

Konec spamu?

Denně je doručováno asi 26 miliard e-mailů, z toho 6 miliard tvoří spam. Tak strašné to ještě nikdy nebylo - denně přichází nesčetné množství reklamních e-mailů, otravných řetězových dopisů a pop-up oken windowové služby messagingu z internetu na PC. Chip pro vás vybral ty nejlepší nástroje na účinné zablokování spamu.

Je to těžký boj. Spamy jsou denně odesílány, zdolávají početné servery, prodírají se celosvětovou datovou sítí a utlačují svým objemem její uživatele. Ale nevyžádaný e-mail to dnes už nemá snadné - z celkového počtu šesti miliard reklamních e-mailů denně "jen" 700 milionů dorazí do svého cíle. Zbytek je odchycen. V průměru dostává každý uživatel do své schránky dvě nevyžádané zprávy denně. A to je (díky technice) jen nepatrný zlomek při dvou miliardách e-mailů odpadu, které jen Hotmail Microsoftu nyní odchytné každých 24 hodin.

Průměr dvě nevyžádané zprávy denně je však stále ještě příliš mnoho, neboť některý uživatel nedostává vůbec žádný spam, zatímco u jiných dosahuje až 90 % všech zpráv v jejich schránce. Zdá se, že jednotliví rozesílatelé spamu přímo soutěží o to, kdo jako první dokáže e-mail jako komunikační médium zcela ochromit. Například poslanci parlamentu německé spolkové země Sasko už uvažují o tom, že budou své e-mailové adresy zveřejňovat na webu jen ve výjimečných případech, protože spam se samozřejmě nezastavuje ani před servery vládních institucí.

Obranu před touto záplavou e-mailů poskytují nové programy. Chip vám představí ty nejlepší nástroje, pomocí nichž se ochráníte před reklamními e-maily a postaráte se o spamu prostou poštovní schránku na svém počítači. Kromě toho vám ukážeme, jak zabránit tomu, aby se vaše e-mailová adresa dostala do rukou rozesílatelů reklamy, a prozradíme, jakými triky se dá blokovat spam u vašeho poskytovatele freemailových služeb.

Jak zastavit sběrače adres

Ještě předtím, než je vaše poštovní schránka zaplavena spamem, odvedou sběrači adres spoustu práce: pomocí speciálních programů se prokousávají webovými stránkami nebo organizují webové soutěže, aby získali e-mailové adresy. Ukážeme vám účinná protipatření.

Webové stránky jako zdroj adres

Internetové stránky jsou pro profesionální sběrače adres nejvydatnějším zdrojem, protože mnoho uživatelů internetu má vlastní webové stránky a téměř na každé webové stránce je zveřejněna kontaktní adresa pro návštěvníky. E-mailová adresa by na webové stránce neměla chybět - více se o tomto tématu dozvíte v připravovaném článku o tvorbě bezpečných webových aplikací.

Problém: Zveřejnění adres zneužívají sběrači adres. Podobně jako se vyhledávač Google pomocí specializovaných programů (nazývaných crawler nebo bot) prohřabává webovými stránkami, pátrají rozesílatelé spamu na stránkách po e-mailových adresách, aby jimi naplnili své databáze.

Řešení: Napište svou e-mailovou adresu tak, aby ji vyhledávač ihned neidentifikoval jako adresu. Například zápis "webmaster at domena dot cz" místo běžného "webmaster@domena.cz" už dokáže tyto zákeřné sběračské nástroje zmást. Vynalézaví programátoři by ale mohli i tuto past obejít. Proto byste měli svou adresu vložit do webové stránky jen jako obrázek. Otevřete grafický editor, napište svou elektronickou adresu do obrázku a ten ještě trochu upravte, například změkčením nebo efektem vodní hladiny. Návštěvníci vaší internetové stránky adresu bez problémů přečtou a "bot" má smůlu.

Soutěže jako návnada

Ať již jde o pár ponožek zdarma nebo o padesát bezplatných SMS zpráv, soutěže na internetu se dají financovat jednoduchým způsobem - prostřednictvím spamu.

Problém: Proč s velkou námahou prohledávat webové stránky, když lze "surfaře" úplně jednoduše přimět k tomu, aby sami zadali svou e-mailovou adresu? Mnoho soutěží a anket na webu slouží právě tomuto účelu.

Řešení: Pokud se těchto losování chcete účastnit, pořídte si druhou e-mailovou adresu. Zřídte si jednoduše účet u některého z poskytovatelů bezplatných e-mailových služeb a pak aktivujte automatické přesměrování pošty na svou běžnou adresu. Výhodou je, že jakmile nová adresa začne být zaplavována nevyžádanou poštou, stačí jen vypnout přesměrování a spamový teror bude padat do prázdna.

Použití testovací zprávy

Někteří rozesílatelé spamu vytvářejí seznamy adres zcela jednoduše náhodným způsobem. Tento postup vyžaduje jen málo času a je nepřekonatelně levný.

Problém: Chce-li například rozesílatel zastihnout svým e-mailovým odpadem všechny zákaznicky freemailové služby Seznam s pětiznakovým uživatelským jménem od aaaaa@seznam.cz do zzzzz@seznam.cz, nechá malým programkem vytvořit všechny možné kombinace a uloží je do adresáře. Protože nemůže vědět, které kombinace skutečně existují, je odkázán na zpětnou vazbu. Tu může získat z chybových hlášení, která při zaslání na neexistující adresu posílá server příjemce. Server ale může být nastaven tak, aby tato chybová hlášení neposílal. Zpětnou vazbu však lze získat i z reakce příjemce. Aby byl příjemce popíchnut k odpovědi, obsahuje většina spamových zaslání řádku, která slibuje, že vás vyřadí ze seznamu příjemců, když kliknete na webový odkaz.

Řešení: Je téměř zbytečné říkat, že tento odkaz spam nezastaví, nýbrž teprve pořádně spustí. Nereagujte tedy na takovou zprávu, jinak odesílatel dostane potvrzení, že adresa je platná.

Trik s e-maily v HTML

Zdánlivě je to skvělá myšlenka: e-maily by měly být barevné, měly by obsahovat obrázky a bohaté formátování textu. Jako na potvoru jsou právě proto e-maily v HTML oblíbené mezi spamery.

Problém: Skutečně zákeřné jsou e-maily ve formátu HTML, které obsahují odkaz na externí objekt, například obrázek (používá se vložení nenápadného obrázku o rozměru 1 x 1 pixel). Ten se totiž okamžitě načítá ze serveru, když zprávu otevřete. To znamená, že odesílatel spamu ví, že vaše adresa existuje, jakmile se na e-mail podíváte.

Řešení: Vypněte ve svém e-mailovém programu zobrazování HTML zpráv a nechte takové zprávy zobrazovat jako obyčejný text (plain text). Uživatelé starších verzí Outlooku však mají smůlu - Microsoft bez ohledu na svou kampaň k bezpečnosti nazvanou Trustworthy Computing ve svých starších e-mailových programech ještě neumožňuje deaktivaci HTML zpráv. Tyto krásně formátované e-maily přitom mohou otevřít dveře do vašeho systému nejen spamérům, nýbrž i autorům virů. Teprve od verze Outlook 2002 Service Pack 1 mohou bezpečnosti dbalí uživatelé internetu kritické HTML e-maily filtrovat a číst jako čisté a nezávadné textové zprávy. A je tu ještě jedna naděje: v aktuální verzi beta 2 nového Outlooku 2003 jsou nebezpečně krásné HTML e-maily implicitně zablokovány. Jen když si to výslovně přejete, jsou pestrobarevné zprávy opět aktivovány. Microsoft navíc do Outlooku 2003 poprvé zabudoval účinný filtr spamu.

Boj proti spamu ve freemailu

Především "surfařům" s běžnou telefonní nebo ISDN linkou vadí, když nesčetné nevyžádané zprávy prodlužují stahování e-mailů. Zde vám pomohou filtry freemailových serverů, neboť ty spam zablokují dříve, než z něj stáhnete jediný bit.

S koncem boomeru "všeho zdarma" na webu jsou freemailové účty zpravidla bezplatné už jen tehdy, vzdáte-li se trochy komfortu. To u většiny poskytovatelů znamená, že své e-maily můžete spravovat jen přes protokol POP3. Jeho nevýhodou je, že pokud chcete zprávy před smazáním důkladněji zkontrolovat, nemůžete je smazat už na serveru poskytovatele, ale musíte je stáhnout na svůj počítač. To stojí především uživatele analogové linky a ISDN mnoho času a tím i peněz. Ušetřit můžete, když váš poskytovatel freemilu předradí antispamovou ochranu.

GMX. Antispamový filtr poskytovatele freemilu z Mnichova, firmy GMX, je nejen dobře promyšlený a bezplatný, ale také spolehlivě funguje. Už na serveru jsou reklamní zprávy oddělovány od normálních e-mailů. Jakmile potom stáhnete obsah schránky svého účtu, obdržíte vedle požadovaných textů dodatečný e-mail přímo od GMX. Jeho obsahem jsou řádky s předmětem a časem odeslání zablokovaných nevyžádaných zpráv. Tak ušetříte drahocenný čas stahování, přesto však můžete v seznamu zkontrolovat, není-li v něm nějaká neprávem vyřazená zpráva. Nejpokročilejší metoda filtrování, modul schopný učení, který se přizpůsobuje vašim e-mailovým zvyklostem, je k dispozici jen za příplatek - profilování podle vzorových textů je zapnuto jen u GMX Pro (tři eura měsíčně).

Yahoo! Také u freemailu s vykřičníkem existuje předřazený filtr spamu pod názvem "složka hromadné pošty". V této složce zmizí všechny zprávy, které systém označí za spam. Do zpráv je možné nahlížet, protože však i stahování přes POP3 je u Yahoo! možné jen tehdy, souhlasíte-li se zasíláním reklamních zpráv, standardně neexistuje žádné upozorňování na nasbíraný spam.

Hotmail. E-mailová služba Microsoftu byla pro spamery vzhledem k obrovskému počtu uživatelů vždy přitažlivým cílem. Každý "surfař" s účtem Microsoft Passport, který je nutný pro Messenger integrovaný do Windows, se totiž musel prokázat účtem Hotmailu. Mezitím však i Microsoft reagoval na hrozbu spamu: softwarový koncern v poslední době zažaloval v patnácti soudních procesech rozesílatel reklamních zpráv, kteří měli uživatelům Hotmailu poslat celkem dvě miliardy spamových e-mailů. Microsoftu však stále chybí efektivní filtr pro účty na Hotmailu. Existuje sice takzvaná "složka pro

nevyžádanou poštu" (junk mail), a Microsoft dokonce nabízí několik nastavení filtru (standardní, zvýšené a exkluzivní), přesto i při nastavení zvýšené ochrany proklouzne do běžné poštovní schránky příliš mnoho spamu, kdežto možnost exkluzivní může být smysluplná pouze pro skutečné "webové poustevníky" - filtrem projdou jen takové e-maily, jejichž odesílatelé byli zařazeni mezi vítané.

Web.de. Dlouhou dobu byly zprávy pro uživatele Web.de jen neradostné - antispamovou ochranu kategorie Premium dostali jen členové klubu Web.de a tato exkluzivita stojí pět eur měsíčně. Od června 2003 však dostávají i spořilci více než rudimentární ochranu přes filtrovací pravidla a` la Outlook, neboť v té době Web.de aktivoval svou "třicestnou ochranu proti spamu", která třídí příchozí poštu do tří složek: složka došlé pošty a složka odpadu pro zjevné spamové zprávy jsou doplněny složkou "neznámé", která slouží jako sběrná nádrž pro potenciální nevyžádanou poštu - tady Web.de označuje e-maily barvami, které symbolizují pravděpodobnost spamu.

Poznámka redakce: Poměry u našich západních sousedů mohou být dobrým příkladem možností; jak to vypadá u nás, se dozvíte v rozsáhlém testu lokálních freemailových služeb, který bude v příštím Chipu.

Nejlepší blokátory spamu

Když nás filtry poskytovatelů e-mailových služeb neochrání, pomůže jen jedno - reklamní zprávy musíme zastavit sami.

SpamNet. Princip peer-to-peer je dobrý nejen pro výměnu hudebních skladeb po internetu - firma Cloudmark jej využívá, aby svým nástrojem SpamNet elektronické poštovní schránky uživatelů chránila před spamem. Jeho funkce je vysvětlena v panelu "Chytré: Antispamový systém SpamNetu". Idea je prostá: Když mnoho uživatelů společně vytvoří velkou databázi spamerů, mohou být otravné nevyžádané zprávy účinně filtrovány. Dnes už přes půl milionu uživatelů hlásí firmě každý spam, který dostanou. Cloudmark tak může vytvářet průběžně aktualizovaný seznam nevyžádaných e-mailů a s těmito znalostmi filtrovat příchozí poštu všech uživatelů SpamNetu. Umožňuje to malý plug-in do Outlooku, který si můžete stáhnout z webového serveru Cloudmarku (www.spamnet.com). SpamNet funguje překvapivě dobře a automaticky přesune identifikované zprávy do složky odpadu. Pokud by se nějaká reklamní pošta přece jen dostala přes filtr, můžete ji pomocí tlačítka v Outlooku zanést do seznamu na serveru Cloudmarku. V testu se SpamNet ukázal také jako částečně hyperaktivní - některé vítané zprávy označil za spam. Pouze beta verze SpamNetu smějí být používány zdarma, finální verze vyžaduje smlouvu: po třiceti dnech bezplatného vyzkoušení pak stojí asi čtyři dolary měsíčně. Zkušební verzi SpamNetu najdete na Chip CD v rubrice Zkuste si sami.

SpamPal. Úplně jinou koncepci sleduje open-source projekt SpamPal (www.spampal.org). Tento chytrý nástroj se instaluje na PC jako lokální proxy server pro e-mail - všechny příchozí zprávy tedy nejprve analyzuje a pak je předá e-mailovému programu (klientu). Tato oklika přináší výhody: nástroj můžete používat s mnoha e-mailovými programy a nasadit jej jako filtr i v malé domácí síti. SpamPal doplní předmět každého identifikovaného spamu o dodatek ****SPAM****. Proto musíte ve svém e-mailovém programu vytvořit filtrovací pravidlo, které tyto zprávy automaticky uloží do zvláštní složky. V programu Outlook Express to lze zařídit v následujících krocích:

Klikněte v okně složek pravým tlačítkem myši na Doručená pošta a v kontextové nabídce zvolte Nová složka. Pojmenujte složku Spam a potvrďte to stiskem OK. Jděte v menu na položku Nástroje | Pravidla pro zprávy | Pošta. V průvodci, který se otevře, zvolte možnost Kde řádek Předmět obsahuje určitá slova a bod Přesunout do určené složky. V poli Popis pravidla vidíte slovy označené filtrovací pravidlo. Klikněte na modře zvýrazněné obsahuje určitá slova a v následujícím dialogu zadejte ****SPAM****. Pak vyberte Přidat a OK. Nyní klikněte na modře zvýrazněné Určené a označte předtím nastavenou složku Spam. Potvrďte dvojím stiskem OK. Pak už Outlook Express každý e-mail s textem ****SPAM**** v předmětu zprávy přesune do speciálně vytvořené složky odpadu. SpamPal přesvědčuje především svou přesností zásahu; spam mu jen zřídka proklouzne. Tato přesnost má své důvody: SpamPal na přání kontroluje až 33 seznamů DNSBL - to jsou centrální encyklopedie, v nichž jsou uloženy adresy známých spamerů. SpamPal najdete na Chip CD v rubrice Zkuste si sami.

Ella. Pro všechny uživatele Outlooku, kteří svou protispamovou ochranu chtějí zařídit jednoduše, se nabízí nástroj Ella (www.openfieldsoftware.com). Stejně jako e-mailový klient Mail firmy Apple (viz odstavec "Jak zablokovat spam pod Mac OS X a Linuxem") se i Ella časem naučí, které e-maily uživatel považuje za spam a které zprávy jsou pro něj užitečné. Trénink sice při prvním spuštění obtěžuje s několika minutami klikání, potom se však Ella může skutečně srovnávat s programem od Applu.

Nevýhodou Elly je to, že tento chytrý nástroj stojí třicet dolarů. Zkušební verzi najdete na Chip CD v rubrice Zkuste si sami.

SpamKiller. Nástroj SpamKiller od firmy McAfee se obrací na tradicionalisty. Jeho nevýhodami jsou všechny přednosti, které lze nalézt u konkurence: není tu žádné filtrování schopné učení jako u Elly, žádné seznamy spamu jako u SpamPalu a žádný princip komunity jako u SpamNetu. SpamKiller

vyžaduje filtrovací pravidla, která například hodnotí určité předměty zpráv jako spam. Jeho výhodou je, že se dotazuje bašty spamu Hotmailu - funkce, kterou dosud nabízel jen Outlook Express (bez účinné antispamové ochrany).

Markus Schmidt

REKLAMA NA DISPLEJI MOBILU

SPAMOVÉ SMS ZPRÁVY

Melodicky pípající mobil stále častěji nevěstí zprávu od přátel, nýbrž ohlašuje další reklamní SMS zprávu. V současnosti sice ještě neexistuje účinná strategie, jak tyto zprávy zastavit, ale jednu reakci byste si měli naléhavě zakázat: odpovídat.

Důvod: Jako takzvaná služba s přidanou hodnotou vás tyto SMS zprávy mohou přijít velmi drahο. Mimo to byste se měli bezplatným SMS službám na internetu vyhýbat stejně jako všem soutěžím, u nichž musíte udat číslo svého mobilu.

JAK DEAKTIVOVAT WINDOWS MESSENGER

MINIWORKSHOP

Interní Windows Messenger je pro spam ideální: reklamní zprávy se otevírají přímo na surfařovu pracovní plochu. To je dostatečný důvod, proč trýznitele provždy odpojit.

1. Otevřít správu systému

Otevřete ve Windows ovládací panely přes Start | Ovládací panely. Přepínačem Přejít vpravo nahoře v okně zapněte klasické zobrazení. Pak dvojným kliknutím vyberte položku Nástroje pro správu systému.

2. Najít zpravodajskou službu

Nyní zvolte Správa počítače | Služby a aplikace | Služby. V seznamu aplikací najdete položku Kurýrní služba, pravým tlačítkem myši otevřete její kontextovou nabídku a vyberte Vlastnosti.

3. Vypnout pomocníka spamu

V okně Vlastnosti kurýrní služby nejdříve klikněte na Zastavit. Potom otevřete rolovací nabídku v poli Typ spouštění a zvolte tam Zakázáno. Tím zabráníte, aby Windows při dalším startu aktivovaly tohoto pomocníka spamu.

CHYTRÉ: ANTISPAMOVÝ SYSTÉM SPAMNETU

SBĚRNA ODPADU

Myšlenka je jednoduchá: Když mnoho surfařů identifikuje spam, budou všichni profitovat z lepší ochrany. Plug-in do Outlooku od SpamNetu pošle "otisk prstu" (hash) každého e-mailu na centrální server. Ten prověří, zda tato zpráva je již známá jako spam. U dosud neznámých zpráv stačí jedno kliknutí myši - a server ji uloží jako spam.

JAK ZABLOKOVAT SPAM POD MAC OS X A LINUXEM

ALTERNATIVNÍ OPERAČNÍ SYSTÉMY

Mac: E-mailovým klientem integrovaným v operačním systému OS X (jmenuje se prostě Mail) Apple vyhovuje volání po jednoduché obsluze, a to i v případě spamu. Po prvním spuštění se software přepne do režimu učení. Potom stačí, když došlé nevyžádané zprávy označujete kliknutím na tlačítko Junk mail; program se snaží ve vašem výběru rozpoznat nějaký systém. Přibližně po dvou týdnech je systém "natrénován" e-mailový nástroj hlásí, že už můžete režim učení vypnout. Příchozí spam pak bude automaticky přesouván do zvláštní složky. Úspěšnost je vysoká, chyby napравíte tlačítkem Junk mail. Ve složce Junk sbírá e-mailový program Applu všechny zprávy, které identifikoval jako spam. Software se přitom mylí překvapivě zřídka.

Linux: Příznivci tučňáka se mohou bránit zaplnění poštovní schránky spamem pomocí bezplatného open-source programu SpamAssassin (www.spamassassin.org). Nastavení sice vyžaduje trochu psaní v různých konfiguračních souborech, společně s programem pro zpracování pošty procmail (www.procmail.org) vám však tento nástroj zajistí poměrně slušnou filtraci příchozí pošty. Příležitostně ovšem SpamAssassin postihne pracovní zuřivost - prohlásí i žádané zprávy za spam. Proto byste jako složku odpadu neměli bezpodmínečně volit odpadkový koš Linuxu /dev/null - jinak jsou podezřelé e-maily navždy vymazány.