SPAM – problematika nevyžádané pošty

SPAM – problem of spam

Bc. Jan Marek

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan MAREK**
Osobní číslo:	**A09516**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**SPAM – problematika nevyžádané pošty**

Zásady pro vypracování:

1. **Identifikujte a uveďte důvody pro tvorbu a šíření nevyžádané pošty.**
2. **Rozdělte a obecně popište postupy obrany proti příjmu nevyžádané pošty.**
3. **Uveďte zákony zabývající se problematikou nevyžádané pošty v ČR a EU.**
4. **Proveďte jednoduchý průzkum povědomí široké veřejnosti o problematice nevyžádané pošty.**
5. **Zhodnoťte a doporučte nejvhodnější technologii pro eliminaci nevyžádané pošty podle testů provedených na testovací množině.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **ADÁMEK, Martin. Spam : jak nepřivolávat, nepřijímat a nerozesílat nevyžádanou poštu. 1. vyd. Praha : Vydala Grada Publishing, 2009. 168 s. ISBN 978-80-247-2638-0.**
2. **POLČÁK, Radim. Právo na internetu : spam a odpovědnost ISP. 1. vyd. Brno : Vydal Computer Press, 2007. 160 s. ISBN 978-80-251-1777-4.**
3. **KOCMAN, Rostislav, LOHNISKÝ, Jakub. Jak se bránit virům, spamu a spyware. 1. vyd. Brno : Vydal Computer Press, 2005. 148 s. ISBN 80-251-0793-0.**
4. **WALTHER, Henrik, SANTRY, Patrick. Jak zabezpečit Exchange Server 2003 a Outlook Web Access. Brno : Vydal Computer Press, 2006. 248 s. ISBN 80-251-0910-0.**
5. **WOLFE, Paul, SCOTT, Charlie, ERWIN, Mike W. Antispam : Metody, nástroje a utility pro ochranu před spamem. Brno : Vydal Computer Press, 2005. 376 s., 1 CD, ISBN 80-251-0479-6.**

Vedoucí diplomové práce: **RNDr. Ing. Miloš Krčmář**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **24. února 2011**

Termín odevzdání diplomové práce: **18. května 2011**

Ve Zlíně dne 24. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Spamová problematika je v práci rozebírána na více úrovních. Je zde probírána stránka vzniku (historie) spamu, dále důvody pro tvorbu a šíření spamu. Aktuální spamová scéna, statistické informace o šíření spamu v Internetu. Čtenář je obeznámen se základními technickými termíny. Je seznámen s technikami obrany ať už preventivního, pasivního či aktivního charakteru. Vybrané techniky obrany jsou podrobeny praktické zkoušce. Jsou představeny klady a zápory jednotlivých technik. Část práce je zaměřena na zákony dotýkající se této problematiky jak v České republice, tak v rámci Evropské Unie. Závěrem práce je jednoduchá statistika o informovanosti široké veřejnosti o této problematice.

Klíčová slova: spam, nevyžádaná pošta, email, smtp, blacklist, whitelist, greylist, bayes

ABSTRACT

Spam issue is discussed on multiple levels in this work. It describes the history of spamming as well as the reasons for creating and distributing spam. Current Spam scene, statistical information about spreading spam on the Internet. The reader is familiarized with basic technical terms and also with the defense techniques, whether preventive, passive or active nature. Selected defense techniques are subjected to practical testing and the pros and cons of each technique are presented. Part of this work is focused on the laws regarding this issue, both in the Czech Republic and the European Union. In conclusion there are simple statistics on awareness of this issue among the general public.

Keywords: spam, spam messages, email, smtp, blacklist, whitelist, greylist, bayes

Chtěl bych poděkovat hlavně své ženě Veronice, za podporu po celou délku mého studia. Svým dětem za to, že v době tvorby této práce nezlobily tak moc jako vždy ☺.

Velký dík patří RNDr. Miloši Krčmářovi, pod jehož vedením tato práce vznikla. Jeho odborné rady a náměty mě vedly po celou dobu tvorby a úpravy této práce.

A konečný dík patří Univerzitě Tomáše Bati ve Zlíně, že mi poskytla možnost vysokoškolského studia.

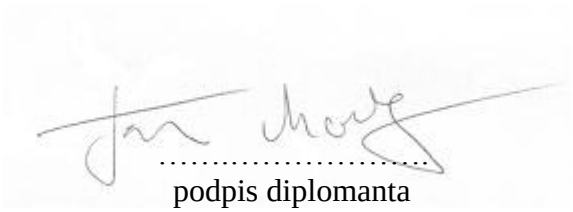
Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně 14.3.2012



……
podpis diplomanta

OBSAH

ÚVOD

Nejčastějším druhem neverbální komunikace je dnes elektronická pošta. Přináší mnoho výhod, mezi které bezesporu patří rychlost doručení zprávy, ověření odesílatele (elektronický podpis), jednoduchá archivace apod… Tak jako každá služby i elektronická pošta má své výhody a nevýhody. Velkou nevýhodou je jednoduché zneužití, ať už v podobě rozesílání obtěžujících mailů, rozesílání zavirovaných mailů, zatěžování poštovních serverů, nebo jen zbytečné vytěžování internetových tras.

Zabránit úplně této aktivitě se zdá skoro nemožné. Nicméně kdo nebojuje, nemůže vyhrát.

Cílem této práce je obeznámit čtenáře s historií nevyžádané pošty, dále s technickými termíny, se kterými se v této problematice setkáváme. V práci jsou popsány technologie, které mohou napomoci při obtížném úkolu eliminace nevyžádané pošty. Vybrané technologie jsou podrobeny praktické zkoušce a čtenář je obeznámen s jejich úspěšností, klady a zápory v reálném světě. Důležité je seznámit čtenáře s podporou zákonů v ČR a EU, které uživatele chrání v případě zneužívání osobních informací a šíření nevyžádané pošty v Internetu.

Po prostudování publikace by měl čtenář lépe pochopit, jak fungují obranné technologie a být schopen plně tak využít jejich potenciál.

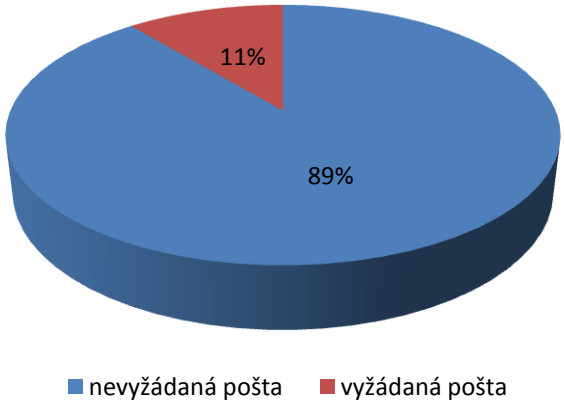
1 ÚVOD DO PROBLEMATIKY, POUŽÍVANÉ POJMY A JEJICH VZNIK

Pokud se chceme orientovat v problematice nevyžádané pošty, zasílání elektronických zpráv internetem a podobně, měli bychom si objasnit používané tvary slov, které tuto problematiku popisují.

1.1 Mail

Slovem MAIL (mail, email, e-mail) se dnes běžně označuje elektronická zpráva, přesněji zpráva zaslaná sítí Internet popř. Intranetem (vnitřní podniková síť).

Email je dnes nejpoužívanější neverbální komunikační kanál. Denně se celosvětově přenese přes 294 bilionů emailů, z čehož nevyžádaná elektronická pošta (spam) je okolo 89%.[1] V hrubém přepočtu to tedy znamená, že na 10 zaslaných mailů je jen 1 mail vyžádaný (obsahově užitný).



Graf 1. Poměr mezi vyžádanou a nevyžádanou poštou

Kořeny této služby sahají před zrod sítě Internet, do doby sálových počítačů (mainframů). Udává se, že služba jako taková vznikla v roce 1965 jako způsob komunikace více uživatelů sdílejících čas mainfraimových počítačů, mezi první systémy se službou zasílání zpráv patřily Q32 od SCD nebo CTSS z MIT.

Udává se, že v roce 1966 bylo poprvé odzkoušeno na systému AUTODIN zaslání síťového emailu.

První užívání znaku @ je připisováno Ray Tomlinsonovi, který začal v roce 1972 tímto znakem oddělovat jména uživatelů od názvů stroje, čímž se měla zlepšit orientace v zasílaných zprávách. Tato komunikace už probíhala na síti ARPANET. [2]

1.2 SPAM a HAM

6. května 2003 se ve Sněmovně lordů konala debata k problematice legislativních opatření k potírání spamu. Hned několik lordů bylo od počátku natolik zmateno použitým výrazem spam', že diskuze nabírala místy velmi podivný kurz. Za vše hovoří promluva Lorda Rentona, který se nechápavě obrátil na přítomného člena kabinetu se slovy: „Mohl by pan ministr laskavě vysvětlit, jak se to přihodí, že se nepoživatelná konzervovaná strava stane nevyžádanou elektronickou poštou, a vzít přitom v potaz, že někteří z nás chtějí být ušetřeni toho mít email?" [3]

Jak tedy vznikla slova SPAM a HAM, a co tedy znamenají?

Slovo ham je anglickým překladem slova šunka. Někdejší americký potravinářský podnik Hormel vyvíjel v době mezi válkami šunkovou konzervu Hormel Flavor-Sealed Ham. Této konzervě chyběla jedna důležitá vlastnost a to, že pro dlouhodobé uchování musela být v chladu. Proto se z této Ham konzervy o jedenáct let později vyvinula odolnější konzerva s novým marketingovým názvem SPAM. [3]

Díky tomu, že nemusela být skladována v chladnu a vydržela i hrubé zacházení stal se SPAM jednou z klíčových potravin v době druhé světové války. Rozšířil se tak prakticky po celém světě a vedle vojáků se jím hojně živilo i civilní obyvatelstvo. [3]

To, jak byl svět zasypán v období druhé světové války zasypán konzervami Spam má určitou analogii s dnešním stavem rozesílání nevyžádaných mailů. Taky se jedná o celosvětový problém (fenomén).

Co přesně zkratka SPAM znamená, se neví, uvádí se několik úsměvných vysvětlení:

- *Specially Processed Armadillo Meat (speciálně upravené maso z pásovce),*
- *Super Pink Artificial Meat (super růžové umělé maso),*
- *Squirrel, Possum And Mouse (veverka, vačice a myš)* [3]

[4]

Obr. 1. Konzerva SPAM

V některých publikacích (i v této) se může tedy čtenář setkat s užitím názvů spam a ham. Slovem spam je obecně označována nevyžádaná zpráva, slovem ham zase naopak zpráva vyžádaná (očekávaná). Zasílání spamu se říká spamování (provádění činnosti).

Z pohledu práva není výraz spam nijak definován a neexistuje ani nějaká obecná právní regulace. *Co se týče jeho významu, můžeme jej definovat buďto s přihlédnutím ke kvalitativním, nebo kvantitativním kritériím. Z hlediska kvantity si všímáme spíše hromadnosti šíření příslušných zpráv a jejího negativního dopadu na komunikační infrastrukturu, zatímco kvantitativní hledisko se zaměřuje spíše na obsah zpráv a jejich nulovou nebo naopak zápornou informační hodnotu. Bez ohledu na specifikaci jednotlivých přístupů však můžeme konstatovat, že ke klasifikaci určitého jednání jako sparingu bude nutné, aby příslušné sdělení bylo minimálně:*

- *elektronické,*
- *zasílané hromadně a*
- *zasílané bez vyžádání.* [3]

1.3 První mail považovaný za spam

Za asi první nevyžádaný mail je považována zpráva od Garyho Thuerka ze dne 3.5.1978 a proběhla na síti ARPANET. Gary Thuerk byl zaměstnanec firmy Digital Equipment Corporation (DEC – největší výrobce počítačů v té době) a pracoval u ní v oddělení marketingu. Seznam uživatelů ARPANETu byl v té době veřejný a vypadal jako dnešní telefonní seznam. Gary Thuerk všechny adresy uživatelů opsal ručně a rozeslal je všem uživatelům ze západního pobřeží Spojených států. Reklama tedy byla cílená na určitou

skupinu lidí v ARPANETu (geograficky). Obsahem zprávy byla pozvánka na prohlídku nového počítače DECSYSTEM-20, která měla proběhnout za pár dní v Californii.

Úryvek z prvního spamu:

SPOLEČNOST DIGITAL BUDE VEŘEJNĚ PREZENTOVAT PRODUKT Z NEJNOVĚJŠÍ ŘADY DECSYSTEM-20: DECSYSTEM-2020, 2020T, 2060 A 2060T. POČÍTAČOVÁ ŘADA DECSYSTEM-20 SE VYVINULA Z OPERAČNÍHO SYSTÉMU TENEX…

ZVEME VÁS K PROHLÍDCE SYSTÉMU 2020 A K PŘEDNÁŠCE O ŘADĚ DECSYSTEM-20 V RÁMCI PREZENTACE OBOU PRODUKTŮ, KTEROU BUDEME POŘÁDAT TENTO MĚSÍC V KALIFORNII NA NÁSLEDUJÍCÍH MÍSTECH…

POČÍTAČ 2020 TU BUDE K DISPOZICI. BUDOU TU I TERMINÁLY ON-LINE K DALŠÍM SYSTÉMŮM DECSYSTEM-20 PŘIPOJENÉ PŘES ARPANET. POKUD SE NEMŮŽETE ZÚČASTNIT, KONTAKTUJTE PROSÍM NEJBLIŽŠÍ KANCELÁŘ DEC, KDE ZÍSKÁTE VÍCE INFORMACÍ O SKVĚLÉ ŘADĚ POČÍTAČŮ DECSYSTEM-20. [5]

Na arpanetu se zvedla velká vlna nevole, firma DEC dostala napomenutí od administrátorů ARPANETU.

Humorná na tom všem je i skutečnost, že Gary Thuerk nebyl žádný počítačový talent a tak se mu nedopatřením povedlo vepsat do pole pro adresy příliš mnoho adres (pole bylo omezeno počtem znaků) a část adres se vypsala do těla zprávy. Gary tak na radu svého kamaráda mail poslal ještě jednou, aby došel všem zamýšleným příjemcům.

1.4 Atraktivita spamování

Většina příjemců spamu si klade otázku, proč spam rozesílat a zda se distribuce spamu vůbec vyplatí.

No rozložme si otázku na části a odpovězme si na každou část zvlášť. Jak uvádí předchozí odstavec původní a první spam byl mířenou reklamou na cílenou skupinu potencionálních zákazníků. Dnes je spamem šířena změť informací, které mají nulovou, nebo většinou spíš zápornou informační hodnotu. I tak je šíření nabídek formou spamu nejlevnějším způsobem reklamy.

Komunikační kanál	Celkové náklady na použití	Počet oslovených	Náklady na osloveného
Directmail	9 700	7 000	1,39
Telemarketing	160	240	0,66
Tištěný inzerát – specializovaný zdroj	7 500	100 000	0,075
Tištěný inzerát – obecný zdroj	30 000	442 000	0,067
Faxový spam	30	600	0,05
On-line inzerce (bannery)	35	1 000	0,035
Emailový spam	250	500 000	0,0005

Tab. 1. Ukázka cen oslovení jedince přes různé komunikační kanály (částky v USD) [3]

Odpovědí na naši předchozí otázku, tedy musí být, z důvodu vydělání co nejvíce peněz. Čím větší skupinu oslovíme s co nejmenšími náklady, tím více vyděláme. Ve spamu je to bohužel pravda.

Druhou částí otázky bylo, zda se distribuce spamu vyplatí? No pravdou je, že vyplatí. Spammer (člověk šířící spam) si může ročně vydělat opravdu hodně. Udává se, že největší spammeři si ročně vydělají něco kolem 9 milionů USD. Za poskytování seznamů adres se dá ročně vydělat kolem 5 milionů USD.

Dále má spam mnohdy charakter škodlivý. Užívá se pro útoky, kdy se hacker snaží zpomalit poštovní server natolik, až systém nekontrolovaně zhroutí a mnohdy odkryje citlivá místa, na která může hacker dále útočit.

1.5 Získání emailových adres

Popsali jsme si, na kolik si může spammer šířením spamu přijít. Popř. kolik vydělá za prodej seznamů s emailovými adresami. Nyní si zodpovíme otázku, kde berou spammeři seznamy emailových adres.

Spammeři je nejčastěji sbírají přímo z webových stránek. Využívají k tomu speciálně napsané programy harvestery (sběrači), spamboty (roboti), kteří prochází webové stránky a přímo v kódu HTML stránky hledají znak @ a podle něj identifikují a ukládají nalezené emailové adresy. Před touto metodou je lehká obrana, stačí nahradit znak zavináč třeba obrázkem. Problém je však, že jak se vyvíjí ochrana, tak se o krok napřed vyvíjí i útok. Dnešní spamboti už umí prohledávat v různých konstrukcích kódů HTML v obrázcích, JavaScriptech a podobně.

```
<tr>
  <td width="144">
    <a href="mailto:[redacted]">[redacted] </a>
  </td>
  <td>
    ředitel divize sport
  </td>
</tr>
<tr>
  <td width="144">
    <a href="mailto:[redacted]">[redacted]</a>
  </td>
  <td>
    hlavní účetní
  </td>
</tr>
<tr>
  <td width="144">
    <a href="mailto:[redacted]">[redacted]</a>
```

Obr. 2. Ukázka HTML kódu webové stránky s emailovými záznamy

Titul, jméno, příjmení	e-mailová adresa
[redacted]. - **starosta**	[redacted](zavináč)[redacted](pomlčka)[redacted](tečka)**cz**
Interní audit [redacted]	[redacted](zavináč)[redacted](pomlčka)[redacted](tečka)**cz**
[redacted]. - **I. místostarosta**	[redacted](zavináč)[redacted](pomlčka)[redacted](tečka)**cz**
[redacted]- **II. místostarosta**	[redacted](zavináč)[redacted](pomlčka)[redacted](tečka)**cz**
[redacted]**Ing. - tajemnice**	[redacted](zavináč)[redacted](pomlčka)[redacted](tečka)**cz**
Útvar tajemníka :	
[redacted]	[redacted](zavináč)[redacted](pomlčka)[redacted](tečka)**cz**

Obr. 3. Ukázka použité ochrany v emailovém seznamu; znaky @, - a . jsou nahrazeny psanými slovy v závorkách, pro spammera je tento způsob ochrany lehce překonatelný

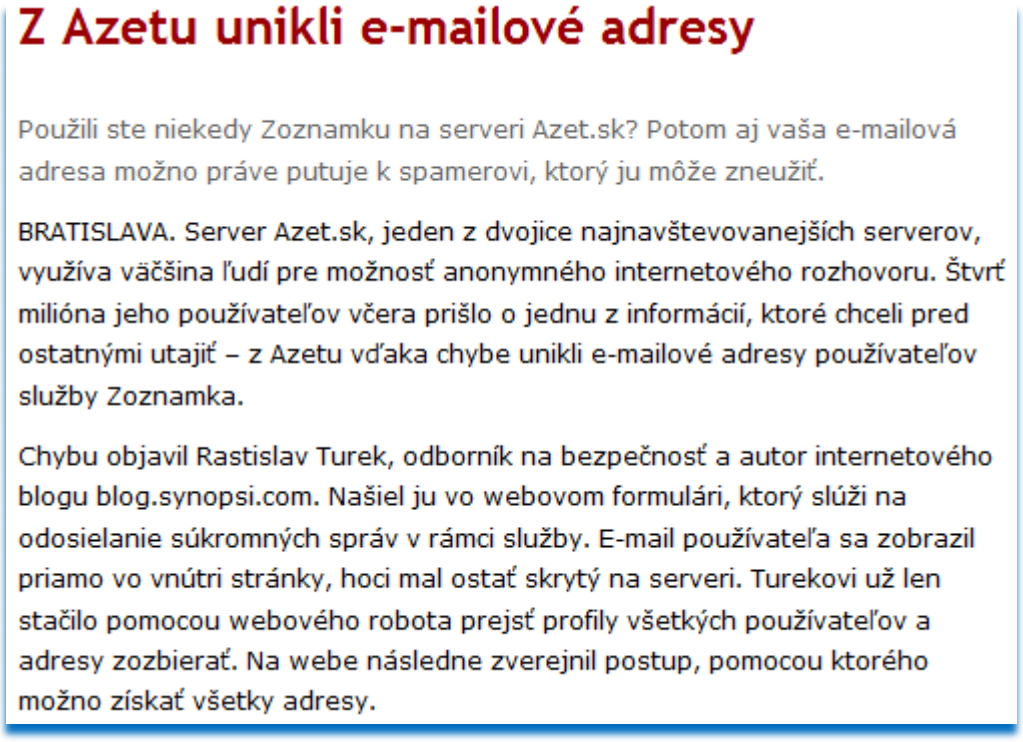
Dalším způsobem získání emailových adres je jejich nákup. Nakoupit se dají různě od poskytovatelů freemailů, warezových (stránky s nelegálním obsahem) nebo porno stránek. Mnoho uživatelů zde své emailové adresy dobrovolně uvede, aby získali přístup k požadovaným datům a informacím. Jak je dále nakládáno s jejich údaji mnohdy neřeší.

Obr. 4 Ukázka inzerátu z Google cache nabízející seznam emailových adres [6]

Časté je tipování, přes DNS dotaz si spammer ověří, že doména existuje a pokud existuje doména, předpokládá se existence emailových účtů. Ať už obecných nebo jiných. Tím může spammer tipovat emailové adres. Př. teoretická doména www.domena.cz bude mít zřejmě emailové adresy administrator@domena.cz nebo admin@domena.cz apod…

Mezi další a dnes hojně užívanou taktiku patří email generátor, jedná se o jednoduché aplikace, do kterých vepíšeme doménovou adresu př. www.domena.cz a zadáme buď náhodné generování adres, nebo tvorbu podle seznamového listu. Je nutné zvolit i formát. Máme-li seznam list naplněný jmény a příjmeními vhodnými pro dané lokality nic nebání tvorbě adres. Z programu pak padají výsledky typu petr.korenek@domena.cz, nebo v případě změny nastavení třeba jen korenek@domena.cz apod...

Jedním z posledních způsobů získání seznamu emailových adres může být jejich krádež. Příkladem může být únik 160 000 emailových adres ze serveru www.azet.sk.



Z Azetu unikli e-mailové adresy

Použili ste niekedy Zoznamku na serveri Azet.sk? Potom aj vaša e-mailová adresa možno práve putuje k spamerovi, ktorý ju môže zneužiť.

BRATISLAVA. Server Azet.sk, jeden z dvojice najnavštevovanejších serverov, využíva väčšina ľudí pre možnosť anonymného internetového rozhovoru. Štvrť milióna jeho používateľov včera prišlo o jednu z informácií, ktoré chceli pred ostatnými utajiť – z Azetu vďaka chybe unikli e-mailové adresy používateľov služby Zoznamka.

Chybu objavil Rastislav Turek, odborník na bezpečnosť a autor internetového blogu blog.synopsi.com. Našiel ju vo webovom formulári, ktorý slúži na odosielanie súkromných správ v rámci služby. E-mail používateľa sa zobrazil priamo vo vnútri stránky, hoci mal ostať skrytý na serveri. Turekovi už len stačilo pomocou webového robota prejsť profily všetkých používateľov a adresy zozbierať. Na webe následne zverejnil postup, pomocou ktorého možno získať všetky adresy.

[7]

Obr. 5. Novinový výstřižek o úniku emailových adres (krádež)

Seznam emailových adres se stále pohybuje na internetu a lze jej najít do pěti minut. Jako nový zdroj emailových adres byl dva dny po odcizení prodán za 20 000 SKK.

2 ZBROJÍME PROTI SPAMU

Obrana proti spamu není jen pusté filtrování mailů podle nastavených pravidel, je to práce kdy se snažíme pochopit patologii spammera. Snažíme se mu jeho práci co nejvíce znesnadnit. Je to taková hra kdo z koho.

Obranné technologie antispamu můžeme rozdělit do několika úrovní:

- **Preventivní** – zde se snažíme o strategické vytvoření emailových adres, tak aby nebyly lehce odhadnutelné a popř. jejich utajení.
- **Pasivní** – postupy, které mají spammerovi zabránit před sběrem a použitím emailových adres.
- **Aktivní** – postupy, které mají za úkol eliminovat přijímaný objem spamu, resp. dále spam nezasílat příjemcům.

2.1 Preventivní postupy

Preventivní postupy jsou doporučením jak chránit emailové adresy před únikem ke spammerům, resp. jak zabránit jejich odcizením. Patří do skupiny pasivní ochrany, ale osobně je řadím jako vlastní skupinu.

Ze způsobů jak spammer získává emailové adresy, víme, že se tak děje nejčastěji sběrem z webových stránek, z mailů (rozesílání na mnoho adres, popř. forwardování mailů), kde v těle emailu zůstává mnoho zobrazených emailových příjemců nebo tipováním.

Emailové adresy si proto rozdělíme do několika úrovní (skupin):

- **Vnitřní adresy** – slouží pro komunikaci v rámci organizace; většinou se jedná o vnitřní názvy (podle procesů, členění organizace apod…) př. uctarna@domena.cz, udrzba@domena.cz, …
- **Vnější adresy** – slouží pro komunikaci mezi pracovníky firmy a vnějším světem, většinou v sobě nesou jméno pracovníka dané firmy, nebo obecný název části organizace př. korenek@domena.cz, obchodni.oddeleni@domena.cz, …
- **Veřejné adresy** – slouží jako obecné adresy pro komunikaci zákazníků, dodavatelů, žadatelů o práci atd… př. adresa info@domena.cz.

Vnitřní směrnice organizace by měla vhodně rozdělit tyto adresy do úrovní a seznámit jejich uživatele s možnostmi těchto adres.

Naprosto běžnou praxí je, že z vnitřních adres nelze zaslat email směrem ven a tak na tyto adresy nejsou ani maily z venku doručovány dovnitř. Snižuje se tak možnost příjmu spammu, nebo neoprávněného mailu.

Vnější adresy se dají většinou najít na webových stránkách organizace, kde jsou proti sběru adres chráněny nějakou pasivní ochranou, př. email není uveden v HTML kódu jako odkaz **mailto:**, ale je zde vložen třeba obrázek s emailovou adresou (o těchto ochranách blíže v dalším bodě). Zde už se spammerovi naskytuje možnost adresu ukrást, opět mu může být práce znepříjemněna typem pasivní ochrany.

Nejvíce na ráně jsou tzv. veřejné adresy, jsou uváděny na všech webových stránkách jako první kontakt s organizací, na vizitkách, v obecných seznamech firem ať už papírových nebo internetových, uváděny v reklamách apod.… Na těchto adresách můžeme s vysokou pravděpodobností očekávat spam, proto je dobré hlavně tyto adresy kvalitně zabezpečit aktivními ochranami.

Poslední dobou se stále častěji setkávám s dalším druhem preventivní ochrany v organizacích tzv. **elitářstvím**, tento způsob ochrany tkví v tom, že se do předmětu zprávy uvádí sjednaný kód, pokud v předmětu tento kód není, zpráva je automaticky vyloučena z příjmu. Toto jednouché pravidlo je velice účinné, i když se spammerovi povede posbírat všechny adresy dané organizace, šance na doručení jediného mailu se spammem je skoro nulová.

Nesmíme také zapomenout, že emailové adresy nejsou v rukou výhradně jen organizací a firem, ale i běžných lidí. Ti se mohou bránit také několika jednoduchými způsoby:

- změna emailové adresy
- více emailových adres
- adresa na jedno použití
- elitářství

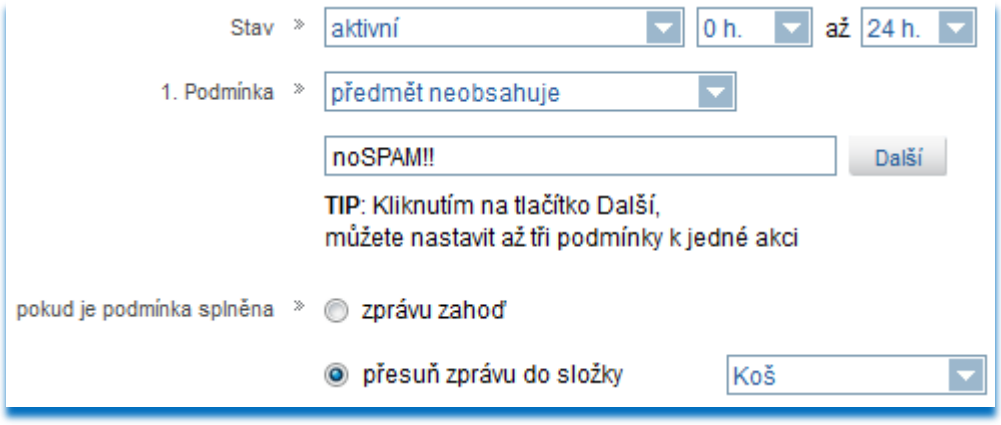
Začneme-li do naší emailové schránky dostávat větší množství spamu, než které bychom chtěli, může to být podnět pro změnu emailové adresy. Tento krok s sebou nese řadu problémů, ale někdy je to opravdu jediná možnost jak se lehce a rychle spamu zbavit.

Zajímavějším způsobem je vlastnictví více emailových adres. Příkladem můžeme mít jednu adresu pro komunikaci s přáteli a rodinou, další adresu pro pracovní komunikaci, další adresu třeba pro nákupy na internetu a poslední třeba pro registraci v internetových

fórech a blozích. Nejvíce spamu budeme pravděpodobně dostávat do emailové schránky zřízené kvůli komunikaci na internetových fórech a blozích.

Vhodným způsobem ochrany je i emailové adresa na jedno použití. Založit emailovou adresu trvá asi kolem 1 minuty. Chceme-li se registrovat na stránky, kde předpokládáme, že může hrozit prodej adresy, nebo získání adresy spammerem můžeme si stránku zaregistrovat na takovou adresu. Po registraci na stránku ověříme z emailu registraci a nikdy se už k emailu nevrátíme, opustíme jej. Tento přístup je trošku pracnější, ale neohrožujeme tak naší hlavní emailovou adresu, která je tak stále v bezpečí.

Efektivním způsobem se mi pro běžného uživatele zdá elitářství. S lidmi, s kterými komunikujeme, si dohodneme heslo, které uvádíme v předmětu zprávy, zavedeme pravidlo pro příjem zprávy, pokud email toto heslo neobsahuje, putuje email do koše. Otázkou je potom co se stane, pokud nás kontaktuje někdo, kdo o daném hesle neví. Je už jen na nás jak často budeme procházet složku koš a tyto jedince do elitářství přidávat. Složku koš je výhodné vybrat proto, že složky vytvořené poskytovateli freemailů jsou automaticky promazávány po určitém počtu dní. Pravidlo pro elitářství může vypadat třeba takto:



Obr. 6 Ukázka filtru pro elitářství

Elitářstvím neomezíme příjem spamu, pokud zprávy neobsahující domluvené heslo automaticky nesmažeme, ale je na každém uživateli, aby si tento krok dobře promyslel.

Provedený pokus: byly založeny 2 emailové adresy, obě měly náhodně generované jméno (malá šance získání emailové adresy tipováním), z jedné adresy se nekomunikovalo vůbec, druhá byla použita pro tvorbu účtů na warezových a porno stránkách. Během prvního týdne dorazily do používané schránky první spammové emaily (celkem 13). Během dalších 3 měsíců už do schránky docházelo několik spammových emailů denně. První schránka je do dnešního dne stále bez jediné emailové zprávy.

2.2 Pasivní ochrana

Mezi pasivní druhy ochrany můžeme zařadit takové postupy, které mají spammerovi, popř. robotovi (spambot), který sbírá emailové adresy ztížit práci ve sběru těchto adres.

Nejčastějším postupem je sklízení přímo z webových stránek. Robot prochází webové stránky a v jejich HTML kódu hledá emailové adresy, ty vyhledává podle struktury emailové adresy. Spambot ví od svého tvůrce, jak emailová adresa vypadá a porovnává nalezené sekvence podle toho.

Vyhledávací vzorec (analýza textu) může vypadat takto:

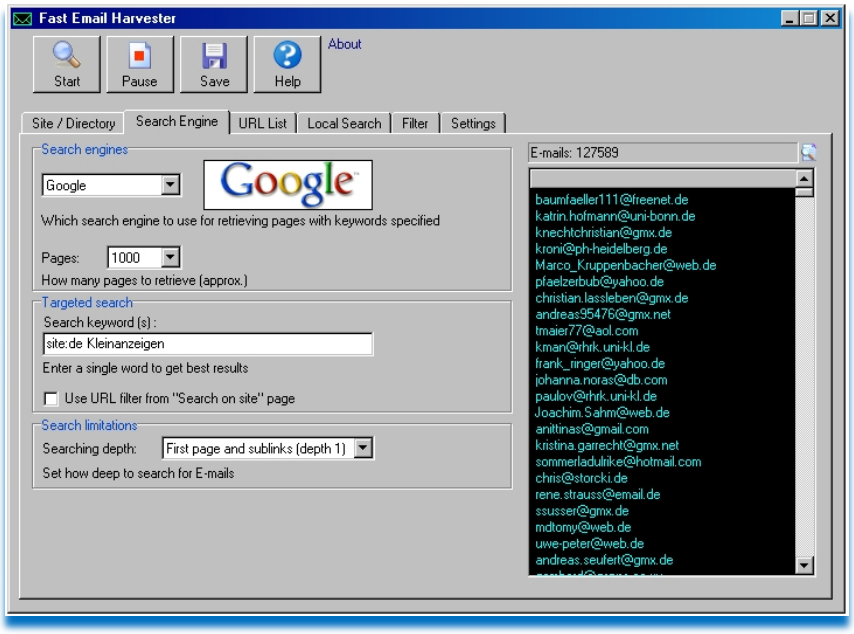
[a-z,0-9;1-*]@[a-z,0-9;1-*].[a-z;2-4],

kde **a-z,0-9** naznačuje znaky, které se na pozici znaku mohou vyskytovat, ***** naznačuje počet znaků **minimálně 1** a maximálně neomezeno, pak znak **zavináče** a **doména** opět a-z, 0-9, pak následuje **tečka** a vše ukončuje přípona domény, která může mít 2-4 znaky. Tento vzorec není ideální a má mnoho chyb, ale pro představu to stačí.

Spammer nebo spambot tedy vyhledá v HTML textu znak zavináč a porovnává okolní text podle vzorce. Lehčí je pokud najde přímo v HTML kódu klíčové slovo **mailto:**

Př: `<a href="mailto:uzivatel@alias.domena.cz">uzivatel@alias.domena.cz</a>`

Najde-li spambot tento tag v HTML kódu ví, že vše za **mailto:** je emailová adresa uživatele a přímo si ji zařazuje do databáze sklizených adres.



Obr. 7. Ukázka Email Harvesteru [8]

Teď když víme, jak spambot adresy sbírá, podíváme se jak mu to znepříjemnit. Popřípadě úplně znemožnit. Postupů pro to známe několik, uvedeme si jen ty nejzákladnější:

- Psát emailovou adresu bez odkazu **mailto:**
- Náhrada části, nebo celé emailové adresy obrázkem
- Náhrada části emailové adresy textem (náhrada znaků @ a .)
- Úpravami textu, skládáním textu
- Zápis adresy JavaScriptem, ASCII kódem, změnou směru textu
- Formuláře
- Antiadresy

2.2.1 Bez odkazu mailto:

Tento odkaz byl vymyšlen kdysi v počátcích internetu, jako součást standardu html, pro zvýšení uživatelského komfortu. Kliknutím na něj se návštěvníkovi webových stránek otevře výchozí e-mailový klient s vyplněnou adresou, příp. předmětem a textem. Návštěvník webu tak vyvine minimální úsilí k tomu, aby autorovi napsal – což je důležitá funkce zejména pro firemní prezentace, ale je příjemná i pro osobní stránky.

Bohužel odkazy mailto: jsou velmi snadno zneužitelné pro spamboty, kterým pak stačí rychle proběhnout obsah html stránky, najít příkaz mailto: a bez dalších zdlouhavých analýz textu si obsah příkazu uložit do výstupní databáze. [9]

Je tedy vhodné popřemýšlet, zda potřebujeme přímo v HTML kódu tento odkaz mít. Zda cílová skupina, která web navštěvuje, bude schopná použít jiný způsob zápisu emailové adresy.

2.2.2 Náhrada části nebo celé emailové adresy obrázkem

Nechceme-li v kódu HTML uvádět emailovou adresu, musíme ji vložit do kódu jinak, třeba jako celý obrázek, provést to můžeme například tímto HTML tagem `<img src="emailova_adresa.gif">`, ten na pozici kódu umístí obrázek s emailovu adresou na webové stránce to pak vypadá nějak takto:

Obr. 8. Ukázka emailové adresy na webové stránce

Adresa se ukáže uživateli ve vizuální podobě jak je zvyklý, modrý a podtržený text. V samotném HTML kódu však není nikde emailová adresa uvedena. Velkou nevýhodou tohoto způsobu je, že snahou o kliknutí na obrázek se nevyvolá obvyklá úloha startu poštovního klienta. Dále na mobilních zařízeních se přeskakováním po odkazech nelze umístit na položku emailové adresy, a tudíž může být položka mezi jinými odkazy přehlédnuta.

V případě kdy vyměníme jen část emailové adresy obrázkem, třeba jen znak zavináč, je situace stejná. Platí pro ni všechny stejné klady i zápory, jako v předešlém odstavci. Kód pak vypadá takto: `<br>(adresa<img border="0" src="zavinac.gif" width="24" height="16">domena<img border="0" src="tecka.gif" width="6" height="16">cz)`.

Obr. 9. Ukázka emailové adresy
na webové stránce

2.2.3 Náhrada části emailové adresy textem (náhrada znaků @ a .)

Někdy je jednodušší na webových stránkách neudávat tyto grafické prvky, které jsou časově náročnější na umístění a designování webových stránek. Jednodušší možností je nahradit znaky v emailových adresách jejich textovým popisem. Vznikají tak opět emailové adresy, které nejsou v HTML kódu lehce čitelné, pro začátek nemůže spambot objevit položky **mailto:** anebo znak **@**, kterým by jednoznačně identifikoval emailovou adresu.

Ukázky používaných kódů:

- adresa**(zavináč)**domena**(tečka)**cz
- adresa**(at)**domena**(dot)**cz
- adresa**#**domena**$**cz, na stránce nesmí chybět instrukce, že # nahradíme znakem zavináče (@) a $ nahradíme znakem tečky (.).
- …

Těchto druhů ochran je na webových stránkách opravdu hodně.

2.2.4 Úprava textu a skládání textu

Velice zajímavé jsou kombinace pasivní ochrany textového typu s možností odkazu **mailto:**. Vznikají tak možnosti sice kliknout na emailový odkaz s otevřením poštovního klienta, ale jsou vybaveny jednou, nebo více logickými operacemi.

Příkladem může být třeba operace, kde nám přímo v adrese emailu napíše logickou operaci **odstrantezirafu**, kód pak vypadá následovně:

```
<a href="mailto:adresa@odstrantezirafudomena.cz">adresa@domena.cz</a>.
```

Velkou výhodou je pak možnost mít na webu standardní emailový odkaz i s tím, že po kliknutí spustí emailového klienta s předvyplněnou adresou příjemce. Musíme však z emailové adresy odstranit logický text **odstrantezirafu.** Výhodou je, že pokud se taková adresa dostane do rukou spammera, nekontroluje její autentičnost a spam na ní zaslaný nikdy nedojde. Nevýhodou je však nezkušenost některých pisatelů, kteří neodstraní požadovaný text a email tak není nikdy doručen.

Velice hezkým a lidským způsobem je třeba podání emailových adres druhem doplňování. Zapisované na webech bývají takto:

Jméno zaměstnance	Funkce	Telefon	E-mail
Jméno1 Příjmení1	Recepce	...	Info*
Jméno2 Příjmení2	...	...	Jmeno*
Jméno3 Příjmení3	...	...	prezdivka*

* všechny naše emaily mají koncovku @domena.cz

[9]

Obr. 10. Ukázka zápisu emailových adres formou doplňování
(samostatného zápisu adresy a domény)

2.2.5 Zápis adresy JavaScriptem, ASCII kódem, nebo změnou směru textu

Výpis adres JavaScriptem je velice oblíbenou metodou, umožňuje užít na webových stránkách emailové odkazy s veškerým možným komfortem. Na web stránce vypadá emailový odkaz následovně:

E-mail: adresa@domena.cz

Obr. 11. Ukázka emailové adresy zapsané v JavaScriptu
na webových stránkách

Na odkazy je možno kliknout, jsou modré a podtržené, navíc v HTML kódu se nikde nevyskytuje znak zavináče, ani tag **mailto:**. Zdrojový kód takové JavaScriptu může vypadat takto:

```
<script language='JavaScript' type='text/javascript'>
 <!--
 var prefix = 'm&#97;&#105;lt&#111;:';
 var suffix = '';
 var attribs = '';
 var path = 'hr' + 'ef' + '=';
 var addy81106 = 'adresa' + '&#64;';
 addy81106 = addy81106 + 'domena' + '&#46;' + 'cz';
 document.write( '<a ' + path + '\'' + prefix + addy81106 + suffix + '\''
+ attribs + '>' );
 document.write( addy81106 );
 document.write( '<\/a>' );
 //-->
 </script><script language='JavaScript' type='text/javascript'>
 <!--
 document.write( '<span style=\'display: none;\'>' );
 //-->
 </script>Emailová adresa je chráněna před spammery a spamboty, pro
zviditelnění prosím, povolte JavaScript.
 <script language='JavaScript' type='text/javascript'>
```

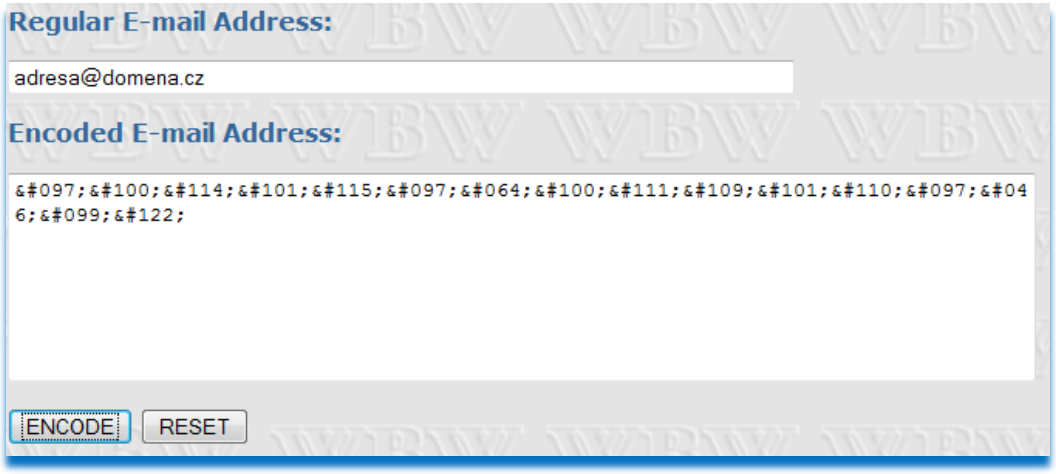
Reálná a použitelná ukázka JavaScriptu, který ochrání Vaši emailovou adresu před běžným spammerem, nebo spambotem. Stačí klíčová slova 'adresa', 'domena' a 'cz' nahradit Vašimi údaji. Velkou výhodou je i to, že spamboti stále neumí interpretovat JavaScript, zatím co uživatel jej má v prohlížeči běžně povolen.

Ochrana a zápis adresy s využitím ASCII kódu je obdobná, zde máme možnosti buď nahradit jen určitý znak ASCII kódem, třeba zavináč (@ = &#064. Zápis v HTML kódu by pak vypadal `<a href="mailto:adresa%40domena.cz">adresa&#064;domena.cz</a>`. Tímto zápisem je v kódu ochráněn znak zavináče. [9]

Pokud bychom chtěli zapsat ASCII kódem celou emailovou adresu, můžeme tak provést třeba na této webové stránce http://www.wbwip.com/wbw/emailencoder.html, kde je k tomu zřízen automat. Ten provede převod celé emailové adresy na ASCII kód. Emailová adresa **adresa@domena.cz** je pak zapsána jako sekvence ASCII znaků **adresa@domena.cz**.

Takto vytvořený kód stačí umístit do tagu **mailto:**. Spammer, ani spambot jej bez další analýzy a ručního či automatického dekódování neměli být schopni použít. Bohužel už se objevily harvestery s automatickým převodem z ASCII zpět do čitelného a použitelného

stavu. Takže je tento postup už tedy překonaný, nicméně mnoho harvesterů tuto vlastnost stále implementovanou nemá.



[10]

Obr. 12. Webová aplikace na převod emailových adres do ASCII kódu

Posledním zmiňovaným postupem v této podkapitole bude změna směru textu. Jedná se o využití tagu <BDO>, který se vyskytuje v XHTML kódu a je určen pro tvorbu webů v arabštině. Námi standardně napsaná emailová adresa adresa@domena.cz by byla v XHTML kódu zapsána jako `<bdo dir="rtl">zc.anemod@aserda</bdo>`, kde atribut dir je povinný a určuje směr textu (rtl = right to left). Při generování webové stránky se emailová adresa zobrazí správně, v kódu jí však spambot vidí otočenou a do databáze jí tedy uloží ve špatném směru. Opět je zde otázka jak pracné bude pro spammera upravit program spambota, aby si v takovém případě text otočil, ale už čas strávený s programováním se spammerovi možná nezaplatí. [9]

2.2.6 Využití webového formuláře

Často používaný, poměrně spolehlivý způsob, je neuvádění e-mailové adresy, a implementace kontaktního formuláře na webovou stránku. Formulář samozřejmě musí být realizován tak, aby v XHTML kódu stránky nebyla uvedena emailová adresa, protože jinak by toto řešení jako ochrana nemělo smysl. Výhodou řešení je možnost rychlého kontaktu, návštěvník ani nemusí spouštět e-mailový program, ani opisovat adresu.

Nevýhodou pro některé pisatele může být absence kopie zprávy v jeho odeslané poště a nemožnost využít některých funkcí běžné elektronické pošty – např. html formátování, příloha nebo potvrzení o přečtení. Navíc zkušení uživatelé internetu mohou mít už z principu nedůvěru k uvádění své e-mailové adresy do jakéhokoliv webového formuláře.

První nevýhoda je odstranitelná zahrnutím zaškrtávacího políčka „poslat kopii na moji adresu“, html formátování lze také doplnit, i když není tak pohodlné jako v mailovém klientu, a poslední nedostatek už je věc důvěry pisatele a majitele webu. [9]

Ochranné prvky vyskytující se ve webových formulářích:

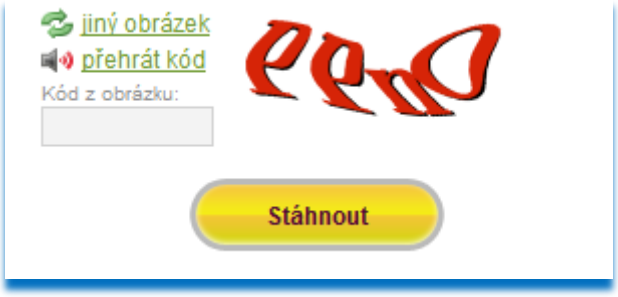
- Opsání kódu CAPTCHA
- Logické otázky
- Kontrola času
- JavaScriptem
- Flash

Na webu hodně užívané a některými lidmi velice zavrhované užívaní textů Captcha. Jedná se o alfanumerické znaky různě zakódované do podkladové grafiky, měly by být špatně čitelné, bohužel dnes existuje množství programů, které umí kód Captcha přečíst lépe než člověk.

[11]

Obr. 13. Ukázka kódu Captcha

Kladem je u této technologie možnost refreshovat obrázek pokud je nečitelný, a dokonce se na webu vyskytují i možnosti si kód nechat zvukově přehrát, takže i pro lidi se zrakovým handicapem je tato technologie přístupná.



[12]

Obr. 14 Ukázka aplikace Captcha z webové stránky www.uloz.to

Dnes asi nejvíce užívaná ochrana formuláře na webu bývá buď logickou otázkou, nebo početní operací. Užívají se dnes i na diskusních fórech a blozích. Spammboti se adaptovali

i na tento druh webových stránek. Nejedná se o nějaké těžké početní operace nebo hádanky, spíše o možnost vyloučit intervenci spambotů. Otázky bývají typu „ **3 + 7 = ?**“ nebo „**Hlavní město ČR je?**“ a podobně… Tyto otázky jsou pro spamboty neřešitelným problémem, navíc se často tyto otázky na formulářích automaticky mění.

Zajímavým řešením je kontrola délky času od příchodu na webovou stránku po odeslání formuláře. Zatímco robot je schopen operaci příchodu a odeslání formuláře provést v rámci 0,5 sekundy, člověku bude daná operace trvat i několik desítek sekund. Vhodně nastavený interval může omezit možnost odesílání formuláře spambotům.

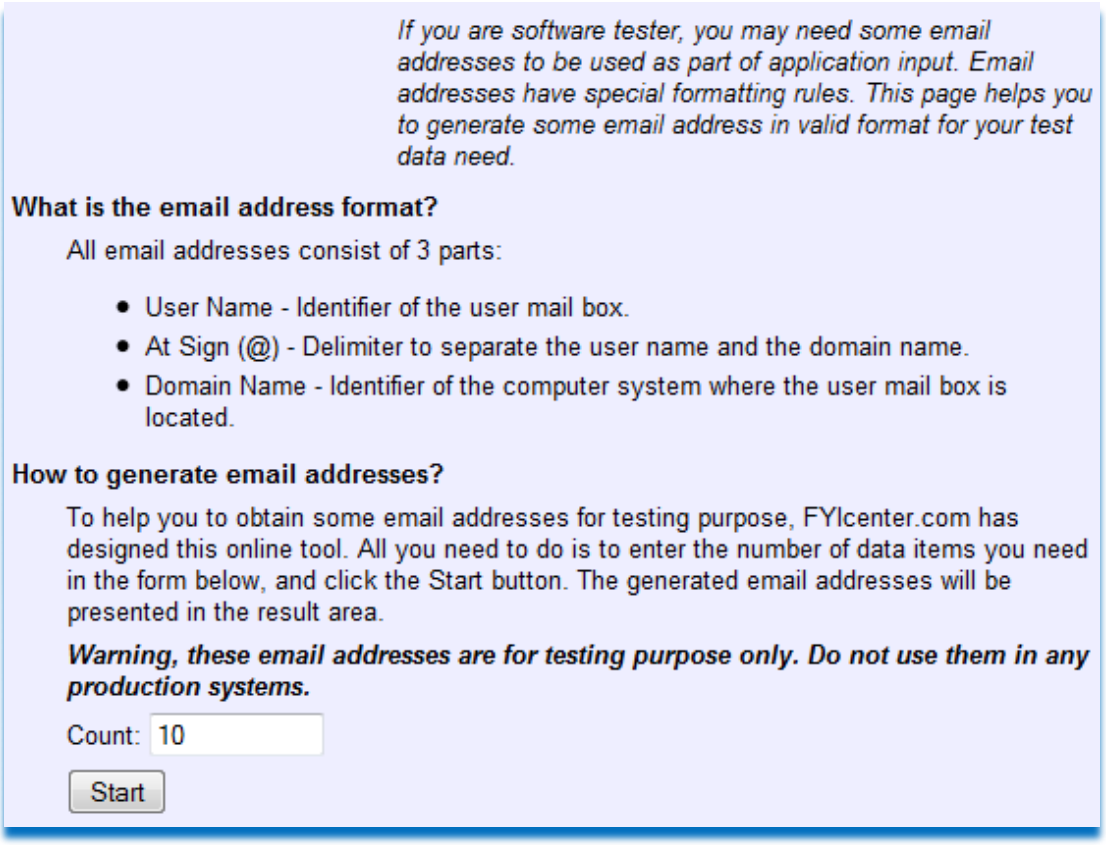
Využívá toho, že roboti neumějí nějakou technologii, kterou podporuje běžný prohlížeč - v tomto případě javascript. Do formuláře se pak přidá javascriptem jedno skryté pole. Jeho hodnota se pak kontroluje při obsluze. Pro uživatele bez javascriptu se ono pole zobrazí normálně, ale s popiskem vysvětlujícím, co mají vyplnit. Do doby, než se objeví roboti, kteří rozumí javascriptu, je tato metoda v podstatě ideální. Drtivou většinu uživatelů neobtěžuje (mají zapnutý javascript), ti ostatní pouze vyplní o jedno pole navíc. Tento způsob je v současnosti jedním z nejúčinnějších. [13]

V poslední době je možno se na webových stránkách setkat s formulářem tvořených ve Flash aplikacích, mají několik velkých výhod oproti standardním XHTML formulářům. Výhodou je, že spamboti s nimi neumí vůbec pracovat (obdoba jako s JavaScriptem), vysoká dynamičnost prvků, lze lehce dosáhnout dynamicky se měnícího kontrolního textu i v průběhu vypisování formuláře. Mezi nevýhody patří náročnější tvorba formuláře, špatná kompatibilita s mobilními zařízeními.

2.2.7 Antiadresy

Říká se, že „oko za oko, zub za zub“ není správné řešení. Co když je, ale maximálně účinné? Řešení antiadres je totiž právě takový bič na spammery a spamboty. Jak funguje? Vygenerujete množství neexistujících emailových adres, které v kódu HTML umístíte viditelně (myslí se pro spambota). Spambot tyto adresy najde a vloží do databáze nalezených emailových adres. Spammer v dobré víře objemné databáze emailových adres rozešle na emailové adresy spam a ejhle on se nikdo na nabídky nezareaguje, útok provést nejde, protože poštovní server na dané emailové adresy odmítá spojení apod… Nebo zkusí takovou databázi prodat, ale kupující chce vědět procentuální existenci uvedených emailů a po pár testech se přijde na to, že je databáze „otrávená“ nefunkční a že obsahuje mnoho antiadres. Databáze se tak nedá použít ani pro rozeslání a ani pro prodej. Spammerova

práce byla zbytečná. Funkční adresy, které byly posbírány společně s antiadresami, jsou tak zachráněny. Neexistuje jednoduchý a rychlý způsob jak antiadresy projít, zkontrolovat jejich funkčnost a odstranit z databáze.



If you are software tester, you may need some email addresses to be used as part of application input. Email addresses have special formatting rules. This page helps you to generate some email address in valid format for your test data need.

What is the email address format?

All email addresses consist of 3 parts:

- User Name - Identifier of the user mail box.
- At Sign (@) - Delimiter to separate the user name and the domain name.
- Domain Name - Identifier of the computer system where the user mail box is located.

How to generate email addresses?

To help you to obtain some email addresses for testing purpose, FYIcenter.com has designed this online tool. All you need to do is to enter the number of data items you need in the form below, and click the Start button. The generated email addresses will be presented in the result area.

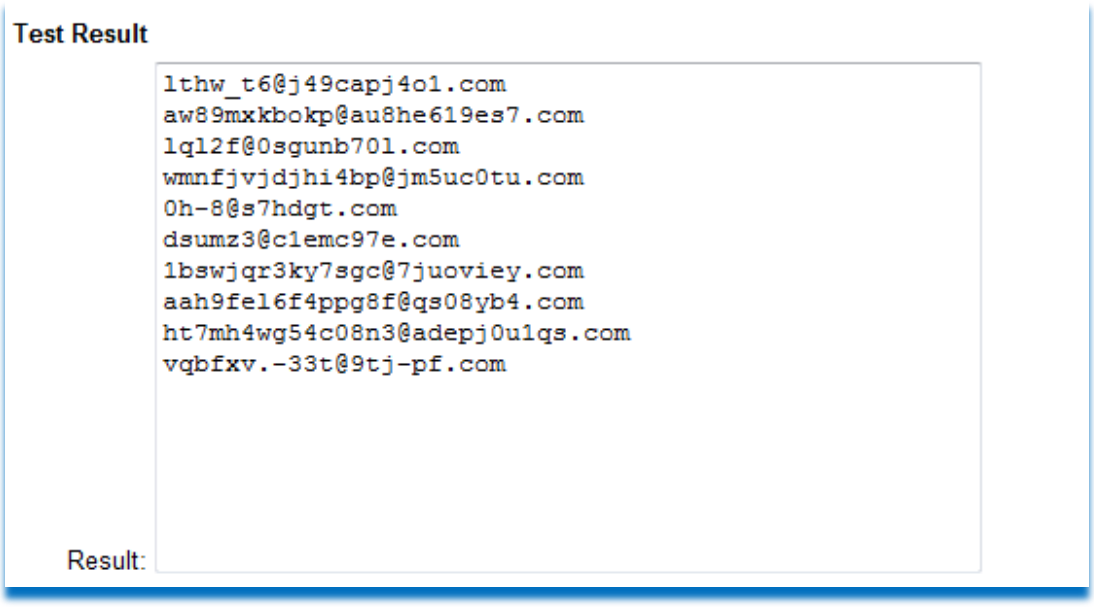
Warning, these email addresses are for testing purpose only. Do not use them in any production systems.

Count: 10

Start

[14]

Obr. 15. Ukázka emailového generátoru



Test Result

```
lthw_t6@j49capj4o1.com
aw89mxkbokp@au8he619es7.com
lql2f@0sgunb70l.com
wmnfjvjdjhi4bp@jm5uc0tu.com
0h-8@s7hdgt.com
dsumz3@c1emc97e.com
1bswjqr3ky7sgc@7juoviey.com
aah9fel6f4ppg8f@qs08yb4.com
ht7mh4wg54c08n3@adepj0u1qs.com
vqbfxv.-33t@9tj-pf.com
```

Result:

[14]

Obr. 16. Výsledek emailového generátoru

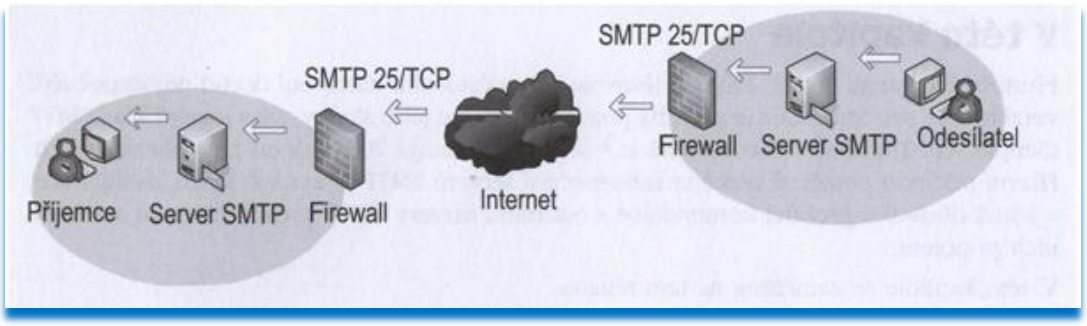
Všechny tyto pasivní ochrany mají jednu velkou nevýhodu a to je plošné užívání. Problémem dnešní doby je rychlá odezva ze strany spammerů, kteří víc než akčně reagují na ochranné technologie. Dnes už existují harvestery s možností uložení stránky do obrázku a jeho zpětnou OCR (převod obrázku na text) analýzou. Použité metody se tak stávají neúčinnými. Některé z nových ochran jako jsou formulářové ochrany JavaScriptem nebo Flash aplikací, ale stále odolávají a dávají nám tak možnost se spammery bojovat.

2.3 Aktivní ochrana

Na to abychom pochopili, jak fungují nástroje aktivní ochrany proti příjmu spamu, se musíme seznámit s principem poštovních protokolů a atributů emailové zprávy.

Protokol SMTP

Simple Mail Transfer Protocol (zkratka SMTP) je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (MTA). Protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem; zpráva je doručena do tzv. poštovní schránky adresáta, ke které potom může uživatel kdykoli (off-line) přistupovat (vybírat zprávy) pomocí protokolů POP3 nebo IMAP. Jedná se o jednu z nejstarších aplikací, původní norma RFC 821 byla vydána v roce 1982 (v roce 2001 ji nahradila novější RFC 2821). SMTP funguje nad protokolem TCP, používá port TCP/25. [15]



[16]

Obr. 17. Ukázka SMTP komunikace mezi odesílatelem a příjemcem skrz celosvětovou síť Internet

Doručování elektronické pošty po Internetu se účastní tři druhy programů:

- ***MUA** - Mail User Agent, poštovní klient, který zpracovává zprávy u uživatele*
- ***MTA** - Mail Transfer Agent, server, který se stará o doručování zprávy na cílový systém adresáta*

- ***MDA*** *- Mail Delivery Agent, program pro lokální doručování, který umísťuje zprávy do uživatelských schránek, případně je může přímo automaticky zpracovávat (ukládat přílohy, odpovídat, spouštět různé aplikace pro zpracování apod.).* [15]

Většina poštovních serverů v sobě obsahuje funkce programů MTA a MDA.

Poštovní klient

Jak uvádí předchozí odstavec, jedná se o program pro správu a práci s emailovými zprávami, zajišťuje přijímání/odesílání mailů, jejich pročítání, ukládání, archivaci a další funkce. Zprávy z poštovního serveru můžeme stahovat pomocí protokolů POP3 nebo IMAP. Mezi nejznámější klienty patří Microsoft Outlook (obsažen v sadě Microsoft Office), Microsoft Outlook Express (zdarma k prohlížeči Microsoft Internet Explorer), dále je to Mozilla Thunderbird a další. Poštovního klienta si většina uživatelů volí dle vzhledu a používaných funkcí.

Poštovní server

Většina dnešních poštovních serverů v sobě již zahrnuje modely MTA a MDA.

Poštovní server (MTA) běží obvykle jako démon a naslouchá na portu TCP/25. K tomuto portu se může připojit (navázat TCP spojení) buď poštovní klient, nebo jiný server, který předá zprávu k doručení. MTA zkontroluje, zda je zpráva určena pro systém, na kterém běží. Pokud ano, předá ji programu MDA (lokální doručení). Pokud je zpráva určena jinému počítači, naváže spojení s příslušným serverem a zprávu mu předá.

Při vyhledávání vzdáleného serveru, kterému má předat zprávu, musí MTA spolupracovat se systémem DNS. Od serveru DNS si vyžádá tzv. MX záznam pro cílovou doménu, který obsahuje IP adresu počítače, který se stará o doručení pošty v této doméně. Pokud DNS tento záznam neobsahuje, pokusí se poštovní server doručit zprávu přímo na počítač uvedený v adrese za zavináčem.

Poštovní server obsahuje v konfiguraci řadu parametrů, pomocí kterých můžeme mimo jiné nastavit, pro které domény MTA přijímá zprávy. Stejně tak je možné určit, od koho bude nebo nebude zprávy přijímat, což je velmi důležité z hlediska bezpečnosti a ochrany proti spamu. [15]

Mezi nejpoužívanější poštovní servery patří Microsoft Exchange, SendMail, Mercury atd… Většina těchto poštovních serverů v sobě již obsahuje moduly a nástroje pro antispamovou a antivirovou ochranu. Lze je doplnit i externími programy.

Formát zprávy

Formát zprávy popisuje norma RFC 2822, která v roce 2001 nahradila původní RFC 822 z roku 1982. Zpráva se skládá z hlavičky a těla zprávy. Tělo může obsahovat kromě vlastní textové zprávy také volitelné přílohy s libovolným obsahem.

Ukázka SMTP komunikace

Po ustanovení spojení mezi klientem a serverem dochází k SMTP přenosu. V následující ukázce je vše, co začíná ***C****, odesláno klientem a vše, co začíná* ***S:*** *odesláno serverem.*

```
C: navázání spojení se serverem (zpravidla na TCP portu 25)
S: 220 mail.example.com ESMTP Postfix
C: HELO example.net
S: 250 Hello example.net
C: MAIL FROM: <sender@example.net>
S: 250 Ok
C: RCPT TO: <friend@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: test message
C: From: sender@example.net
C: To: friend@example.com
C:
C: Hello,
C: This is a test.
C: Goodbye.
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

Poznámka: Příkaz HELO se používá pro starší SMTP spojení, novější servery používají ESMTP a příkaz EHLO:

```
S: 220 mail.example.com ESMTP Postfix
C: EHLO example.net
S: 250-mail.example.com
...
C: .
S: 250 Ok
C: QUIT
S: 221 Goodbye
```

Chyby SMTP protokolu

Doprava dopisu protokolem SMTP může selhat z mnoha různých příčin. SMTP protokol rozeznává dva typy chyb.

Trvalé chyby (jejich číselný kód začíná 5) *jsou např. „uživatel neexistuje“, „server neexistuje“. V případě trvalé chyby se odesílateli okamžitě posílá zpráva o nedoručení a jeho příčině.*

Dočasná chyba (její číselný kód začíná 4) *může být způsobena např. tím, že cílový server je momentálně nedostupný, nekomunikuje nebo je zaneprázdněn. Odesílající server má v tom případě dopis uložit do fronty a po nějakou nastavenou dobu (typicky několik dní) by měly být činěny opakované pokusy (typicky po několika málo desítkách minut) o doručení.*

Některé servery posílají po několika hodinách neúspěšných pokusů odesílateli zprávu, že doručení se prozatím nepodařilo, ale že to server bude zkoušet dál. Pokud pokusy o doručení jsou po nastavenou dobu neúspěšné, posílá se odesílateli zpráva o nedoručitelnosti a dopis se zahodí. [15]

SMTP návratový kód	význam
421	<domain> Service not available, closing transmission channel
450	Requested mail action not taken: mailbox unavailable
550	Requested action not taken: mailbox unavailable
554	Transaction failed

Tab. 2. Ukázka některých návratových kódů SMTP protokolu [17]

Všechny SMTP návratové kódy a další popis komunikace SMTP protokolu lze najít třeba na této webové stránce http://www.greenend.org.uk/rjk/2000/05/21/smtp-replies.html.

Protokol POP3

POP3 (Post Office Protocol version 3) je internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta. Jedná se o aplikační protokol pracující přes TCP/IP připojení. POP3 protokol byl standardizován v roce 1996 v RFC 1939. [18]

Protokol POP3 používá pro komunikační účely port 110, přes tento port zajišťuje komunikaci s emailovou schránkou, zasílá přes něj ověřovací údaje a stahuje poštu do poštovního klienta. Ke schránce se připojuje, jen když chceme emailové zprávy přijímat nebo odesílat. Při práci v poštovním klientovi je protokol neaktivní.

```
S: <server naslouchá na TCP portu 110>
C: <otevření spojení>
S:    +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C:    APOP mrose c4c9334bac560ecc979e58001b3e22fb
```

Klient posílá jméno a heslo (USER, PASS) -->

```
C:    USER mrose
S     +OK User accepted
C:    PASS mrosepass
S     +OK Pass accepted

S:    +OK mrose's maildrop has 2 messages (320 octets)
C:    STAT
S:    +OK 2 320
C:    LIST
S:    +OK 2 messages (320 octets)
S:    1 120
S:    2 200
S:    .
C:    RETR 1
S:    +OK 120 octets
S:    <POP3 server posílá 1. zprávu>
S:    .
C:    DELE 1
S:    +OK message 1 deleted
C:    RETR 2
S:    +OK 200 octets
S:    <POP3 server posílá 2. zprávu>
S:    .
C:    DELE 2
S:    +OK message 2 deleted
C:    QUIT
S:    +OK dewey POP3 server signing off (maildrop empty)
C:  <uzavření spojení>
S:  <server čeká na další spojení>
```

V základní implementaci POP3 mají příkazy 3 nebo 4 znaky. Za příkazem mohou následovat další argumenty oddělené mezerami. Řádky jsou oddělovány pomocí CRLF. Každá odpověď od serveru musí začínat indikací stavu operace - buď +OK, nebo -ERR. [18]

Protokol IMAP

IMAP (Internet Message Access Protocol) je internetový protokol pro vzdálený přístup k emailové schránce. Na rozdíl od protokolu POP3 vyžaduje IMAP trvalé připojení (tzv. on-line), avšak nabízí pokročilé možnosti vzdálené správy (práce se složkami, přesouvání zpráv, prohledávání na straně serveru a podobně). V současné době se používá protokol IMAP4 (IMAP version 4 revision 1 - IMAP4rev1), který je definován v RFC 3501.
Protokol IMAP standardně používá port 143 protokolu TCP. [19]

Protokol IMAP se užívá v případech, kdy máme zprávy uloženy na serveru a přistupujeme k nim vzdáleně, jen v případě čtení si v emailovém klientu zprávu zobrazíme, zpráva nadále zůstává na serveru. Velkou výhodou protokolu IMAP je jeho vícenásobné připojení k jedné schránce. Více uživatelů tak může sdílet jednu schránku (v reálném čase). Pravidelnou synchronizací se jim zobrazují nové odeslané a přijaté zprávy. To protokol

POP3 nedovoluje. I přes své zjevné výhody není tento protokol rozšířenější než jednodušší protokol POP3.

Hlavička emailu a MIME

MIME, plným názvem Multipurpose Internet Mail Extensions („Víceúčelová rozšíření internetové pošty“), je internetový standard, který umožňuje pomocí elektronické pošty zasílat zprávy obsahující text s diakritikou, lze k ní přiložit přílohu v nejrůznějších formátech, umožňuje funkci digitálního podpisu apod. V současné době ho využívají i další protokoly aplikace (např. HTTP). Standard MIME je definován šesti dokumenty: RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 a RFC 2049.

Původní standard elektronické pošty byl vytvořen tak, aby umožňoval přenos anglického textu, k čemuž stačí pouze tabulky znaků ASCII. Proto nebylo dlouho možné používat v elektronické poště znaky s diakritikou a posílat současně se zprávou i přílohy. Částečným řešením bylo například použití uuencodingu nebo jiných metod, avšak citelně scházela celosvětová standardizace.

MIME rozšiřuje formát e-mailu o tyto možnosti:

- *podpora textu psaného ve znakových sadách jiných než US-ASCII*
- *podpora příloh (obrázky, zvuky, filmy, programy a podobně)*
- *vícedílné zprávy*
- *informace v hlavičce v jiné znakové sadě než ASCII*

Základní formát e-mailu je definován v RFC 2822. Tento standard specifikuje formátování hlaviček, těla e-mailu a pravidla pro běžně používané pole hlavičky jako „Komu:“, „Předmět:“, „Od:“ a „Datum:“. MIME definuje sadu hlaviček pro specifikaci doplňkových atributů zprávy obsahující "content-type" a definuje sadu "transfer-encoding", která může být použita pro reprezentování 8bitových binárních dat užívajících znaky 7bitového ASCII. [20]

Zpráva elektronické pošty se skládá ze dvou částí:

*Ze **záhlaví** tvořeného řádky, které se nazývají hlavičky. Hlavička začíná klíčovým slovem následovaným dvojtečkou a mezerou (např. From:, To:, Subject: atp.). Za mezerou následují hodnoty.*

*Vlastním **textem zprá**vy. Text zprávy je od záhlaví oddělen právě jedním prázdným řádkem.*

Následující rámec schématicky znázorňuje zprávu elektronické pošty:

Received: ..... *Received: .....* *Date: .....* *From: .....* *Subject: .....* *To: .....* *Message-Id: .....* *Text zprávy*

Zajímavá je hlavička Received:. Tuto hlavičku připisuje na počátek mailu každá mailova gateway (mailový server), kterou zpráva prochází. Takže čteme-li hlavičky Received: od spodu nahoru, tak zjistíme celou trasu, přes které mailové servery zpráva šla.

RFC822 zavádí hlavičky:

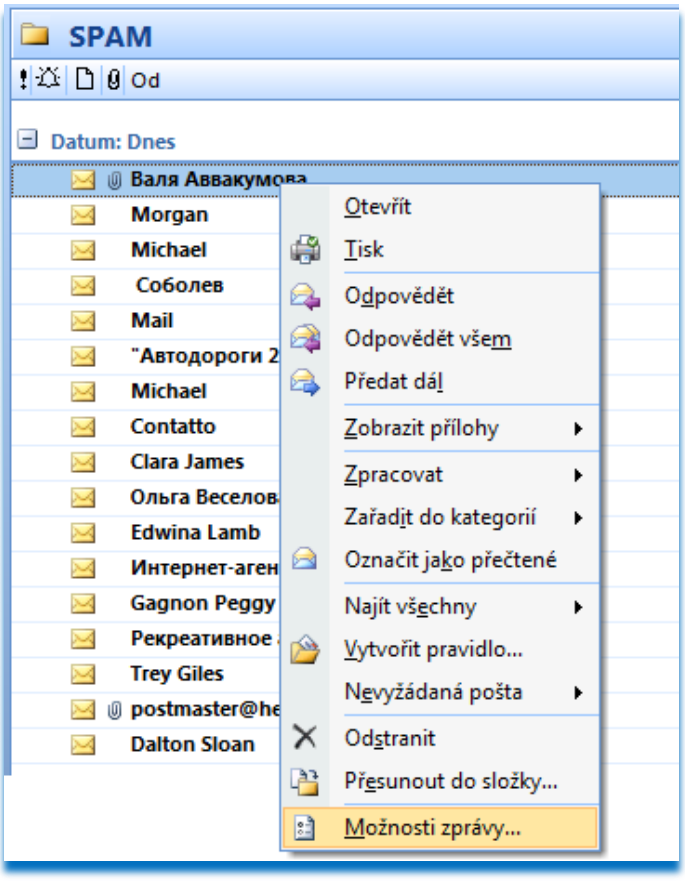
Hlavička	***Význam***
Received:	*Viz výše*
From:	*Odesilatel (autor)*
Sender:	*Vyřizuje (sekretářka)*
Date:	*Datum odeslání* *(Den, datum, čas a časová zóna)*
Reply-To:	*Odpověď zasílejte na*
To:	*Adresát*
Cc:	*Na vědomí*
Bcc:	*Na vědomí (tajná kopie - tato hlavička* *se před odesláním zruší)*
Message-Id:	*Identifikace zprávy*
In-Reply-To:	*Odpověď na*
Keywords:	*Klíčová slova charakterizující obsah*
References:	*Další odkazy*
Subject:	*Věc* *(krátká charakteristika obsahu zprávy)*
Comments:	*Komentář*
Encrypted:	*Šifrováno (zastaralé)*
X-	*Uživatelsky definovaná hlavička* *(uživatelem se rozumí autor software)* *Např. X-Mailer se často používá* *pro specifikaci programu, kterým* *odesilatel odesílá zprávu*

Resent-	*Při automatickém předávání (forward) zprávy se před původní hlavičky vloží řetězec Resent-* *Např.Resent-From nebo Resent-Cc apod.*

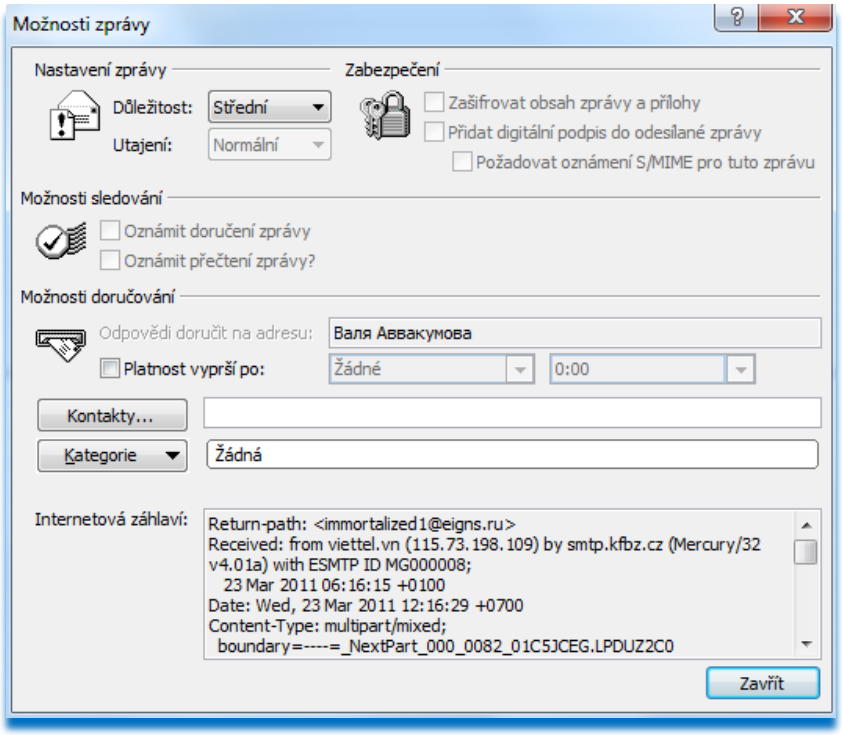
[21]

Struktura a ukázka MIME formátu je zde uvedena, protože se často jedná o falšovaný údaj v nevyžádané zprávě. Falšování MIME, patří k základním obranám spammerů. Naprosto běžnou praxí je, že příjemce emailové zprávy je i zároveň jejím odesílatelem (samozřejmě se jedná o falešnou hlavičku mailu), jak je potom možné takovou adresu dát do seznamu zakázaných příjemců a zabránit tak dalšímu příjmu spamu? Existují samozřejmě postupy, které MIME a hlavičku analyzují a v případě odhalení spammera, je taková zpráva vyřazena z příjmu, ale o těchto možnostech až dále.

Na hlavičku emailu se dá podívat relativně jednoduše, stačí třeba v emailovém klientu Microsoft Office Outlook 2007 kliknout pravým tlačítkem myši na zprávu a dát položku **Možnosti zprávy**.



Obr. 18. Položka **Možnosti zprávy**



Obr. 19. Možnosti zprávy

Na obrázku č. 19. Vidíme ve spodní části okna položku **Internetová záhlaví**, která obsahuje detailní výpis hlavičky emailu, můžeme se tak podívat od koho, komu, kudy apod… zpráva šla. Nevýhodou je lehké zfalšování MIME hlavičky.

2.3.1 Blacklist a whitelist

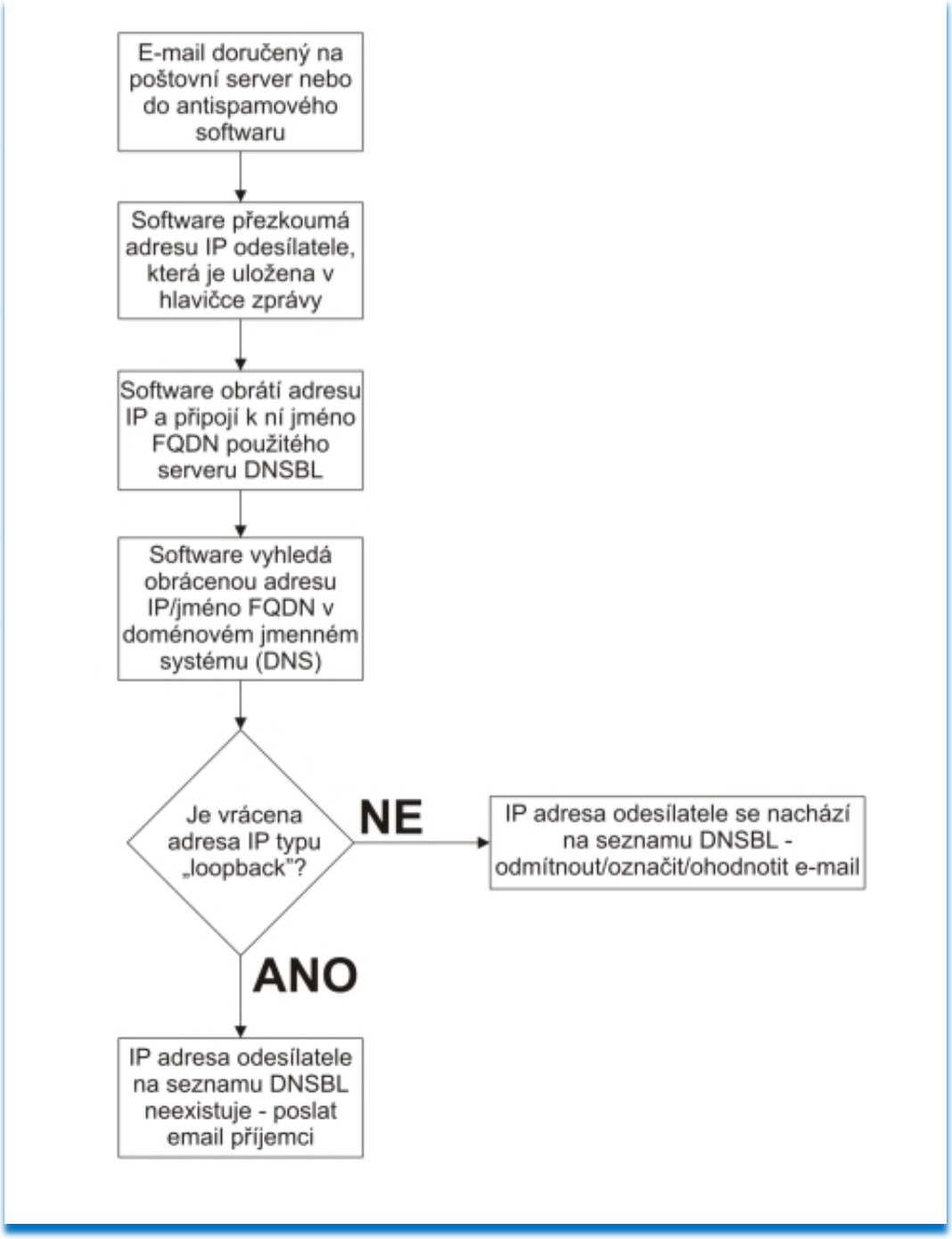
Černé a bílé seznamy se v posledních letech staly oblíbeným mechanismem pro dohled nad spamem. Téměř všechny balíčky, které jsou dnes k dispozici, a to bez ohledu na to, zda jsou distribuovány komerčními společnostmi nebo jsou k dispozici ve formě freewaru, sharewaru nebo projektů typu „open source" (otevřený software), mají nějakým způsobem integrovánu možnost použít černých/bílých seznamů.

Seskupování známých rozesílatelů spamu na černé seznamy představuje jednoduchý způsob jak rychle a účinně blokovat nevyžádaný obsah na základě původu odesílatele. Černé seznamy mohou obsahovat přesné elektronické adresy (jako např. spmaster@spam.tld), variace e-mailových adres vyjádřené pomocí standardních zástupných znaků nebo regulérních výrazů (např. @spam.tld, [0-9] [0-9] [0-9] [0-9]@spam.tld nebo getrichquick@.com) nebo dokonce seznamy adres IP.

Existují dva rozdílné typy černých seznamů: na bázi sdílené sítě a na bázi místní databáze. Vzhledem k nesmírnému počtu odesílatelů spamu a k obtížím souvisejícím s udržováním

účinného, neustále aktualizovaného seznamu, vynesli mnozí provozovatelé své zdroje na světlo a sdílejí je přes síť s jinými, čímž zjednodušují jejich zpracování a snižují zátěž a velikost úložiště pro svá data. Lokální databáze s černými seznamy se běžně nacházejí v souborech programů pro filtrování spamu a rozšiřují účinnosti těchto řešení. [5]

Černým seznamům obsahujícím DNS údaje (IP adresy, názvy domén) se často přezdívá DNSBL. Princip činnosti DNSBL nastiňuje tento diagram.



Obr. 20. Vyhodnocení zprávy pomocí blacklistu (s využitím SMTP protokolu)

Kritéria výběru na černý seznam DNS:

- *Seznam otevřených poštovních serverů*
- *Seznam otevřených serverů proxy*
- *Seznam známých rozesílatelů spamu*
- *Seznam vytáčených uživatelů*

Seznam otevřených poštovních serverů

Seznam otevřených poštovních serverů je jednou z nejpopulárnějších forem DNSBL. Systém je brán jako otevřený, pokud dovoluje neautorizovaným uživatelům rozesílat elektronickou poštu třetím stranám. To znamená, že ani osoba odesílající zprávu, ani osoba přijímající zprávu není uvedena uvnitř domény, pro kterou systém funguje jako poštovní server. [5]

Dříve byly takto nakonfigurované mnohé emailové servery. Označení takových serverů je Open Relay. *SMTP server, který funguje jako open relay, převezme k dopravě jakýkoli dopis bez ohledu na odesílatele i adresáta. Open relay usnadňuje rozesílání spamu tím, že umožňuje přijmout dopis (spam) odkudkoli a dopravit jej kamkoli, často je jeden dopis adresován na stovky cílových adres. Tím jednak snižuje zátěž na straně spammerova rozesílacího robota, jednak se průchodem přes open relay zamaskuje IP adresa, odkud dopis přišel, což silně ztěžuje filtraci spamu na straně cílového SMTP serveru.*

SMTP server by měl být konfigurován tak, aby nepřebíral k dopravě dopisy, které přicházejí z vnějšku domény (domén) a nemají adresáta uvnitř domény, kterou server pokládá za „vlastní“. [22]

Dnes už je většina serverů výhradně pro uživatele daného ISP. Všimněte si, že když budete nastavovat svého poštovního klienta, vyplňujeme položku **SMTP server** ne jako server, kde máte tvořenou schránku, ale jako server od koho máte poskytován internet.

Příkladem mám-li email u poskytovatele **www.centrum.cz** nevyplňuji smtp server jako **smtp.centrum.cz**, ale smtp server podle poskytovatele internetu příkladem **smtp.o2isp.cz** (platí pro ISP Telefónica O2). Poštu sice stahujete přes **pop3.centrum.cz**, ale odesíláte přes **smtp.o2isp.cz**. Zdá se to být domotané, ale je to logické, že www.centrum.cz nemá poštovní server v open relay módu, tím se chrání, aby se nedostal na světové blacklisty, a aby spammeři skrze něj nemohli zasílat neidentifikovatelný spam.

Seznam otevřených serverů proxy

Otevřené servery proxy jsou snad ještě horší než otevřené poštovní systémy. Služba proxy (zplnomocnění) ve světě sítí se podobá principu zplnomocnění v reálném světě – tj., existuje někdo nebo něco, kdo funguje jako náhrada za někoho nebo něco jiného. V tomto případě službu proxy vykonává síťové zařízení nebo server, který zprostředkuje spojení k síťovému zdroji pro koncového uživatele, místo toho, aby se uživatel připojil přímo ke zdroji sám. [5]

Teď trošku lidsky o tom co to je proxy a jako službu poskytuje. Proxy server má za úkol, převzít od Vás požadavek a do internetu jej poskytnout přes sebe. To znamená, že anonymizuje Vaši IP adresu a další údaje. Ano, občas je takový přístup výhodou, ale je-li zneužíván k rozesílání spamu, bez možnosti odpovědnosti už to tak v pořádku není.

Seznam známých rozesílatelů spamu

Seznamy známých rozesílatelů spamu jsou domény, systémy nebo sítě známé jako skrýše pro tvůrce spamu. Na rozdíl od otevřených poštovních systémů a otevřených serverů proxy nejsou tyto na seznamu z technologických příčin, ale proto, že již někdy spam odeslaly.

Seznam vytáčených uživatelů

Myšlenka, která se ukrývá za seznamy vytáčených uživatelů, je snaha znemožnit takzvaný „spam trespassing“. Tento termín používá organizace provozující systém pro ochranu před zneužíváním elektronické pošty – Mail Abuse Prevention System (MAPS) a znamená, že se odesílatel vytáčenou linkou připojí na poskytovatele ISP (pokud možno přes falešný „testovací“ účet) se systémem, na kterém běží poštovní server nebo tzv. „ratware“ a odešle masový e-mail. Tímto způsobem se odesílatel dostane mimo dosah tradičních metod pro detekci spamu. Odesílatel využívá síťové zdroje poskytovatele ISP, ale nikoliv jeho serverové zdroje. Seznamy tohoto typu také často zahrnují i jiné účty poskytovatele, které mají dynamické adresy IP. Jako jejich příklad mohou sloužit kabelové modemy a digitální linky DSL. [5]

Mezi nejznámější blacklistové databáze patří databáze spamhaus.org, dsbl.org, sorbs.net, spamcop.net a njabl.org.

Nevýhodou blacklistů je jejich permanentní potřeba aktualizace, rychlost jakou spammeři mění adresy, z nichž se rozesílá spam, někdy se zdá být neúčinné do databáze vpisovat adresu spammera, protože ten přes ni vychrlí do internetu milion zpráv a změní ji na jinou. Další nevýhodou je když se do blacklistu dostane IP adresa poskytovatele freemailu,

protože přes něj někdo odešle dostatečné množství spamu, ale co ostatní majitelé poštovních účtů u tohoto poskytovatele? Zde přináší částečnou pomoc bílé seznamy tzv. whitelisty.

Bílý seznam je jednoduše přesný protiklad černého seznamu. Černý seznam identifikuje odesílatele, jehož sdělení jsou nežádaná, protože při předchozích příležitostech rozesílal spam. Bílé seznamy definují známé odesílatele, kteří i když pošlou něco, co by mohlo být označeno jako nevyžádaná pošta, mají právo projít bez filtrování. [5]

Opět můžeme užít víceúrovňové kombinace blacklistů a whitelistů. Je víc než důležité ve filtrování předřadit whitelist před blacklist. Vynutíme tím totiž průchod zprávy naším kontrolním místem, kdyby to bylo přesně naopak, zpráva by byla vyřazena na blacklistu a k whitelistu by se nikdy ani nedostala. Naprosto běžnou praxí je na blacklistu uvedena IP adresa poskytovatele ISP a na whitelistu emailová adresa někoho, kdo je u daného ISP registrován.

O tom, zda je nějaká IP adresa (nebo doména) na některém z předních blacklistů je možno se lehce dozvědět na kontrolních stránkách, jedna z takových stránek je třeba na serveru Paranoia.cz na odkaze http://www.paranoia.cz/tools/blacklist.

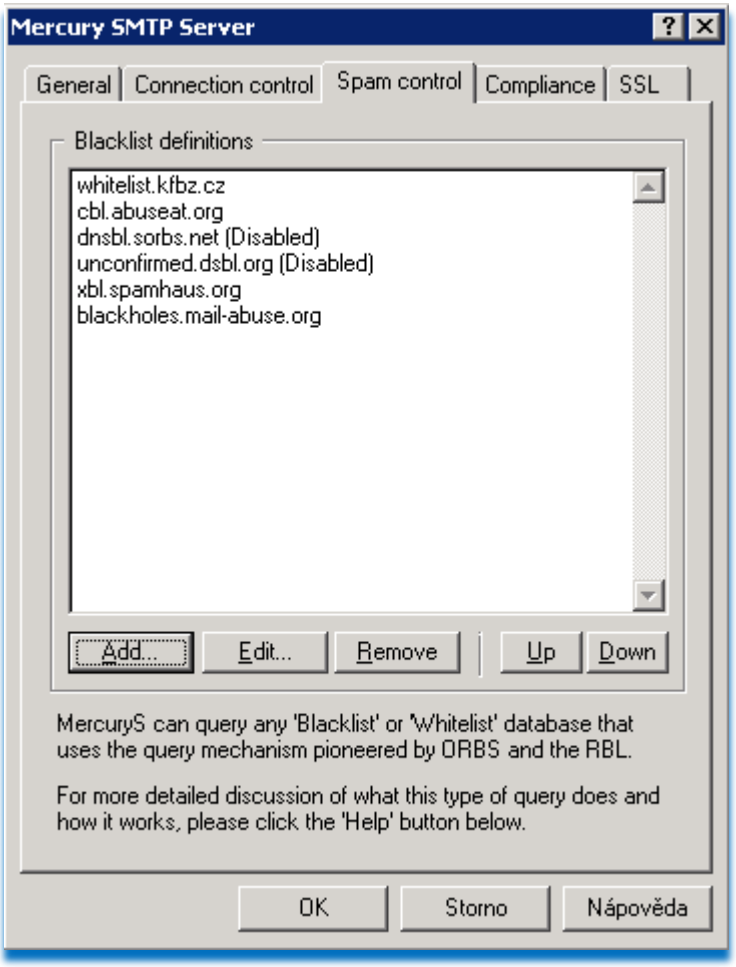
O tom zda jsou blacklisty účinné se vedou vleklé spory, jedna skupina se přiklání k názoru, že doby kdy blacklisty pomáhaly, jsou dávno pryč, druhá skupina lidí se stále přiklání k tomu, že kdyby měly blacklisty odrazit jen pár procent spammu, má jejich údržba smysl. Blíže se této problematice věnují články na Lupa.cz, odkazy na tyto články jsou zde: http://www.lupa.cz/clanky/nepouzivejte-ip-blacklisty-1/ http://www.lupa.cz/clanky/nepouzivejte-ip-blacklisty-2/.

Praktické zkušenosti s blacklisty v Krajské knihovně F. Bartoše, p. o. ve Zlíně jsou následující:

Počet SMTP spojení za 24 hodin	3695
Počet emailů vyřazených na blacklistech	1382
Počet emailů přijatých poštovním serverem	522

Tab. 3. Funkčnost blacklistů (reálné údaje z 22.3.2011)

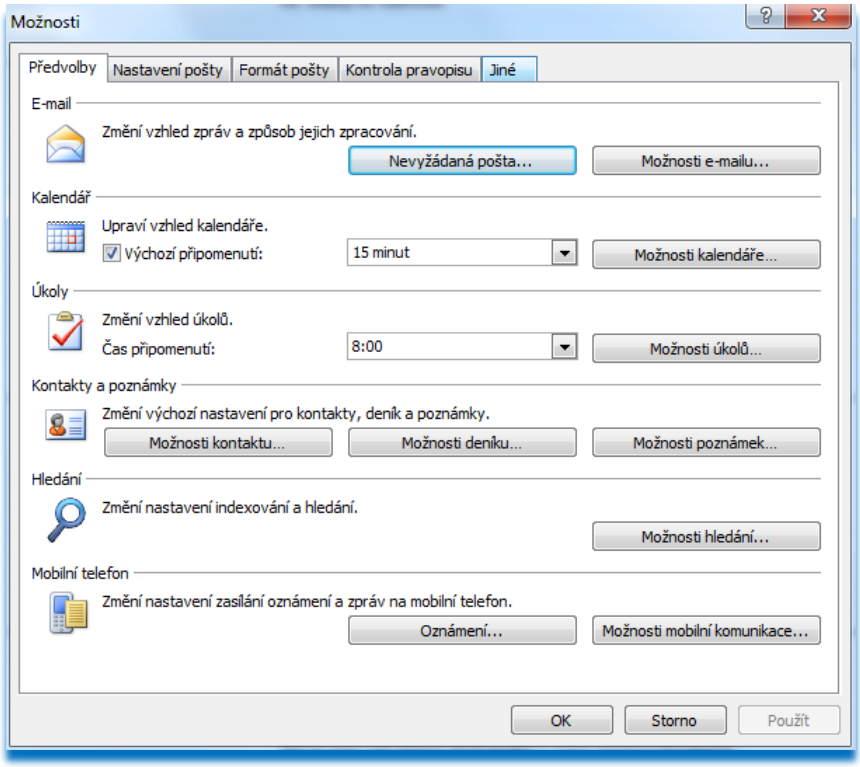
Nakonfigurování blacklistů a whitelistů se může zdát obtížné, nicméně jedná se opravdu o velice jednoduchou operaci. Ukážeme si konfiguraci na poštovním serveru Mercury (www.pmail.com), jedná se o volně šiřitelný poštovní server.



Obr. 21. Konfigurace DNSBL v Mercury Mail Serveru

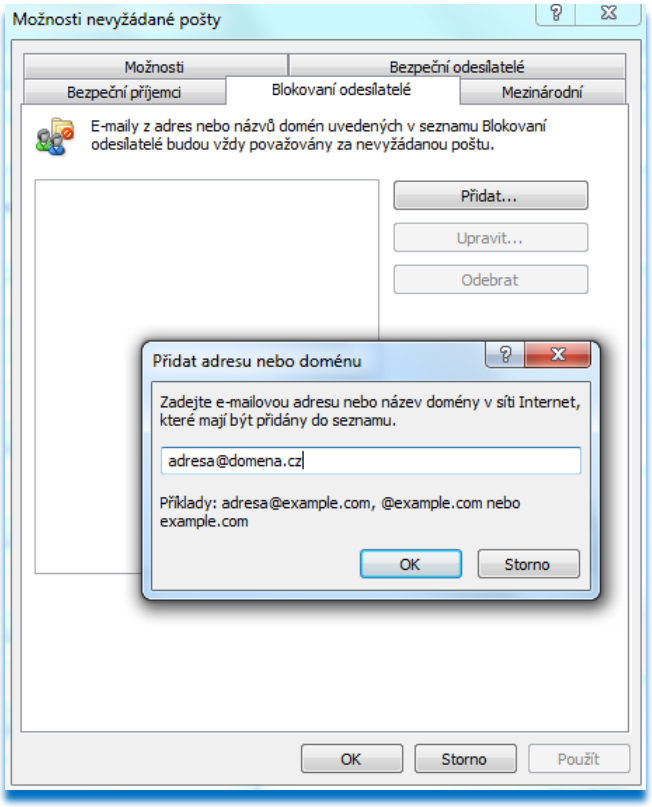
Z obrázku je patrné, že stačí uvést adresu DNSBL a maily se hned prověřují vůči těmto blacklistů, dále si všimněme skutečnosti, že whitelist knihovny je na první pozici, před všemi blacklisty. V detailech blacklistů lze nastavit, zda se jedná o blacklist nebo whitelist, zda a jaká hláška se má odesílateli zobrazit apod…

Stejně tak lze nastavit blacklist a whitelist na klientském poštovním programu, jako ukázku si vybereme Microsoft Office Outlook 2007. Stačí v programu zvolit menu **Nástroje – Možnosti** a kartu **Předvolby**.



Obr. 22. Možnosti aplikace Microsoft Office Outlook 2007

Dále už stačí jen kliknout na tlačítko **Nevyžádaná pošta** a můžeme začít zařazovat adresy a domény do seznamů.



Obr. 23. Seznam blokovaných odesílatelů

V této aplikaci se blacklist nazývá **Seznam blokovaných odesílatelů** a lze do něj zapisovat přímo emailové adresy, z kterých chodí spam, nebo celé domény. Na kartě pod názvem **Bezpeční odesílatelé** je veden whitelist s adresami, které mají vždy projít.

2.3.2 Greylist

Tato technologie je ve svém základu velice jednoduchá a značně úspěšná, udává se až 95%. Využívá možností SMTP protokolu a chování poštovních serverů. MTA poštovního serveru řeší výměnu emailů mezi poštovními servery, pokud nelze zprávu doručit (identifikováno podle SMTP Error kódu), zařadí ji do fronty a zkusí to později. To samozřejmě spammer nedělá, ten se snaží po připojení poslat co největší objem spamových zpráv a o jejich doručení se dál nestará. Greylist je nasazen na straně poštovního serveru v MTA. Vždy, když přijde požadavek na SMTP spojení, si systém zjistí tyto tři údaje:

- IP adresu poštovního serveru snažícího se o spojení
- Odesílatelovu emailovou adresu podle hlavičky
- Příjemcovu emailovou adresu podle hlavičky

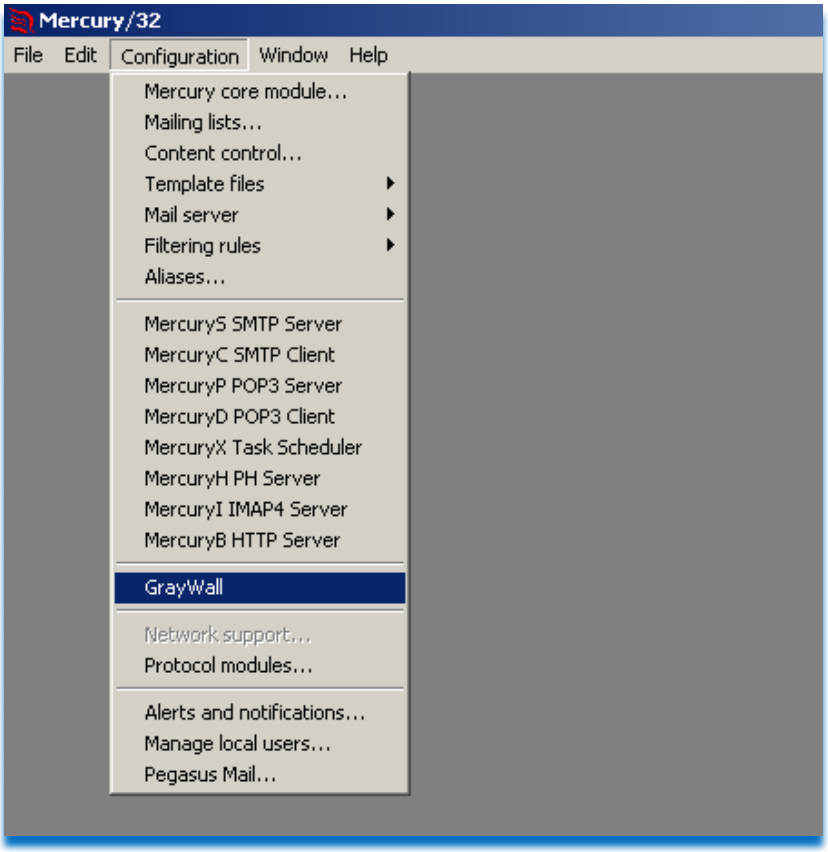
Porovná je s existujícími údaji v databázi (čekatelé na spojení), pokud takovou trojici nalezne a záznam v databázi je již starší, než minimální nastavený čas čekání pustí takovou zprávu rovnou na poštovní server ke zpracování, v jiném případě založí v databázi záznam s těmito údaji a připojí aktuální čas a odmítne spojení. Pokud by se jednalo o spam, už se žádost o spojení opakovat nebude, pokud se nebude jednat o spam zprávu, pokusí se jí poštovní server doručit znovu po nějaké době. Dokud nevyprší nastavená časová prodleva, mezi prvním kontaktem a předpokládaným přijetím emailu emailový server (většinou 1 hodina), jsou všechny SMTP požadavky na spojení pro tuto trojici odmítány. Pokud se i po hodině opakuje SMTP požadavek je pravděpodobné, že se nejedná o spam, zpráva je přijata na poštovní server a v databázi se nastaví jiný časovač, tentokrát třeba na délku 14 dní a po tuto dobu jsou maily s touto trojicí identifikátorů automaticky vpuštěny rovnou na emailový server ke zpracování. S každou novou zprávou s touto trojicí identifikátorů se 14ti denní cyklus obnovuje. Logicky z toho vyplívá, že hodinová prodleva je jen při první komunikaci. Pokud se trojice během 14ti dní neobnoví, je smazána a je na ní příště nahlíženo jako na nový záznam v databázi (nové SMTP spojení). Aby záznamy v databázi nenarůstaly (hlavně ty spammerské) může být každých 8 hodin záznam smazán, pokud nebyl od jeho prvního kontaktu server kontaktován opakovaně.

Celý systém má velkou výhodu těžící z toho, že spammeři neútočí z jednoho místa vícekrát (až na výjimku open relay a proxy systémů), nicméně ty lze omezit na blacklistu. Greylist jako takový je sice samostatný systém, ale bez blacklistu by nebyl plně účinný. Další velkou výhodou je, že se odmítá SMTP spojení, ještě před přenosem dat, takže to značně ulehčí při omezené kapacitě sítě.

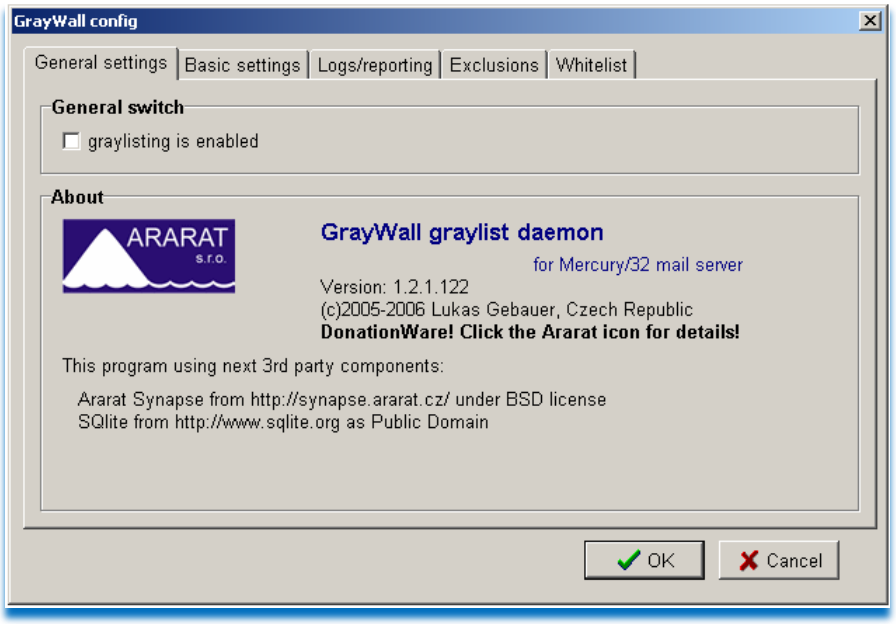
Za jedinou nevýhodu greylistu, lze považovat prvotní hodinovou prodlevu. Tuto nevýhodu je možno částečně odstranit zápisem IP adres a emailových adres do whitelistu. Ve whitelistu zapsané adresy jsou bez uložení v greylistové databázi ihned poslány na poštovní server (mají výjimku).

Tento systém se nastavuje výhradně na poštovní servery, neboť u poštovních klientů by neměl smysl. Ukázka nastavení pro poštovní server Mercury se jmenuje GrayWall a jeho popis lze najít na http://community.pmail.com/files/folders/mercadd/entry3505.aspx.

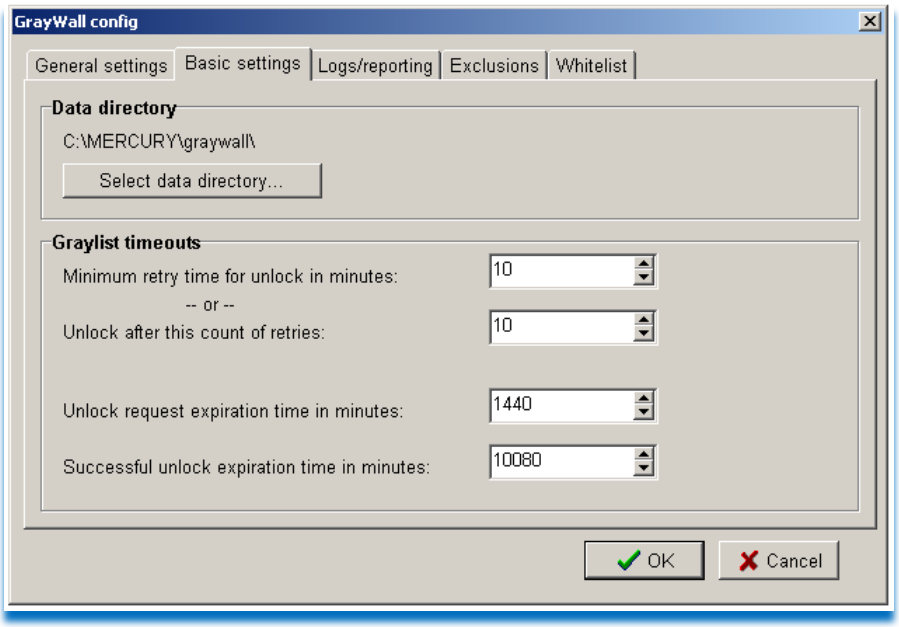
Jeho instalace i konfigurace je velmi jednoduchá. Položka je obsažena už v základní instalaci poštovního serveru Mercury.



Obr. 24. Ukázka umístění modulu GrayWall (greylistu) v Mercury Mail Serveru



Obr. 25. Zapnutí/vypnutí funkce greylistu



Obr. 26. Základní nastavení greylistu

Nejdůležitější kartou při nastavování GrayWallu je karta **Basic settings**, kde lze nastavit délky časovačů. Dále jsou zde karty **Logs/reporting** pro logování, hloubku logování (debugging) a SMTP hlášku, která se má odeslat čekajícímu serveru, při prvním pokusu o spojení. Karta **Exclusions** poskytuje možnost vyloučení IP adres (rozsahů IP adres/masek) nebo domén pro, které je greylist zřízen. Není vhodné, aby i lokální emaily čekaly na greylistu. Poslední kartou je **Whitelist**, lze jej zadat URL adresou (odkaz na uložený whitelist v Internetu), lze nastavit i pravidelnou automatickou aktualizaci.

Praktické zkušenosti s greylistem v Krajské knihovně F. Bartoše, p. o. ve Zlíně jsou následující:

Počet SMTP spojení za 24 hodin	3378
Počet emailů přijatých po 60 minutovém zdržení	413
Počet spamových emailů přijatých poštovním serverem	18

Tab. 4. Funkčnost greylistu (reálné údaje z 10.3.2011)

Podle praktické ukázky je greylisting velice kvalitním a funkčním nástrojem, jeho jedinou nevýhodou je časové zpoždění při příjmu první zprávy z určeného emailového účtu (což může hlavně v obchodním prostředí být velkým problémem).

2.3.3 Bayessova analýza

Thomas Bayes *(1701–1761) byl anglický duchovní, dnes známý především pro formulaci tzv. Bayesovy věty, která udává, jak podmíněná pravděpodobnost nějakého jevu souvisí s opačnou podmíněnou pravděpodobností.* [23]

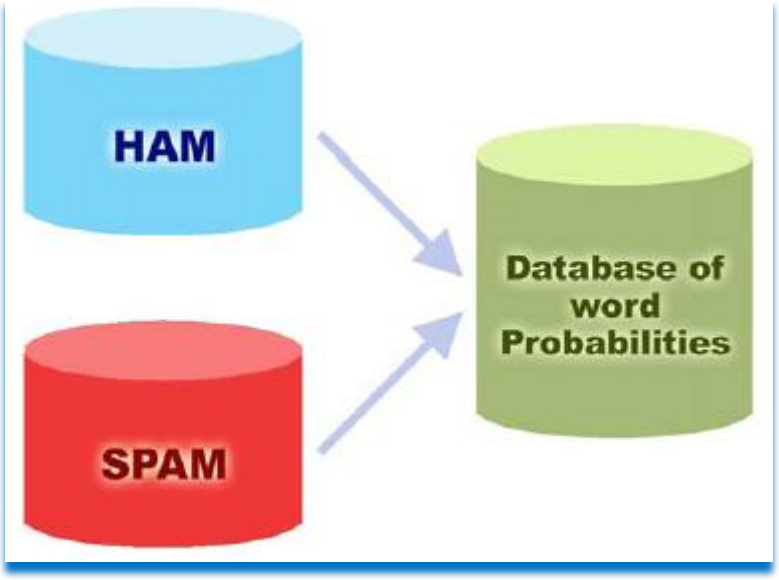
Bayesovu větu *lze formulovat takto:*
Mějme dva náhodné jevy A a B s pravděpodobnostmi P(A) a P(B), přičemž P(B) > 0. Potom platí

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)},$$

kde P(A|B) je podmíněná pravděpodobnost jevu A za předpokladu, že nastal jev B, a naopak P(B|A) je pravděpodobnost jevu B podmíněná výskytem jevu A. [24]

Bayesova analýza je tedy hodnotou pravděpodobnosti. Tuto hodnotu získáváme výše uvedeným výpočtem ze statistického výskytu znaků, slov a statí v přijímaných emailech.

Bayesovo filtrování je založeno na principu odlišnosti většiny událostí a pravděpodobnosti toho, že jedna událost bude shodná s budoucím výskytem stejné události. Stejnou techniku lze využít při hodnocení spamu. Jestliže je výskyt konkrétního textu ve spamu častější, než je tomu u validní pošty, a objeví se nová zpráva s tímto textem, můžeme takovou zprávu logicky považovat za spam.



[25]

Obr. 27. Skladba Bayesovy databáze

Tvorba databáze je náročný a zdlouhavý proces. Pro kvalitní naučení Bayesova filtru je potřeba trénovací množinu zpráv. Trénovací množina zpráv musí obsahovat minimálně 200 spamů a 200 hamů, aby byl filtr schopen připravit si základní databázi. Většinou se k těmto účelům použijí poštovní složky uživatele, kde přijatá a odeslaná pošta slouží pro tvorbu databáze hamu a složka se spamem pro databázi spamu. Nesmíme zapomenout na to, že Bayesova analýza neprovádí analýzu slov jen z těla zprávy (BODY), ale i z prvků z hlavičky (MIME).

Pravděpodobnost se počítá zhruba následovně: Jestliže se slovo „hypotéka" objeví ve 400 z 3 000 spamů a pouze v 5 ze 300 legitimních zpráv, tak hodnota pravděpodobnosti dosáhne čísla 0,8889 (tj.: [400/3000] děleno [5/300 + 400/3000]). [25]

Doba, po kterou by se měl Bayesův filtr učit je minimálně 14 dní. Čím větší a čím kvalitněji rozdělená data na spam a ham Bayesovu filtru poskytneme, tím lepší detekci spamu můžeme očekávat.

Velkou výhodou Bayesových filtrů je jejich adaptivnost. To, že se filtr naučil z trénovací množiny, neznamená, že se během provozu (třídění zpráv) dále neučí.

Příkladem: filtr se naučil rozpoznávat spam podle slova **Sex**, v případě, že by přišel email s obměnou tohoto slova třeba **5es** nebo **S e X**, nebyl by filtr schopen mail rozpoznat jako spam. Vzhledem k tomu, že Bayesův filtr nefunguje jen na základě výskytu jednoho slova, ale na skutečnosti, že sčítá hodnoty pravděpodobností výskytu spamových a hamových slov je schopen kvalifikovaně rozhodnout. Mez, kterou filtr detekuje spam, lze uživatelsky

nastavit – říká se jí prahová hodnota, je to hranice mezi spamem a hamem. V našem případě označí email jako spam kvůli výskytu dalších slov (jiných než **sex**), která limitují email jako spam (prahová hranice pro spam byla překročena součtem hodnot pravděpodobností). Samozřejmě si při této operaci vloží do databáze další klíčová slova z mailu, příkladem slovo **5ex**. Další analýzy budou prováděny už i s tímto slovem a podle četnosti výskytů v přijímaných emailech bude hodnota pravděpodobnosti tohoto slova růst.

Uživatel může vždy zasáhnout a email Bayesovým filtrem označený jako spam, může pokládat za ham. V takovém případě na to reaguje Bayesův filtr přepočítáním všech hodnot pravděpodobností vyskytovaných znaků, slov a statí.

Čím déle se takto Bayesův filtr používá, tím kvalitnější je jeho detekce.

Bayesův přístup je při posuzování spamu velmi efektivní – v květnu 2003 informoval článek BBC o faktu, že Bayesova technologie může dosáhnout přesnosti 99,7% při minimálním množství falešných pozitiv.

Výhody Bayesových filtrů:

- ***Bayesova metoda bere v úvahu celou zprávu*** *– Rozpoznává slova, která identifikují spam, ale i slova, které označují validní zprávu.*
- ***Bayesův filtr se neustále zdokonaluje*** *– Učením z nového spamu i validní odesílané pošty se Bayesův filtr vyvíjí a přizpůsobuje novým praktikám spammerů.*
- ***Bayesova technika je citlivá k uživateli*** *– Aby spam dosáhl svého adresáta, musejí spammeři zasílat takové emaily, jenž filtry objetí nezastaví. Jelikož Bayesovo filtrování bere v úvahu profil firemních emailů, rozpoznává spam daleko snadněji: tento profil by spammeři museli k obelstění filtru znát. Ale protože spam používá svůj vlastní slovník a charakter, na Bayesův filtr si jen tak nepřijde.*
- ***Bayesova metoda je multilingvální*** *– Bayesův antispamový filtr může být – díky adaptabilitě – použit pro jakýkoliv jazyk.*
- ***Oklamání Bayesova filtru je obtížnější než oklamání filtrování klíčových slov*** *– Pokročilý spammer, který chce Bayesův filtr obejít, může buď použít méně slov ukazujících na spam (např. Viagra, Cash, atd.) nebo použít více slov identifikujících validní email (platné jméno z kontaktů, apod.). Provedení druhého způsobu můžeme vyloučit, jelikož spammer nemůže znát poštovní profily jednotlivých příjemců, a ani nikdy nemůže v získání takových informací doufat.* [25]

Nevýhody Bayesových filtrů:

Jediným obecně známým problémem Bayesových filtrů je paradoxně snaha firmy Microsoft o rychlejší ochranu klientů, tím že dodává v programech Microsoft Outlook Express, Microsoft Office Outlook a Internet Message Filtr pro Microsoft Exchnage server už integrovanou databázi hamu. Toto řešení má jednu výhodu a to tu, že systém je hned po instalaci schopen fungovat a třídit emaily, nevýhodou je však, že se spammerům dostal do ruky seznam hamu a je tak lehčí napsat spamový email, který bude schopen tímto filtrem v těchto programech projít. Je nutno podotknout, že po určité době se databáze hamu stane z univerzální spíše klientskou a to během příjmu a odesílání zpráv, univerzální databáze se pomalu bude učit a přizpůsobovat emailům klienta (databáze se adaptuje na nové prostředí), nicméně než se tak stane, může se stát, že bude spam a ham detekován chybně. Záleží jen na uživateli jak rychle a kvalitně si filtr vycvičí.

Jiné nevýhody nejsou zatím známy.

Nesmíme však zapomenout, že to jak kvalitní náš Bayesův filtr bude, záleží hlavně na nás, jak kvalitně budeme naše emaily třídit na spam a ham v době učení. Doba učení je minimálně 14 dní a minimálně po tuto dobu musíme být opravdu trpěliví a svědomití v práci učitele. Práce se jistě zúročí, hned jak začne filtr sám rozhodovat co je spam a co ham.

Praktické zkušenosti s Bayesovým filtrem v Krajské knihovně F. Bartoše, p. o. ve Zlíně jsou následující:

Filtr se učil standardních 14 dní a analyzoval maily od začátku měsíce prosince 2010. Data za prosinec 2010 (přijatých zpráv 6925, odeslaných zpráv 4864, spamových zpráv 3004) – celý měsíc prosinec. **Údaje jsou za leden 2011, kdy byl Bayesův filtr v ostrém provozu.**	
Správně rozpoznaných mailů (ham a spam)	96,43%
Špatně detekováno (ham a spam) – chybovost	1,72%
Nerozpoznaných mailů (propuštěný spam)	1,85%

Tab. 5. Funkčnost Bayesova flitru (reálné údaje z období od 1.1. – 1.2.2011)

Bayesovy filtry jsou považovány za elitu v potírání spamu.

2.3.4 Filtrování obsahu

Filtrování podle obsahu bylo základní zbraní proti spammerům. Jednalo se vlastně o první technologii v boji proti spamu. Jedná se o statické pravidlo, kterému je podrobena každá zpráva zpracovávaná poštovním serverem. Filtrování obsahu má určité výhody, mezi které bezesporu patří jednoduchost, rozšiřitelnost, transparentnost a hlavně možnost lehce ovlivnit co bude s výsledkem (kontrolovaným mailem) provedeno. Mezi základní nevýhody této technologie patří nutnost zprávu přijmout (pak se teprve provádí její analýza), časem je seznam pravidel velice dlouhý, brzo se seznam stává neúčinným (pokud není pravidelně aktualizován a doplňován).

Pravidla pro filtrování obsahu mají mnoho možností, je však potřeba si dobře promyslet nasazovaná pravidla, ne vždy úmysl zrcadlí výsledek.

Praktické zkušenosti s filtrováním obsahu v Krajské knihovně F. Bartoše, p. o. ve Zlíně jsou následující:

V kontrole obsahu jsou zahrnuty všechny níže popisované postupy (hlavička a MIME, předmět i obsah zprávy).	
Počet emailů přijatých poštovním serverem	522
Počet spamů smazaných podle filtrování obsahu	86
Počet spamů propuštěných dále k uživatelům	73

Tab. 6. Funkčnost filtrování obsahu (reálné údaje z 22.3.2011)

Tato jednoduchá pravidla dokážou redukovat příjem spamu i o 50%.

2.3.4.1 Podle hlavičky a MIME

Operace zahrnuje prověřování hlavičkových polí a MIME. Můžeme kontrolovat pole FROM (odesílatel), pole TO (příjemce), můžeme kontrolovat, zda souhlasí zvolená jazyková sada s textem v těle zprávy apod…

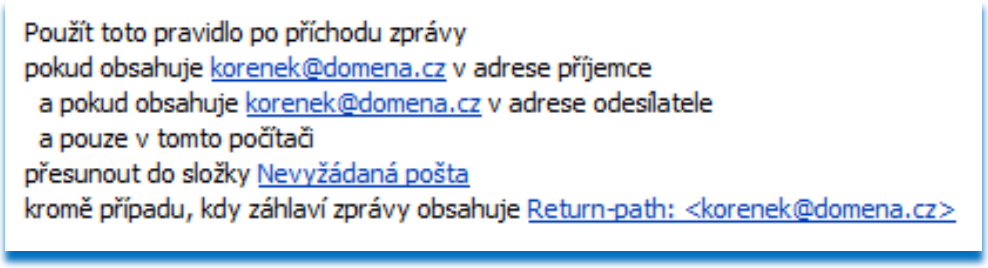
Nejčastěji je tato kontrola prováděna jen jako rutinní, kde se kontroluje, zda mail obsahuje všechny potřebné prvky hlavičky a MIME, pokud některý z nich chybí je zpráva podezřelá a systém se na ní dále zaměří.

Běžnou praxí spammerů je třeba, že odesílatel i příjemce emailové zprávy je stejná osoba. To by bylo ještě možno pochopit, že si někdo pošle mail sám sobě, hůř lze ale chápat jak může být v atributu RETURN-PATH jiná adresa, než odesílatele apod…

```
Return-path: <ekdiaz@cain.cl>
Received: from microsof-c20e5f (94.178.93.190) by smtp.domena.cz (Mercury/32 v4.01a)
with ESMTP ID MG0001C7;
   15 Jan 2011 12:51:13 +0200
Received: from  94.178.93.190 (account 0-commercial@marineland.fr HELO
tjvrjmn.qmeectuztq.va)
        by microsof-c20e5f (CommuniGate Pro SMTP 5.2.3)
        with ESMTPA id 743643259 for korenek@domena.cz; Tue, 15 Jan 2011 13:51:26 +0300
From: <korenek@domena.cz>
To: <korenek@domena.cz>
Subject: Buenas tardes
Mime-Version: 1.0
Content-type: text/html; charset="utf-8"
Content-Transfer-Encoding: 7bit
```

Obr. 28. Ukázka spamu detekovaného podle MIME

Na obr. 28 je vidět modifikovaná hlavička emailové zprávy (bylo nutno odstranit reálné údaje), ale i tak je patrné, že se údaje z **Return-path:**, **From:** a **To:** neshodují. Pokud by se jednalo o mail odeslaný z adresy korenek@domena.cz na adresu korenek@domena.cz musela by být tato adresa i v atributu Return-path.



Obr. 29. Aplikace filtrovacího pravidla v Microsoft Office Outlook 2007

Tímto jednoduchým pravidlem zabráníte, aby spamové zprávy procházeli až do vaší složky doručené pošty, těžko dáte asi svou emailovou adresu (adresu odesílatele) na černou listinu.

2.3.4.2 Podle předmětu zprávy

Velice podobný způsob třídění emailových zpráv jako u využití hlavičky MIME, zde máme jednu velkou výhodu a to že se limitujeme jen na jedno pole emailu. Anglicky je toto pole označeno jako SUBJECT.

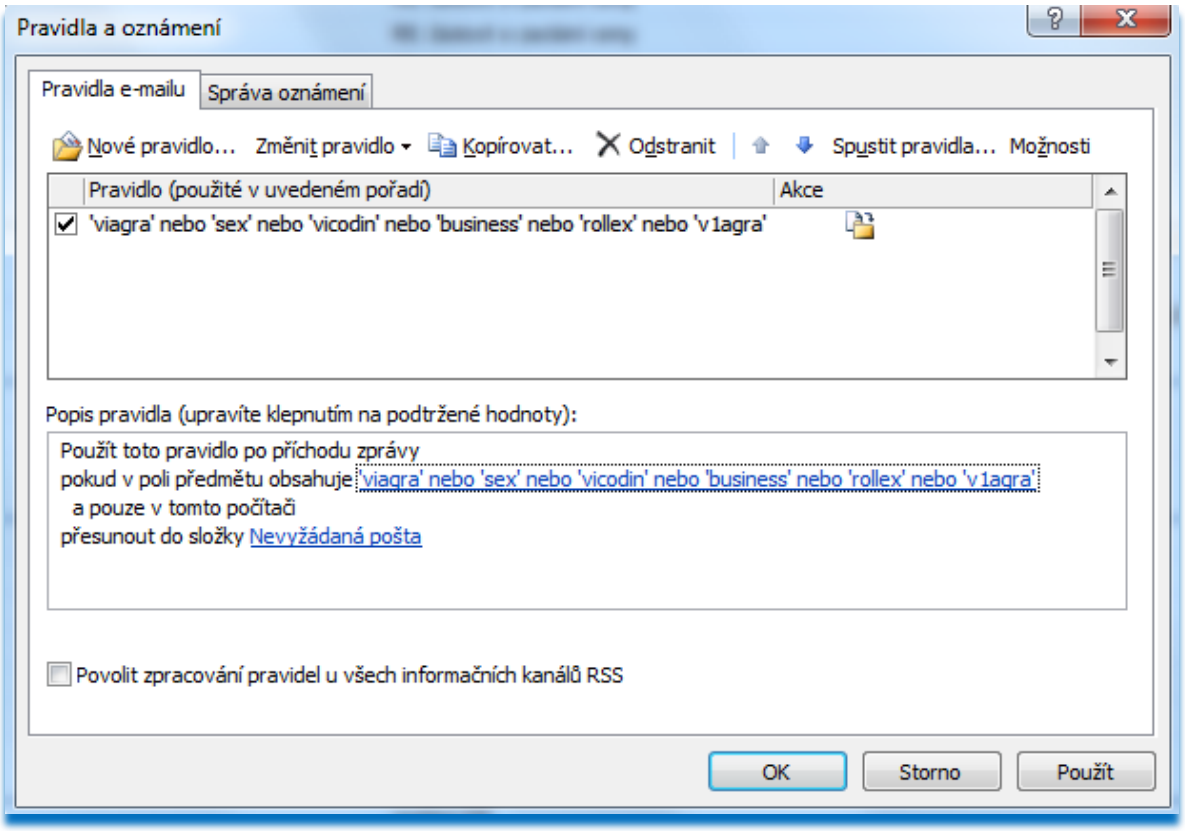
Do filtrovacích pravidel můžeme vkládat jak znaky, slova, tak celé věty. Občas se setkáme s možností, kdy nám jedno slovo vadí jen v určitém kontextu, v takovém případě je potřeba dobře popřemýšlet, než filtrovací pravidlo nastavíme.

Pokud budeme chtít pravidlo třeba, které omezí všechny zprávy se slovem **sex**, ale propustí všechny se slovem **sexting**, musíme pravidlo se slovem **sexting** předřadit, nebo nastavit pro takové slovo v předmětu výjimku.

```
If header "S" contains "Sale 70%" Delete ""
If header "S" contains "Beste Qualitaet" Delete ""
If header "S" contains "Low priced" SendTextFile "C:\\Program Files\\MERCURY\\spam.txt"
If header "S" contains "Low priced" Delete ""
If header "S" contains "Low-priced" Delete ""
If header "S" contains "Luxury Watches" Delete ""
If header "S" contains "oRo1exWatches" Delete ""
If header "S" contains "Werkzeug" SendTextFile "C:\\Program Files\\MERCURY\\spam.txt"
If header "S" contains "Werkzeug" Delete ""
If header "S" contains "Stir up your libido" Delete ""
If header "S" contains "We will call you back" SendTextFile "C:\\Program Files\\MERCURY\\spam.txt"
If header "S" contains "We will call you back" Delete ""
If header "S" contains "nur 1" Delete ""
```

Obr. 30. Část filtrovacích pravidel ze serveru Mercury v Krajské knihovně F. Bartoše

Všimněme si možnosti, že pokud si nejsme jisti, že tento předmět je 100% spam, můžeme na odesílatelovu emailovou adresu doručit obecnou zprávu o tom, že jeho mail byl z důvodu předmětu vyřazen jako spam. Dotyčný odesílatel pokud zprávu příjme (nejedná se o spammera), může předmět zprávy upravit a zprávu zaslat znovu.



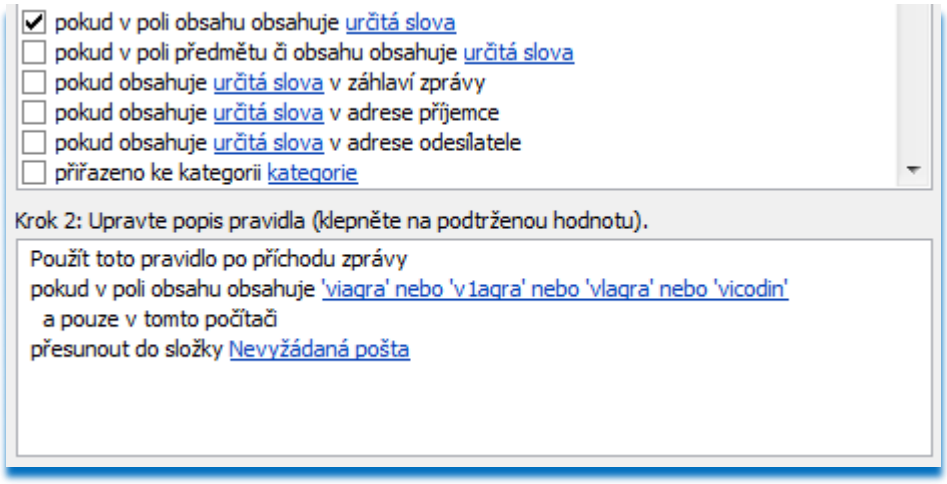
Obr. 31. Nastavení filtrovacího pravidla podle předmětu ve zprávě v aplikaci Microsoft Office Outlook 2007

Pro domácí účely je aplikace předmětového filtru v kombinaci s blacklistem plně dostačující. Nicméně, toto řešení není jen pro koncové stanice, lze jej efektivně nasadit i na serveru.

2.3.4.3 Podle obsahu v těle zprávy

Filtrování obsahu těla (BODY) zprávy je obdobné filtrování předmětu. Užívají se stejné mechanismy, častěji se využívá logický operátor AND i několikrát, vznikají tak vazby mezi určitými slovy, kterými detekujeme spam. Tyto pravidla se zřídka užívají samostatně, spíš se jedná o doplněk k jiné filtrovací technice.

Vzhledem k tomu, že většina mailů je dnes přenášena v HTML formátu, využívá se u této techniky, ne přímo vyhledávání klíčových slov, ale spíš kontrola (validace) HTML tagů (značek). Spammerům moc nezáleží na kvalitě provedeného mailu, spíš na jeho množstevním rozeslání a zde je možná slabina. Existují programy, které prochází tělo mailu a validují HTML použité tagy, pokud nejsou tagy správně uzavírány (což spammeři dost často dělají), klasifikují takové maily jako možný spam a podrobují jej dalším analýzám.



Obr. 32. Nastavení filtrovacího pravidla podle obsahu ve zprávě v aplikaci Microsoft Office Outlook 2007

2.3.5 Oceňování mailů – využití filtrování podle obsahu

Velmi zajímavou technikou, která využívá především filtrování podle obsahu těla zprávy je tzv. oceňování mailu (HITS). Je postaveno na skutečnosti, že email obsahuje znaky spamu, ale to ještě neznamená, že se musí jednat o spam.

Za každé takové slovo, které připomíná spamový email dostane email bodové ohodnocení, body se nakonec sečtou a pokud jsou přes přednastavenou hranici, je email vyhodnocen jako spam. Tuto hranici může uživatel zvolit, stejně tak může volit oceněný různých slov. Tato technika se nefixuje jen na prohlížení a bodování těla zprávy, ale na celý email.

```
X-Spam-Status: Yes, hits=35.2 required=5.0
X-Spam-Level: ++++++++++++++++++++++++++++++++++
X-Spam-Report: SA TESTS
 (analyzed by wiggum.onebit.cz)
  1.1 URIBL_RHS_DOB          Contains an URI of a new domain (Day Old Bread) [URIs: leadswhole.com]
  2.0 URIBL_BLACK            Contains an URL listed in the URIBL blacklist [URIs: leadswhole.com]
  1.9 URIBL_AB_SURBL         Contains an URL listed in the AB SURBL blocklist [URIs: leadswhole.com]
  1.5 URIBL_WS_SURBL         Contains an URL listed in the WS SURBL blocklist [URIs: leadswhole.com]
  1.5 URIBL_JP_SURBL         Contains an URL listed in the JP SURBL blocklist [URIs: leadswhole.com]
  1.5 URIBL_OB_SURBL         Contains an URL listed in the OB SURBL blocklist [URIs: leadswhole.com]
  3.5 BAYES_99               BODY: Bayesian spam probability is 99 to 100% [score: 1.0000]
  0.0 MISSING_MID            Missing Message-Id: header
  0.0 MISSING_DATE           Missing Date: header
  1.2 RCVD_IN_SORBS_DUL      RBL: SORBS: sent directly from dynamic IP address [62.21.51.101 listed
in dnsbl.sorbs.net]
  0.4 HTML_IMAGE_RATIO_02    BODY: HTML has a low ratio of text to image area
  1.6 HTML_IMAGE_ONLY_28     BODY: HTML: images with 2400-2800 bytes of words
  0.0 HTML_MESSAGE           BODY: HTML included in message
  1.5 MIME_HTML_ONLY         BODY: Message only has text/html MIME parts
  1.5 RAZOR2_CF_RANGE_E8_51_100 Razor2 gives engine 8 confidence level above 50% [cf: 100]
  2.0 RAZOR2_CHECK           Listed in Razor2 (http://razor.sf.net/)
  0.5 RAZOR2_CF_RANGE_51_100 Razor2 gives confidence level above 50% [cf: 100]
  3.7 PYZOR_CHECK            Listed in Pyzor (http://pyzor.sf.net/)
  2.7 DCC_CHECK              Listed in DCC (http://rhyolite.com/anti-spam/dcc/)
  1.3 RCVD_IN_PBL            RBL: Received via a relay in Spamhaus PBL [62.21.51.101 listed in
zen.spamhaus.org]
  3.0 RCVD_IN_XBL            RBL: Received via a relay in Spamhaus XBL
  3.0 URIBL_SBL              Contains an URL listed in the SBL blocklist [URIs: leadswhole.com]
  0.0 DIGEST_MULTIPLE        Message hits more than one network digest check
```

[26]

Obr. 33 Ukázka ocenění emailu, email je nakonec vyhodnocen jako spam

Na obr. 33 je vidět, že email obdržel **hits=32,5 bodů** a hranice je nastavena na **required=5 bodů**. Pod protokolem je výpis za co a kolik bodů email obdržel. Tato technika je skladbou všech předchozích uváděných technik a zakončuje tedy hromadně techniky filtrování obsahu emailů.

Tuto technologii hodně používají poskytovatelé volně zřizovaných emailových schránek tzv. poskytovatelé freemailů. Podle těchto hits scóre bodů je email mapován do složky doručených zpráv nebo nevyžádané pošty.

Výpis hlavičky ham zprávy u poskytovatele emailové služby na www.centrum.cz.

```
X-Virus-Scanner: This message was checked by ESET Mail Security
        for Linux/BSD. For more information on ESET Mail Security,
        please, visit our website: http://www.eset.com/.
X-CentrumSpamScore: +43
X-SpamDetected: 0
```

Atribut **X-CentrumSpamScore: +43**, tímto je detekováno, že se nejedná o spam, uvádí to i atribut **X-SpamDetected: 0**.

```
X-Virus-Scanner: This message was checked by ESET Mail Security
        for Linux/BSD. For more information on ESET Mail Security,
        please, visit our website: http://www.eset.com/.
X-Barracuda-Spam-Flag: YES
X-CentrumSpamScore: -79
X-SpamDetected: 1
```

U této zprávy je již situace jiná podle atributů je vidět, že skóre zprávy je -79 bodů a zpráva je i označena jako spam. Systém se může samozřejmě mýlit, nicméně poskytovatelé těchto emailových systémů zprávy nemažou, tuto operaci nechávají na uživatelích.

2.4 Praktická ukázka nasazení volně dostupných produktů

Nyní si ukážeme aplikace antispamových produktů, které se dají běžně najít v Internetu a jsou ke stažení buď v podobě freeware, open source nebo trial (zkušební) verze. Záměrně se zaměříme na platformu Windows, je přece jen více užívaná. Ukážeme si dva produkty pro koncové stanice (uživatele) a pak jeden produkt pro poštovní server.

2.4.1 SpamBayes

Program SpamBayes je open sourcový projekt, je vyvíjen pro operační prostředí Windows, Linux a MacOS. Stránky projektu jsou na http://spambayes.sourceforge.net/ zde je možno najít instalační soubory, zdrojové kódy i dokumentaci. Software je distribuován zdarma. My se zaměříme na vývojovou verzi pro Windows XP a 7, jedná se o **starší verzi 1.0.4** s integrací do Microsoft Office Outlook 2007. Je možno ji přímo stáhnout z tohoto odkazu http://sourceforge.net/projects/spambayes/files/spambayes/1.0.4/spambayes-1.0.4.exe.
Tato verze sice není nejnovější, ale za to je dobře odzkoušená a je k ní napsáno mnoho rad a návodů na Internetu. Instalační soubor má asi 3 MB.

Program se dá nainstalovat celkem se třemi moduly:

- Jako plugin ori Microsoft Outlook (MS Office Outlook musí být nainstalován)
- Server/Proxy aplikace pro POP3 poštovní klienty
- Server/Proxy aplikace pro IMAP poštovní klienty (jen v nejnovější verzi 1.1a6)

Instalace nepotřebuje žádné úpravy nastavení, proběhne sama automaticky (v instalaci nic neměňte). Před instalací je nutno mít nainstalovaný program Microsoft Office Outlook 2007.

Obr. 34 Uvítací obrazovka programu SpamBayes po startu aplikace Microsoft Office Outlook 2007

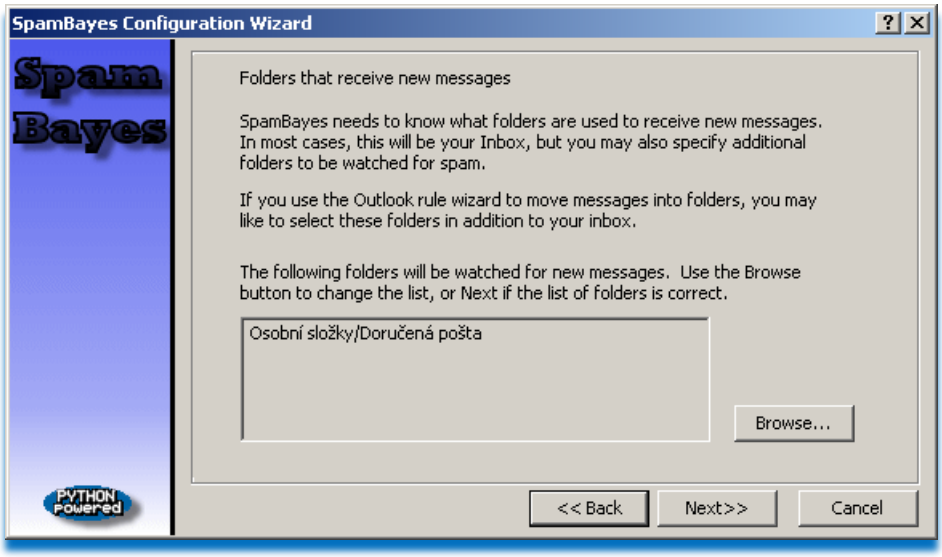
Nyní nám dává program SpamBayes na vybranou (volný překlad):

- Nemám připraveno pro SpamBayes vůbec nic (čistá schránka nebo neroztříděné maily)
- Mám rozřazeny dobré zprávy (ham) a spamy do složek, ty jsou vhodné pro účely učení (pokud máme roztříděné emaily, na kterých by se mohl začít filtr učit)
- Nastavil bych raději SpamBayes ručně (!! Jen pro zkušené uživatele!! – nedoporučuji)

Podle naší potřeby zvolíme možnosti jedna nebo možnost dvě. Poslední možnost je spíše pro zkušené uživatele.

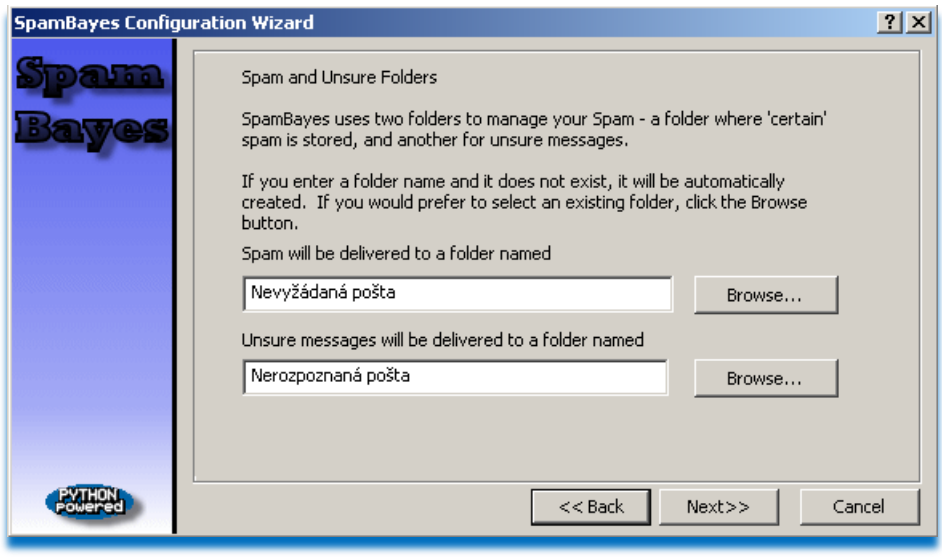
Obr. 35 Vybrání způsobu trénování SpamBayes filtru

Informace o tom, že SpamBayes je bez předchozího naučení neúčinný a ptá se nás jakým způsobem se má naučit spam rozeznávat. Prvním výběrem je možnost učení za chodu systému, systém bude emaily řadit do neutrální složky a na nás bude, abychom mu emaily třídili na ham a spam. SpamBayes se naučí přímo z naší pošty (velice účinné). Druhou možností je ukončit průvodce a řazení mailů nastavit později.



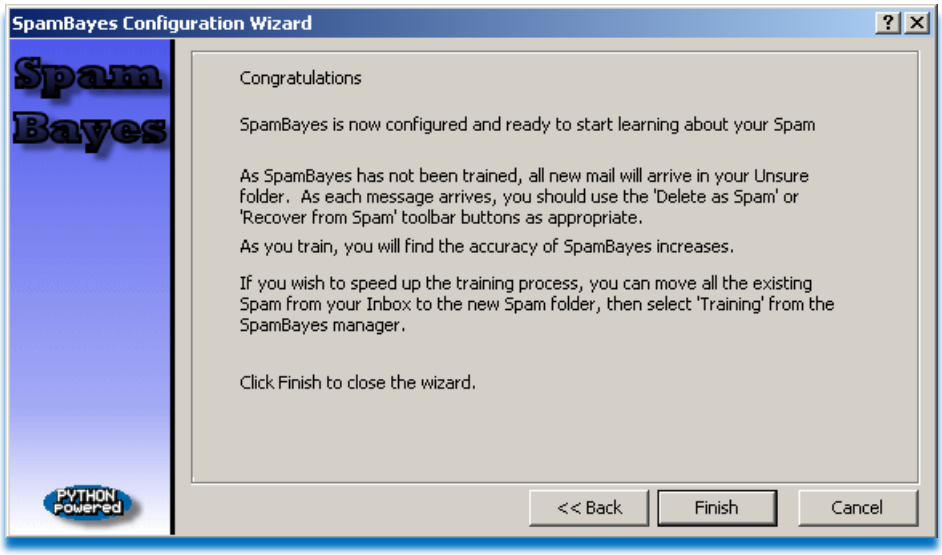
Obr. 36 Výběr složky pro příjem zpráv

Na Obr. 36 se nás program ptá, které složky jsou určeny pro příchozí zprávy (aby se z nich mohl učit), kde mu budeme provádět třídění na spam a ham. Pokud máme nějaké filtrovací pravidla, která roztřiďují zprávy do dalších složek, můžeme je přidat tlačítkem **Browse**. Je vhodné nechat přednastavené.



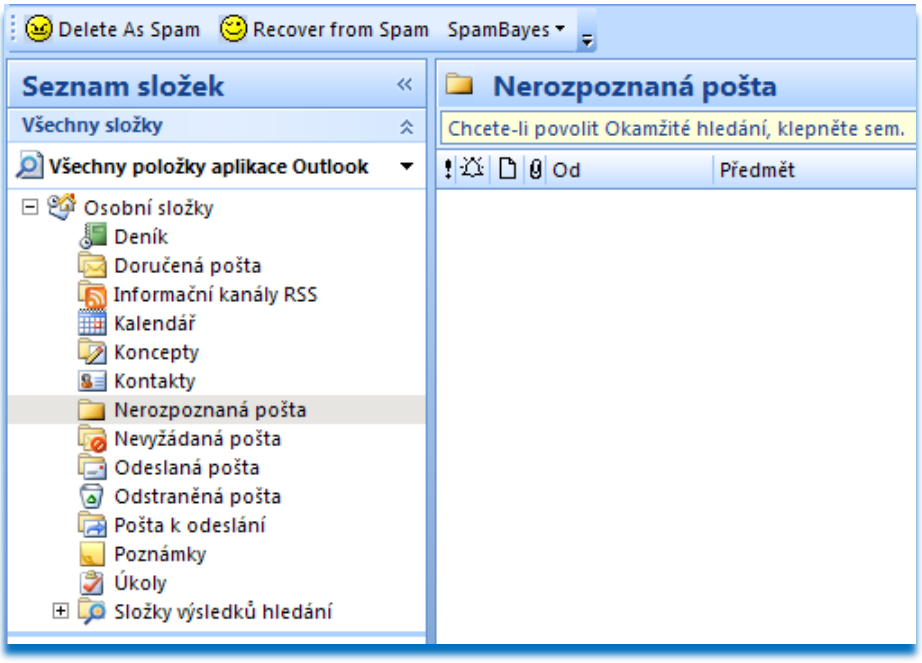
Obr. 37 Definování složek pro spamové a nerozpoznané zprávy

Zde si volíme složky, do kterých bude ukládán rozeznaný spam (s původním popisem **Junk E-Mail**) a složku pro nerozpoznané zprávy (ham nebo spam?, s původním popisem **Junk Suspects**), které musíme roztřídit my. Pokud složky existují, můžeme je vybrat pomocí **Browse**, pokud složky neexistují, můžeme napsat, jak se budou jmenovat a průvodce je sám ve stromové struktuře složek vytvoří.



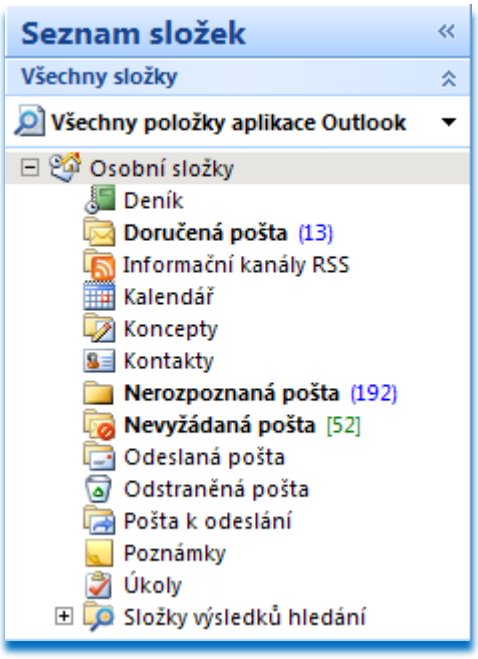
Obr. 38 Dokončení konfigurace

Od této chvíle je systém připraven pro příjem emailů a jejich filtrování, během tohoto učícího procesu, cca 14 dní (popř. minimální hranice 200 emailů), je vhodné přijímat a poctivě třídit jak hamové, tak spamové maily.



Obr. 39 Ukázka ovládacích tlačítek **DELETE** a **RECOVER**

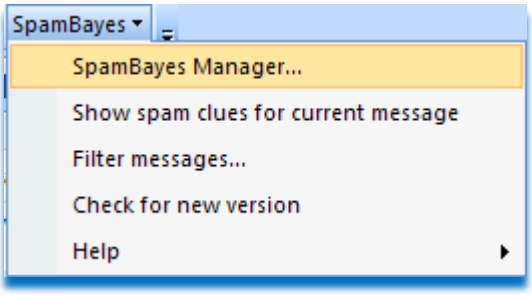
V místě plovoucích panelů přibyl nový panel programu SpamBayes, podle toho v které složce se nacházíme, nám ukazuje příslušné ikonky. Ve složce doručené pošty je vidět jen ikona **Delete As Spam** (Smaž jako spam), ve složce Nevyžádané pošty je to zase ikonka **Recover from Spam** (Obnov ze spamu), pouze u složky Nerozpoznaná pošta jsou vidět obě ikony zároveň. Ještě je zde ikona **SpamBayes**, ta je obecná pro všechny složky a je v ní konfigurace a další ovládací menu programu. Na některé nastavení se nyní podíváme.



Obr. 40 První příjem zpráv

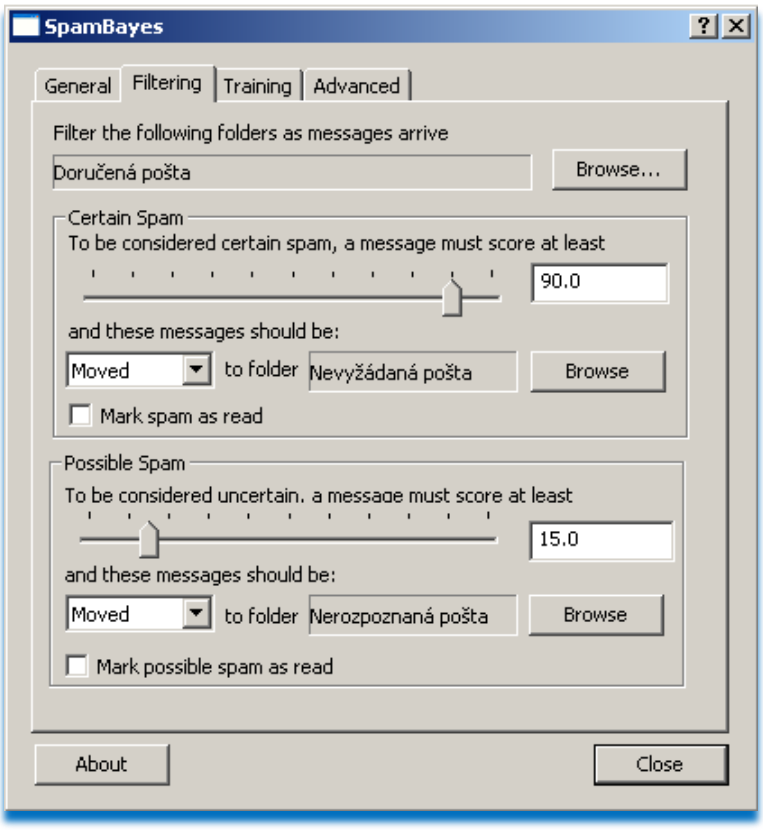
Po prvním příjmu roztřídil SpamBayes zprávy podle Obr. 40. Správně by měl všechny maily vložit do složky Nerozpoznaná pošta. To ale neudělal, z nějakého důvodu dal 13 zpráv do složky Doručená pošta. SpamBayes tak učinil, protože těch 13 zpráv byly jen doručenky. Dále zařadil 52 zpráv do složky Nevyžádaná pošta, což ale neučinil SpamBayes, ale Outlook sám (má v sobě jednoduchý Bayesův filtr, který mu dovoluje, takové filtrování provádět hned po instalaci). Zajímavé může být to, že se spletl jen v 9 případech. Složku nerozpoznaných zpráv musíme projít a označené maily můžeme dát tlačítkem Recover from Spam přesunout do složky Doručené pošty. Stejně tak bychom pak měli zprávy ze složky Nevyžádané pošty přesunout do složky Nerozpoznané pošty a dát ji přesunou pomocí Delete As Spam zpět do složky Nevyžádané pošty. Tuto na první pohled nesmyslnou operaci musíme provést, abychom ukázali SpamBayesovu filtru ne jen hamy (předešlý krok), ale i spamy. Tím se program učí. Nyní když jsme program novým spamům a hamům naučili, můžeme třeba spamové maily smazat. Jejich statistika se v programu uchová pro další učení.

Nastavení programu můžeme kdykoliv změnit a upravit podle potřeby, vše potřebné najdeme v nabídce plovoucího panelu.



Obr. 41 SpamBayes nastavení

V tomto nastavení můžeme hned na první kartě General filtr zapnout (enable) nebo vypnout (disable). Jde zde i spustit průvodce, který je popsán na začátku. Nás bude zajímat hlavně karta Filtering. Zde jsou nastaveny hranice pro rozeznání spamu (90.0) a nerozpoznaných emailů (15.0). Tyto hranice jsou nastaveny optimálně.

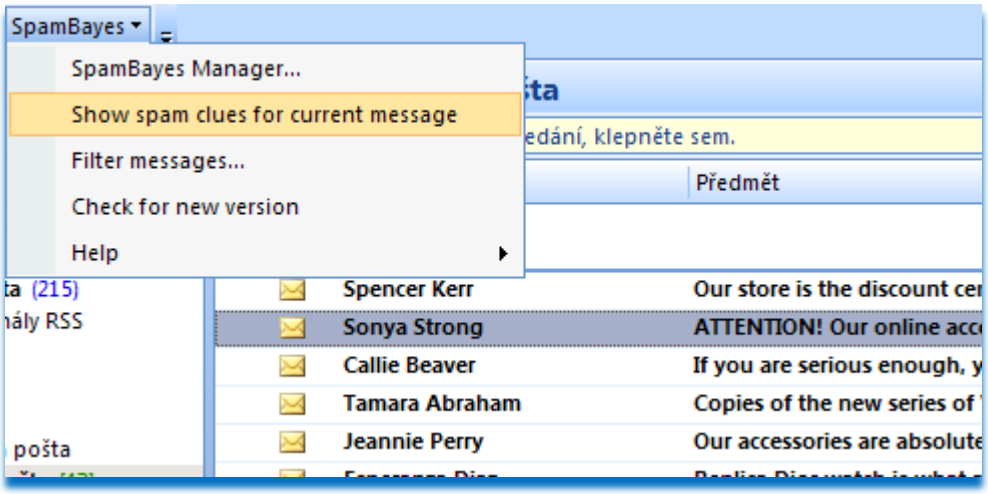


Obr. 42 Karta Filtering z nastavení programu SpamBayes

Karta Training ukrývá nastavení pro trénování SpamBayes filtru na existujících a roztříděných emailových složkách. Poslední karta Advanced má v sobě možnost nastavit

jak dlouho se má s každou zprávou pracovat, nastavení jsou v sekundách. Žádné z těchto nastavení není nutno měnit, už po instalaci jsou nastaveny optimálně.

Poslední zajímavou položkou může být podívat se na detail, proč který email obdržel jaké hodnocení, to provedeme umístěním kurzoru na příslušný email a zvolení položky **Show spam clues for current message**. Dostane se nám vyčerpávající statistiky, proč daný mail dostal jaké hodnocení, za které slovo a položku a kolik takových je již evidováno atd…



Obr. 43 Detail emailové zprávy – statistika emailů (Bayesova analýza)

SpamBayes je výborný produkt, jeho instalace, nastavení i užívání, patří mezi ty nejjednodušší a jeho výsledky jsou více než uspokojivé. Bayesovy filtry patří k tomu nejlepšímu, s čím lze proti spamu bojovat.

2.4.2 SpamButcher

Program SpamButcher je jeden z mnoha produktů nabízených na Internetu na potírání spamu. Tento produkt je vyvíjen jako placený nástroj. Jeho cena se pohybuje kolem 30 USD (cca 516 Kč). Tento produkt lze vyzkoušet i jako trial (21 denní zkušební verze). Program lze stáhnout zde http://www.spambutcher.com/download/spambutcher.exe. Instalační soubor má 2,3 MB. Instalace je standardní a bezproblémová.

Program funguje jako POP3 proxy brána. Využívá možnosti protokolu POP3. Vřadí se mezi vybíranou schránku a poštovního klienta uživatele, kontroluje všechny příchozí zprávy a porovnává je s whitelisty, blacklisty a dalšími filtrovacími pravidly. Zprávy, které jsou vyhodnoceny jako spam zastaví a dále je nepředává do klientského poštovního programu. Výhodou těchto POP3 proxy bran je fakt, že je lze aplikovat k libovolnému poštovnímu klientu, který tento protokol používá (což je skoro každý).

Po instalaci programu se program spustí a umístí do SysTray (systémová lišta). Odtud kontroluje doručenou poštu, program neuzavřeme křížkem, jak jsme zvyklí, tímto uzavřením jej jen minimalizujeme do SysTray.

Obr. 44. Ikona programu SpamButcher v SysTray

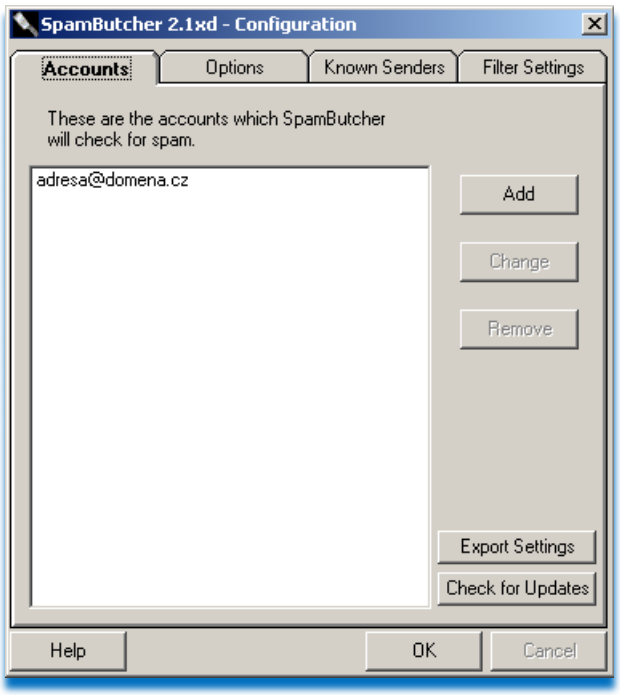
Pokud SpamButcher po své instalaci a spuštění nalezne nakonfigurovaný poštovní účet, automaticky si z něj natáhne nastavení pro POP3 a jsme o této skutečnosti informováni.

Obr. 45. SpamButcher oznamuje, že automaticky neimportoval nalezený poštovní účet

Pokud bychom nějakým nedopatřením tyto konfigurační kroky zrušili, lze je kdykoliv vyvolat spuštěním programu a kliknutím na tlačítko s popisem **Configure** (levý seznam tlačítek).

Karty jsou rozděleny na čtyři základní menu: **Accounts**, **Options**, **Known senders** a **Filters Settings**.

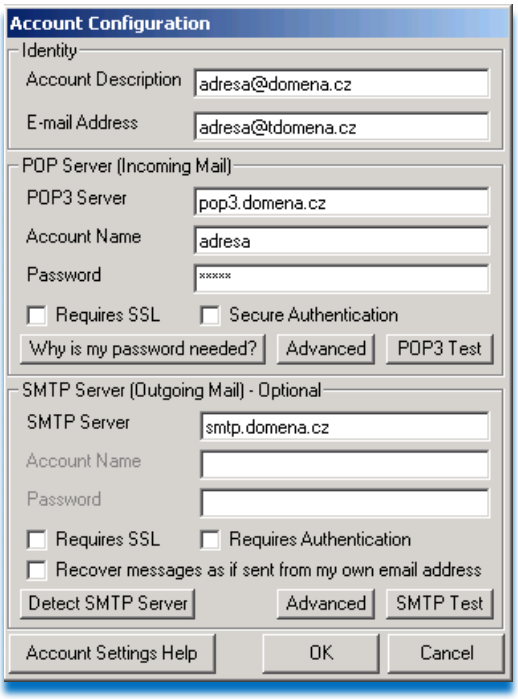
V první kartě je seznam definovaných účtů, které má SpamButcher kontrolovat.



Obr. 46. Karta Accounts

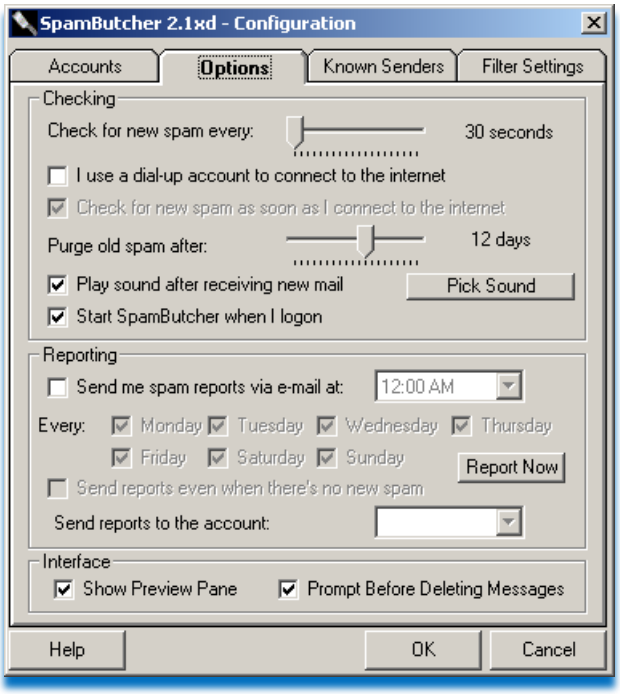
Na této kartě je nyní uveden jediný účet a to ten, který po instalaci SpamButcher našel a automaticky neimportoval. Je-li v poštovním klientu nastavených více účtů, budou všechny naimportovány automaticky. Nesmíme pak, ale zapomenout, že je nutno u všech doplnit přihlašovací hesla pro POP3.

Pokud se rozhodneme upravit konfiguraci poštovního účtu, stačí jej označit myší a kliknout na aktivované tlačítko **Change**.



Obr. 47. Konfigurace poštovního účtu

Obr. 47 ukazuje editaci poštovního účtu. Zda je vše nakonfigurováno v pořádku můžeme testovat tlačítky **POP3 test** a **SMTP test**. Toto nastavení je pro mírně zkušené uživatele.

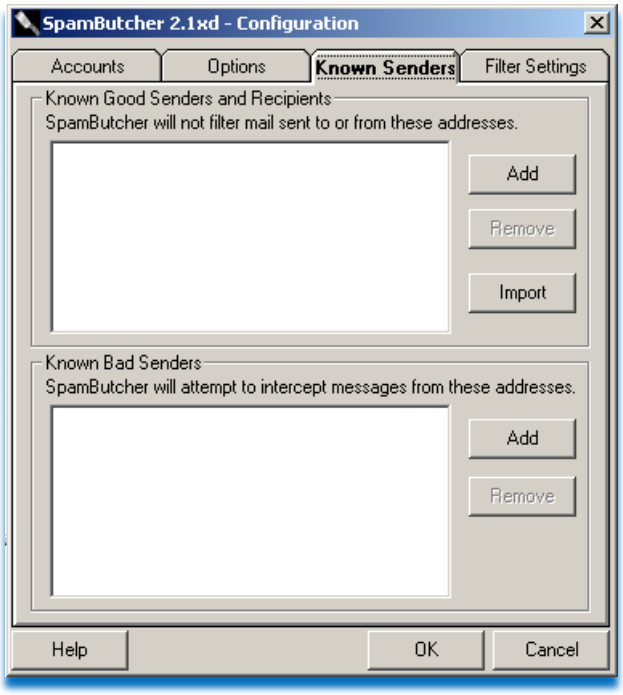


Obr. 48. Karta se systémovými možnostmi

Karta na obr. 48 je věnována nastavení programu SpamButcher. Máme zde možnosti změnit časy pro periodickou kontrolu zpráv (**Check for new spam every**; výchozí hodnota **30s**), nebo automatické mazání spamových zpráv (**Purge old spam after**; výchozí hodnota

12 dní). Dále lze nastavit automatické spouštění po startu (**Start SpamButcher hen I logon**; výchozí je zapnuto a nedoporučuje se vypínat). V rámečku **Reporting** lze aktivovat pravidelné hlášení o zachyceném spamu, resp. okamžité vyžádání reportu po stisku tlačítka **Report Now**.

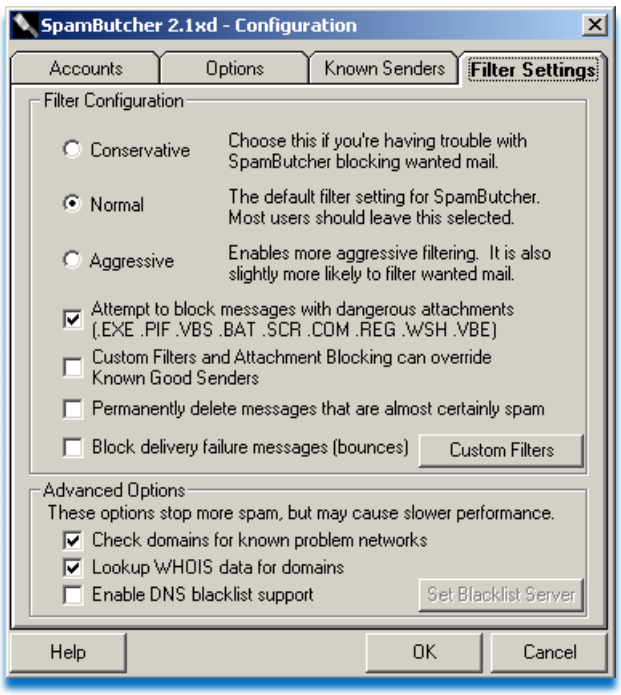
Karta **Known Senders** poskytuje dvě velice důležité okna pro kvalitní chod programu. Horní okno patří známým dobrým odesílatelům a příjemcům (**Known Good Senders and Recipients**; whitelist emailových adres nebo domén), spodní zase známým špatným odesílatelům (**Known Bad Senders**; blacklist emailových adres nebo domén). Adresy lze do těchto sezamů přidávat ručně (vepsat), nebo automaticky neimportovat z adresáře poštovního klienta. Stejně tak při mazání spamu, nebo obnově špatně detekované zprávy, jsme vyzíváni k vložení adresy do whitelistu nebo blacklistu. Adresy můžeme přidávat tlačítkem **Add** nebo odstraňovat tlačítkem **Remove**.



Obr. 49. Karta známých odesílatelů

Zbraně a jejich nastavení, kterými SpamButcher disponuje, nastavujeme na poslední kartě s názvem Nastavení filtru (**Filter Settings**). V této kartě můžeme nastavit agresivitu filtrovacího mechanismu a to buď na **Conservative** což je opatrné filtrování (pravděpodobně bude zachytávat méně spamových zpráv) nebo **Normal** což je výchozí hodnota (doporučeno) a nebo **Aggressive** což je nejagresivnější nastavení, s tímto nastavením daleko častěji dochází k špatnému ohodnocení legální zprávy jako spam. Filtr

je vhodné nechat na citlivost **Normal**. Další od instalace povolenou funkcí je blokování emailů s nebezpečnými přílohami, mezi které patří **Exe**, **Pif**, **Scr** apod. Pokud užíváme program Microsoft Office Outlook 2007, můžeme tuto volbu zrušit (vyčistit), jelikož Outlook už sám tyto zprávy blokuje a dává uživateli jasnou informaci, jak má pokračovat.



Obr. 50. Nastavení antispamového filtru

Další položkou je možnost potlačit uživatelské filtry a blokování příloh, pokud je emailová adresa uvedena na předchozí kartě v oddílu whitelist (**Custom Filters and Attachment Blocking can override Known Good Senders**). Dále lze zatrhnout položku **Permanently delete messages that are almost certainly spam**, tato položka říká, že lze automaticky mazat emailové zprávy, které jsou téměř jistě spam. Zde bych doporučoval velkou opatrnost a důkladně si volbu rozmyslet. Výchozí hodnota (podle mě optimálně zvoleno) je vypnuto. Jedním z posledních důležitých prvků je tlačítko **Custom Filters**, kde má opět uživatel možnost definovat filtr správných a špatných slov nebo frází.

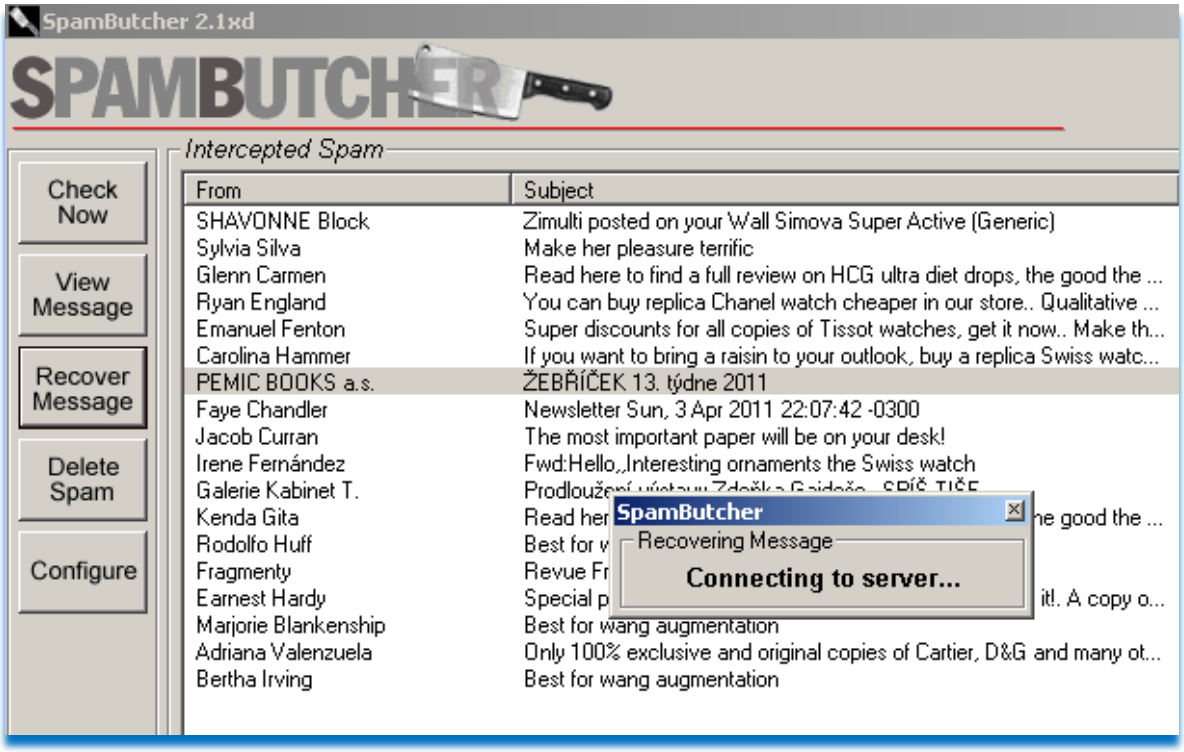
Rozšířené nastavení ukrývá další filtrovací metody, které však mohou výrazně zpomalit analýzu přijímaných zpráv, nicméně vyplatí se zaškrtnout nabízené položky. První položkou je **Check domains for known problem network**, která zajistí prohlížení databáze známých domén, ze kterých je směrováno do Internetu velké množství spamu (obdoba DNSBL), dále je to položka **Lookup WHOIS data for domains**, ta zajišťuje zjišťování informací o doménách, z kterých přijímané zprávy údajně pocházejí. A poslední položkou je zapnutí podpory DNS blacklistů, jako výchozí je nastaven cbl.abuseat.org,

který patří mezi lídry v DNSBL. Zde doporučuji, zapnout všechny tři nabízené možnosti filtru. Tím je filtr nastaven a připraven k užívání.

Při příjmu zpráv, který se automaticky spouští dle zvoleného časového limitu (pro nás je to 30s), se zobrazuje v programu tato hláška o tom, že SpamButcher prochází emailové adresy a analyzuje, které jsou spam. Po analýze jsou spamové zprávy ze schrány stáhnuty do SpamButchera, kde čekají na uživatelskou aktivitu nebo automatické smazání po námi navolených dvanácti dnech.

Obr. 51. Analýza zpráv

Pokud je nějaká zpráva mylně detekována jako spam, lze jí jednoduše označit a kliknutím na tlačítko **Recover Message** vrátit zpět do poštovní schránky, při této operaci je adresa odesílatele vložena do whitelistu, aby se příště omylu zabránilo.



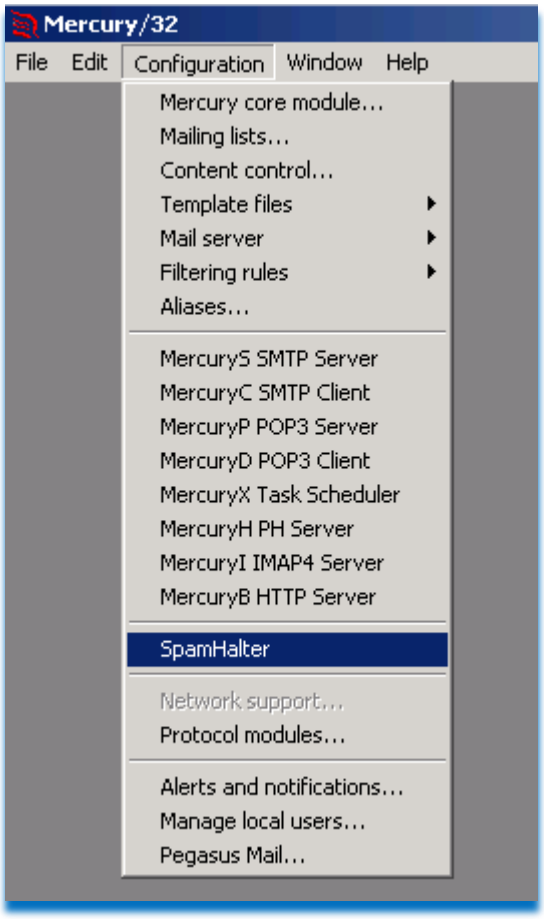
Obr. 52. Ukázka opravy špatně detekované zprávy (**Recover Message**)

SpamButcher je kvalitní nástroj, bohužel jeho vyladění je celkem obtížný úkol a proto bych jej nedoporučil začátečníkům a méně zkušeným uživatelům.

2.4.3 SpamHalter

Program SpamHalter je nadstavba poštovního serverového softwaru Mercury Mail serveru. Je k dispozici na webové adrese http://www.ararat.cz/doku.php/cs:spamhalter, kde lze nalézt i instalační manuál. V nové verzi Mercury Mail serveru je již v základní instalaci. Instalace je již pro mírně zkušené uživatele, je nutno konfigurovat smtp servery, popř. MX záznamy, nebo údaje z domény (odkud se mají zprávy stahovat). Nastavení poštovního serveru není předmětem této publikace, nebude se zde tedy rozebírat. Podíváme se jen na nastavení SpamHalteru v tomto poštovním serveru. Software SpamHalter je zdarma. Funguje na bázi Bayesova filtru. Jedná se o robustní systém, který lze zatížit stovkami až tisícovkami emailových schránek.

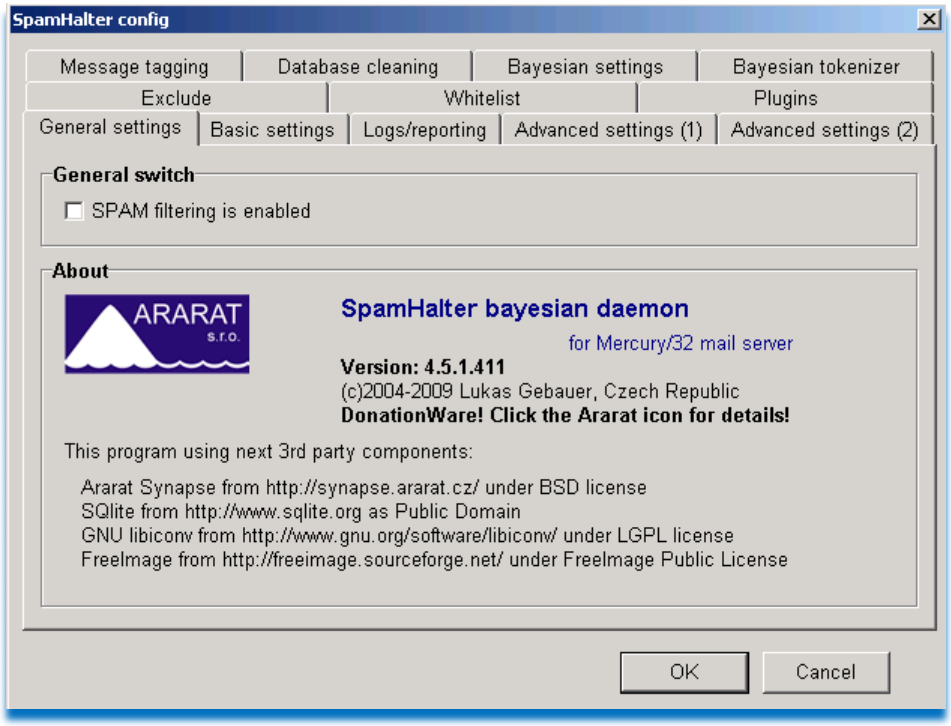
Modul SpamHalteru najdeme přímo v konfiguračním menu poštovního serveru.



Obr. 53. Modul SpamHaleru v Mercury Mail Serveru (konfigurace SpamHalteru)

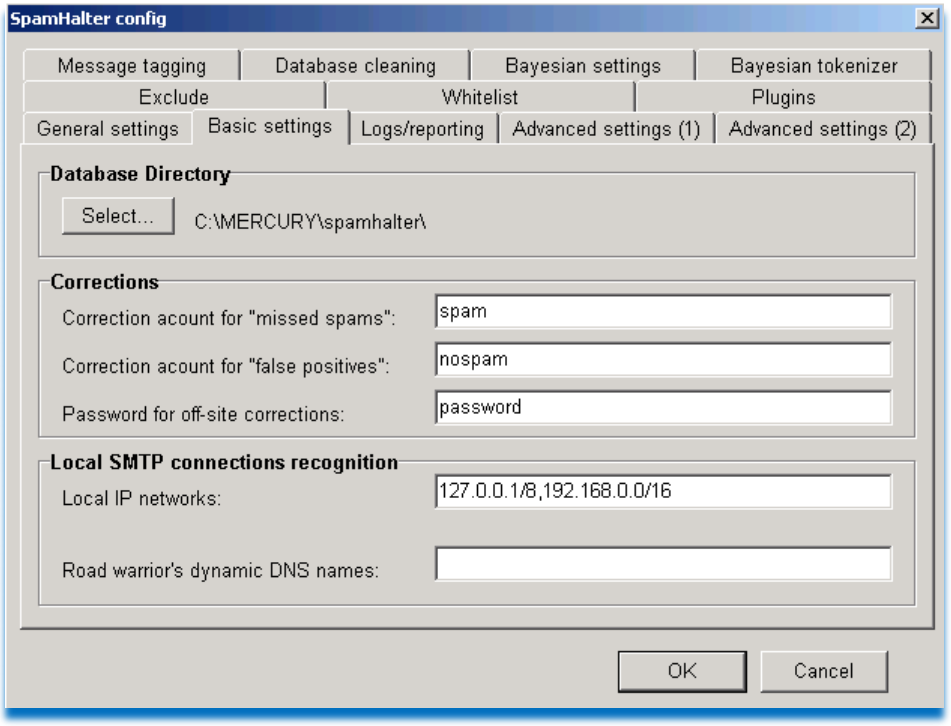
Nebudeme se zabývat rozsáhlým popisem Bayesových filtrů a detailním rozborem každé karty nastavení programu SpamHalter. Ukážeme si základní karty a jejich nastavení, které je důležité pro správný chod SpamHalteru.

Výhodou serverových edic antispamových řešení je, že je vše řešeno na straně serveru a klient tak nemusí udržovat žádnou databázi, nemusí provádět žádné učení apod. Musíme samozřejmě Bayesův filtr nějakým způsobem naučit rozeznávat spam a ham, ale tím že se tak koná pro všechny příjemce zpráv z jednoho místa, je celý proces jednodušší a lehčí. Zprávy jsou vyhodnoceny a označeny, dále je pak možno filtrovacími pravidly nastavit co se má s kterým typem zpráv provést.



Obr. 54. Konfigurace SpamHalteru

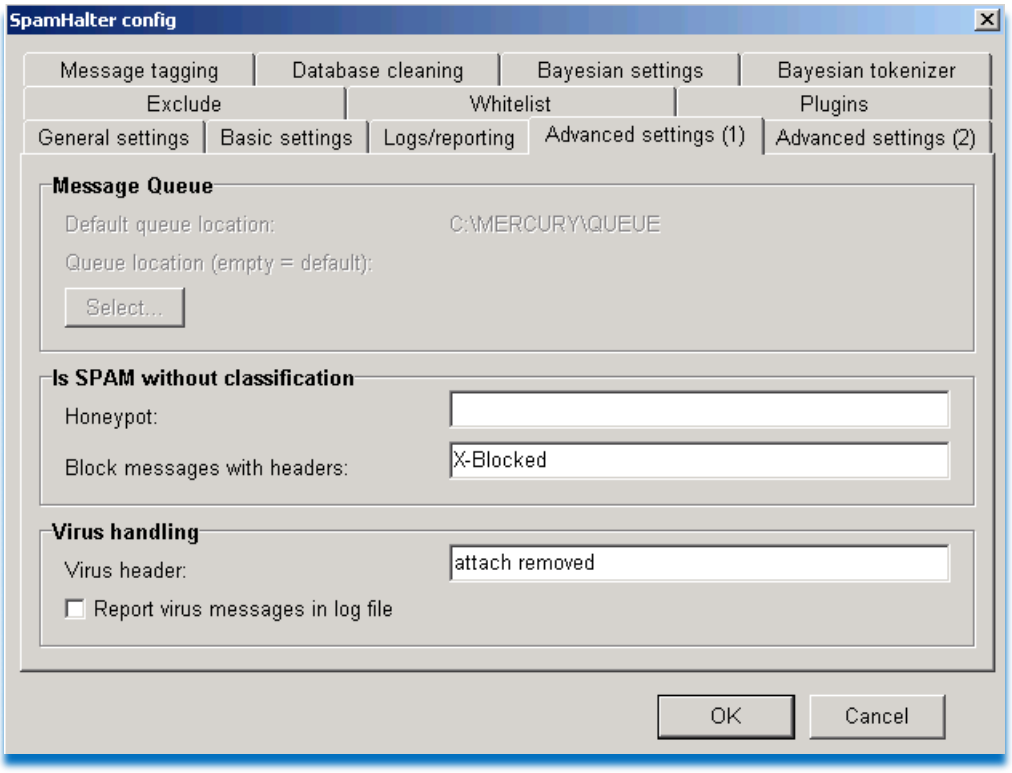
Hlavní vypínač (General switch) umožňuje zapnout pomocí checkboxu spuštění modulu SpamHalteru. SpamHalter je již od první chvíle nakonfigurován pro provoz, samozřejmě je možné a důležité si jeho nastavení projít a upravit si jej pro vlastní účely.



Obr. 55. Základní nastavení SpamHalteru

V základním nastavení SpamHalteru je nutno vybrat složku pro pracovní databázi Bayesova Filtru (**Database directory**), databáze pro velkou firmu může zabrat i několik stovek megabajtů. Tlačítkem **Select** provedeme a nastavením na požadovanou složku.

Úpravy (**Correction**) je jedna z nejdůležitějších položek nastavení, zde musíme zvolit dvě emailové schránky existující na tomto poštovním serveru. Tyto schránky jsou zřízeny výhradně pro účely učení Bayesova filtru. První adresa je pro zasílání zpráv, které jsou spamem, ale nebyly tak označeny (jedná se o pole **Correction acount for „missed spams“.**). Druhá adresa je pro ham zprávy, které byly nesprávně označené jako spam (pole má popis **Correction acount for „false possitives“.**). Pokud uživatelé dostanou do své emailové schránky zprávu, která je mylně označena, rozhodnou se a zašlou ji na jednu z těchto adres. SpamHalter tyto schránky pravidelně kontroluje a provede podle zpráv úpravu v Bayesově filtru. Položka **Password for Off-Site corrections** je zde pro účely vzdálených pracovišť (odhlašování z Internetu). Zadané heslo je kontrolováno v přijímaných mailech na tyto dvě korekční adresy, pokud jsou zaslané z Internetu a heslo neobsahují, nebude operace provedena.

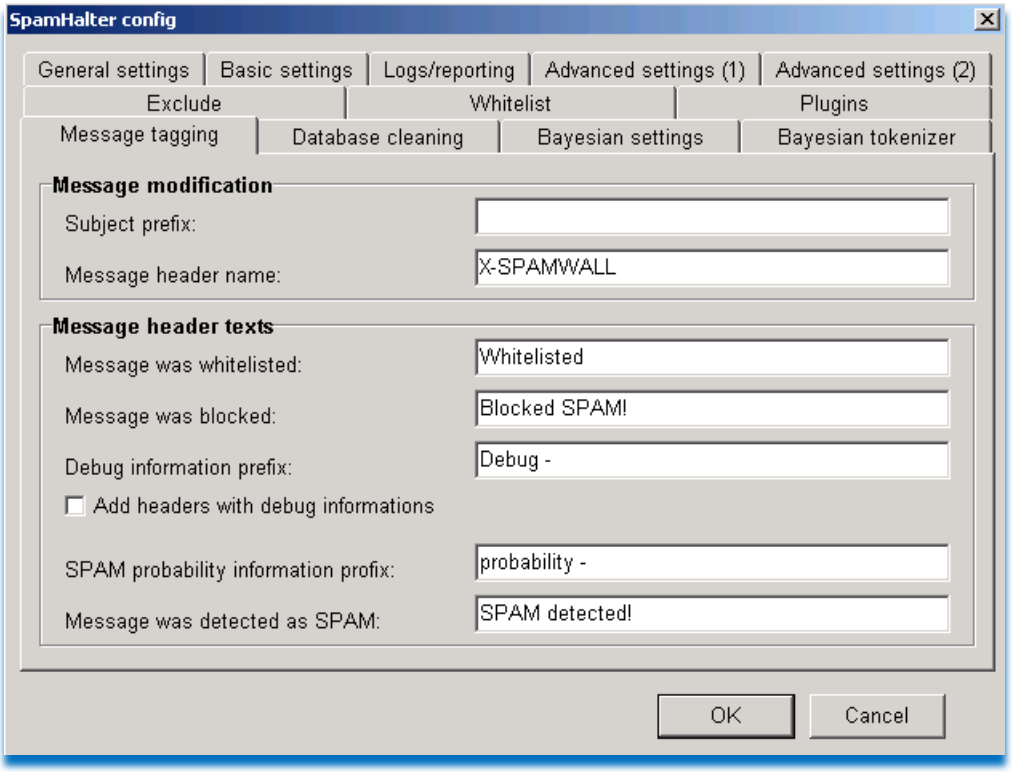


Obr. 56. Rozšířené nastavení SpamHalteru

Rozšířené nastavení obsahuje zajímavou položku a to pole **Honeypot**, jedná se o pole, kde lze vypsat emailové adresy, které byly použity jako vábničky (antiadresy). Tyto adresy je vhodné umístit čitelně (pro spamboty) na webové stránky, ale aktivně je neužívat. Pokud přijde mail na tuto adresu je to jasný spam.

Karty Exclude a Whitelist lze využít pro výjimky. Zde napíšeme emailové adresy, nebo rovnou celé domény, které nemají být kontrolovány (Exclude), nebo mají výjimku (Whitelist).

Neméně důležitou kartou je popisování zpráv (**Message tagging**). V této kartě máme možnost nastavit, co se má vepsat do hlavičky emailu. Podle čeho budeme dále rozeznávat, zda byla zpráva spam nebo ham.

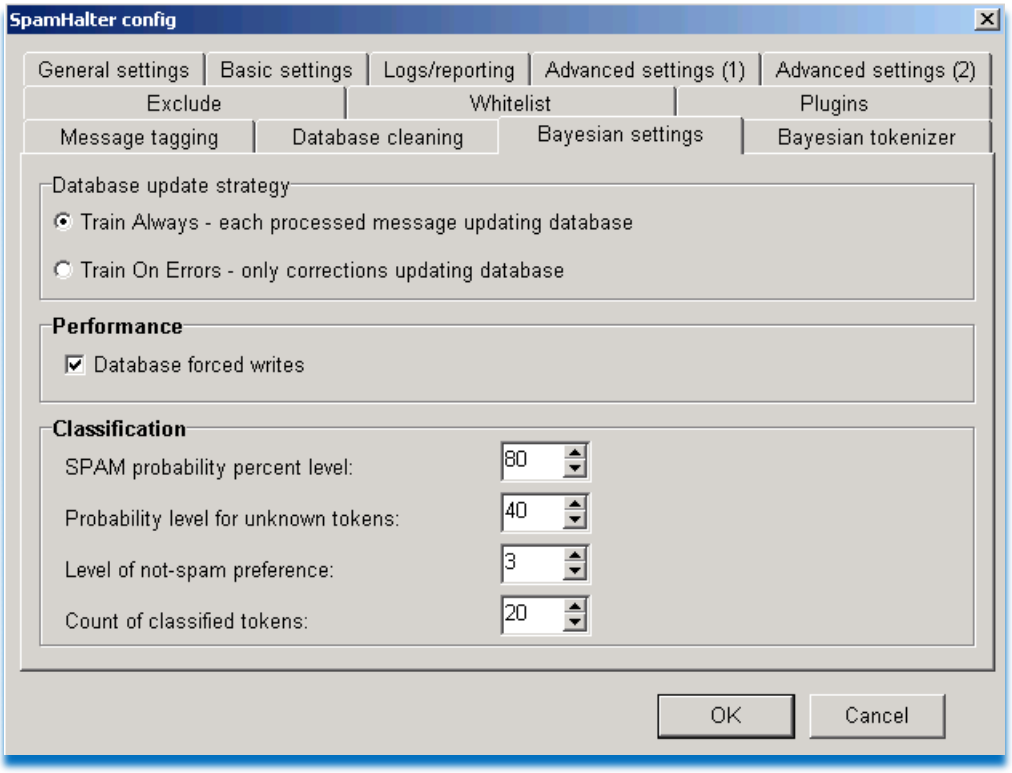


Obr. 57. Popis zpráv

Pole **Subject prefix** určuje, co se má vložit před původní předmět, můžeme podle této úpravy uživateli třeba říct, že zpráva byla zkontrolována.

Message header name nám určuje, jak se bude jmenovat tag v hlavičce emailu, který budeme dále doplňovat textem z polí uvedených v rámečku **Message header texts**.

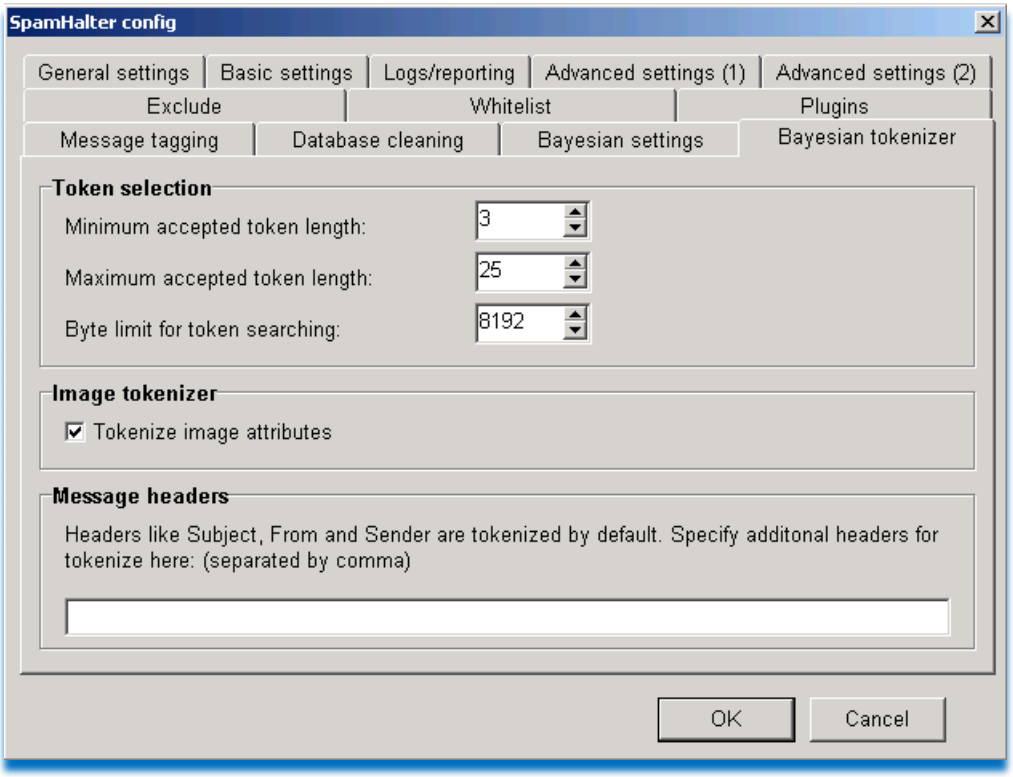
V rámečku **Message header texts** máme na výběr hned z několika doprovodných textů. O tom že zpráva byla ukončena s výjimkou na Whitelistu, nebo že byla detekována jako spam podle blacklistu (pole **Message was blocked**), dále informace o procentuální pravděpodobnosti, že se jedná o spam (**Spam probability informatik prefix**) a konče informací o tom, že zpráva je spam (**Message was detected as SPAM**) – rozpoznáno podle Bayesova filtru. Všechny tyto hlášky si můžeme editovat, libovolně popsat a dále s nimi pracovat v třídících pravidlech na straně serveru nebo klienta.



Obr. 58. Nastavení Bayesova Filtru

Na kartě nastavení Bayesova filtru obr. 58 můžeme upravit hranice procentuálních hodnot pro vyhodnocení, zda je zpráva spam nebo ham. Zajímavá je položka **Probability level for unknown tokens**, která udává, jak bude procentuálně ohodnoceno slovo, které v databázi ještě není. Dále je vhodné podle potřeby upravit kolik důležitých slov musí být ve zprávě vyhodnocena, aby se jednalo o kvalitní posudek, to udává pole **Count of classified token**. Tyto hodnoty lze samozřejmě uživatelsky upravit, nicméně už původní nastavení je optimální a nedoporučuje se ho měnit.

Poslední důležitou kartou je nastavení slov pro Bayesův filtr (**Bayesian tokenizer**), jedná se o nastavení minimální a maximální délky posuzovaných slov. Jako slovo se zde chápe řetězec znaků, který může obsahovat i mezery a další zástupné znaky, pro tvorbu regulérních dotazů (hvězdičky, otazníky apod…). Důležité je i pole **Byte limit for token searching**, které udává, na jakou velikost bude zkrácena dlouhá zpráva, před Bayesovou analýzou.



Obr. 59. Nastavení slov pro Bayesův filtr

Mezi poslední zmiňované položky uvedu **Image tokenizer**, tento checkbox je zde pro tzv. obrázkový spam. Jedná se o formu spamu, kde je ve zprávě pouze HTML kód a vložený obrázek. Pokud je pole zatrženo, hlídá si SpamHalter i takový druh spamových zpráv.

Nastavení SpamHalteru je bohaté. Nelze jej celé obsáhnout a kvalitně popsat. Hodně položek a nastavení je individuálních, nicméně jak již bylo napsáno už po instalaci je systém plně provozuschopný a optimálně nastavený.

Ještě poslední poznámka, nezapomeňme, že Bayesův filtr je jen natolik kvalitní a účinný jako je naše učení tohoto filtru, je tedy důležité a podstatné ze začátku trpělivě rozdělovat maily a posílat je zpět SpamHalteru na přednastavené emailové adresy pro případné korekce.

3 PRÁVO A SPAM

Zdánlivě banální a jednoduchá regulace spammingu může postihnout hned několik práv, jejichž existence je pro svobodnou společnost životně důležitá – jedná se o právo na vlastnictví, právo na svobodu projevu, právo na práci (včetně souvisejících práv) a právo na ochranu osobní integrity (především právo na ochranu osobnosti a soukromí). K tomu ještě přistupují možnosti omezení uvedených práv ve prospěch zájmů společnosti a státu ve smyslu ochrany veřejného pořádku, ochrany veřejné komunikační infrastruktury apod. Regulací spamu můžeme tedy v těchto souvislostech chápat například jako:

- *omezení práva na svobodu projevu ve prospěch práva na ochranu osobní integrity,*
- *omezení práva na svobodu projevu ve prospěch práva na vlastnictví příjemce spamu,*
- *omezení práva na ochranu vlastnictví spammera (zákaz užít vlastnictví určitým způsobem) ve prospěch ochrany vlastnictví příjemce spamu,*
- *omezení práva na práci spammera ve prospěch práva na ochranu osobní integrity,*
- *omezení práva na práci spammera ve prospěch ochrany veřejného pořádku*
- *…*

Debata o poměru výše zmíněných práv se vedla především v USA a sama by rozsahem vydala na několik monografií. Pro nás je však důležité, že jejím výsledkem byla vždy proporcionalita ochrany výše uvedených hodnot ve prospěch právní regulace spammingu (tj. ve prospěch zásahu do práv spammera). Takový výstup je pak, mírně řečeno, překvapivý, neboť v jiných obdobných otázkách je možné pozorovat zásadní rozdíly mezi chápáním poměru základních společenských hodnot, a to i mezi příbuznými kulturami evropskou a severoamerickou. Jednotné zhodnocení základní ústavněprávní otázky regulace spamu může přitom ukázat i na pozitivní skutečnost, že partikulární kulturní rozdíly v off-line světě hrají pro informační společnost a její právo stále menší roli. [3]

Většina států již přijala alespoň základní zákonné nebo formální úpravy ústavy, které by měly občany ochránit před přímým zneužíváním jejich osobních údajů a zamezit tak obchodu s jejich osobními údaji a následným rozesíláním spamu. Problém je však v tom, že většina destinací odkud je stále šířen spam jsou oblasti, kde lze zákon jen těžce prosazovat. Častým jevem jsou pak spamové adresy z Brazílie, Chile, ale i Číny, Ruska apod. Většina států (domén) ze kterých je spam zasílán mají mnohdy jiné a důležitější problémy s bezpečností, takže není na spammování pohlíženo jako na vážnější nezákonný počin.

Pro individuálního českého spotřebitele nebo i podnikatele tak není až tak nebezpečný jihokorejský spam nabízející pilulky na potenci, ale spíše český spam s konkrétní nabídkou produktů pro české zákazníky. Právě nebezpečí spamu pocházejícího z příslušného kulturního (jazykového) prostředí a cíleného na relativně úzkou skupinu adresátů je pak tím aspektem spammingu, na který může národní legislativa účinně odpovědět. [3]

V tomto je Česká republika zatím světlou výjimkou, je pravda že 99,99% spamu není českého, ale zahraničního původu. Pokud nám nepřijde nějaká informace o „slevách v horském hotelu“ nepotkáme v naší emailové schránce skoro žádný jiný český spam.

3.1 Právo v Evropské unii

Z různých typů obrany před spamem se nejprve zaměříme na jeho právní postih, který v současné době tvoří jádro takzvané antispamové legislativy.

Podobně jako u odpovědnosti ISP je příslušná evropská legislativa provedena formou harmonizační směrnice, která stanoví základní standardy a dává členským státům možnost zvolit konkrétní legislativní řešení. V případě spamu je harmonizačním předpisem směrnice Evropského parlamentu a Rady č. 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) známá též jako EPD (Electronic Privacy Directive). Směrnice se netýká jen spamu, ale obecně ochrany jednotlivců proti nežádoucím zásahům do jejich právní sféry prostřednictvím služeb informační společnosti. Jádrem antispamové legislativy se stal článek 13 EPD následujícího znění:

Článek 13

Nevyžádaná sdělení

1. ***Automatické volací systémy bez zásahu člověka (automatické volací přístroje), faximilní přístroje (faxy) nebo elektronickou poštou je možno použít pro účely přímého marketingu pouze v případě účastníků, kteří k tomu dali předchozí souhlas.***
2. ***Bez ohledu na odstavec 1, pokud fyzická nebo právnická osoba získává od svých zákazníků podrobnosti jejich elektronického kontaktu pro elektronickou poštu v souvislosti s prodejem výrobku nebo služby a v souladu se směrnicí 95/46/ES, může tato fyzická či právnická osoba využít tyto podrobnosti elektronického kontaktu pro účely přímého marketingu svých vlastních obdobných výrobků nebo služeb pouze za předpokladu, že je zákazníkům jasně a zřetelně poskytnuta možnost zdarma a jednoduchým způsobem nesouhlasit s takovým využitím***

podrobností jejich elektronického kontaktu v době, kdy se shromažďují, a při zasílání každého jednotlivého sdělení, pokud zákazník původně toto využití neodmítl.

3. ***Členské státy musí přijmout vhodná opatření zajišťující, že nevyžádaná sdělení, zdarma, pro účely přímého marketingu, v případech jiných než uvedených v odstavcích 1 a 2, nebudou povolena buď bez souhlasu dotčených účastníků, nebo ve vztahu k účastníkům, kteří si nepřejí taková sdělení dostávat, přičemž výběr z uvedených možností bude stanoven vnitrostátními právními předpisy.***
4. ***V každém případě je nutno zakázat praxi posílat elektronickou poštu pro účely přímého marketingu, pokud tato skrývá nebo utajuje totožnost odesílatele, jehož jménem se sdělení přenáší, anebo ji posí1at bez platné adresy, na kterou by příjemce mohl odeslat žádost o ukončení zasílání takových sdělení.***
5. ***Odstavce 1 a 3 se použijí na účastníky, kteří jsou fyzickými osobami. V rámci práva Společenství a použitelných vnitrostátních právních předpisů členské státy také zajistí, že budou dostatečně chráněny oprávněné zájmy účastníku, kteří nejsou fyzickými osobami, pokud jde o nevyžádaná sdělení.***

Jak můžeme vidět, dává tento článek relativně široké možnosti pro legislativu jednotlivých států k přijetí konkrétních ochranných opatření. Směrnice tedy pouze stanoví základní standardy s tím, že jejich provedení v národních právních řádech je relativně volné.

Problematikou spamu se v tomto směru okrajově zabývalo dřívější Rozhodnutí Evropského parlamentu č. 276/1999/ES, kterým se přijímá víceletý akční plán Společenství k podpoře bezpečnějšího používání Internetu prostřednictvím potírání nezákonného a škodlivého obsahu v globálních sítích. Pro oblast spamu je však nejdůležitějším dokumentem Sdělení Komise č. COM/2004/0028 o nevyžádaných obchodních sděleních či spamu. Zde jsou s odvoláním k výsledkům výzkumu a empirickým studiím (především z USA) vysvětleny důvody a základní momenty evropské regulace spamu včetně doporučení státům k přijetí nikoli jen národních legislativ, ale komplexních politik potírání spamu ve spolupráci se soukromým sektorem. [3]

3.2 Právo v České republice

V České republice byl článek 13 směrnice č. 2002/58/ES proveden především zákonem č. 480/2004 Sb. Český právotvůrce se přitom držel evropského modelu a správní regulaci tak podrobil jen takové typy spamu, které mají obchodní charakter. Česká právní úprava tedy pracuje s kategorií obchodního sdělení vymezeného v ustanovení § 2 písm. f zákona č. 480/2004 Sb. následovně:

f) ***obchodním sdělením [se pro účely tohoto zákona rozumí] všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama podle zvláštního právního předpisu. Za obchodní sdělení se nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle[.]***

Vymezení věcné působnosti zákona č. 480/2004 Sb. vzhledem ke spamu je pak konkretizováno ještě ustanovením § 7 odst. 1 následujícího jednoduchého znění:

(1) Obchodní sdělení lze šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem.

Z uvedených ustanovení můžeme pak vyvodit následující praktické interpretační závěry stran působnosti antispamových ustanovení zákona č. 480/2004 Sb.:

- *Zákon se vztahuje je na obchodní spam - nezakazuje tedy politický, náboženský či jiný spamming.*
- *Zákon upravuje pouze rozesílání zpráv elektronickými prostředky - nevztahuje se tak na letákové nebo poštovní kampaně, naopak se kromě e-mailu vztahuje i na ostatní formy elektronické komunikace, tj. fax, SMS, diskusní skupiny apod.*
- *Za spam se nepovažují metadata, tj. linky a nejrůznější formy elektronických adres - není tedy zakázáno distribuovat elektronickými prostředky bez dalšího například linky na WWW stránky nebo e-mailové adresy.* [3]

Obr. 60. Ukázka emailu, který nelze považovat za spam,
podle zákona č. 480/2004 Sb.

Bohužel emailovou schránkou může přicházet spam v různých podobách viz obr. 60. Pokud email obsahuje jen metadata (webovou adresu) nelze takový email za spam podle zákona považovat, nicméně pokud Vám takových mailů chodí denně stovky, stále je to ještě v pořádku?

3.3 Co se smí podle zákona č. 480/2004 Sb.

Zákon č. 480/2004 Sb. se sice obecně drží principu opt-in, dává však zájemcům o rozesílání elektronické inzerce určité možnosti jak postupoval bez rizika sankce. Podmínky pro rozesílání nevyžádaných obchodních sdělení upravuje § 7, a to následovně:

§7

(1) Obchodní sdělení lze šířit elektronickými prostředky jen za podmínek stanovených tímto zákonem.

(2) Podrobnosti elektronického kontaktu lze za účelem šíření obchodních sdělení elektronickými prostředky využít pouze ve vztahu k uživatelům, kteří k tomu dali předchozí souhlas.

(3) Nehledě na odstavec 2, pokud fyzická nebo právnická osoba získá od svého zákazníka podrobnosti jeho elektronického kontaktu pro elektronickou poštu v souvislosti s prodejem výrobku nebo služby podle požadavků ochrany osobních údajů upravených zvláštním právním předpisem 5), může tato fyzická či právnická osoba využít tyto podrobnosti elektronického kontaktu pro potřeby šíření obchodních sdělení týkajících se jejích vlastních obdobných výrobků nebo služeb za předpokladu, že zákazník má jasnou a zřetelnou možnost jednoduchým způsobem, zdarma nebo na účet této fyzické nebo právnické osoby odmítnout souhlas s takovýmto využitím svého elektronického kontaktu i při zasílání každé jednotlivé zprávy, pokud původně toto využití neodmítl.

(4) Zaslání elektronické pošty za účelem šíření obchodního sdělení je zakázáno, pokud

a) tato není zřetelně a jasně označena jako obchodní sdělení,

b) skrývá nebo utajuje totožnost odesílatele, jehož jménem se komunikace uskutečňuje, nebo

c) je zaslána bez platné adresy, na kterou by mohl adresát přímo a účinně zaslat informaci o tom, že si nepřeje, aby mu byly obchodní informace odesílatelem nadále zasílány.

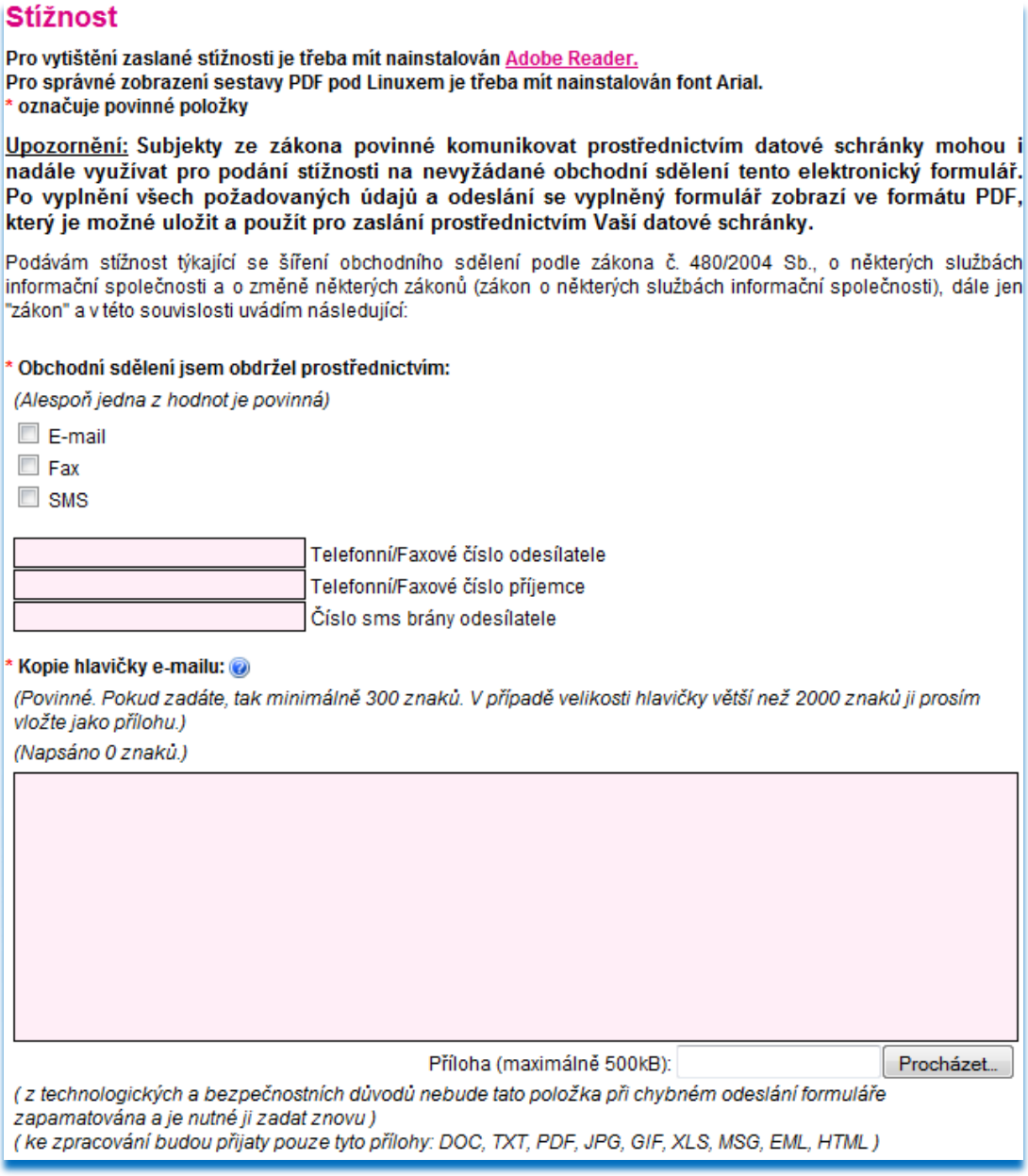
Jak vyplývá z ustanovení odst. 3, funguje režim opt-in pouze v případech, kdy obchodník získal elektronické kontaktní adresy jinak než přímo od svých zákazníků v souvislosti se svou obchodní činností. O souhlas se zasíláním obchodních sdělení je tedy třeba žádat tehdy, získá-li podnikatel adresy například z nějakého veřejně dostupného zdroje nebo zakoupením kontaktní databáze. Forma žádosti o souhlas i jeho udělení muže být přitom různá, je však třeba pamatovat na to, že v případě řízení bude muset podnikatel existenci souhlasu prokázat. [3]

Je tedy vhodné pokud získáme kontakt příkladem z webových stránek vyžádat si prvním emailovým stykem souhlas ohledně zaslání obchodního sdělení. Nesmíme však do emailu o souhlasu uvést jakékoliv informace z následujícího obchodního sdělení. Příkladem, kdybychom poslali email s textem: „Žádáme o souhlas se zasláním obchodního sdělení, ve kterém bychom vám chtěli nabídnout bazény, na které je nyní sleva 30% ...“, je to špatně. Tím, že bychom do emailu o souhlasu uvedli i část nabídky, jednalo by se již o porušení zákona č. 480/2004 Sb. Je tedy potřeba opatrně volit slova, kterými zákazníka o souhlas žádáme. Stejně se jedná i o služby faxem, sms a dalšími způsoby elektronické komunikace.

3.4 Správní postih spamu v České republice

Nedodržíme-li při obchodním spammingu zákonné požadavky, vystavujeme se nebezpečí správního postihu, konkrétně pokuty. Zákon č. 480/2004 Sb svěřuje dozor nad dodržováním stanovených podmínek Úřadu na ochranu osobních údajů (ÚOOÚ) a v některých případech ještě orgánům profesních samospráv. Tyto instituce tedy aktivně dohlížejí na to, aby nedocházelo k zakázanému spammingu, případně aby se dovolený spamming držel v zákonných limitech.

Úřad i orgány profesních samospráv postupují při své činnosti ***ex officio****, tzn., jednají z vlastní iniciativy. V praxi se však můžeme spíše setkat se situací, kdy úřad nezákonný spamming aktivně nevyhledává, ale většinou pouze prověřuje podněty od veřejnosti. I český ÚOOÚ tak zřídil speciální stránky s návodem jak oznámit nezákonný komerční spamming. Součástí stránek je i jednoduchý formulář, který je možné použít k okamžitému on-line nahlášení spammera. Úřad se tím snaží veřejnosti maximálně usnadnit oznámení nezákonného spamrningu a urychlit tak jeho následný postih. Užitečné jsou i zde zveřejněné pokyny k tomu jak poskytnout úřadu právě ty informace, které pro své šetření potřebuje.* [3]



Stížnost

Pro vytištění zaslané stížnosti je třeba mít nainstalován Adobe Reader.
Pro správné zobrazení sestavy PDF pod Linuxem je třeba mít nainstalován font Arial.
*** označuje povinné položky**

Upozornění: Subjekty ze zákona povinné komunikovat prostřednictvím datové schránky mohou i nadále využívat pro podání stížnosti na nevyžádané obchodní sdělení tento elektronický formulář. Po vyplnění všech požadovaných údajů a odeslání se vyplněný formulář zobrazí ve formátu PDF, který je možné uložit a použít pro zaslání prostřednictvím Vaší datové schránky.

Podávám stížnost týkající se šíření obchodního sdělení podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), dále jen "zákon" a v této souvislosti uvádím následující:

*** Obchodní sdělení jsem obdržel prostřednictvím:**
(Alespoň jedna z hodnot je povinná)
E-mail
Fax
SMS

Telefonní/Faxové číslo odesílatele
Telefonní/Faxové číslo příjemce
Číslo sms brány odesílatele

*** Kopie hlavičky e-mailu:**
(Povinné. Pokud zadáte, tak minimálně 300 znaků. V případě velikosti hlavičky větší než 2000 znaků ji prosím vložte jako přílohu.)
(Napsáno 0 znaků.)

Příloha (maximálně 500kB): Procházet...

(z technologických a bezpečnostních důvodů nebude tato položka při chybném odeslání formuláře zapamatována a je nutné ji zadat znovu)
(ke zpracování budou přijaty pouze tyto přílohy: DOC, TXT, PDF, JPG, GIF, XLS, MSG, EML, HTML)

[27]

Obr. 61. Část formuláře pro oznámení spamu na stránkách ÚOOÚ

Celý formulář je možno nalézt na webové adrese ÚOOÚ, jeho přímou adresu uvádím zde: http://www.uoou.cz/uoou.aspx?menu=23&submenu=27&loc=464.

3.5 Odhlášení spamu

Některé spamové maily obsahují ve spodní části položku odhlášení z odběru (unsubscribe mail). Jedná o kontroverzní otázku, zda se odhlašovat nebo ne? Odpovědí na tuto otázku může být citace z jedné knihy: *Ze spamerských seznamů se rozhodně neodhlašujte – tím jen potvrdíte, že vaše adresa je „živá", že ji používáte.* [28]


Od: Laura Allan [noreply@serverbg3.com]
Komu: [redacted]
Kopie:
Předmět: Business Update 2011-2012
Zpráva | ebg2011_1.pdf (25 kB)

Ladies and Gentlemen.

In order to have your company inserted in the registry of World Businesses for 2011/2012 edition, please print, complete and submit the enclosed form (PDF file) to the following address:

Europe Business Guide
P.O. BOX 2021
3500 GB, UTRECHT
THE NETHERLANDS

email: register@the-ebg-2011.net
FAX: +31 (20) 524-8107

Updating is free of charge!

If you are not the intended recipient, please submit an email to unsubscribe@the-ebg-2011.net Your request shall be dealt with accordingly.

Message ID: Lyjdyipun

Obr. 62. Ukázka možnosti podvodného odhlášení spamového emailu

Důvodem proč nevěřit těmto možnostem odhlášení ze spamových seznamů může být skutečnost, že údajná doména the-ebg-2011.net je zřejmě podvodná a nelze ani nalézt podrobnosti o této doméně v systémech DNS. Při dotazu na MX záznamy se z DNS vrací informace o nemožnosti načtení podrobností pro tuto doménu.

4 DOTAZNÍK

Vytvořil jsem krátký dotazník, který nastiňuje veřejné povědomí o problematice nevyžádané pošty. Byly pokládány základní a předpokládám i důležité otázky. Dotazník je přiložen jako

PŘÍLOHA Č. 1 - **DOTAZNÍK**.

Pokládané otázky:

1. Máte emailovou schránku (adresu), pracovní či soukromou, více schránek?
2. Kolik mailů pošlete měsíčně?
3. Víte co znamená slovo SPAM?
4. Setkáváte se s nevyžádanou poštou (spamem) ve své emailové schránce?
5. Využíváte nějakou aktivní technologii proti příjmu nevyžádané pošty (spamu)?
6. Kolik nevyžádaných (spamových) mailů dostáváte měsíčně?
7. Řekl(a) by jste, že je globální (celosvětový) problém s nevyžádanou poštou (spamem)?
8. Byl(a) by jste rád(a), za informace, které by Vám pomohli omezit příjem nevyžádaných mailů (spamu)?

4.1 Vyhodnocení odpovědí

Dotazník byl zodpovězen stovkou dotázaných. Dotázaní byli náhodně vybráni, nebylo rozlišováno mezi pohlavím, ani věkem dotazovaných. Nejmladší z dotazovaných měli 15 let a nejstarší kolem 86 let, z jejich odpovědí jsou tvořeny následující tabulky. Tabulky jsou vyplněny v procentech podle odpovědí dotázaných, s případným textovým doplněním.

Otázka č. 1 – Máte emailovou schránku, pracovní či soukromou, více schránek?		
ANO	**NE**	**Více schránek**
96 %	4 %	80 %

Tab. 7. Otázka č. 1

Z celkového počtu dotázaných má 96% mailovou schránku, z toho 80% má více než jednu emailovou schránku. Průměrně vyšlo na jednoho dotazovaného zaokrouhleně 2,5 schránky. Paradoxně schránku neměli muži kolem 30-40 let. Více schránek měli lidé v produktivním věku (soukromé a pracovní).

Otázka č. 2 – Kolik mailů pošlete měsíčně				
Méně než 10	**Méně než 50**	**Méně než 100**	**Více než 100**	**Neodpovědělo**
12 %	42 %	17 %	24 %	1 %

Tab. 8. Otázka č. 2

Veřejnost byla dotázána na počet odeslaných mailů (lépe se tak určí aktivní práce se schránkou, než z doručených mailů). Na jednu schránku vychází průměrně 22,8 odeslaných zpráv měsíčně.

Otázka č. 3 – Víte co znamená slovo SPAM?			
ANO	**NE**	**Neodpovědělo**	**Správně formulovalo**
88 %	11 %	1 %	87 %

Tab. 9. Otázka č. 3

Otázka číslo 3 byla zaměřena na znalost pojmu SPAM. V 87% byli dotazováni schopni správně formulovat, co dané slovo znamená. Nejčastěji se vyskytovala formulace jako nevyžádaná pošta, nevyžádaný mail. Povědomí o významu slova SPAM je vysoké.

Otázka č. 4 – Setkáváte se s nevyžádanou poštou (SPAMem) ve své emailové schránce?		
ANO	**NE**	**Neodpovědělo**
79 %	17 %	4 %

Tab. 10. Otázka č. 4

S nevyžádanými maily přímo ve složce pro doručenou poštu se ve své emailové schránce setkává 79% dotázaných. Polovina z dotázaných, kteří odpověděli, že se s nevyžádanou poštou ve své schránce nesetkávají, připustili skutečnost, že do složky pro nevyžádanou poštu jim občas nějaký mail dojde. Nicméně i tak se jedná o vysoké procento.

Otázka č. 5 – Využíváte nějakou aktivní technologii proti příjmu nevyžádané pošty (SPAMu)?		
ANO	**NE**	**Neodpovědělo**
29 %	67 %	4 %

Tab. 11. Otázka č. 5

Zda využívají dotazovaní, nějakou aktivní technologii proti příjmu nevyžádané pošty odpovědělo 29%, že ANO. 67% dotazovaných odpovědělo, že žádnou aktivní technologii nevyužívají, popř. jen to co mají na freemailových serverech. Nejpoužívanější aktivní ochranou jsou nastavení freemailových poskytovatelů emailových schránek, dále filtrovací pravidla a časté je užívání blokování emailových adres v Microsoft Office Outlook. Výjimečně byli dotazovaní schopni určit přímo název aktivně užívané technologie (produkt), objevily se pojmy jako SpamAssassin nebo Barracuda spam. Většina dotazovaných se sama nijak aktivně nebrání, nechávají řešení na poskytovatelích freemailových serverů.

Otázka č. 6 – Kolik nevyžádaných (SPAMových) mailů dostáváte měsíčně?				
Méně než 10	**Méně než 50**	**Méně než 100**	**Více než 100**	**Neodpovědělo**
34 %	38 %	11 %	12 %	5 %

Tab. 12. Otázka č. 6

Otázka č. 6 byla mířena na zjištění kolika lidem, dojde nějaký spam do složky pro doručenou poštu. Přes 70% dotázaných se setká s méně jak 50 spamovými zprávami ve své emailové schránce ve složce pro doručenou poštu a to i přesto, že většina spamových zpráv je automaticky směřována do složky se spamem.

Otázka č. 7 – Řekl(a) by jste, že je globální (celosvětový) problém s nevyžádnou poštou (SPAMem)?		
ANO	**NE**	**Neodpovědělo**
89 %	8 %	3 %

Tab. 13. Otázka č. 7

Veřejnost má výborné povědomí o skutečnosti, že se jedná o globální (celosvětový) problém. Velice zajímavé bylo, že většina odpovědí NE byla od lidí mladšího věku (odhadem do 20 let).

Otázka č. 8 – Byl(a) by jste rád(a), za informace, které by Vám pomohli omezit příjem nevyžádaných mailů (SPAMu)?		
ANO	**NE**	**Neodpovědělo**
72 %	25 %	3 %

Tab. 14. Otázka č. 8

Převážná většina dotázaných (72 %) by uvítalo informace o tom, jak omezit příjem nevyžádaných mailů do svých emailových schránek, popř. jak zajistit kvalitnější a lepší třídění na SPAM a HAM.

Celkové povědomí veřejnosti v problematice nevyžádané pošty je velmi dobré. Paradoxem je spíše nevědomost ze strany mladších dotázaných, u kterých by se spíše předpokládaly lepší vědomosti o problematice kyberprostoru.

ZÁVĚR

Cílem práce bylo čtenáře seznámit s historií a používanými termíny v problematice nevyžádané pošty – SPAMu.

V práci byly uvedeny a podloženy důvody pro masové šíření nevyžádané pošty, jedná se o stále lukrativní trh s prodejem různých produktů (viagra, rolex, prodloužení penisu apod). Ačkoliv je povědomí veřejnosti o této problematice na vysoké úrovni, což dokazuje vyhodnocení jednoduchého dotazníku, jsou v Internetu a Internetové poště stále skupiny lidí, které jsou schopny nabízené produkty zakoupit. Šiřitelé nevyžadaných mailů mají tak stále otevřený trh, finance získávají buď ze samotného šíření a následného prodeje nabízených produktů, nebo z prodeje seznamů emailových adres.

Dále byly rozebrány a názorně ukázány technologie pro preventivní, pasivní a aktivní přístup k problematice nevyžádané pošty. Každá ukázka byla dostatečně popsána, v některých případech bylo i nastíněno buď klíčové, nebo celé praktické použití. Nejedná se samozřejmě o kompletní popis všech existujících technologií, ale o nejpoužívanější a nejefektivnější postupy. U aktivních technologií byly uvedeny statistiky funkčnosti.

Problematika nevyžádané pošty byla konfrontována s existujícími zákony platnými v Evropské unii a České republice. Většina těchto zákonů i přes svou existenci není úřady nikterak aktivně kontrolována. Úřady stále evidují nevyžádanou poštu jako určitý aspekt kyberprostoru, který nelze od něj odloučit a je tedy nevyhnutelný. Nicméně každým dnem jsou úřady stále víc a víc tlačeny k řešení tohoto fenoménu internetové komunikace.

Doporučením běžnému uživateli i velké firmě by mohlo být vhodné strategické plánování nasazení emailových adres s aplikacemi popsanými v preventivních technologiích. Dále nutná pasivní ochrana a nezbytná aktivní ochrana. Podle předchozí věty by se tedy dalo doporučit běžnému uživateli užívání více emailových schránek a aktivní omezování přijímaného spamu třeba Bayesovým filtrem. Stejně tak i firmy by se měly lépe chránit proti příjmu spamu. U firem je však vhodné ochranu rozvrhnout do několika oddělených úrovní a užít i více času pro přípravu na boj s nevyžádanou poštou. Je rozdíl mezi uživatelem s měsíčním příjmem desítek až stovek emailů a firmy s tisíci až statisíci mailů měsíčně.

Budoucnost omezování nevyžádané pošty vidím v užívání úmělé inteligence pracující na principu Bayesových filtrů. Toto řešení bych i doporučil jako minimum.

FINALLY

The aim of this work was to make the reader familiar with the history and terms used in the issue of unsolicited mail – spam.

The work presents reasons for the mass distribution of spam; it is still a lucrative market for selling different products (Viagra, Rolex, penis enlargement, etc.). Although public awareness of this issue is high, which proves a simple questionnaire evaluation, there are still groups of people on the Internet and Internet mail who are able to purchase the offered products. So the distributors of junk mail have open market available and get the finance either from the actual distribution and subsequent sale of product offerings or the sale of email address lists.

Furthermore the technologies for preventive, passive and active approach to dealing with spam were discussed and exemplified. Each example was well described with outlining either the key or full practical use in some cases. Of course it can not be considered as a complete description of all existing technologies, but more likely as a summary of the most common and effective procedures. The active technologies include statistics of functionality.

The issue of spam has been confronted with the existing laws in force in the European Union and the Czech Republic. Despite their existence the most of these laws are not actively controlled by the authorities in any way. The authorities still think of spam as a certain aspect of cyberspace that can not be separated and it is therefore inevitable. However, the authorities are pushed more and more to solve this phenomenon of Internet communication on a daily basis.

Recommendation to the ordinary users and large companies may be the appropriate strategic planning (and/by?) using the e-mail addresses with applications described in preventive technologies. In addition, passive protection and necessary active protection is needed. According to the previous sentence the ordinary user should be recommended to use multiple mailboxes and active reduction of received spam, e.g. by applying the Bayes filter. Similarly, the companies should better protect themselves against receiving spam. For companies it is advisable to divide the protection into several separate levels and take more time to prepare for the fight against spam. There is the difference between a user with a monthly reception of tens to hundreds of emails and a company receiving thousands to hundreds of thousands of emails per month.

In my opinion the future way of reducing spam lies in using artificial intelligence operating on the principle of Bayes filters. I would also recommend this solution as a minimum.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[3] POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP.* 1. vyd. Brno: Computer Press, a.s., 2007. 160 s. ISBN 978-80-251-1777-4.

[5] WOLFE, Paul, SCOTT, Charlie, ERWIN, Mike W. *Antispam: Metody, nástroje a utility pro ochranu před spamem.* 1. vyd. Brno: Computer Press, a.s., 2005. 376 s., 1 CD. ISBN 80-251-0479-6.

[9] ADÁMEK, Martin. *Spam: jak nepřivolávat, nepřijímat a nerozesílat nevyžádnou poštu.* 1. vyd. Praha: Grada Publishing, a.s., 2009. 168 s. ISBN 978-80-247-2638-0.

[16] WALTER, Henrik, SANTRY, Patrick. *Jak zabezpečit Exchange Server 2003 a Outlook Web Access.* 1. vyd. Brno: Computer Press, a.s., 2006. 248 s. ISBN 80-251-0910-0.

[28] KOCMAN, Rostislav, LOHNISKÝ, Jakub. *Jak se bránit virům, spamu a spyware.* 1. vyd. Brno: Computer Press, a.s., 2005. 148 s. ISBN 80-251-0793-0.

Internetové zdroje:

[1] *ROYAL PINGDOM* [online]. [cit. 2011-02-19]. Dostupný z WWW: <http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers>.

[2] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-02-23]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/E-mail>.

[4] *WISHLIST* [online]. [cit. 2011-02-25]. Dostupný z WWW: <http://www.wishlist.nu/2006/12/21/hormel-spam>.

[6] *GOOGLE ARCHIV* [online]. [cit. 2011-02-03]. Dostupný z WWW: <http://webcache.googleusercontent.com/search?q=cache:qJCIhJPqBA8J:www.1-inzerce-zdarma.cz/index.php%3Fpage%3Dinzerce%26idx%3D166918+koup-%C3%ADm+seznam+emailov%C3%BDch+adres&cd=7&hl=cs&ct=clnk&gl=cz&source=www.google.cz>.

[7] *SME.CZ: Internetový denník* [online]. [cit. 2011-03-07]. Dostupný z WWW: <http://www.sme.sk/c/3965275/z-azetu-unikli-e-mailove-adresy.html>.

[8] *SUGESTSOFT.COM* [online]. [cit. 2011-03-17]. Dostupný z WWW: <http://www.suggestsoft.com/soft/emarksofts/fast-email-harvester>.

[10] *WEST BAY WEB: Internet Publishing* [online]. [cit. 2011-03-21]. Dostupný z WWW: <http://www.wbwip.com/wbw/emailencoder.html>.

[11] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-03-22]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/CAPTCHA>.

[12] *ULOZ.TO* [online]. [cit. 2011-03-22]. Dostupný z WWW: <http://www.uloz.to>.

[13] *SYMBIO: Internetová agentura* [online]. [cit. 2011-03-22]. Dostupný z WWW: <http://www.symbio.cz/clanky/ochrana-formularu-proti-spamu.html>.

[14] *SOFTWARE QA AND TESTING RESOURCE CENTER* [online]. [cit. 2011-03-22]. Dostupný z WWW: <http://sqa.fyicenter.com/Online_Test_Tools/Test-_Email_Address_Generator.php>.

[15] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-03-07]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol>.

[17] *GREEN END ORGANISATION* [online]. [cit. 2011-03-08]. Dostupný z WWW: <http://www.greenend.org.uk/rjk/2000/05/21/smtp-replies.html>.

[18] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-03-08]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Post_Office_Protocol_version_3>.

[19] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-03-08]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Internet_Message_Access_Protocol>.

[20] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-03-23]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Multipurpose_Internet_Mail_Extensions>.

[21] *COMPUTER PRESS* [online]. [cit. 2011-03-23]. Dostupný z WWW: <http://www.cpress.cz/knihy/tcp-ip-bezp/CD-dalsi/CD-mime/mime.htm>.

[22] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-03-23]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Spam#Blacklisting>.

[23] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-03-29]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Thomas_Bayes>.

[24] *WIKIPEDIE: Otevřená encyklopedie* [online]. [cit. 2011-03-29]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Bayesova_věta>.

[25] *WEBLOG Tomáš Hanus* [online]. [cit. 2011-03-29]. Dostupný z WWW: <http://ixulot.ooo.cz/blog/tipy-triky/proti-spamu-je-bayesovo-filtrovani-nejefekti-vnejsi-323.aspx>.

[26] *ONEBIT web hosting* [online]. [cit. 2011-03-30]. Dostupný z WWW: <http://www.onehelp.cz/onebit/kb/jake-testy-antispam-provadi>.

[27] *ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ* [online]. [cit. 2011-03-30]. Dostupný z WWW: <http://www.uoou.cz/uoou.aspx?menu=23&submenu=27-&loc=464>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ASCII	American Standard Code for Information Interchange
DNS	Domain Name System
DNSBL	Domain Name Systém Blackhole List, Block List nebo Black List
DSL	Digital Subscriber Line
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISP	Internet service provider
MAPS	Mail Abuse Prevention System
MDA	Mail Delivery Agent
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transfer Agent
MUA	Mail User Agent
MX	Mail eXchange
POP3	Post Office Protocol version 3
RFC	Request for Comments
SKK	Slovak koruna
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
USD	United States dollar
XHTML	eXtensible HyperText Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA Č. 1 - DOTAZNÍK

1. **Máte emailovou schránku (adresu), pracovní či soukromou, více schránek?**

   ANO NE kolik: ……

2. **Kolik mailů pošlete měsíčně?**

   Méně než 10 méně než 50 méně než 100 více než 100

3. **Víte co znamená slovo SPAM?**

   ANO NE definice: ……

4. **Setkáváte se s nevyžádanou poštou (SPAMem) ve své emailové schránce?**

   ANO NE

5. **Využíváte nějakou aktivní technologii proti příjmu nevyžádané pošty (SPAMu)?**

   ANO NE jakou: ….……

6. **Kolik nevyžádaných (SPAMových) mailů dostáváte měsíčně?**

   Méně než 10 méně než 50 méně než 100 více než 100

7. **Řekl(a) by jste, že je globální (celosvětový) problém s nevyžádnou poštou (SPAMem)?**

   ANO NE

8. **Byl(a) by jste rád(a), za informace, které by Vám pomohli omezit příjem nevyžádaných mailů (SPAMu)?**

   ANO NE