Základy bezpečnosti na Internetu

RNDr. Václav Hník, CSc., Mgr. Oldřich Krulík, Ph.D., Mgr. Eva Staňová
Ministerstvo vnitra, odbor bezpečnostní politiky

Internet umožňuje rychlou a relativně anonymní výměnu informací a názorů. Tím slouží jak legálním účelům, tak zločincům, včetně teroristů. Ti mohou jeho prostřednictvím šířit svou propagandu a oslovovat sympatizanty. Jak teroristé, tak vyzvědači nebo zločinci, vedení zištnými pohnutkami, mohou v rámci Internetu rozesílat viry. To jsou programy, které mohou poškodit, změnit nebo zničit určitá data, případně umožní přístup k údajům uvnitř konkrétního systému. V důsledku takového počínání může dojít i k poruchám zařízení kritické infrastruktury, jejichž některé ovládací systémy jsou propojeny se sítí Internet.

- Aniž by musela být řeč rovnou o „kybernetickém terorismu“ nebo špionáži, je obecně vhodné dodržovat základní pravidla bezpečnosti na Internetu, která Vám mohou mimo jiné ušetřit nemalé finanční prostředky či řadu dalších komplikací, spojených se ztrátou či nechtěným zveřejněním konkrétních dat.
- Následující rady jsou určeny primárně těm, kteří jsou připojeni k síti Internet, ale využít jich částečně mohou i ostatní uživatelé informačních a komunikačních technologií.

Pravidla všeobecné prevence:

- Nikdy o sobě v rámci internetové komunikace bezdůvodně nesdělujte zneužitelné informace (adresu bydliště, telefon, číslo kreditní karty, e-mailovou adresu, heslo e-mailu a podobně).
- Používejte výhradně legální software. Dávejte důsledný pozor na pochybné hry a jiné programy, nabízené zdarma (freeware, shareware, utilities).
- Nezapojujte se do jakéhokoli nelegálního dění na Internetu (stahování či sdílení nelegálního software včetně hudby, videa a pornografie).
- Nikdy neotevírejte soubory přiložené k elektronickým zprávám (e-mailům) od Vám neznámých osob. Zpravidla se jedná o nevyžádanou reklamu (spam), pokud ne přímo o viry.
- Užívejte účinné antivirové programy a dostatečně často je aktualizujte.
- Informace z externích zdrojů (e-mail, CD-ROM, DVD, diskety, USB média) vždy kontrolujte antivirovým programem. Pravidelně kontrolujte i celý obsah pevného disku.
- Zvláštní nebezpečí znamenají spustitelné programy (zejména – ale nikoli výlučně – se jedná o koncovky *.exe, *.com a *.bat). Nenechte se zmýlit používáním tzv. dvou přípon souborů. Skutečná přípona je ta, která je zcela na konci souboru (tj. soubor „obrazek.jpg.exe“ není obrázek, ale program, a to s největší pravděpodobností virus).
- Dávejte bedlivý pozor na možné přesměrování (re-dial). Pečlivě prostudujte aktivní okna některých internetových stránek, která Vám dávají na vybranou mezi „ano“ a „ne“. Někdy i obě volby mohou znamenat, že se Vaše účty za připojení vyšplhají do astronomických výšek. V takovém případě vypněte nejen konkrétní okno (křížek v pravém horním rohu), ale raději i celý prohlížeč.
- Pravidelně, například jednou měsíčně, zálohujte důležitá data (vypálením na CD-ROM, atd.).
- Nepouštějte ke svému počítači osoby, které nejsou ochotny dodržovat bezpečnostní pravidla (to platí i o vlastních příbuzných).
- Svůj počítač chraňte i dostatečně komplikovanými a často obměňovanými hesly.
- Dbejte i na fyzickou ochranu výpočetní techniky a dat (v odůvodněných případech to může znamenat i náležité stavební úpravy, kvalitní dveře s bezpečnostním zámkem, bezpečnostní fólie a mříže na oknech, poplachové zařízení, atd.).
- Chraňte příslušná data před dětmi, Zamezte jejich přístupu na pornografické, extremistické a další nežádoucí stránky.
- Jestliže na Internetu naleznete něco, o čem jste přesvědčeni, že je to nelegální (extremistická propaganda, dětská pornografie, návody na výrobu improvizovaných zbraní) ohlaste tuto skutečnost Policii České republiky.

Možnosti rozpoznání viru v osobním počítači:

- Na výskyt viru Vás upozorní antivirový program.
- Svou přítomnost někdy virus oznámí sám, tzv. „hláškou“ na obrazovce.
- Na virus Vás upozorní ta skutečnost, že přestanou fungovat určité programy nebo počítač zkolabuje jako celek.

- Ani samo zjištění viru v počítači nemusí být vždy přímo důvodem k panice.
- Pokud zjistíte, o jaký virus se konkrétně jedná (to Vám zpravidla oznámí Váš antivirový program), pokuste se na Internetu najít (nejlépe pomocí jiného počítače, než nakaženého) jeho účinky a nejvhodnější způsob „léčby“.
- Pokud komplikace trvají, obraťte se na někoho informovanějšího, případně přímo na specializovanou firmu.

Z dalších zdrojů informací Vám doporučujeme:

- http://www.bezpecneonline.cz/:chraňte sebe, svůj počítač a firmu před nástrahami na Internetu (Ministerstvo informatiky)
- http://www.egovernment.cz/archiv/pdf 3-06/1.pdf: pravidla bezpečnosti elektronické komunikace (magazín E-Government)
- http://www.myslenka.cz/: více k tématu ochrany duševního vlastnictví (iniciativa „Právo na straně myšlenky“)
- http://www.zatepla.cz/: více k tématu bezpečného Internetu a legálního software (server "zatepla.cz")
- http://www.bsa.org/czechrepublic/: více k tématu bezpečného Internetu a legálního software (Business Software Alliance)
- http://www.cpufilm.cz: Česká protipirátská unie;
- http://www.filmynejsouzadarmo.cz: více k tématu ochrany duševního vlastnictví
- http://www.itpravo.cz/: server o právních a bezpečnostních otázkách, spojených s informačními technologiemi.
- http://www.mojebanka.cz/cs/security.shtml: desatero bezpečnosti Komerční banky, a. s.
- http://www.csas.cz/banka/content/inet/internet/cs/standard_content_pi01_005001.xml: Internetbanking, Česká spořitelna a. s.
- http://www.citibank.cz/czech/consumer-banking/czech/files/phish_cz.pdf: rady pro bezpečné internetové bankovnictví (Citibank)