JAK NA INTERNET

Online bezpečnost

“Tyhle aféry každého jenom otravují. Já bych všechny ty internety a počítače zakázala,” posteskla si v roce 1999 důchodkyně Věra Pohlová v anketě deníku Metro. Touto dnes již ikonickou větou reagovala na zprávu o úniku klientských dat z jedné z českých bank. Je fakt, že málokterá technologie nabízí tak pestrou škálu možností zneužití jako právě Internet, ale je to pořád “pouze” technologie. Tedy to, zda poslouží k něčemu dobrému, nebo naopak, mají v rukou jen samotní uživatelé. Nejen útočníci, ale i potenciální oběti, které podceňují zabezpečení svého pohybu na Internetu.

Zákeřný software

Nástrojů, jimiž lze na Internetu škodit, či dokonce páchat trestnou činnost, je opravdu celá řada. Jedním z nejrozšířenějších je tzv. malware. Jde o složeninu anglických slov malicious (zákeřný) a software. Malware souhrnně označuje různé techniky, jimiž lze poškodit nebo zneužít cizí počítač.

Sem se řadí:

- Viry a červi, které se dokáží samy šířit a reprodukovat
- Trojské koně, tedy malware nastrčený do zdánlivě užitečné aplikace
- Spyware monitorující činnost uživatele
- Adware, který počítač zahltí nevyžádanou reklamou

Zvláštním pojmem, který stojí trochu mimo uvedenou kategorii, je botnet, tedy autonomní softwarový robot, který samostatně pracuje v rámci sítě, obvykle za účelem finančního prospěchu na úkor napadeného.

Útoky na e-mail

Další rozšířený způsob zákeřného jednání na Internetu stojí na zneužití e-mailu. Asi každý se setkal se spamem - nevyžádanou poštou s reklamním nebo klamavým obsahem. Mnohem nebezpečnější technikou je ale tzv. phishing, tedy metoda snažící se napodobit oficiální korespondenci a webové stránky bankovních institucí či dalších služeb.

Nejčastěji phishing funguje tak, že útočník hromadně rozešle podvrženou e-mailovou zprávu, často s uvěřitelnou grafikou a relevantním obsahem zprávy, a požaduje citlivá data jako uživatelská jména a hesla, PIN, číslo platební karty nebo hesla. Případně uvede do zprávy odkaz na falešné stránky, které vypadají třeba jako přesná kopie formuláře pro přihlášení do elektronického bankovnictví. Zadané přihlašovací údaje se pak nedostanou na server banky, ale přímo k útočníkovi.

JAK NA INTERNET

A na závěr několik pravidel, která Vám pomohou k bezpečnějšímu používání Internetu:

- Nainstalujte si antivirový program a pravidelně jej aktualizujte. I ty zdarma nabízí kvalitní ochranu počítače.
- Zabezpečte přístup na domácí wi-fi síť silným heslem (použijte velká i malá písmena, číslice a další znaky).
- Na veřejných wi-fi sítích nenavštěvujte stránky, kde je třeba zadávat osobní nebo jiné citlivé údaje.
- Používejte spamový filtr svého poštovního klienta.
- V podezřelých e-mailech neklikejte na žádné odkazy. Pamatujte, že banky a podobné instituce NIKDY nevyžadují osobní údaje ani důvěrná uživatelská data e-mailem.
- Na stránkách typu internetové bankovnictví vždy zkontrolujte jméno domény uvedené v řádku pro adresu. Pokud se neshoduje s oficiální internetovou adresou služby, okamžitě stránky opusťte.
- Stažené soubory jako instalační programy, archivy souborů apod. z neověřených zdrojů vždy nechte individuálně skenovat antivirem.
- Na stránkách s problematickým obsahem vždy pečlivě zvažte, na jaký odkaz kliknete.
- Mějte na paměti, že malware může být součástí i zdánlivě neškodných souborů - .mp3, .jpg, .avi, .zip atd.
- V závažných případech jakékoliv formy kybernetické kriminality se neváhejte obrátit na Policii České republiky.

Další informace:

Bezpečný Internet (www.bezpecnyinternet.cz)

wikipedia.org - Malware

wikipedia.org - Spam

wikipedia.org – Phishing

CZ.NIC | SPRÁVCE DOMÉNY CZ