Jak se chránit proti spamu

Miroslav Bartošek, ÚVT MU

Idylické časy, kdy Internet byl výlučnou doménou vědců a ohleduplných uživatelů respektujících psaná i nepsaná pravidla síťové etikety (netiquette), jsou nenávratně pryč. Dnešní Internet je nástroj, který na jednu stranu fantastickým způsobem rozšiřuje informační a komunikační možnosti běžného člověka, na druhou stranu skýtá mnohá rizika a nebezpečí – zejména pro nepoučeného a neopatrného uživatele.

V oblasti elektronické pošty jsou hlavními riziky šíření virů/červů a spam. Přestože hlavní tíha boje proti těmto rizikům leží na správcích počítačů a síťových služeb, na individuální úrovni rozhoduje o mnohém sám uživatel. Svými znalostmi a svým chováním ovlivňuje z nemalé části míru svého vlastního ohrožení i ohrožení dalších uživatelů. V případě elektronické pošty může podstatným způsobem ovlivnit množství spamu přicházejícího z Internetu na jeho adresu, stejně tak jako množství spamu, který skončí nerozpoznaný přímo v jeho poštovní schránce. K tomu je ale třeba znát a dodržovat jistá pravidla. Ty lze shrnout do sedmi oblastí:

1. Chraňte svou e-mailovou adresu.
2. Svou poštu čtěte bezpečným způsobem.
3. Poštu posílejte bezpečným způsobem.
4. Neodpovídejte na spam.
5. Filtrujte svou poštu.
6. Buďte obezřetní.
7. Udržujte své počítače v zabezpečeném stavu.

1 Chraňte svou e-mailovou adresu

Obecná zásada říká, že nejefektivnější způsob jak se vyhnout spamům je neumožnit spammerům získat vaši e-mailovou adresu. Nejčastěji získávají spammeři adresy automatizovaným sběrem přímo z webu (z webových stránek, diskusních skupin) nebo tím, že jim ji sami předáte (vyplněním e-mailové adresy při on-line nákupech a registracích). Z toho vyplývají i následující doporučení:

- Neuvádějte svou nechráněnou adresu na webu ani ve volně přístupných elektronických diskusích.
- Pokud již svou adresu potřebujete či musíte na webu uvést, zamaskujte ji tak, aby ji byl schopen přečíst a správně interpretovat člověk, nikoliv však program-sběrač (např. jantecka-novak (na) muni-tecka-cz). Případně použijte speciální dočasnou adresu, kterou můžete později snadno změnit či zrušit.
- Ověřujte si, zda se vaše adresa vyskytuje všude na webu pouze v chráněném tvaru. Zatímco adresy uváděné na univerzitním webu jsou chráněné, uživatelé sami (nebo jejich partneři) zřizují různé osobní stránky, stránky řešených projektů, konferencí apod., kde již adresy chráněné být nemusí.
- Pro případné on-line nákupy a rizikovější operace na webu si založte svou druhou e-mailovou adresu u volně dostupných poskytovatelů (seznam, gmail apod.). Nikdy nepoužívejte pro tyto účely svou primární pracovní adresu. Sekundární adresu v případě její kompromitace snadno změníte, kdežto měnit primární pracovní adresu je problematické. Adres můžete mít samozřejmě i více – každou z nich pro jiný účel.

2 Svou poštu čtěte bezpečným způsobem

Některé spammerské e-maily jsou konstruovány tak, aby poskytly spammerům informaci o tom, zda je vaše e-mailová adresa platná či nikoliv. V kladném případě se cena vaší adresy pro spammery zvyšuje a můžete očekávat ještě větší přísun spamu. Často také dochází k propojování spamu s viry a červy. Při čtení spamů můžete být přesměrováni na spammerské stránky, odkud mohou být do vašeho počítače zavlečeny různé typy nákazy. Proto je užitečné zavést a dodržovat určitou disciplínu, pravidla a nastavení pro bezpečné čtení pošty:

- Buďte obezřetní, podezřelé dopisy raději vůbec neotevírejte; případně je čtěte pouze v režimu zobrazení jednoduchého textu (plaintext).
- U svého poštovního klienta si vypněte automatické zobrazování náhledů (preview), automatické stahování grafiky v HTML e-mailech a další potenciálně nebezpečné funkce, které sice zvyšují uživatelské pohodlí, současně ale lze jejich prostřednictvím aktivovat škodlivý

software obsažený ve zprávách či odkazovaných www-stránkách.
- Obraťte se na svého počítačového správce, ať vám doporučí vhodného poštovního klienta a pomůže s jeho bezpečným nastavením.
- Nikdy neklikejte na odkazy uvedené ve spammerských dopisech.

3 Poštu posílejte bezpečným způsobem

Některé způsoby rozesílání pošty mohou znamenat větší riziko prozrazení vaší adresy, či adres vašich kolegů. Současně je vhodné vždy uvažovat nad tím, co a jak vy sami rozesíláte, abyste (byť nevědomky) nepřispívali ke zvyšování spamové zátěže:

- Nerozesílejte řetězové dopisy. Vaše adresa se tak dostává na nekontrolovatelné množství počítačů, odkud může prosáknout až do spammerských databází.
- Ochraňujte e-mailové adresy jiných lidí. Při posílání e-mailu na velké množství adres může být vhodnější uvést tyto adresy do pole BCC (blank copy), namísto klasického CC (copy to).
- Zvažujte pečlivě, které vaše e-maily je skutečně nutné posílat na hromadné adresy, za nimiž se skrývá velké množství příjemců (např. posílání e-mailů na aliasy celé organizace či pracoviště).
- Nespamujte.

4 Neodpovídejte na spam

Z hlediska reakce na obdržený spam může být v našich zeměpisných šířkách někdy vhodné rozlišovat „měkký spam" rozesílaný spíše nezkušenými či naivními tuzemskými podnikateli od „tvrdého spamu" valícího se zpravidla ze zahraničí. Zatímco v prvním případě se dá uvažovat o vhodné formě komunikace s odesílatelem za účelem dalšího zamezení spamu (ale pouze pokud jste si jisti jeho identitou a relativní seriózností), ve druhém případě je doporučení jednoznačné – na spam nikdy nereagujte!

- Ignorujte spamy, které proniknou až do vaší poštovní schránky (smažte je bez čtení, neodpovídejte na ně).
- Nereagujte na výzvy REMOVE, tj. na informaci vyzývající vás k tomu, abyste klikli na zadanou webovou adresu, pokud si dané zprávy nepřejete dále dostávat. Nejenže skuteční spammeři nemají žádný zájem vás chránit (proč by to také dělali), takže z databáze adres vás neodstraní; tyto webové adresy jsou navíc často určeny pouze k ověření platnosti vaší adresy, v horším případě i k zavlečení infekce do vašeho počítače.
- Nikdy nekupujte žádné zboží/služby přes spam. Spammerství může fungovat pouze proto, že se spammerům vyplácí. Při obrovském množství rozeslaných spamů jim k tomu stačí, aby na jejich nabídky zareagovalo třeba jen mizivé procento oslovených. Proto nikdy nepodporujte spam tím, že byste využívali jím nabízených služeb.
- Nebombardujte spammery odvetnými e-maily. Adresy odesílatele jsou u spamu dočasné, zfalšované, nebo jsou použity zneužité adresy nevinných obětí, takže na skutečného původce spamu nemáte obvykle šanci dosáhnout.

5 Filtrujte svou poštu

Spam je do jisté míry individuální záležitost – co je spamem pro jednoho uživatele, nemusí být spamem pro jiného. Proto jsou hromadné antispamové filtry (univerzitní, fakultní) nastaveny dost konzervativně a nemohou zajistit absolutní ochranu všem uživatelům. Přestože účinnost fakultního filtru bývá obecně velmi vysoká, i více než 90 %, může se stát, že ve vašem konkrétním případě nemusí být dostatečná (a na druhou stranu se dokonce může stát, že je pro vás příliš restriktivní). V takovém případě se může vyplatit nastavit si svůj osobní antispamový filtr. Záleží samozřejmě na vašich znalostech, dovednostech a ochotě naučit se něco nového k dané problematice a v praxi to aplikovat.

- Ověřte si u vaší fakultní Laboratoře výpočetní techniky či správce vaší pošty, jak vaše fakulta/katedra provádí filtraci spamů, zda je fakultní ochrana skutečně aktivována i pro vaši e-mailovou adresu a jak s ní uživatel může dále pracovat (změny nastavení, přístup

k zachyceným spamům při vyhledávání nedoručené pošty atd.).
- Není-li ve vašem případě fakultní antispamový filtr dostatečně účinný, aktivujte po dohodě se správcem vaší pošty svůj osobní filtr. Může jít buď o filtr nabízený přímo vaším poštovním klientem na vašem počítači nebo o osobní nastavení fakultního filtru na fakultním poštovním serveru.
- Pokud váš osobní filtr podporuje techniku učení se na příkladech, doučujte ho tím, že mu budete předkládat jak nezachycené spamy (spam) tak i zprávy označené chybně za spam (ham). Obvykle je třeba předložit učícímu se filtru až několik stovek spamů a současně také několik stovek hamů, aby se dosáhlo maximální účinnosti rozpoznání vašeho typu spamu při minimální chybovosti. Toto je důležité také proto, že spammeři reagují na tento typ ochrany změnou struktury svých e-mailů a bez trvalého „doučování" se kvalita filtrace může v čase postupně zhoršovat.
- Filtrační program spamassassin používaný na fakultách MU umožňuje vytvářet relativně jednoduchým způsobem i osobní filtrační pravidla, a to přímo koncovými uživateli [1]. Tato pravidla mohou poskytnout nejvyšší stupeň ochrany ušitý na míru přímo danému uživateli.
- Aktualizujte své osobní antispamové filtry.

6 Buďte obezřetní

Internet v současnosti již není (a stěží kdy v dohledné době bude) tak idylické a bezpečné prostředí jako ve svých počátcích. Je třeba s tím počítat, a být poučený a obezřetný. V případě spamů již nejde dnes jen o to, že obtěžují. Čím dál více dochází k jejich propojování s počítačovými viry, červy, trojskými koni a různými podvodnými aktivitami. Čili stávají se i nebezpečnými.

- Buďte obezřetní a podezřívaví při otevírání dopisů od neznámých osob či institucí, při jejich čtení a reakcích na ně.
- Buďte obezřetní při brouzdání po Internetu; nebezpečné mohou být zejména stránky s pornografií, hrami a dalšími „chytlavými" tématy.

7 Udržujte své počítače v zabezpečeném stavu

Podle některých odhadů je až 7% počítačů připojených do Internetu napadeno různou formou nákazy, včetně programů, které se navenek zdánlivě nijak škodlivě neprojevují, umožňují však hackerům ovládat váš počítač bez vašeho vědomí a zneužívat ho pro různé účely. Například pro rozesílání spamu. Proto:

- Mějte na svých počítačích nastaveny ochranné firewally, pravidelně aktualizované antivirové programy a další ochranné nástroje proti škodlivým programům.
- Provádějte pravidelné instalace bezpečnostních záplat svého operačního systému a programů (lze nastavit, aby se provádělo automaticky – konzultujte se svým počítačovým správcem).
- Čas od času požádejte počítačového správce o provedení bezpečnostního auditu vašeho počítače (kontrolu a vyčištění od případných nákaz a nežádoucích programů, aktualizaci používaného programového vybavení, kontrolu bezpečnostních nastavení apod.)
- Zabezpečte a pravidelně aktualizujte bezpečnostní opatření nejen pro svůj počítač v práci, ale i pro své domácí počítače.

Jako v každém nebezpečném prostředí, ochrana „policií" (v případě Internetu pak správci počítačů a počítačových služeb) je vždy omezená, a její úspěšnost je velmi závislá na ochotě a spolupráci jednotlivců. V případě Internetu to platí dvojnásob – bez aktivního zapojení poučených (a trvale vzdělávajících se) uživatelů zůstane boj proti spamům sysifovským úsilím.

Literatura

[1] M. Bartošek. *Vylaďte si svůj SpamAssassin (2).* Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XVI., č. 2, str. 5–8. □