače mohou zcela samočinně stáhnout škodlivé kódy a skripty. Znovu opakujeme, že e-mailová zpráva v daném případě funguje jako okno prohlížeče, přičemž jeho kontrola je pro antivirové programy poměrně obtížná. Navíc i dnes je stále ještě významné procento antivirových programů, které nedokážou provádět v reálném čase kontrolu příchozích dat a jsou schopny je prověřit až při ukládání na disk. (Pozor, nezaměňujte to se schopností kontroly práce v reálném čase – při ní dochází k načítání souborů z lokálního pevného disku a k jejich zpětnému zápisu, což je přesně ta situace, ke které při natahování dat z internetu nedochází.)

ALTERNATIVNÍ PROHLÍŽEČ

Problémy může někdy vyřešit používání jiného prohlížeče, než je Internet Explorer. Byť se jeho bezpečnost v poslední době významně zlepšila, přece jen je nejvíce útoků vedeno právě proti němu – a to kvůli jeho dominantnímu postavení. Ovšem ani používání jiného prohlížeče není všelékem:

- Díky provázanosti IE s operačním systémem dochází mnohdy k tomu, že nepoužívání (a nezáplatování) IE zanechává na počítači slabá místa, která pak zasahují ostatní prohlížeče.
- Každý prohlížeč má širokou paletu slabých míst. (Většina útoků je však vedena právě proti IE, v důsledku již výše zmíněného značného rozšíření.)
- Je statisticky prokázáno, že uživatelé s alternativními prohlížeči se na internetu chovají méně opatrně než uživatelé s IE. To je velká chyba, protože základem bezpečnosti je nejen aplikace sama, ale i bezpečné chování.

POZOR NA LÁKAVÉ NABÍDKY!

Internet je plný nabídek, jak něco získat zdarma: jde o bezplatný přístup na nejrůznější stránky, bezplatné zasílání informačních bulletinů, bezplatné zkušební verze programů... Zpravidla je to podmíněno jen nepatrnou drobností: uvedením e-mailové adresy nebo vyplněním krátkého osobního formuláře. To se přece nemůže nic stát...

Omyl! Uvědomte si, že pokud „zdarma“ je opravdu „zdarma“, pak bez jakýchkoliv jiných podmínek. Při vyplňování formulářů nebo při poskytnutí e-mailové adresy jako platidlo sice nepoužíváte peníze, ale poskytujete své osobní údaje. Výměnou za nějakou pochybnou protihodnotu je to, že vaše e-mailová schránka se zaplní nevyžádanou elektronickou poštou (spamem) nebo se stane terčem jiného typu útoku (v důsledku toho, že bylo zadáno několik osobních údajů, dosud anonymní IP adresa vašeho počítače získala konkrétní podobu).

Snažte se podobným lákadlům odolat a prozrazovat na sebe co nejméně informací!

Tomáš Přibyl