Internetové hrozby

Kromě zábavy a poučení číhá na internetu i nemalé množství hrozeb. S označením mnohých z nich jste se jistě již setkali, ale víte skutečně, co se za jejich názvy ukrývá?

NEVĚŘTE VŠEMU!

Základním pravidlem bezpečnosti na internetu je nevěřit všemu. Na každou výzvu k zadání osobních údajů se dívejte s podezřením a dobře si ověřte, zda je důvěra namístě. Zejména dětem pak vysvětlete, že na internetu není problém si „změnit totožnost“, a že tedy není dobré bezmezně věřit lidem, s kterými se tam seznámí.

ADWARE

(česky *reklamní předměty*) Programy, které po nainstalování na počítač zobrazují reklamu. V lepším případě je zobrazování reklamy cenou za používání dalších funkcí programu, v horším případě je adware jen jakýmsi typem viru – pouze obtěžuje uživatele nevyžádanou reklamou.

COOKIES

(česky *sušenky*) Krátká informace, kterou předává webový server prohlížeči při návštěvě stránky – prohlížeč ji pak ukládá na vyhrazené místo na disku. Cookies nejčastěji slouží k identifikaci uživatele, případně k uložení jeho osobních nastavení. Cookies lze v konfiguraci prohlížeče zakázat či omezit, může to však vést k narušení funkčnosti některých internetových stránek. Cookies však mohou být i zneužity – kupříkladu ke sledování „pohybu“ uživatele po internetu.

ČERV

(někdy také anglicky *worm*) Internetové červy jsou vlastně speciálními druhy virů. Jsou však ještě o něco zákeřnější. Na hostitelském počítači totiž nepotřebují žádný soubor, ve kterém by se mohly „usadit“. O svoje rozmnožování se starají samy, nejčastěji pomocí zabudovaného rozhraní pro rozesílání zpráv elektronické pošty. Díky této vlastnosti dokážou červy často zaplavit celý internet během několika málo desítek minut či hodin.

DIALER

Škodlivý program, který přesměrovává internetové připojení na telefonní čísla s vysokými sazbami (60 Kč za minutu a více). Toto riziko se však týká jen vytáčeného připojení, tzv. dial-upu.

DOS ÚTOK

(DoS – zkratka z angl. *Denial of Service – odepření služby*) Útoky mající za cíl vyřadit z provozu internetové služby. Provádí je buď přímo lidé (hackeři), nebo častěji škodlivé programy (viry, červy). Tyto útoky jsou de facto formou „internetového terorismu“, pomocí něhož se skupinka radikálů obvykle snaží dosáhnout nějakého cíle (nebo na sebe jen upozornit). Pro běžného uživatele však nepředstavují žádné větší riziko – maximálně to, že jeho oblíbená internetová služba nebude fungovat.

FORMULÁŘ

Prvek internetových stránek sloužící pro zadání údajů uživatelem. Typickým příkladem jsou registrační formuláře (po jejich vyplnění lze využívat různých služeb a objednávat zboží v internetových obchodech), webmailový klient, chaty a fóra. Riziko internetových formulářů spočívá v tom, že často vyžadují zadat osobní údaje, avšak nezaručují jejich bezpečnost.

HACKOVÁNÍ

(z angl. *hack – rozsekat, zničit*) Snaha o neoprávněné získání přístupu do cizích počítačů, počítačové sítě či různých zabezpečených uživatelských účtů. Důvodem pro tento druh elektronické kriminality je nejčastěji snaha dokázat si (popř. někomu), že s počítači něco umím dělat. Výjimkou nejsou ani průmyslové špionáže, dále útoky mající za úkol vyřadit cílový počítač z provozu a pokusy o elektronickou loupež peněz.

HOAX

(česky *smyšlenka, podvod*) Poplašné zprávy šířené po internetu nejčastěji prostřednictvím e-mailových zpráv a/nebo programů pro rychlou komunikaci (např. ICQ). Tyto zprávy obvykle varují před neexistujícími viry (uveden je i „návod na odstranění“) či před zpoplatněním volné služby, nebo naopak obsahují žádost o pomoc pro někoho těžce nemocného apod. Nedílnou součástí je také naléhavá žádost o přeposlání zprávy dalším uživatelům, díky čemuž hoaxy takto v nezměněné podobě kolují i několik let.

JAVA APPLET / ACTIVEX SKRIPT

Programy vkládané do internetových stránek. Pro jejich spuštění je třeba mít nainstalováno speciální rozhraní, jež je výrobcem distribuováno zdarma. Typickým příkladem jsou hry ve webových hernách a aplikace pro ověření šifrovaného klíče uživatele při přihlášení do internetového bankovnictví. Riziko těchto programů spočívá v tom, že mohou obsahovat i různé škodlivé kódy, kterými si autor internetové stránky zajišťuje přístup do počítače uživatele.

PHARMING/PHISHING

(z angl. *fishing* – rybaření, resp. *farming* – farmaření) Snaha o podvodné získání citlivých údajů (hesla, čísla kreditních karet apod.) za účelem jejich pozdějšího zneužití. Nejčastěji se tyto útoky provádí tak, že uživatel je „oficiálním“ dopisem vyzván k zadání citlivých údajů na stránkách, které vypadají, jako by patřily nějaké důvěryhodné instituci (bance aj.).

POP-UP OKNA

(česky *vyskakovací okna*) Okna prohlížeče, která se samovolně otevřou při vstupu na nějakou webovou stránku. Obvykle obsahují reklamu. Moderní prohlížeče tato většinou nežádoucí okna již umí blokovat.

SPAM

Nevyžádané e-mailové zprávy obsahující reklamu zpravidla na levný software a zázračné farmaceutické přípravky. Spam bývá odesílán hromadně z neexistujících či zfalšovaných e-mailových adres, což znesnadňuje boj s ním. Hlavním negativem spamu je zahlcování (uživatele i počítačů provozovatele) obrovským množstvím elektronických dopisů.

SPYWARE

(česky *špionské předměty*) Drobné programky či soubory, které se (často se souhlasem nepozorného uživatele) „usadí“ v počítači a vyhledávají a zasílají svému autorovi různá citlivá data, jako např. e-mailové adresy (cíl pro spam), uživatelská jména a hesla a čísla kreditních karet.

TROJSKÝ KŮŇ

Jeden z typů škodlivých programů. Stejně jako viry a červy se i trojské koně šíří nejčastěji e-maily, ale s tím rozdílem, že nepáchají škody okamžitě. Usadí se v systému a svému autorovi umožňují v případě potřeby takto infikovaný systém napadnout nebo zneužít k napadení jiného počítače.

VIRY

Různě škodlivé programky, které se samy a bez vědomí uživatele šíří zpravidla prostřednictvím počítačové sítě (internetu) – nejčastěji v dopisech elektronické pošty. Jejich název je díky podobné parazitní podstatě převzat od jejich biologických jmenovců.

WAREZ

(z angl. *wares – zboží*) Díla chráněná autorským zákonem, která jsou nelegálně šířena prostřednictvím internetu. Zpravidla se jedná o hudbu, filmy, hry a software. Součástí warezu ovšem často jsou různé viry, spyware, adware a podobně. ■ **aha**