Opatrenie obmedzujúce rozosielanie spamu

Last updated 26 septembra, 2024

Veľa spamu je rozosielaného z počítačov napadnutých počítačovým vírusom alebo červom. Vírus nebo červ často na počítači otvára tzv. zadné vrátka (backdoor), ktoré umožňujú útočníkovi počítač ovládať na diaľku a zneužiť ho napríklad pre rozosielanie spamu. Robot aj databáza adries môže byť na napadnutom počítači dočasne, rozosielanie nemusí prebiehať neustále. Obranou proti distribuovanému rozosielaniu je klasická antivírová ochrana. Pre správcov siete je dôležité, aby vedel napadnutý počítač lokalizovať a izolovať v čo najkratšom čase. SMTP server musí byť konfigurovaný tak, aby nepreberal maily, ktoré prichádzajú bez identifikácie a preto je na našich serveroch povinná autentifikácia aj pri posielaní mailov cez SMTP server (menom a heslom).

Blacklist

(je používaný aj na našich serveroch)

Blacklist rozhoduje, či mail je nebo nie je spam, podľa IP adresy, z ktorej mail prišiel na cieľový SMTP server. Blacklisty obsahujú IP adresy, z ktorých bolo zaznamenané rozosielanie spamu, bývajú zverejňované najčastejšie pomocou systému DNS. Výskyt adresy v blackliste môže má za následok priame odmietnutie (neprevzatie) mailu ešte behom SMTP spojenia, alebo môže byť informácia z blacklistu použitá ako dodatočná informácia pri následnej filtrácii podľa obsahu.

Greylist

(je používaný na našich serveroch)

Greylist rozhoduje podľa IP adresy a emailovej adresy odosielateľa a adresáta, ale robí to dynamicky. SMTP server, ktorý prevádzkuje greylisting, udržuje databázu, kde pre trojicu (IP adresa, odosielateľ príjemca) je uvedené, či mail s týmito atribútmi má byť doručený alebo má byť doručenie dočasne zamietnuté. Prvý mail je odmietnutý a je zaznamenaný čas, kedy k tomu došlo. Počas istej doby(typicky niekoľko minút) sú maily s týmito atribútmi zamietané, po uplynutí tejto doby sú naopak doručované bez zdržania. Po ďalšej dobe (typicky niekoľko málo týždňov) je záznam z databáze zmazaný, takže ďalší mail bude znova oneskorený.

Využíva sa tu fakt, že protokol SMTP rozlišuje chyby trvalé, ktorých číselný kód začína číslicou 5 a chyby dočasnej s kódom začínajúcim číslicou 4. V prípade dočasnej chyby má

odosielajúci SMTP server mail uložiť do fronty a pokúsiť sa odoslanie opakovať (typicky o niekoľko desiatok minút). Robot rozosielajúci spam však často chyby neošetruje a druhý pokus nespraví. Tiež je možné, že než sa zopakuje druhý pokus odosielateľova IP adresa je už zaznamenaná a zverejnená na blackliste a tým pádom mail už nebude doručený vôbec.

Whitelist

(je používaný na našich serveroch)

Je presný opak, pokiaľ máte záujem dostávať maily z nejakej domény a ich IP adresa je často na zozname spamerov, pridáte si doménu do white listu (napr gmail.com, yahoo.com atď.). Mail z tejto domény Vám bude potom doručený vždy, nebude sa brať zreteľ na to či má príznaky spamu.

Domény si môžete pridávať do blacklistu a whitelistu v control paneli cez https://kp.wy.sk v časti Ochrana e-mailov.

Filtrácia podľa obsahu mailu

Automatické rozpoznávanie nemôže z princípu fungovať dokonale, pretože názor, či konkrétny mail je spam je individuálny. Preto filtrovanie podľa obsahu dáva použiteľné výsledky a veľmi sa používa. Existujú dve základné metódy, niektoré antispamové programy (napr. SpamAssassin) ich kombinujú. Filtrácia podľa obsahu ale nefunguje korektne ak spamer pošle mail ako obrázok. Implementovali sme na server aj rozoznávanie textu z obrázku (OCR) ale pokiaľ je text rôznofarebný a písmo nerovnomerné OCR nemusí fungovať korektne.

Filtre založené na pravidlách

Filtre založené na pravidlách vyhľadávajú v mailoch rysy, ktoré sú pre spam typické. Ide jednak o niektoré slová (napr. viagra) a slovné spojenia, potom sú vyhľadávané chyby pre spam typické. Príkladom je napríklad dátum odoslania v budúcnosti, nedovolené znaky v hlavičke, chybne označený MIME-typ správy atď. Za každý rozpoznaný rys je mailu pridelené bodové hodnotenie, body sa spravidla spočítajú a pokiaľ súčet presiahne hranicu ktorá bola nastavená, je mail pokladaný za spam. Rozpoznávané rysy sú definované podľa pravidiel, ktoré je potrebné pravidelne aktualizovať a prispôsobovať praktikám spamerov. K vytváraniu a údržbe súboru pravidiel je potrebné mať znalosti.

Ako zistím či IP adresa ktorú používam nie je blokovaná antispam spoločnosťou?

Najprv si zistite IP adresu cez http://ip.wy.sk

Potom si pozrite či IP adresa nie je blokovaná cez adresu http://www.dnsstuff.com/tools/ip4r.ch?ip= Pokiaľ je Vaša IP adresa blokovaná konkrétny riadok antispam spoločnosti bude červený.