



**Implementace antispamu v produktech
602LAN SUITE 2004 a
Mail602 MESSAGING SERVER 4.5**

Účinná ochrana před nevyžádanou poštou pro Vaši síť

Obsah

Kontakty	2
Úvod do problematiky nevyžádané pošty	3
Co je spam.....	3
Proč existuje spam.....	3
Jak vypadá spam	3
Význam ochrany proti nevyžádané poště	3
Škodlivost spamu	3
Několik statistických údajů	4
Legislativní rámec v ČR	4
Možnosti boje proti spamu	5
Prevence	5
Blokování zdrojů spamu	5
Filtrování spamu	5
Jak funguje antispam v produktech Software602	6
Schéma fungování antispamu při SMTP příjmu	6
Schéma fungování bayesovského filtru.....	6
Manuálně udržovaný seznam blokováných serverů a odesílatelů	7
Výjimky z blokováných adres	7
Ověřování SMTP serverů prostřednictvím DNSBL	7
Bayesovský filtr	8
Uživatelská bílá a černá listina	9
Třídění spamu v klientských programech.....	9
Ochrana před zneužitím vlastního SMTP serveru.....	10
Závěr	10

Kontakty

Další informace naleznete na <http://www.602.cz/>

Software602 a.s.

P.O. Box 1, 140 00 Praha 4

infolinka: 222 011 602, info@602.cz

Úvod do problematiky nevyžádané pošty

Nevyžádaná pošta neboli spam představuje jeden z neaktuálnějších problémů současné elektronické komunikace, hned vedle počítačových virů a dalších bezpečnostních rizik.

Co je spam

Termínem nevyžádaná pošta neboli spam se zpravidla označuje taková zásilka, která adresátovi cosi nabízí či sděluje, aniž by adresát v minulosti deklaroval, že o takové informace má zájem. Mezi další znaky spamu dále patří:

- Zásilka bývá rozepisována na velké množství adresátů.
- Zásilka spotřebovává adresátův čas a peníze za připojení.
- Poslání SPAM zázilky lze klasifikovat jako zneužití osobních údajů adresáta.

Proč existuje spam

Spam je v podstatě jedna z mnoha forem reklamy, která se na nás jinak řítí ze všech stran. Rozesílatelům spamu jde o finanční zisk, který se typicky odvíjí od následného zvýšení prodeje zboží. Při současném intenzivním využívání e-mailu jako prostředku komunikace neustále roste „rozšířenost“ e-mailové adresy každého z nás. Čím rozšířenější naše adresa je mezi dalšími uživateli a na čím více místech se na internetu vyskytuje, tím větší je pravděpodobnost, že se stane terčem rozesílatelů nevyžádané pošty neboli spamu.

Jak vypadá spam

Obsahem spamu bývá nejčastěji reklama na zboží, které je žádané a ideálně i problematicky dostupné pro běžného uživatele, a které je nabízeno za „výhodných“ podmínek. Může se ale také jednat o různé pokusy o podvod či vylákání citlivých osobních nebo bankovních informací.

Většina uživatelů, kteří spam dostávají, ho obvykle pozná na první pohled. Přesto by asi nešlo dát dohromady jeho vyčerpávající popis. To by pak ochrana proti spamu byla celkem jednoduchá. A právě v proměnlivosti spamu je podstata problému. Neboť jak se uživatelé spamu brání, musí spameři vymýšlet nové a nové formy a způsoby, jak přelstít systémy, jejichž úkolem je spam filtrovat.

Význam ochrany proti nevyžádané poště

Škodlivost spamu

Pokud se zeptáme, čím spam vlastně škodí, odpověď nebude jednoduchá. Spam totiž škodí ve více směrech a je dobré si uvědomit všechny škody, které může působit. Nebudeme-li se zabývat etickými hledisky a omezíme se na škody technického rázu, pak do nich patří zejména:

- Práce a čas uživatele, které vynaloží na mazání příchozího spamu a identifikaci legitimních zázilek.
- Možnost přehlédnutí anebo smazání legitimní zázilky v množství spamu.
- Zahlcování přenosových linek.
- Platby za síťový provoz spotřebovaný spamem (platby za přenesená data nebo zbytečně vysokou kapacitu linky).
- Zkolabování sítí nebo poštovních serverů zahlcených spamem.
- Škody způsobené zneužitím technických prostředků (např. serverů) třetích osob.
- Škody způsobené zneužitím jmen třetích osob při falšování adresy odesílatele.
- Celkové snižování důvěry v obchodování na internetu.

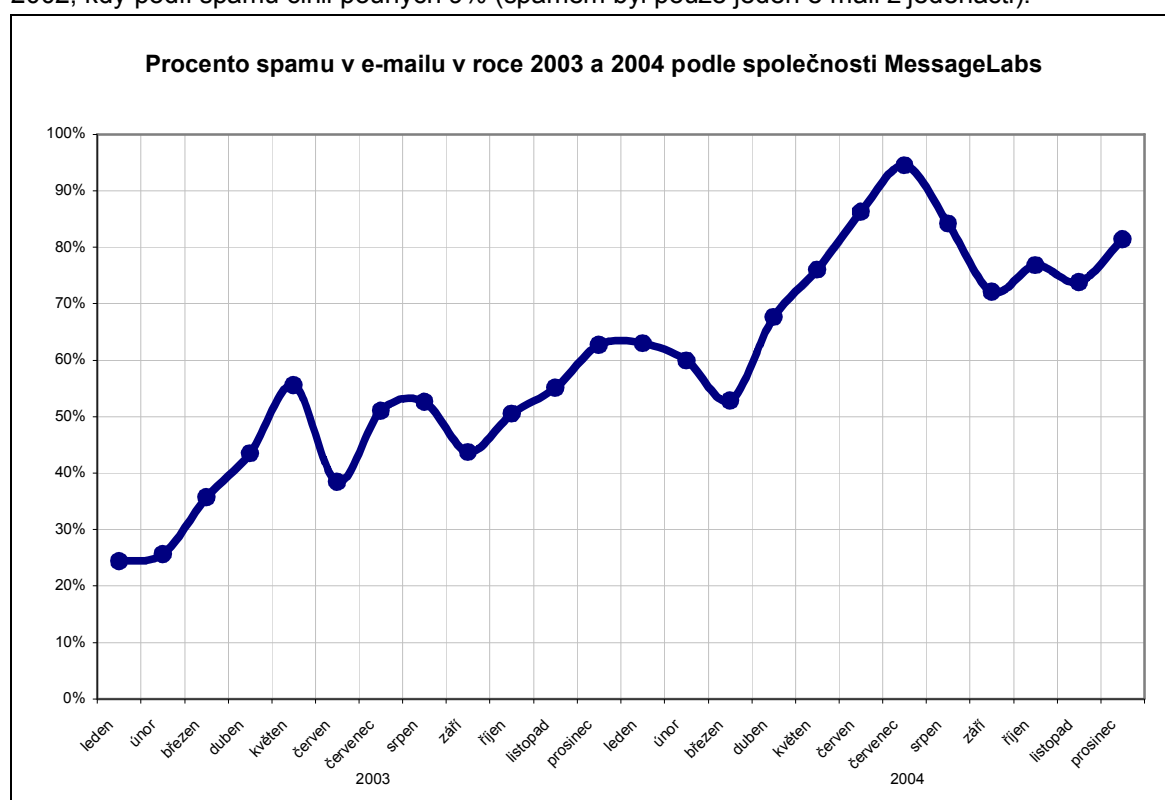
Smutným paradoxem je, že mezi škody způsobované spamem lze zařadit také různá omezení uživatelů a provozu e-mailových služeb, která jsou důsledkem „protispamových“ opatření. Může pak docházet k blokování příjmu zásilek z některých IP adres nebo k odmítnutí či chybné klasifikaci legitimních mailů antisпамovým filtrem u poskytovatele služeb nebo přímo u adresáta zásilky.

Několik statistických údajů

Podle výročních statistik společnosti [MessageLabs](#) za rok 2004 tvořil spam 73,2% všech e-mailů, neboli z každých čtyř e-mailů se ve třech případech jednalo o spam.

Objem spamu se každý měsíc mění a je ovlivňován řadou různých faktorů, jako je například zatčení některých spamérů, zpříšňování legislativy v jednotlivých státech, rostoucí znalost uživatelů i vliv nových technologií. Společnost [MessageLabs](#) očekává, že během letošního roku objem spamu zůstane na přibližně stejné úrovni tj. 60 – 90% veškeré elektronické pošty.

Pro srovnání lze ještě uvést procentuální hodnoty za rok 2003, kdy spam tvořil 40% e-mailů, a za rok 2002, kdy podíl spamu činil pouhých 9% (spamem byl pouze jeden e-mail z jedenácti).



Legislativní rámec v ČR

Dne 7. září 2004 nabyl účinnosti zákon č. 480/2004 Sb., o některých službách informační společnosti. Ten mj. reguluje nevyžádanou elektronickou inzerci, spam, a povoluje pouze obchodní sdělení podle takzvaného systému opt-in, tedy pouze s výslovným souhlasem adresáta. Rozesílání nevyžádaných sdělení tento zákon zakazuje pod hrozbou sankcí. Hlavním smyslem této úpravy bylo posílit ochranu soukromí občanů.

Další informace naleznete na stránkách [Ministerstva informatiky ČR](#).

Možnosti boje proti spamu

Prevence

Jednou ze základních ochran před nevyžádanou poštou je prevence. Ta spočívá v dodržování určitých pravidel, která se týkají zejména zveřejňování nebo používání e-mailových adres.

Obecně lze říci, že by uživatelé neměli používat svou „základní“ e-mailovou adresu pro účast v diskusních skupinách, neměli by ji zadávat do různých registračních formulářů pro zaslání informací nebo ji dokonce zveřejňovat na webových stránkách. Pro tyto účely je vhodné založit a používat „zvláštní“ adresy, které v případě potřeby může uživatel snadno zrušit nebo změnit. Rovněž není vhodné zveřejňovat na firemních webových stránkách seznam e-mailových adres jednotlivých zaměstnanců. Pokud je to nutné, lze adresy zveřejnit např. formou obrázku, aby nemohlo dojít k jejich nalezení a následnému zneužití pomocí speciálních robotů pro vyhledávání adres.

Blokování zdrojů spamu

Další z metod boje proti nevyžádané poště spočívá v jejím odmítnutí již při příjmu (zpravidla protokolem SMTP). Jinými slovy pokud se na základě adresy odesílatele nebo adresy odesílajícího serveru zjistí, že se jedná o spam, je taková zpráva ihned serverem odmítnuta a nedojde vůbec k jejímu přijetí a přenosu dat.

Server v tomto případě může odesílatele spamu poznat nějakého podle manuálně udržovaného seznamu spamérů nebo může adresy odesílajících serverů porovnávat s databázemi typu DNSBL (DNS-based spam blocking list), které obsahují IP adresy serverů, které rozesílají spam nebo mohou být k tomuto účelu zneužitelné.

Nevýhodou tohoto řešení je, že závisí na databázi, která je provozována třetí stranou a která může být dočasně nedostupná, nebo může dojít k situaci, při níž bude odmítnut zcela legitimní e-mail odeslaný přes blokováný server. Při použití manuálně udržovaného seznamu rostou nároky na údržbu. Obě tyto metody nejsou navíc aplikovatelné na zprávy stahované z POP3 schránek.

Filtrování spamu

Filtrování spamu z přijatých zpráv může probíhat jak na serveru tak přímo v klientském programu uživatele, přičemž obě metody lze kombinovat. K rozpoznání spamu se používají v zásadě dvě metody:

- **analýza integrity e-mailu** – zkoumá pomocí řady algoritmů strukturu a formát zprávy,
- **analýza obsahu e-mailu** – pomocí detekce klíčových slov nebo tzv. bayesovského filtru analyzuje vlastní obsah zprávy.

Analýza integrity e-mailu představuje poměrně exaktní metodu detekce spamu. Její asi jedinou nevýhodou je, že využívá sadu předem daných algoritmů a není schopna se pružně přizpůsobit neustále se měnícím formám rozesílání spamu.

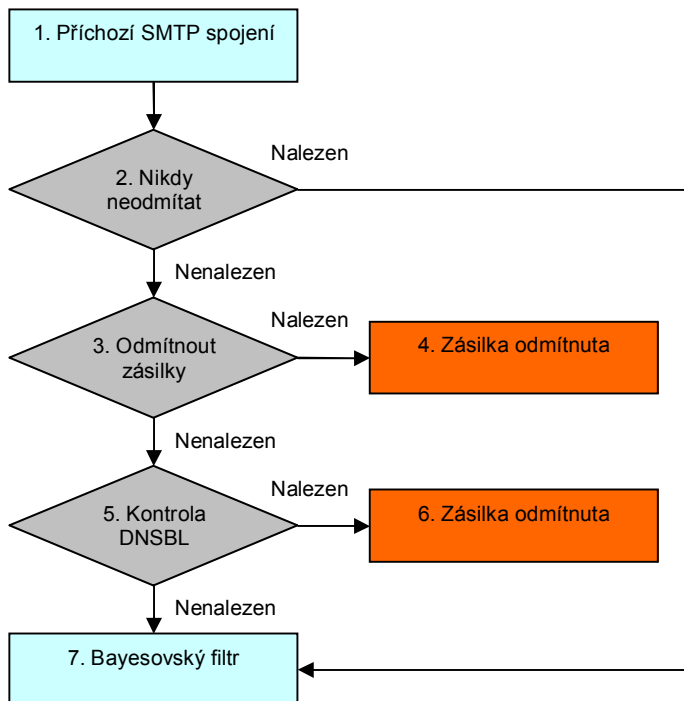
Analýza obsahu prostřednictvím detekce klíčových slov fungovala pouze z počátku a dnes je již nepoužitelná, neboť spaméři používají různé modifikace často se vyskytujících slov (například vkládají mezi jednotlivé znaky pomlčky či podtržítka).

Zajímavou možností v boji proti spamu představuje tzv. **bayesovský filtr**, který v podstatě porovnává obsah zprávy s databází e-mailů, u kterých uživatel nebo administrátor již dříve prohlásil, že se jedná o spam. Výhodou bayesovského filtru je jeho schopnost se průběžně učit, který e-mail je spam, a který naopak není. Další výhodou je fakt, že ho lze používat i u zpráv získaných výběrem POP3 schránky. Nevýhodou je naopak to, že se filtr nejprve musí naučit nejméně sto „spamových“ i „nespamových“ zpráv, aby začal správně fungovat. Uživatelé musí být navíc proškoleni, jak správně označovat nevyžádané zprávy jako spam a naopak legitimní zprávy jako „nespam“. Filtr by totiž mohl v důsledku chybného označování zpráv začít vyhodnocovat jako spam i legitimní zprávy.

Jak funguje antispam v produktech Software602

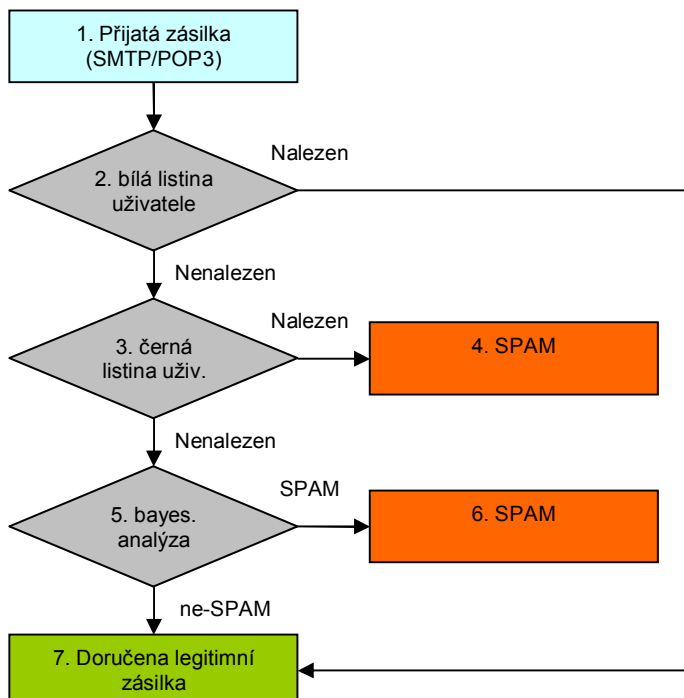
Oba komunikační servery z produkce Software602 – **602LAN SUITE 2004** a **Mai602 MESSAGING SERVER 4.5** – obsahují několikastupňovou ochranu před nevyžádanou poštou. Postup antispamového zpracování přijímaných zásilek ilustrují následující schémata.

Schéma fungování antispamu při SMTP příjmu



1. Příchozí SMTP spojení.
2. Adresy SMTP serverů nebo adresy odesílatelů mohou být zadány do seznamu „nikdy neodmítaných odesílatelů“, který naleznete v nastavení Antispamu u služby SMTP.
3. Obdobně mohou být adresy serverů či odesílatelů zadány do seznamu „vždy odmítaných odesílatelů“.
4. Pokud je odesílatel nalezen v tomto seznamu, je zásilka odmítnuta.
5. Adresa odesílajícího serveru je porovnána se zvolenými databázemi DNSBL.
6. Pokud je některou službou DNSBL odesílající server identifikován, je zásilka odmítnuta.
7. V posledním kroku je zásilka předána k analýze do bayesovského filtru.

Schéma fungování bayesovského filtru



1. Zásilka přijatá protokolem SMTP nebo vybraná z POP3 schránky.
2. Každý uživatel si může přidávat adresy odesílatelů do své Bílé listiny v klientském programu. Zásilka od odesílatele na Bílé listině je vždy legitimní.
3. Obdobně si může uživatel přidávat odesílatele na svou Černou listinu.
4. Pokud je odesílatel na Černé listině, je zásilka vždy označena jako spam.
5. Pokud není odesílatel na žádné z listin, analyzuje bayesovský filtr zásilku a označí ji pravděpodobností, že se jedná o spam.
6. Pokud je překročeno požadované procento, označí bayesovský filtr zásilku za spam.
7. Pokud není dosaženo požadované procento, je zásilka prohlášena za legitimní a je doručena uživateli.

Manuálně udržovaný seznam blokových serverů a odesílatelů

V rámci nastavení parametrů služby SMTP lze nadefinovat seznam, který může obsahovat adresy serverů a konkrétních odesílatelů, od kterých bude vždy odmítán příjem jakýchkoliv zásilek rovnou při navázání spojení SMTP protokolem. Tím pádem nedoje vůbec k přenosu zásilek jako takových. Toto nastavení má globální platnost a vztahuje se tedy na všechny uživatele bez výjimky.



Odmítnout zásilky od těchto serverů nebo odesílatelů:

- *@nabidky.com
- 123.124.125.126
- mail.spam.com
- spammer@spam.com

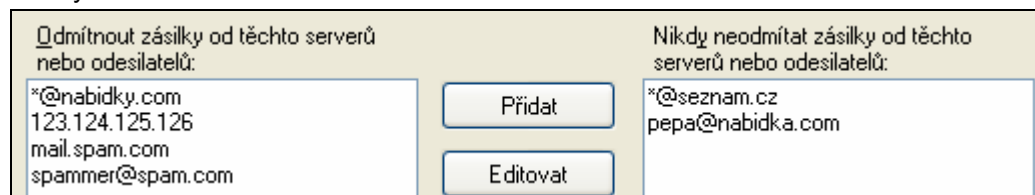
Po stisku tlačítka **Antispamové nastavení pro SMTP příjem** (nebo **Anti-Spam nastavení**) můžete zadat příslušné odesílatele do seznamu **Odmítat zásilky od těchto serverů nebo odesílatelů**.

Možnosti nastavení:

- **přidání adresy serveru** – zadejte jméno serveru, od kterého chcete všechny zásilky odmítat (např. mail.spam.com), nebo jeho IP adresu (např. 123.124.125.126)
- **přidání e-mailové adresy** – zadejte konkrétní adresu odesílatele (např. spammer@spam.com) nebo její část s využitím zástupných znaků (pro odmítání zásilek z celé domény tedy např. *@spam.com)
- **odmítání všech nepovolených adres** – zadejte znak * (hvězdička). Takto budou odmítány zásilky od všech odesílatelů s výjimkou těch, kteří budou uvedeni v seznamu výjimek ve vedlejším okně.

Výjimky z blokových adres

Pro případ, že je zapotřebí definovat výjimku ze zadaných blokových adres odesílatelů nebo serverů, lze použít seznam pojmenovaný **Nikdy neodmítat zásilky od těchto serverů nebo odesílatelů**. Do tohoto seznamu lze analogicky zadat servery či odesílatele, od nichž nechcete nikdy zásilky odmítnout. Tímto způsobem lze také zajistit, aby například nedošlo k odmítnutí zásilky od důležitého obchodního partnera, byť by se náhodou adresa jeho serveru dostala do seznamu některé služby DNSBL.



Odmítnout zásilky od těchto serverů nebo odesílatelů:

- *@nabidky.com
- 123.124.125.126
- mail.spam.com
- spammer@spam.com

Přidat

Editovat

Nikdy neodmítat zásilky od těchto serverů nebo odesílatelů:

- *@seznam.cz
- pepa@nabidka.com

Na obrázku je vidět příklad nastavení, při kterém budou odmítány e-maily z celé domény nabidka.com kromě adresy pepa@nabidka.com. Dále nebudou nikdy odmítány e-maily z domény seznam.cz.

Ověřování SMTP serverů prostřednictvím DNSBL

Při příjmu zásilek protokolem SMTP lze kromě manuálně definovaného seznamu serverů a adres, od kterých jsou zásilky odmítány, použít ke kontrole odesílajícího serveru také vyhledávací služby DNSBL. Po navázání komunikace je IP adresa odesílajícího serveru posouzena zvolenými službami a v případě pozitivního nálezu je příjem zásilky odmítnut –nedoje vůbec k přenosu zásilky. Toto nastavení má globální platnost a vztahuje se tedy na všechny uživatele bez výjimky.

Použit zvolené vyhledávací DNSBL služby k odmítnutí zásilek od spamovacích serverů:

- Blackholes at five-ten-sg.com (Spam) [ZDARMA] - http://www.five-ten-sg.com/blackhole.php
- Blackholes at five-ten-sg.com (Dial-up) [ZDARMA] - http://www.five-ten-sg.com/blackhole.php
- Blackholes at five-ten-sg.com (Unconfirmed opt-in) [ZDARMA] - http://www.five-ten-sg.com/blackl
- Open Relay Database (Open Relays) [ZDARMA] - http://www.ordb.org/
- NJABL.ORG (Open Relays) [ZDARMA] - http://njabl.org/
- NJABL.ORG (Dial-up) [ZDARMA] - http://njabl.org/
- NJABL.ORG (Spam) [ZDARMA] - http://njabl.org/
- Spamhaus SBL (Spam) [ZDARMA] - http://www.spamhaus.org/sbl/index.lasso

Které DNSBL služby se budou pro kontrolu používat lze zvolit po stisku tlačítka **Antispamové nastavení pro SMTP příjem** (nebo **Anti-Spam nastavení**) jejich zaškrtnutím v nabízeném seznamu. Pokud není Vámi používaná služba uvedena, můžete ji do seznamu přidat spolu s potřebnými parametry. Je ale třeba mít na paměti, že používání velkého množství DNSBL služeb může výrazně zpomalit proces doručování zásilek.

Bayesovský filtr

Jednou z hlavních výhod bayesovského filtru je, že na rozdíl od výše uvedených metod je použitelný jak pro filtrování zásilek přijatých protokolem SMTP, tak stažených z POP3 schránky. Bayesovský filtr analyzuje obsah přijímané zprávy a klasifikuje ho mírou pravděpodobnosti, že daná zpráva je nevyžádaná zpráva (spam). Tuto činnost provádí na základě porovnání slov v obsahu zprávy s obsahem své databáze, kam zařazuje slova ze zásilek, které uživatel již dříve označil za spam nebo naopak za legitimní zprávy.

Z toho plyne, že **filtr je třeba nejdříve „naučit“**, tedy naplnit jeho databázi zprávami, o nichž sám uživatel rozhodne zda jsou či nejsou spamerem. Na první pohled se to možná nezdá, ale legitimní zprávy jsou pro učení stejně důležité jako spam, ne-li důležitější. Kdyby se totiž k učení používal jenom spam, po nějaké době by všechno bylo pokládáno za spam. Doporučuje se dokonce, aby pro učení bylo použito více legitimních zpráv než spamu.

Administrátor může globálně **Povolit používání bayesovského filtru pro kontrolu došlých zpráv** zaškrtnutím stejnojmenné volby na záložce Antispam v konfiguraci. Dále může nastavit, jaké míry pravděpodobnosti, že se jedná o nevyžádanou zprávu (spam), musí zpráva dosáhnout, aby byla bayesovským filtrem označena za spam.

Povolit používání bayesovského filtru pro kontrolu došlých zpráv

Klasifikovat zprávu jako SPAM, pokud přesáhne skóre %

Antispamová schránka:

Akce

Pokud je zpráva klasifikována bayesovským filtrem jako SPAM

- Smazat
- Zaslát adresátovi
- Zaslát do Antispamové schránky
- Vkládat do hlavičky kontrolovaných zpráv pole X-LNS-Spam-Check s informací o výsledku kontroly
- Označovat spamy vložím tohoto řetězce do předmětu zprávy:
- na začátek předmětu na konec předmětu

Zprávy, které jsou bayesovským filtrem klasifikovány jako spam, mohou být doručeny původnímu adresátovi s tím, že je do předmětu zprávy přidán speciální řetězec, který umožňuje tyto zprávy automaticky zatřídit v klientských programech. Další možností je nechat spamy doručovat do speciální schránky, o kterou se stará pověřený uživatel.

Učení bayesovského filtru probíhá na základě zpráv, které uživatelé označují za spamy nebo naopak za legitimní zprávy. Toto označování zpráv se provádí přímo v klientských programech (ve

webovém rozhraní nebo v aplikaci Mail602 Klient¹⁾ pomocí tlačítek **Spam** a **Nesbam**. Uživatelé používající pro přístup k poště klientské programy na bázi SMTP/POP3 (např. Outlook Express, Mozilla Mail apod.) mohou zásilkou označovat jejich přeposláním (funkcemi Předat dál, Forward) na adresy spam@spam.spam pro nevyžádanou poštu resp. notspam@spam.spam pro legitimní zásilkou.

Server takto označenou zásilkou zpracuje podle nastavení na záložce **Učení bayesovského filtru**, který se zásilkou buď automaticky naučí nebo po naučení vloží do antispamové schránky zprávu, podle které může administrátor naučení dané zásilkou dodatečně odvolat. Existuje i nastavení, při kterém se filtr označené zásilkou učí až po schválení administrátorem.

Filtr se také může **učit automaticky** zcela bez zásahu uživatelů z obsahu zásilek, jejichž odesílatel je uveden na uživatelské bílé listině, a které tedy nejsou spamem.

Uživatelská bílá a černá listina

Každý uživatel může kromě centrálního nastavení antispamové kontroly používat ještě tzv. uživatelskou bílou a černou listinu, která odráží jeho preference. Tyto listiny jsou individuální pro každého uživatele, který je může spravovat v prostředí klientských programů v **Nastavení antispam** ve webovém rozhraní nebo v **Nastavení prostředí Mail602 Klienta**.

Na bílou listinu si uživatel přidává ty adresy, o kterých je přesvědčen, že zásilkou z nich přicházející není spam. Uživatel přitom nemusí plnit bílou listinu manuálně, neboť do ní mohou být automaticky ukládány ty adresy, na které uživatel sám e-mailou odesílá. Vložením adresy na bílou listinu lze také zabránit budoucí chybné klasifikaci zásilkou od daného odesílatele bayesovským filtrem. Bílé listiny využívá i bayesovský filtr, který se může automaticky učit z obsahu zásilek od odesílatelů uvedených na bílé listině.

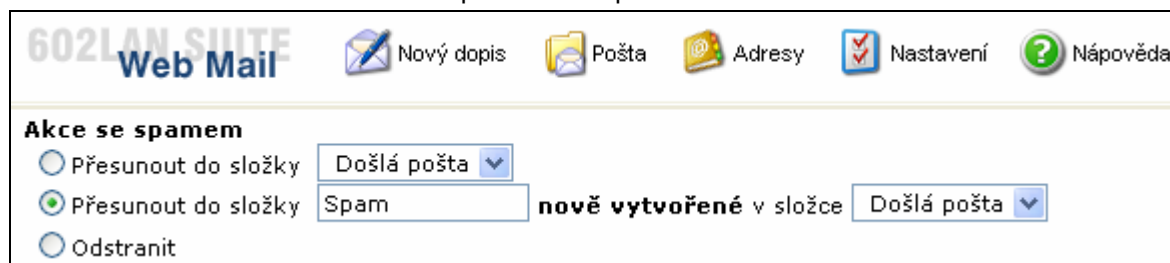
Černá listina je pravým opakem bílé. Všechny zásilkou od odesílatelů, kteří jsou uvedeni na černé listině, jsou automaticky považovány za spam. Uživatel se tak může sám bránit obtěžování zásilkami z nežádoucích adres.

Třídění spamu v klientských programech

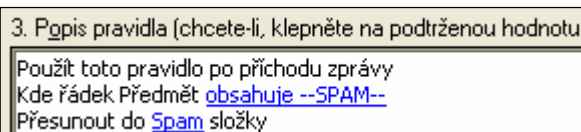
V případě, že jsou rozpoznané spamy doručovány do schránek uživatelů, mohou být dále zpracovávány jejich klientskými programy.

¹ Aplikace Mail602 Klient je součástí komunikačního řešení Mail602 MESSAGING SERVER.

Webové rozhraní a aplikace Mail602 Klient podporují v zásadě dvě možnosti zpracování spamu – zatřídění do určené přihrádky nebo vymazání. V případě třídění do přihrádky lze s výhodou využít funkce automatického mazání zásilek po zadaném počtu dnů.



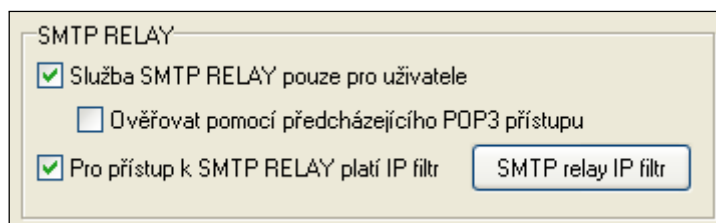
V ostatních klientských programech na bázi SMTP/POP3 (např. Outlook Express, Mozilla Mail apod.) lze většinou nadefinovat pravidla nebo filtry pro třídění zásilek splňujících určitá kritéria. Stačí tedy nadefinovat pravidlo pro zásilky, které obsahují v předmětu řetězec --SPAM--.



Ochrana před zneužitím vlastního SMTP serveru

V předchozím textu jste se seznámili s možnostmi ochrany před příjmem nevyžádané pošty, která spočívala v odmítání příjmu zásilek resp. filtraci již přijatého spamu. Ochrana proti spamu má ale i druhou rovinu, a tou je ochrana vlastního SMTP serveru proti zneužití k rozesílání spamu. Princip ochrany spočívá v omezení přístupu k tzv. funkci SMTP RELAY, která umožňuje SMTP serveru přijímat a odesílat zásilky určené adresátům s e-mailovými adresami nacházejícími se mimo tento server.

Ve standardním nastavení se při přístupu k této funkci kontroluje pouze platnost e-mailové adresy odesílatele, kterou bohužel není pro případného útočníka problém podvrhnout. Proto je jednou z metod jak zvýšit zabezpečení SMTP serveru proti zneužití zavedení kontroly IP adresy počítače, ze kterého se odesílatel pokouší zásilky odesílat, neboť IP adresu prakticky nelze fingovat. V rámci nastavení parametrů služby SMTP lze specifikovat **používání speciálního IP filtru**, kterým je možno omezit používání SMTP serveru například jen na počítače resp. IP adresy vnitřní sítě.



Další možností ověření oprávněnosti uživatele/počítače k použití funkce SMTP RELAY (tedy odesílání zásilek mimo server) je jeho ověření pomocí předcházejícího POP3 přístupu, které se zapíná prostřednictvím

stejnomené volby. Při takovém nastavení se musí uživatel nejdříve úspěšně přihlásit do své schránky (většina programů se o to pokouší ihned po svém spuštění), a až potom může po dobu 120 minut odesílat zásilky ze svého počítače.

Závěr

Boj s nevyžádanou poštou (spamem) patrně nikdy úplně neskončí. Uvedené nástroje pro redukci spamu představují dostupné řešení, jehož nasazením lze významně snížit zahlcování e-mailových schránek uživatelů, a tak přispět ke zvýšení produktivity jejich práce. Rovněž nelze opomenout ani pozitivní vliv filtrování spamu na bezpečnost uživatelů. Zároveň tyto nástroje snižují zátěž poštovních serverů a síťového provozu jako takového.