Antispam, antivir – ano, ale...

Vyslechněte si rady zkušeného uživatele

JAN DVOŘÁK

V současné době se stává stále aktuálnější potřeba filtrovat elektronickou poštu proti spamu a virům. Stále více lidí si instaluje tyto filtry na své domácí počítače a servery svých sítí a mnozí poskytovatelé internetu jsou nuceni je zapínat i bez požadavku uživatele. Rozhodl jsem se podělit se s vámi o své zkušenosti s touto problematikou.

Doufám, že tento článek bude užitečný při rozhodování, jestli filtr použít nebo nikoli. Hlavně mám v úmyslu upozornit na nejčastější chyby a problémy při používání těchto prostředků, a to jak při „domácím" použití, tak i při použití na serveru.

Nevhodné použití filtru proti spamu a virům totiž může stát hodně času, stresu a peněz.

Nejprve stručné vysvětlení pojmů

- Virus přenášený elektronickou poštou je e-mail, který vám obvykle odešle něčí zavirovaný počítač bez vědomí svého majitele. Na vašem počítači může virus způsobit nějakou škodu (například zničit vaše dokumenty) a většinou se odešle všem vašim známým, s nimiž jste v e-mailovém kontaktu. A tam rovněž může způsobit nějakou škodu a rozeslat sám sebe dál. Vzniká řetězová reakce, škody u uživatelů a přetížení internetu.
- Spam je naopak rozesílán většinou vědomě člověkem, který je za to mnohdy dokonce placen a je to jistá forma reklamy. Možná jste již někdy (nebo mnohokrát) dostali e-mail s obsahem například „Jsem třetí syn rolníka ze Zimbabwe, vyděláte miliony, když mi pošlete sto tisíc…" anebo nabídku nějaké firmy, že jste vyhráli letecký zájezd na Kanáry, pokud si koupíte její zboží a budete mezi první tisícovkou zákazníků…

Klasickou papírovou obdobou e-mailového spamu není nic jiného než třeba reklamní letáky obchodních domů, jež pravidelně nacházíme doma ve svých poštovních schránkách.

Před několika dny jsem viděl aktuální statistiku za poslední dubnový týden – 78,3 % pošty na světě tvořil spam, 3,8 % viry a pouze zbytek je skutečná pošta. Tahle čísla jsou poměrně šokující, i když v ČR je situace (zatím) poněkud příznivější. Problémem spamu je, že globálně přetěžuje poštovní infrastrukturu internetu a zahlcuje uživatele – příjemce pošty – množstvím e-mailů, které je nutné prohlédnout, identifikovat jako nesmysl a smazat.

Problémem virů je, že působí uživatelům mnohdy nenahraditelné škody a rovněž nárazově přetěžují internet. Je tedy rozumné a nutné poštu filtrovat, tedy nechat počítač, ať e-maily obsahující spam a viry automaticky smaže. Zdá se, že technologie k tomuto určené v současnosti „hýbou světem". Například na letošním InfoSecurity veletrhu v Londýně byl právě toto možná úplně nejvíce nabízený artikl.

Antispamové a antivirové filtry (dále jen filtry) lze rozdělit podle několika hledisek.

Například podle toho, ve kterém místě cesty pošty internetem se filtr aplikuje. Zjednodušeně řečeno: filtr může použít přímo koncový příjemce pošty na počítači, na němž poštu přijímá a čte. Tedy na svém počítači doma nebo v kanceláři. Nebo může být filtr aplikován někde v infrastruktuře internetu, například na poštovním serveru u providera. Použití filtru doma má výhodu, že je přímo v rukou uživatele a nastavení a použití filtru záleží jen na jeho rozhodnutí.

Ale na druhou stranu filtr aplikovaný až na konci cesty e-mailu od odesílatele k příjemci vůbec nesnižuje zatížení sítě, a to ani koncové linky od providera k uživateli. Je poněkud nepříjemné půl hodiny stahovat po modemu e-maily a pak zjistit, že to bylo 20 spamů a 6 zavirovaných e-mailů, ale e-mail od tetičky stejně nepřišel. Navíc antivir aplikovaný až na cílovém stroji teoreticky neznamená 100% ochranu před virem. Co když virus hackne něco v systému ještě před filtrem? Ještě jsem to v praxi na vlastní oči neviděl, ale prý se to občas stává…

Použití filtru na mail serveru u providera nebo jinde „uvnitř" internetu tyto nevýhody nemá, ale zase je uživatel zcela bezbranný proti nežádoucím účinkům filtru. Což také občas stojí nervy a peníze, viz níže. Typickým představitelem filtru, který je určen pro aplikaci „doma" jsou např. produkty Symantecu, McAfee nebo známé AVG. Typickým představitelem filtru, který se používá převážně na serverech, je třeba clamav.

Dále lze filtry rozdělit na hardwarové a softwarové. SW filtr někdy viděl asi každý – třeba právě zmíněné AVG. Prostě je to program, který převezme e-mail, zkontroluje ho, jestli je „nezávadný", a pokud ano, tak ho předá dál.

Pokud ne, tak ho zahodí. Popřípadě místo něj odešle upozornění, že e-mail přišel, ale byl zahozen. HW filtr naopak viděl zatím málokdo, i když je to zboží, jež právě prožívá svůj veliký boom. HW filtr pro „domácí" použití je prostě malá krabička, která se vloží do kabelu mezi síť a počítač. A kupodivu závadné e-maily do počítače nikdy nedorazí a ta kouzelná krabička je odstraní. Domácí HW filtr připomíná modem. Ostatně většinou jej vyrábějí právě výrobci modemů. Mnohdy mají HW filtry ještě další funkce: třídění pošty, archivaci pošty, odesílání pošty v off-peak hodinách, příjem pošty při vypnutém počítači a rozblikání se, když přišel touženě očekávaný e-mail, šifrování pošty, funkci firewallu, VPN atd… Serverové HW filtry mají podobné funkce, ale jsou to velké bedny anebo racky, dají se obhospodařovat na dálku a tak dále. Prostě běžný kus síťového železa.

Jak to funguje?

Filtrování pošty proti spamu i proti virům většinou realizuje jeden program. Ale principy jsou poněkud rozdílné. Použité algoritmy mohou být mnohdy poměrně složité, zde popíši pouze základní princip. Detekce zavirovaného e-mailu se dělá podobně jako detekce zavirovaných souborů na disku. Antivirový filtr obsahuje databázi řetězců, které se vyskytují ve všech známých virech. Pokud e-mail jeden z těchto řetězců obsahuje, tak je prohlášen za zavirovaný a zlikvidován.

Detekce spamu se takto dělat nedá. Nelze vytvořit databázi všech existujících spamů a řetězců, které je identifikují. Není to možné ze dvou důvodů:

- Spam píše na světě mnoho milionů lidí, viry píše jen několik programátorů. Různých spamů tedy existuje o několik řádů více než virů. Databázi spamu tudíž nelze vytvořit a udržovat pro její rozsáhlost.
- Viry jsou programy. Tedy člověku nesrozumitelný „text", určený pro čtení počítačem. Ale spam je běžná lidská řeč. Pokud by se používala databáze řetězců identifikujících spam, tak by za spam bylo prohlášeno množství běžné pošty. Možná skoro veškerá pošta. Texty používané ve spamu se prostě a jednoduše používají i v normálních e-mailech. Pro detekci spamu se používají tzv. blacklisty, provozované většinou různými antispamovými nadacemi.

Funguje to zhruba takto

Přijde vám spam. Vy se naštvete a tento mail přepošlete správci blacklistu (což může být buď živý člověk, nebo program). Ten uváží, jestli jde opravdu o spam a jestli se mu sešlo podobných stížností několik. Pokud ano, zveřejní identifikaci odesilatele v blacklistu.

Pozor – tohle je důležité! V blacklistech je zveřejněna identifikace ODESILATELE, nikoli jen identifikace konkrétního e-mailu! A protože každý správný spamer každých 10 minut změní svoji e-mailovou adresu a každou půlhodinu IP adresu svého počítače, tak se jako identifikace odesilatele používá hlavně IP adresa serveru, přes který spam odešel. Jinak řečeno, spam nebývá identifikován svým obsahem a dokonce ani svým odesilatelem, ale identifikátorem SÍTĚ, ze které odešel! Například IP adresou SMTP serveru příslušného internet providera. Vyřazení z blacklistu se děje obvykle na žádost správce postiženého serveru, popřípadě uplynutím nějakého času bez stížností.

Antispamové filtry tedy vezmou váš e-mail a podívají se, jestli náhodou nebyl odeslán z adresy uvedené na blacklistu. Pokud e-mail pro vás z takovéto adresy odeslán byl, tak je zahozen. A naopak pokud vy odesíláte e-maily přes server, jenž se náhodou dostal na blacklist, tak se dostane ke svému adresátovi jenom tehdy, pokud cestou nenarazí na antispamový filtr.

Největší problém

Právě tohle je největší problém v praxi při snaze o správné použití antispamové filtrace pošty. Totiž většina uživatelů pošty je připojena přes velké providery. Velcí provideři mají mnoho klientů. Mezi nimi se vždy najde nějaký spamer. Čili čas od času se právě váš poštovní server (resp. server vašeho providera) dostane na blacklist. A vaše e-maily pak filtry po celém světě považují za spam, i když tomu tak ve skutečnosti není. Tohle se čas od času stává všem velkým poštovním serverům všech velkých providerů.

Řešení jednoduchá, ale dosti problematická

Jedno z častých řešení je filtrovat pouze viry a spam nechat procházet. V ČR je to zatím asi přijatelné „řešení", ale na jak dlouho? Viz výše uvedená statistika – cca 80 % světové pošty dnes tvoří spam. A bude hůř...

Jiné často používané řešení je zahozené e-maily nahradit e-mailem obsahujícím informaci, že byl zahozen. Ale co to řeší? Snad objem dat prošlý mailserverem. Ale pro uživatele se situace spíše zhoršila – neustále se musí vyrovnávat s hromadou „divné"„ pošty a navíc si musí složitě vyžádat od odesilatele poštu, která měla dojít, ale nedošla. Navíc mohou vznikat trapasy. Zde je opět příklad z praxe:

Jednou jsem přišel na jistou univerzitu. A vidím, že ctihodný pan profesor se chová – mírně řečeno – velmi nectihodně. Opatrně jsem ho obešel a v bezpečné vzdálenosti se zeptal jeho sekretářky, co že se přihodilo? Bylo mi vysvětleno, že pan profesor pět let bádal, potom dva roky psal článek a pak půl roku prováděl na žádost redakce korektury. A dnes mu ona ctihodná redakce skutečně velmi prestižního světového vědeckého časopisu oznámila, že jeho článek přijímá a žádá o definitivní souhlas s otištěním.

Jenže SMTP server providera té redakce byl tou dobou zrovna na blacklistu. Takže odpověď té redakci neposlal pan profesor, ale poštovní server fakulty. Bylo to cosi rádoby vtipného ve stylu „Spamerům e-maily nedoručuju, příště neotravuj!". A navíc s chybou v angličtině. Pan redaktor se hluboce urazil, zavolal panu profesorovi telefonem a měl pro něj rovněž jen jednu větu - podobného obsahu. Raději jsem toho dne odešel a přišel si svoje věci vyřídit o dva dny později.

Další častá metoda je smazat viry a spam doručovat. Ale doplněný o upozornění, že jde o „***SPAM***". Mě osobně ale smysl tohoto opatření uniká. Zátěž sítě se nezmenší a zátěž uživatele také ne. Spíše naopak.

Dvě velmi dobrá, ale asi složitá řešení

Znám dvě dobrá, ale složitá řešení. Musí se totiž vždy naprogramovat pro konkrétní podmínky na konkrétní síti. Viry považuji za dobré (skoro) vždy je\dnoduše smazat. Níže uvedené se tedy týká jen antispamové filtrace.

První řešení je technicky zajímavé a uspokojivě funkční, ale vyžaduje nepřetržitou spolupráci živého člověka. Je tedy vhodné jen pro sítě střední velikosti s dobrým rozpočtem. Pro běžné podmínky příliš vhodné není. Druhé řešení já osobně považuji za zcela ideální řešení – vše probíhá zcela automaticky, vše je přímo v rukou uživatele, žádný e-mail se nemůže ztratit, ale zároveň je pošta filtrována s maximální možnou účinností.

První řešení: Adaptivní omezení šířky pásma pro odchozí i příchozí poštu plus ruční obsluha

Představme si typickou kancelářskou síť střední velikosti. Omezme šířku pásma pro e-maily řekněme na 50 KBd pro každou jednotlivou IP adresu. Pokud některá naše adresa odešle nebo z nějaké vnější adresy přijde během půl hodiny více než 10 e-mailů, tak omezme (pouze!) této adrese šířku pásma na polovinu. Pokud intenzivní mailování pokračuje, tak za půl hodiny zase na polovinu. A tak dále až na cca 1 KBd. Pokud se provoz zmenší, tak zase postupně šířku pásma obnovíme. Pokud jde o náhodné zvýšení užitečného provozu, v praxi příliš nevadí, že e-maily začnou po půlhodině odcházet pomaleji. Pokud ale jde o záplavu spamem nebo novým (tedy antivirem nerozpoznaným) virem, tak se expozice naší sítě podstatně sníží – díky omezení šířky pásma. Samozřejmě musí být neustále nablízku obsluha, jež se o vzniklé situaci včas dozví, situaci vyhodnotí a ručně provoz z dané adresy zablokuje – pokud jde skutečně o spam nebo nový virus. Bez obsluhy živým člověkem by toto opatření nemělo žádný smysl.

Druhé řešení: Uživatelský WWW interface – možná ideální řešení

Spam detekujeme běžným způsobem pomocí blacklistů. Ale nesmažeme ho, nýbrž umístíme tyto „podezřelé" e-maily na WWW adresu, která je přístupná adresátovi oněch e-mailů po zadání jeho loginu a hesla (pochopitelně s použitím https).

Na této stránce tyto e-maily zůstanou řekněme měsíc a pak se automaticky vymažou. Dvakrát denně adresátovi těchto odsunutých podezřelých e-mailů pošleme souhrnnou informaci o tom, co mu bylo odsunuto. Souhrn obsahuje čas, odesilatele, předmět, několik náhodně vybraných vět z těla e-mailu a referenci na URL, kde si lze tento e-mail vyzvednout. Pokud adresáta některý z odsunutých e-mailů zaujme, tak si ho na WWW stránce vyzvedne a přečte. Pokud ho nezaujme, tak se odsunuté e-maily po měsíci samy smažou. Vygenerovat zmíněný souhrn ovšem není zcela triviální. Spam totiž často přijde v mnoha kopiích a souhrn je pak nepřehledný. Takže je užitečné jednotlivé odsunuté e-maily vzájemně porovnávat a do souhrnu opakovaný e-mail uvést pouze jednou s poznámkou, že počet opakování se rovná například 12.

Jenže každý správný spamer mění adresy, počítače, předmět, oslovení, na konec přidává náhodné řetězce znaků a vůbec se snaží takovéto porovnávání znesnadnit. V praxi se osvědčilo při porovnávání vynechat celou hlavičku včetně předmětu a v těle e-mailu vynechat první a poslední (nonwhite) řádek. A ve zbytku e-mailu připustit 5 % rozdílných znaků z celkové délky zbylého textu pro porovnávání (porovnáváno pomocí diff a počítáno pomocí wc s podporou unicode).

Tato kombinace klasické blacklistové filtrace, porovnávacího enginu, pravidelných e-mailů uživateli se souhrnem a WWW rozhraní pro vyzvednutí odsunuté pošty mě osobně připadá jako ideální řešení. Ale není implementačně jednoduché.

Nebo řečeno totéž, ale z opačného úhlu pohledu: pokud si doma na svém počítači nainstalujete antispamový filtr, tak musíte počítat s tím, že vám občas nějaký e-mail nedojde, ale ztratí se. Protože jeho odesilatel sice není spamer, ale náhodou používá server, který je zrovna náhodou na blacklistu. Tudíž váš filtr tyto e-maily nepropustí.

Možná řešení

Existují různé možnosti a přístupy, jak se pokusit tento problém řešit. Úvahu o možnostech řešení rozdělím na použití „doma" (tj. na koncovém počítači) a „na síti" tj. například v rámci poštovního serveru vaší lokální sítě nebo pomocí prostředků vašeho providera.

Doma

Doma je úvaha poměrně jednoduchá. Pokud zrovna nejste specialista na viry a jiné speciality, tak si určitě aktivujte antivir. Ničemu totiž neuškodí, ale naopak velmi prospěje, když vám nebudou doručeny zavirované e-maily. Ale úvaha jestli aktivovat i antispamovou filtraci je něco jiného. Zde se musíte rozhodnout, co vám vadí víc. Jestli záplava spamu nebo ztrácející se užitečné e-maily. Instalace filtru „doma" samozřejmě nesníží zatížení linky, takže doma je to opravdu jen o tomto uživatelském rozhodnutí.

Poznámka: Přesněji řečeno filtr instalovaný „doma" nesníží zátěž linky v příchozím směru, odchozí záplavu e-mailů ze zavirovaného počítače samozřejmě filtr zachytit může. Ale obvykle bývá užitečný jen HW filtr. Když je totiž počítač zavirovaný, tak je často SW filtr nefunkční a viry přes něj nerušeně odcházejí ven. Ale HW filtry u nás zatím nejsou příliš obvyklé, zejména ne při domácím a kancelářském použití.

Na síti

Na síti je situace mnohem složitější. Správce sítě (nebo internet provider) je pod několika různými protichůdnými tlaky. Uživatelé na něj tlačí, aby jim spam a viry nebyly doručovány. Zároveň ale uživatelé velmi neradi vidí, když jim „omylem" nepřijde užitečný e-mail. Zatížení poštovního serveru ho může nutit k filtraci pošty. K témuž ho může nutit práce spojená s řešením opakovaně zavirovaných počítačů. A také je tu snaha nedostat se na blacklist. A když už se na blacklist dostane, tak ho stojí nemálo práce to zjistit a vyřešit. Není se tedy čemu divit, že správci pošty inklinují k použití intenzivní filtrace pošty. Mám mnohé zkušenosti z praxe, že správcové podceňují riziko spojené s tím, že filtr omylem e-mail „sežere". Vždyť pošta přece není zabezpečený protokol, e-maily se občas ztrácejí a stejně o nic moc nejde. Být zasypán spamem a viry je přece mnohem horší. Já osobně jsem ale přesvědčen, že e-maily omylem označené za spam jsou problém. Stojí to totiž čas a peníze.

Uvedu dva příklady z praxe:

1. Na blacklistech často bývají cestovní kanceláře. Z povahy jejich práce vyplývá, že si občas tak trochu zaspamují… Představte si, že si u jedné z nich objednáte levnou letenku. Cestovka pak několik dnů sleduje ceny a vybírá. Když vybere něco levného, tak vám nabídku pošle e-mailem a 24 hodin čeká na vaše potvrzení. Jenže e-mail cestou antispam spolkne (protože cestovka je na blacklistu), vy se o nabídce nedozvíte, takže ji tudíž ani nepotvrdíte. A nakonec letíte, ale o několik tisíc dráž.

2. Extrémní případ tohoto jevu je zkušenost jedné mé kamarádky. Ta se jednoho krásného letního dne posadila před počítač v internetové kavárně kdesi uprostřed Evropy. Na webu si vybrala letenku od EasyJetu a samozřejmě ji hned kreditkou zaplatila (u EasyJetu to dnes snad už ani jinak nejde). A pak čekala na e-mail. EasyJet totiž funguje tak, že po zaplacení kreditkou pošle e-mail, ten si člověk vytiskne, a to je jeho letenka. S tímto vytištěným e-mailem se jde na letiště a odletí se.
Jenže e-mail nepřišel. Tedy zavolala do EasyJetu. Neboť ale neznala číslo své objednávky (spoléhala se, že bude v tom e-mailu), tak pro ni nemohli nic moc udělat. Platby kreditkou totiž trvají několik dní než skutečně fyzicky proběhnou a letadlo mělo odlet ještě téhož dne.

Takže kamarádka zatnula zuby a zaplatila ještě jednou. Tentokrát již byla chytřejší a číslo objednávky si zapsala. Ale e-mail ji opět nepřišel. Takže se vypravila na letiště s číslem na papírku v ruce. Než se domluvila, našla příslušného člověka a vysvětlila situaci, tak letadlo opět odletělo. Následkem toho letěla až další den mnohem dražším letadlem. Čili to máme celkem dvě letenky levné, jedna drahá, noc ve drahém hotelu poblíž letiště – rovná se několik desítek tisíc korun a ztráta času. To byla cena za to, že toho dne došlo v jejich firmě k nasazení antispamového filtru… Již následující den byl filtr opět vypnut.

Z těchto příkladů je vidět, že v praxi nelze jednoduše direktivně smazat podezřelý e-mail uvnitř infrastruktury sítě (třeba na úrovni mail-serveru). Jediný, kdo se pro tento krok může rozhodnout, je uživatel. Nikoli správce sítě. Jenže správce sítě je nucen řešit výše uvedené problémy. Jinak by byl vystaven kritice uživatelů a možná by byla narušena i samotná funkčnost sítě. Pokusů o řešení tohoto problému jsem v praxi viděl mnoho. Dvě řešení tohoto problému jsou popsána v rámečku.

Další časté chyby při použití filtru

Upozorním ještě na dvě časté chyby v praxi při používání filtrace pošty.

1. Musíme si uvědomit, že denně na světě vznikne i několik stovek nových virů (rekord je tuším 300 nových virů za 24 hodin, ale jistě bude brzy překonán). Antivirový filtr má tudíž smysl jedině tehdy, pokud se jeho virová databáze aktualizuje několikrát denně. Osobně používám aktualizaci po třech hodinách. Což musíte podporovat jak vy (nastavením aktualizací), tak i váš dodavatel antivirového softwaru (rychlostí tvorby upgradu). Ale ani tak neexistuje jistota, že virus skutečně neprojde! Virů totiž vzniká mnoho a šíří se rychle, takže i nejnovější virová databáze od dobré firmy není s jistotou aktuální. To prostě není technicky možné. Je tedy nutno pravidelně skenovat disk na viry. Nehledě na to, že viry se do počítačů dostávají i jinak nežli jenom poštou. Jinak řečeno, mnoho uživatelů si myslí, že jsou v bezpečí, protože používají antivirovou filtraci pošty, ale to není pravda.

2. Antispamová filtrace používá blacklisty, které se velmi rychle mění v čase. Prakticky každou minutu a častěji. Antispam je tedy správně a plně funkční pouze pokud k má přístup k aktuálním blacklistům, platným v době doručení konkrétního e-mailu. Tedy musíte být on-line na síti a příjem pošty a její filtrace musí běžet kontinuálně v reálném čase. Při dávkovém stahování pošty například jednou týdně mnohdy antispam filtrace nadělá ještě více zmatku a chyb než normálně: skutečný spam často pustí, neboť odesilatel již na blacklistu není.

Závěrem

Doufám, že jsem čtenářům umožnil poznat aktuální žhavé téma a pomohl uživatelům a správcům pošty vzájemně se domluvit a nedopustit se v praxi často opakovaných chyb.

Vaše případné čtenářské dotazy, návrhy na další články na toto téma a připomínky můžete zasílat na mailovou adresu devic@seznam.cz. 4 0353/FEL ❑