SPAM и стстеми за защита от SPAM

Цветко Ценков Румен Рачков

Дата: 2007-06-06

Съдържание:

1. Въведение

В днешно време, едва ли има някой, който да си няма никаква идея какво представлява email-а. Според статистики направени от RadicatiGroup в началото на 2006, в света има повече от 1.1 милиард хора, ползващи електронна поща. Иначе казано всеки шести човек на планетата има поне един регистриран email account. Всички тези хора са заплашени от сериозния проблем свързан с безпроблемното им използване – а именно от непрестанното получаване на купища досадни и в повечето случаи нежелани писма, които само "задръстват" тяхната електронна поща. Spam-а е пречка за потребителите заради загубата на време и нерви, отделени за прочистването от нежеланите писма. Също така води до финансови разходи свързани с интернет трафика, който се генерира от получените електронни писма.

Така нареченият spam, не тормози само email потребителите, а и интернет доставчиците. Колкото повече spam получават клиентите на един интернет доставчик, толкова повече се товари неговата мрежа, което води до намаляването на качеството на предлаганите от него услуги.

Все повече хора хвърлят все повече пари за борба със spam-а. Неотдавна Щатският Сенат прие закон, според който спамът се наказва с до една година затвор и глоба до 500 000 долара! А само преди месец - двадесет и седем годишен мъж, смятан за един от най-големите спам-изпращачи в света, беше арестуван от федералните власти в Сиатъл. Робърт Алан Солоуей е обвинен в използване на мрежата за изпращане на милиони спам съобщения по e-mail.

Спамът също така е голяма пречка за много фирми, които не са интернет доставчици по следните причини:

- При големи и средно големи фирми, кореспонденцията между служителите с помощта на email е силно разпространена. При наличието на spam, тя силно се затруднява.
- Spam-а задръства фирмените mail server-и
- Spam-а губи страшно много корпоративно време, пречейки на служителите на фирмата да се съсредоточат в това което вършат.
- Spam-а, в комбинация с незнанието на фирмените работници, може да е причина за проникването на вируси, в иначе добре защитената локална фирмена мрежа.

2. Какво всъщност е спам ?

Има различни схващания но в общия случай за спам се смятат анонимни, нежелани писма. Анонимни в такъв смисъл, че по някакъв начин реалният изпращач е прикрил своя email адрес. Обикновено спам съобщенията се изпращат в огромни количества, защото самите спам изпращачи печелят от малкото отговори които получават(или от проявения интерес към съдържанието на писмата). Най-често спама е с цел реклама, заразяване с вируси, flood на електронни пощи.

Кое точно е спам и кое не?

Много е важно когато се създава защита от спам съобщения, добре да се разграничава коя част от съобщенията са спам и коя не. Този въпрос е зависещ от много фактори, като например цели на използване на пощата, интереси на хората които я ползват и т.н. Има различни спам филтри, които са до някаква степен добра защита от нежеланите съобщения, но никой от тях не може да гарантира 100% сигурност.

Една надеждна анти-спам система трябва да е способна да разграничава желаните от нежеланите съобщения – да вземе в предвид с какво се занимава тя, партньорството и с други фирми, дори интересите на различните отдели във фирмата. Например транспортният отдел може да се интересува от новини свързани с развитието на транспортната инфраструктура. Програмистите на Java пък може да се интересуват от последните новости в Java 6 Enterprise и всичко свързано с нея. Всичко това е свързано с настройки и човешка намеса.

В Microsoft например е-мейлът е предпочитаното средство за връзка и той се употребява по-често от телефонните обаждания, документите, блоговете или срещите. Бил Гейтс: “На ден получавам средно по 100 е-мейла. Прилагам следния начин на филтриране – получавам само е-мейли от хора и компании, с които вече съм кореспондирал – служители на Microsoft, компании-партньори и т.н.”

3. Мейл услугата в интернет

Тази секция на кратко представя как работи email услугата, начина на изпращане на електронна поща, ползвани протоколи. Изпращането на едно електронно писмо много прилича на изпращането на обикновена поща. Как става това ? Написваме писмото, поставяме му адрес на получателя и собствения си пощенски адрес, след което отиваме в пощата и го поставяме в определената за региона пощенска кутия. След това служителите от пощата проверяват за къде е писмото(до къде е адресирано) и по това преценяват на коя поща да го доставят. След доставянето на писмото до пощата отговаряща за региона на получателя, писмото пристига в точната пощенска кутия, която е посочена в адреса на получателя. На подобен принцип работи и email-а, с тази разлика че ролята на пощите играят компютрите с помощта на нужния софтуер.

Нека разгледаме някои от основните елементи на email технологията и използваните **протоколи**:

- *Mail User Agent* (**MUA**) – това са клиентски програми (като Emacs, Microsoft Outlook, Thunderbird) с помощта на които се пишат и четат електронни писма.
- *Mail Transfer Agent* (**MTA**) наричан още mail server – програма (като qmail, sendmail, postfix) отговаряща за пренасянето на електронните писма от изпращача до получателя. **SMTP**(Simple Mail Transfer Protocol)

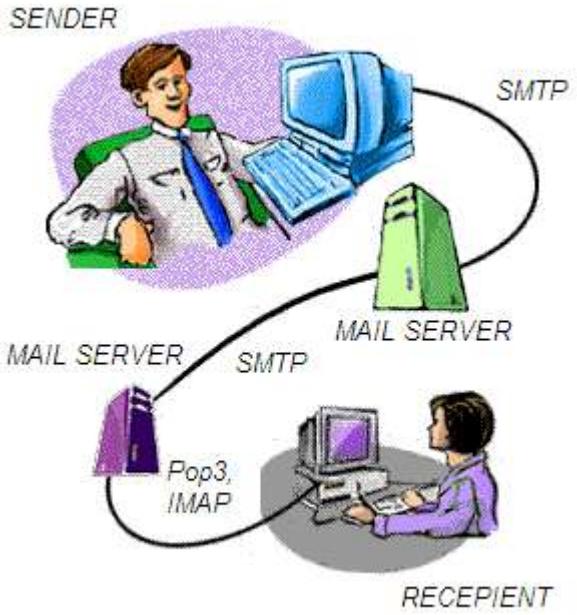
– протокол за предаване на електронна поща от клиент (MUA) към сървър (MTA) или от сървър към друг сървър . Обикновено работи с TCP на порт 25. Независимо дали използват POP3 или IMAP4 за получаване на съобщения, клиентите използват SMTP протокола за изпращането им. SMTP разделя съобщението на envelope и body. Envelope е аналогия на плик при нормалните съобщения, на които пише до кой е адресирано съобщението (“чете” се само от машините не от хората). В envelope-а има и адреса на изпращача, за да може той да бъде уведомен при евентуален неуспех при изпращане на съобщението(както е и при не електронните писма). В body-то се съдържа самото съобщение, от кой е то, за кой е адресирано(“чете” се само от хора, т.е. не представлява интерес за машината).При комуникацията между клиента и сървъра, клиента изпраща команди и евентуално писмото, а сървъра изпраща отговори за да каже на клиента дали е приел/изпълнил командите или нещо се е объркъло. Отговорите от сървъра са в специален формат: три цифри последвани от интервал (или тире) и след това някакъв произволен текст(при грешки обикновено е обяснение за грешката, иначе просто бележка). Ако има тире след третата цифра вместо интервал, следователно отговора продължава; иначе това е последния ред от него. Единствената наистина важна част от отговора е първата цифра:

Код	**Значение**
2xx	Всичко е наред
4xx	Временен проблем, опитай отново по-късно
5xx	Сериозна грешка. Откажи се

- *Post Office Protocol* (**POP3** – тройката е заради текущата версия на протокола) - протокол за извличане на електронна поща от email сървър на клиент, с помощта на клиентска програма(MUA). Поддържа се от повечето такива(Microsoft Outlook, Thunderbird, Eudora). Специфичното, е че сървъра (MTA) запазва писмата при него, и с помощта на протокола и MUA писмата се издърпват на клиентската машина и могат да се изтрият от сървъра или да си останат на него. По този начин електронната поща може да се чете от различни места, като заедно с това печелим и надеждност (при евентуален проблем с машината изтеглила писмото). Както се вижда типично за протокола е еднопосочност. Той е проектиран е за user-to-mailbox(потребител към пощенска кутия) връзка, като са създадени и възможности за authentication, но данните за автентикация се предават като чист текст, затова трябва да се внимава при ниско ниво на сигурност.
- *Internet Message Access Protocol* (**IMAP**) – протокол за отдалечено свързване на mail клиент с mail сървър, за който се твърди че е създаден за да запълни недостатъците на POP. За разлика от POP(който се свърза само за да изтегли съобщенията от сървъра) IMAP може да поддържа постоянна връзка със сървъра, и редовно да проверява за нови писма. Както POP, IMAP също се поддържа от повечето съвременни mail клиенти. Чрез IMAP съобщенията могат да бъдат търсени по дадени критерии още на сървъра, без да е нужно предварително да се изтеглят на клиента. Също така IMAP4 позволява състоянието на

съобщенията(прочетени, непрочетени и т.н.) да се запазва на сървъра с помощта на специални флагове.

И така когато искаме да изпратим електронно писмо, първо го пишем, адресираме го, след което натискаме бутона “изпрати”. От там съответния MUA изпраща писмото до съответния мейл сървър отговарящ за нашата поща. SMTP слага envelope на писмото и се грижи за пренасянето му до съответния мейл сървър, отговарящ за пощата на получателя. След получателят сваля(чрез POP или IMAP протокол) и чете писмото си с неговият MUA.



4. Филтри за SPAM

Тъй като спамът е постоянно нарастващ проблем за email потребителите а и не само за тях, постоянно се разработват методи за защита от него – от такси за регистрация на email до отказването на всички писма идващи от хора които се считат за непознати. Спам филтрите, са един от начините за решаването на проблема, но за жалост само до някаква степен. В най – проста форма, спам филтрите са метод за класифициране на на съобщенията, били те спам или не. Съществуват най – различни начини за класифициране на съобщенията. Може те да бъдат проверявани за обичайните спам белези като например: вече известни адреси които изпращат спам, обичайни спам заглавия(едни от най – честите са предлагането на виагра или пък съобщаването на това, че сте спечелили 1 000 000 долара примерно), известни препращащи машини от където може да дойде спама, известни спам фрази и т.н. За тези обичайни белези могат да се проверяват header-ите и body-тата на идващите съобщения. Друг начин на филтриране на съобщения е отказването(маркирането им като спам) на всички такива, които пристигат от непознати. Може също да сравним съобщението с други съобщения, които други са получили, и да открием общи спам съобщения. Едни от известните спам филтри са SpamEaterPro, CA Anti-Spam, Spam Killer, всички тези са платени и безплатни Spam Assassin, Spam Butcher. Когато едно съобщение бъде класифицирано като спам може да бъде изтрито(това не е добра практика, защото винаги има вероятност да се изтрие съобщение което не трябва да бъде трито), да бъде маркирано като спам(за лесното забелязване че съобщението е спам, като например добавяне на [[[SPAM]]] към subject-а на съобщението) или да бъде

преместено на място определено за спам съобщенията, но това изисква допълнителни ресурси.

4.1. Филтриране по съдържание

При филтриране по съдържание главната идея е да се прави анализ на съдържанието на писмото и от този анализ да се вадят изводи дали писмото е спам или не. Товам може да стане чрез използването на **регулярни изрази**, които да засичат обичайните за спам писмата думи, фрази, изречения. Също се гледа **header**-а на полученото съобщение, където се съдържа информацията за него. Изпращачите на спам могат да прикрият самоличността си или да направят съобщението да изглежда нормално(не спам), но тези методи често се хващат. Статичното филтриране обаче си има и своите недостатъци, като нуждата от поддръжка и прекалено многото **false positives.** False positives са такива съобщения които не са спам, но класифицирани като такива. **Miss** пък са такива които са спам, но не са класифицирани като такива.

4.2. Филтриране по статистика

Тези филтри класифицират съобщенията като спам/не спам на базата на събрани статистики. Когато филтъра разполага с много съобщения спам и не спам, си прави индексация за отделните думи/фрази, за това каква е вероятността им те да са спам. Така филтъра индексира и думите вероятни да са спам, и думи при които вероятността да са от спам съобщение е малка. След това, на базата на тези статистики анализира пристигналото съобщение и го класифицира. Този вид филтриране на пръв поглед много прилича на филтрирането по съдържание, но всъщност много се различава. При това филтриране броят на false positives е доста по-малък. Например ако в едно съобщение се съдържа текст “buy Viagra”, филтъра по съдържание веднага би го маркирало като спам, но филтъра по статистика би анализирал и останалата част от съобщението, и би изчислил каква е вероятността това съобщение да е спам. Това му поведение дава хоризонт на атаки срещу този филтър, като слагането на невалидни HTML тагове, обкръжаването на спам съобщението в легитимен текст, който да заблуди филтъра. Base64 кодирането също се използва, за да залъже филтъра. Но с течение на времето и спам филтъра е еволюирал заедно с атакуващите, и вече декодира съобщението преди да го анализира. Недостатък на този тип филтриране, е че му е нужен голям брой спам и не спам съобщения за да се обучи и да събере достатъчно информация за по-правилен анализ на идващите съобщения. Едни от програмите които ползват филтриране по статистика са Bogofilter, DSPAM, SpamBayes и някои e-mail програми като Mozilla and Mozilla Thunderbird, Mailwasher.

4.3. Checksum филтриране

Този тип филтриране се базира на това, че един спам изпращач обикновено изпраща почти идентични съобщения. Така филтъра си вади статистика за тези съобщения и им генерира checksum-и (като изключва нещата които се различават в различните съобщения). Когато пристигне съобщение, филтъра проверява дали вече няма записана такъв checksum и ако има, отказва съобщението или го маркира като спам. Недостатъка на този тип филтриране е, че спам изпращачите могат да добавят безсмислени фрази в съобщението известни като **hashbusters**, които променят checksum-а на съобщението и заобикалят филтъра.

4.4. Хибридно филтриране

Това е филтриране обединяващо няколко други типа филтриране. Всеки филтър прави анализ на съобщението и то се точкува за това какъв е шанса да е спам. След това ако точките на съобщението са надминали определена граница, съобщението се reject-ва или се маркира като спам. Този вид филтриране е полезен защото се намалява шанса за false positive съобщения, защото се филтрира не само от един филтър.

4.5. Bayesian Spam Filtering

Bayesian е популярен метод за филтриране на спам използван от много сървърни спам филтри (SpamAssassin, SpamBayes, Bogofilter and ASSP). Базиран на теоремата на Bayesian, този метод на филтриране е известен с това, че е доста ефективен обучаващ се филтър. Bayesian спам филтъра ползва съдържанието на писмата за да определи дали те са спам или не са. Обикновено в писмата има обичайни за спама думи, въз основа на които се прави анализ на това, дали писмото е спам или не. Когато потребител на една електронна поща получи писмо и го маркира като спам, този филтър си вади изводи за писмото и съдържанието му, въз основа на което си води статистика за обичайните спам думи и именно за това този филтър се обучава с времето от потребителя. Известна атака срещу този филтър е **Bayesian poisoning**. Тази техника ползвана от спам изпращачите е начин за заобикаляне на филтъра, като в текста на спам съобщението се добавя огромно количество легитимен текст(не обичаен за спама) с цел да заблуди филтъра. Много често срещан такъв вариант е добавянето на поезия в съобщението.

4.6. Collaborative Content Filtering

Това е техника, при която вместо да се наемат хора, които да анализират кое е спам и кое не, или пък да се ползва Bayesian Spam Filtering и потребителя да го обучава, ползва мощта на голяма част от интернет общността ползваща този филтър. Предимството му се крие у това, че съществува връзка между клиентите ползващи електронна поща. Когато потребител на услугата електронна поща получи писмо, филтъра прави предположение за това писмо дали е спам или не. Клиента може да се съгласи с предположението на филтъра или да не го направи, от което филтъра си записва, че писма от този тип са спам/не са такива и така при следващо пристигнало такова писмо, филтъра ще вземе по – добро решение, вземайки предвид вашето. Хитростта се крие у това, че когато филтъра прави предположението, той първо поглежда в записите си, дали вече се е сблъсквал с такова, ако нищо не открие се обръща към другите милиони хора практикуващи филтриране на електронна поща, и така всеки от тях си дава мнението дали това писмо е спам или не. Така ако клиент получи писмо с вирус, опитало се да зарази още примерно 10 000 клиента, на спам филтъра веднага му става ясно, че това е спам(дори клиента да не е на машината си). Съществува и ниво на доверие между, различните клиенти, въз основа на което се решава до колко е достоверно мнението на другите потребители на електронна поща с такива филтри. Предимство на този тип филтриране е, че може да се определи дали едно писмо е спам за много кратко време(по – малко от минута), и затова ако има много потребители които участват в обществото, пораженията които те ще понесат ще бъдат много малки. Друго предимство е, че нито анти-спам организации трябва да пращат информация за спама нито се разчита само на единствения краен потребител да си обучава филтъра.

4.7. Филтриране според изпращача

При този вид филтриране се използват техниките на whitelist based filtering и blacklist based filtering. Системите, предлагани от Microsoft и AOL, разчитат на проверка дали пристигналите мейлове наистина идват от адреса, указан от изпращача. Технологиите на Yahoo и Cisco действат по-различно - те добавят цифров подпис към изпращаните съобщения, така че получателят да може да провери от кого са те и да е сигурен, че не са променяни по пътя.

Черни списъци – При този метод на сървър са записани хората които някога са изпращали спам. От там нататък, сървъра счита за спам всяко съобщение изпратено от хора от черния списък. Това не е много добра практика, защото в интернет пространството съществуват много хора които превземат компютри на обикновени потребители и ги ползват като зомбита. Когато едно от многото зомбита бъде използвано за изпращане на спам, то от там на татък всички съобщения изпратени от този компютър биват считани за спам. По този начин, обикновения потребител не може да кореспондира нормално с повечето хора, поради простата причина, че сървъра на който изпраща, маркира съобщенията му като спам. Друг проблем е че заради един спам изпращач, всички потребители на сървъра губят възможността за нормално изпращане на писма(ако филтъра е настроен да отказва всички писма от сървъра). Тази защита също не е много ефективна, защото обикновено спам изпращачите използват различни идентичности.

Бели списъци – тук нещата стоят обратно. Той съдържа такива системи, на които може да се има доверие, че не са спам изпращачи. От там нататък, съобщенията, които са получени от хора в белите списъци 100% не са спам. Този вариант за филтриране на спам има минимален процент miss-ове, т.е. много малък е шанса да получим спам и филтъра да не го класифицира като такъв. Това се получава, когато компютър зомби, който е в белия списък, изпрати спам – тогава този тип филтриране е неефективен. От друга страна филтриране чрез бели списъци е филтриране с доста голям брой false positives. Друг недостатък на този тип филтриране, е че адресите на изпращача лесно могат да бъдат променени с някои от тези в белите списъци в SMTP съобщението.

Проверка на изпращача – проблемът в общия случай при горните два варианта е че SMTP позволява лесно един изпращач да се представи за друг(mail spoofing), което размива идеята за бели и черни списъци, затова много системи проверяват надеждността на това, дали наистина са получили поща от човека който е указан в sender полето. Един от вариантите е поставяне на електронен подпис в съобщението(криптиран), което гарантира идентичността на изпращача(гаранцията е зависеща от криптографския алгоритъм използван за подписа). Друг начин е чрез **Reverse Domain Name System** – това е начин от IP адрес да получен domain name, също както при DNS получаваме IP за даден domain name. Обикновено спам изпращачите, за да скрият самоличността си, изпращат електронна поща от фалшив IP адрес т.е. неотговарящ на дадения domain name. RDNS филтрирането, взима IP адреса на изпращача и чрез RDNS lookup програма получава реалния domain name. Ако няма такъв валиден domain name за този IP адрес, филтъра маркира писмото като спам. Ако има то се прави още една проверка – дали откритият domain name отговаря на този на изпращача. Това от една страна е добре, защото е един вид защита от mail spoof, но от друга страна не е, защото много често сървъра който иска да изпрати съобщението, използва друг сървър за изпращането му. Този начин на филтриране не е много ефективен. Често се получава така, че се маркират писма като спам, които всъщност не са спам(false positive). Проблеми със забавянето на мрежата също могат да доведат до отказването на иначе легитимно съобщение.

5. Настройки и филтри за предпазване от СПАМ

5.1. Филтриране на SMTP трафик от хостове с лош DNS

Днес операционните системи като Linux и FreeBSD при стандартна инсталация включват механизми за блокиране на трафик по зададен от администратора критерий. Тези механизми могат да бъдат използвани за да бъде блокиран трафика идващ от хостове, които не отговарят на валиден IP адрес. Благодарение на това може да блокираме електронната поща, която идва от хостове, които са с грешна DNS информация.

Ако използвате inetd в FreeBSD следният ред написан в /etc/hosts.allow ще направи горното:

```
ALL : PARANOID : RFC931 20 : deny
```

Същият ефект може да се постигне и ако използвате ucspi-tcp tcpserver пакетите (които днес са препоръчвана алтернатива на inetd) като добавим "-p" параметъра, за paranoid, по точно в /service/qmail-smtpd/run може да се напише:

```
#!/bin/sh
QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
exec softlimit -m 3000000 \
tcpserver -v -p -x /etc/qmail/tcp.smtp.cdb \
-u $QMAILDUID -g $NOFILESGID 0 smtp \
sh -c 'test -z "$TCPREMOTEHOST" \
&& echo "451 bad reverse DNS" \
|| exec /var/qmail/bin/qmail-smtpd' 2>&1
```

Тези няколко реда казват на tcpserver да премахне системната променлива „TCPREMOTEHOST” ако не успее да превърне IP при DNS заявката. Ако „TCPREMOTEHOST” не е идентифициран qmail-smtpd не се стартира.

5.2. Филтриране на SMTP и POP3 трафика на локално ниво (ако нямаме достъп до мейл сървъра)

Тук имаме няколко варианта, но двата основни са: или да сложим на всеки клиент в мрежата ни филтър на компютъра или на рутера и да прекараме всичкия SMTP и POP3 трафик през филтър. На първото решение няма голяма нужда да обръщаме внимание тъй като то е тривиално. Но второто е малко по-интересно и вече има решения, които предоставят тази функционалност.

Едно такова решение е P3Scan. За неговото успешно използване се нуждаете от Linux машина с iptables. P3Scan е абсолютно невидим прокси сървър за e-mail клиентите. През него минават всички изпращани/получавани съобщения от клиентите в мрежата.

За да използвате P3Scan трябва да пренасочите всики „e-mail връзки” към порт на вашия рутер, на който програмата слуша. След като обработи съобщението програмата го изпраща. В комбинация със SpamAssasin P3Scan е едно перфектно решение за защита на вътрешната мрежа от Спам, без да товарите компютрите на клиентите и.

5.3. SpamAssassin

5.3.1. За филтъра

SpamAssassin е интелигентен филтър за електронна поща, който благодарение на редица от тестове разпознава и неутрализира нежелана поща. Той анализира хедърите и тялото на съобщенията като използва различни предварително заложени методи за разпознаване на Спам. SpamAssasin разполага с модулна архитектура, която лесно може да бъде надграждана с нови методи за анализ. Той е разработен да може да бъде лесно интегриран с практически всяка мейл система. SpamAssasin работи добре както на сървъри така и на работни станции, той е широко използваем във всички аспекти на мейл услугите. Той работи безпроблемно на различни операционни системи и със своята модулна структура дава възможност за много надстройки и различни ограничения. SpamAssasin се използва в много интернет доставчици, мейл доставчици, правителствени, частни и некомерсиални организации, учебни заведения и крайни клиенти. Той стои в основата на много комерсиални продукти.

SpamAssasin различно от предшествениците си използва комплексна оценка от различни тестове за да класифицира едно съобщение като Спам, използвайки набор от Perl приложения.

Основните му предимства са:

- Header тестове
- Тестване на фрази от тялото на съобщението
- Bayesian филтриране
- Автоматично класифициране на адрес в черен/бял списък
- Ръчно класифициране на адрес в черен/бял списък
- Проверка в анти-спам бази данни (DCC, Pyzor, Razor2)
- DNS черни списъци, наричани още RBLs (Realtime Blackhole Lists)
- Проверка на символи и анализ

Дори да бъдат измамени няколко от критериите, комплексната оценка трудно бива сгрешена.

Следващите две системи които ще разгледаме ще разчитат на SpamAssasin за защита от Спам.

5.3.2. Инсталация и конфигурация

Инсталацията на филтъра от код под Linux е стандартна:

```
 (unzip/untar the archive)
cd Mail-SpamAssassin-3.2.0
perl Makefile.PL
make
make install      (as root user)
```

После е нужно да добавите в init.d да се стартира автоматично:

```
cp spamd/suse-rc-script.sh /etc/init.d/spamassassin
chmod +x /etc/init.d/spamassassin
```

Примерен конфигурационен файл за SpamAssasin:

```
smoke@linux:~> cat /etc/mail/spamassassin/local.cf
# SpamAssassin config file for version 3.x
# NOTE: NOT COMPATIBLE WITH VERSIONS 2.5 or 2.6
# See http://www.yrex.com/spam/spamconfig25.php for earlier versions
# Generated by http://www.yrex.com/spam/spamconfig.php (version 1.50)

# How many hits before a message is considered spam.
required_score           5.0

# Change the subject of suspected spam
rewrite_header subject         *****SPAM*****

# Encapsulate spam in an attachment (0=no, 1=yes, 2=safe)
report_safe              1

# Enable the Bayes system
use_bayes                1

# Enable Bayes auto-learning
bayes_auto_learn              1

# Enable or disable network checks
skip_rbl_checks          0
use_razor2               1
use_dcc                  1
use_pyzor                1

# Mail using languages used in these country codes will not be marked
# as being possibly spam in a foreign language.
# - bulgarian english
ok_languages             bg en de

# Mail using locales used in these country codes will not be marked
# as being possibly spam in a foreign language.
ok_locales               bg en de

# My options added
blacklist_to spam@tobo-bg.com
bayes_auto_learn_threshold_nonspam 0.1
bayes_auto_learn_threshold_nonspam 9.0
```

5.3.3. Qmail и qmail-scanner

Qmail-scanner е add-on, който позволява сканирането на пощата според критерии на администратора. Той работи на по-ниско ниво от повечето други скенери като следи не само локалните получените/изпратени съобщения, но и съобщенията, които минават през сървъра.

Интегрирането на SpamAssassin към qmail е изключително улеснено благодарение на qmail-scanner. Филтъра бива автоматично намерен след инсталацията. Примерна инсталация:

```
$ ./configure --spooldir /var/lib/qmailscan \
--qmaildir /var/qmail --bindir /var/qmail/bin \
--qmail-queue-binary /var/qmail/bin/qmail-queue  \
--admin postmaster@example.com \
--domain example.com --notify none --local-domains \
example1.com,example3.com,some.other.domain.net \
--silent-viruses auto \
--lang de_DE --debug 1 --unzip 0 --add-dscr-hdrs 0 \
--archive 1 --redundant no --log-details \
--fix-mime 1  --scanners "verbose_spamassassin" --install 1
...
$ ./qmail-scanner-queue.pl (за инсталация)
...
$ ./contrib/test_installation.sh (за да тествате инсталацията
си)
```

При дадената ситуация получаваме едно перфектно решение за защита от спам, което е лесно за имплементация.

5.3.4. Sendmail и milter-spamc

Milter-spamc е интерфейс към SpamAssasin, който спомага за връзката между филтъра и sendmail.

Milter-spamc изпраща хедърите и първата част от тялото (колкото е зададено от spamd-max-size) до spamd (даемон на SpamAssassin) за анализ. Резултата се връща във хедъра на съобщението като не се засяга тялото му. Ако съобщението е класифицирано като спам Milter-spamc променя Subject хедъра със subject-tag и изпраща копие до mail-spam адреса.

Хедърите, които добавя milter-spamc са:

- X-Spam-Flag („да” или „не” в зависимост дали е спам)
- X-Spam-Level (оценка според спам филтъра)
- X-Spam-Status („да”/”не”, заключение за съобщението)
- X-Spam-Report (доклада от SpamAssassin)
- X-Original-Recipient (ако е прехвърлено към адреса за колекция от спам, тук може да се провери за кой е било насочено съобщението)
- X-Scanned-By (допълнителна информация за филтъра и т.н.)

За успешна инсталация се нуждаете от:

- milter-spamc/1.11
- LibSnert
- Sendmail 8.14
- Berkeley DB

Ако искате да имате поддръжка на черни/бели списъци се нуждаете от Berkeley DB 3 или по-нова.

Ако до сега не сте използвали milter за Sendmail, подсигурете се че имате build-нати и инсталирани libmilter библиотеките, които не се build-ват автоматично със senmail.

След като имате инсталиран libmilter инсталирането на libsnert и milter-spamc е абсолютно стандартно:

```
cd (path to)/com/snert/src/lib
./configure
make build
cd ../milter-spamc
./configure
make build
make install
```

Пример за ${prefix}/share/examples/milter-spamc/milter-spamc.mc ви е предоставен по-долу. От този файл нужните елементи трябва да бъдат добавени в Sendmail.mc и sendmail.cf да бъде преправен.

```
dnl ----------------------------------------------------------------
dnl milter-spamc.mc                                    $custom$
dnl ----------------------------------------------------------------
dnl Example configuration to be added to sendmail.mc.
dnl
dnl Copyright 2003, 2007 by Anthony Howe. All rights reserved.
dnl
dnl $OpenBSD$
dnl

define(`_FFR_MILTER', `1')dnl

dnl ----------------------------------------------------------------
dnl Enable this for debug output from Sendmail.

dnl define(`confLOG_LEVEL', `14')dnl

dnl ----------------------------------------------------------------
dnl Enable this to see even more debug output.
dnl Defaults to confLOG_LEVEL.
dnl
dnl If Milter.LogLevel is greater-than:
dnl
dnl 0         Communication errors
```

```
dnl 8        Header & RCPT modification messages
dnl 9        Connect to info
dnl 10       Milter error return codes, abort messages
dnl 12       More return code info, connection/open errors
dnl 14       grey & rcpts info
dnl 17       Show headers & body sent to a milter.
dnl 18       Quit
dnl 21       Time a milter

dnl define(`confMILTER_LOG_LEVEL', 14)dnl

dnl ---------------------------------------------------------------
dnl The S= by default specifies a unix domain socket to be used between
dnl sendmail and the milter. It can also be an Internet domain socket.
dnl The accepted forms are:
dnl
dnl          {unix|local}:/path/to/file          A named pipe. (default)
dnl inet:port@{hostname|ip-address}              An IPv4 socket.
dnl inet6:port@{hostname|ip-address}    An IPv6 socket.
dnl
dnl Note that the F= says what to do with the message if the milter
dnl is not running.
dnl
dnl F=T    Temporary fail connection if filter unavailable
dnl F=R    Reject connection if filter unavailable
dnl
dnl If no F= specified and there is a problem with the milter, then
dnl the default is to continue normal handling, skipping the milter.
dnl
dnl Note that the T= specifies timeouts for communication. The
dnl following fields are defined:
dnl
dnl C        Timeout for connecting to a filter. If set to zero (0),
dnl          the system's connect() timeout will be used. Default: 5m
dnl S        Timeout for sending information from the MTA to a
dnl          filter. Default: 10s
dnl R        Timeout for reading reply from the filter. Default: 10s
dnl E        Overall timeout between sending end-of-message to filter
dnl          and waiting for the final acknowledgment. Default: 5m
dnl
dnl So the Sendmail default values are equivalent to:
dnl
dnl T=C:5m;S=10s;R=10s;E:5m
dnl

INPUT_MAIL_FILTER(
    `milter-spamc',
    `S=unix:/var/run/milter/milter-spamc.socket, T=C:1m;S:1m;R:2m;E:4m'
)dnl
```

```
dnl The default for confMILTER_MACROS_CONNECT is
dnl `j, _, {daemon_name}, {if_name}, {if_addr}'
define(`confMILTER_MACROS_CONNECT', confMILTER_MACROS_CONNECT`,
{client_name}, {client_resolve}')dnl

dnl ------------------------------------------------------------
dnl End milter-spamc.mc
dnl ------------------------------------------------------------
```

След като е инсталиран и конфигуриран стартирайте milter-spamc и след това рестартирайте Sendmail. Примерен скрипт за стартиране в началото има в ${prefix}/share/examples/milter-spamc/milter-spamc.sh. Можете да промените настройките по default в /etc/mail/milter-spamc.cf.

5.4. M$ Exchange 2007

С излизането на новия Exchange 2007 Майкрософт са заложили сериозно на защитата от вируси и Спам. Всяко съобщение минава през няколко слоя на сигурност, като на всякъде бива проверявано по различни критерии и характеристики в специфичен ред:

- Филтър на връзката – проверява дали сървъра от който идва съобщението съществува и решава какво да прави със съобщението. В този слой имаме IP Block листове и IP Allow листове, както и IP Allow Services и IP Block Services, според които се определя дали даден IP адрес да бъде разрешен да изпраща до организацията или не.
- Филтриране на изпращача – сравнява MAIL FROM: SMTP командата със списък дефиниран от администратора с изпращачи, на които е забранен достъп.
- Филтриране на получателя – сравнява RCPT TO: SMTP командата със списък дефиниран от администратора с получатели, на които е забранено да получават поща. Също проверява дали получателя е валиден на сървъра и ако не е валиден съобщението бива отхвърлено.
- Филтър по ID на изпращача – проверява дали изпращача е spoof-нал името си според IP-то на сървъра и Purported Responsible Address (PRA). PRA се базира на следните хедъри:
  Resent-Sender:
  Resent-From:
  Sender:
  From:
- Филтриране по съдържание – Майкрософт са разработили и патентовали доста технологии за разпознаване на Спам според съдържанието на съобщението, които се използват при този филтър. Интересни тук са Safe list-овете, които потребителите на Outlook дефинират и Exchange сървъра получава тези листове посредством Edge Transport сървъра към него. Ако администратора е конфигурирал правилно филтъра по съдържание, той пропуска съобщенията от потребители, които са в тези safe листове без проверки.
- Филтриране според репутацията на изпращача – тук се гледа главно IP адреса, но и други критерии като изпращач и т.н. и се изчислява sender

reputation level (SRL), като основен фактор е репутацията на изпращача според анти-спам ъпдейтите към Exchange, които се обновяват автоматично от Microsoft Update. Ако за даден изпращач се знае, че е склонен да изпраща спам, той бива блокиран.

- Филтриране на прикрепените файлове – тук се следят файловетем които са прикрепени към съобщението.
- Outlook Junk E-mail филтър – След обстойни анализи от анти-спам филтрите на Exchange, ако съобщението бива класифицирано като Junk, то бива изпратено в специална папка в Outlook - Junk E-mail, която по-късно може да бъде прегледана от потребителя.

Microsoft Exchange 2007 Standard Anti-spam Filter се обновява автоматично на всеки 2 седмици посредством Microsoft Update. The Forefront Security for Exchange Server anti-spam update service е допълнителна услуга, която може да се ъпдейтва по няколко пъти на ден като обновява Spam signatures и IP Reputation Service с адреси, които се знае, че изпращат Спам.

Този път Майкрософт наистина са заложили доста нови технологии и са се постарали да спомогнат за намаляването на спам-а посредством техния Exchange сървър.

6. Възможни начини за заобикаляне на филтрите

В последните години борбата със спама е на много високо ниво. Появяват се нови продукти, нови организации и все повече частни фирми и лица започват да се замислят за вредата. Но за съжаление и спамерите не спят, те измислят все по-нови и по гениални техники за разпространение на Спам. И комплексните филтри за които говорихме в предните глави остават беззащитни срещу тях.

6.1. Заобикаляне на филтрите за защита по съдържание

Бавно започва да отминава времето на „V*i^a&g%r^a” съобщенията и техните производни в които се включваха html tag-ове или символи от кодови таблици, които спам филтрите не разпознават. Добавянето на произволни символи или безсмислени кодове вече не помага. Тези атаки вече са минало и за тях има лесни решения да бъдат спрени.

Спам-а картинка – днес това е един от често разпространяваните начини за заобикаляне на филтрите за защита по съдържание. Спамът се съдържа в картинка, която променя по някой пиксел при всяко препращане. Така дори спам филтъра да направи „снимка” на съобщението следващото се различава с 1 пиксел или няколко и е по различно и не се класифицира като спам от филтъра.

Спам в защитен архивиран файл – при тази техника със съобщението се изпраща файл, който е архивиран и защитен с парола като в него се съдържа спам-а, а паролата е в съдържанието на писмото като удостоверява, че този файл е специално за вас. Тук проблемът е че спам филтъра не може да разархивира архива и да го провери.

6.2. Заобикаляне на филтрите за защита по изпращач

Промяна на IP адрес – най-често използваната техника

Тъй като повечето IP адреси на спамери са в черните списъци, една от техниките за успешно изпращане на нежелана поща е като се сдобият с IP на машина, която не е в черните списъци. Това става по няколко начина: чрез използване на proxy сървър, чрез заразяване на потребителски машини и създаването на така наречените зомби машини, които заедно образуват – бот мрежи. В последно време често срещана спам атака е, когато писмото прескача през няколко заразени машини и накрая бива изпратено от машина извън черните списъци.

Използване на грешки при конфигурацията на мейл сървъра

Често администраторите не се замислят за сигурността и просто оставят някакви default настройки или слагат за конфигурационен файл „нещо намерено в Интернет" и по-този начин сървърите им стават удобен инструмент за използване от спамерите. Като използват несъществуващи потребителски имена към техния домейн или пък ботове успяват да регистрират куп акаунти, които да изпозват за собствените си цели.

Набавяне на листове с валидни потребителски пощи

Било то чрез ботове, които претърсват мрежата за е-мейли или чрез успешни пробиви на сървъри с потребителски пощи, поради дупки в сигурността. Друг начин е чрез ботове, които изпращат писма и чакат отговор за проверка дали съществува пощата. Това е един доста добър начин за набавяне на съществуващи пощи, които после са извън черните списъци и стават за успешно разпространяване на СПАМ.

6.3. Защита

Мейл сървъра трябва да бъде настроен да проверява валидността валидността на домейните в DNS зоната. Проверката за валидността на потребителските пощи е също от изключителна важност. Прикачените файлове също трябва да бъдат проверявани. Да се защити сървъра от така наречените атаки по речник за откриване на валидни потребителски имена. Листите с потребители да бъдат под строг контрол. Главно за защитата трябва да бъдат и обучени потребителите, доколкото това е възможно да не отговарят на съмнителни писма и да не отварят съмнителни файлове изпратени до тях. И най-важното винаги да бъдат обновени филтрите към вашия мейл сървър. Бъдете параноични и следете за всяка нова излизаща техника както за защита така и за спам.

7. Заключение

Спамери винаги ще има и може би никога няма да се намери универсалната защита от тях. За да се предпазите от тях най-сигурното решение е да пазите електронния си адрес и да го давате само на хора, които познавате и са „сигурни”. Отговаряйте само на писма, чиято достоверност е гарантирана. А когато се налага да го обявите в публичното пространство да не го предавате в чист вид, така че спам ботовете да го „грабнат” на секундата, а да се опитате да ги затрудните максимално (е разбира се внимавайте да не затрудните и потребителите, които трябва да го видят).

Пример: ime <at> mail (dot) com.

За администраторите на мейл сървъри – използвайте филтри, погрижете се максимално да подсигурите удобството и сигурността на вашите клиенти да не получават СПАМ. Обновявайте ги и се старайте винаги да сте в крак с новите технологии за защита от най-голямата напаст в Интернет – СПАМа.

8. Използвана литература и материали

http://news.bg/
http://www.bgpro.com/1spam.html
http://www.viruslist.com/en/spam/info?chapter=153350526
http://luxsci.com/extranet/articles/email-security.html
http://bglog.net/pclog/6210
http://en.wikipedia.org/
http://arts.monash.edu.au/artsit/email/workings.php
http://spam-filter-review.toptenreviews.com/
http://www.iseca.org/
http://www.techworld.com/security/news/index.cfm?newsid=8733
http://www.techworld.com/security/features/index.cfm?featureid=3029
http://email.about.com/od/emailtrivia/f/how_many_email.htm
http://www.techworld.com/security/news/index.cfm?newsid=8733
http://www.techworld.com/security/features/index.cfm?featureid=3029
http://technet.microsoft.com/en-us/library/42cd5fe3-15f9-44eb-8dc2-c30a247a6686.aspx
http://www.chrishardie.com/tech/qmail/qmail-antispam.html
http://wiki.apache.org/spamassassin/IntegratedInQmailWithQmailScanner
http://www.microsoft.com/exchange/evaluation/features/default.mspx
http://wiki.apache.org/spamassassin/SpamAssassin
http://www.milter.info/sendmail/milter-spamc/#Installation

9. Използван софтуер

Suse 9.3 (http://www.novell.com/linux/)
SpamAssassin 3.2.0 (http://spamassassin.apache.org/)
P3Scan 2.3.2 (http://p3scan.sourceforge.net/)
netqmail-1.05 (http://www.qmail.org/netqmail/)
Sendmail 8.14.1 (http://sendmail.org/)
qmail-scanner-2.01 (http://qmail-scanner.sourceforge.net/)
milter-spamc/1.11 (http://www.snertsoft.com/sendmail/milter-spamc/)

10. Полезни сайтове

http://www.yrex.com/spam/spamconfig.php
http://www.faqs.org/rfcs/rfc2505.html