Maia Mailguard és amavisd-new a Spam levelek és a vírusok réme

Úgy érzi nem engedheti meg magának, hogy vállalkozása vezető spam és vírusvédelmet használjon? Két jó indok, amiért érdemes ezt újragondolni.

Manapság ahogy a spam és e-mail férgek egyre terjednek, eljött az anti-spam és anti-vírus megoldások szállítóinak aranykora. Az ***Európában*** és az ***USA***-ban bevezetett anti-spam törvények nem túl sok eredményt értek el, így az áldatlan állapotok sok embert késztettek technikai megoldások, spam és vírus szűrők vásárlására.
A tartalom szűrése minden egyes gépen ugyanakkor meglehetősen drága és nem is túl praktikus megoldás. Ideális esetben a spam és vírus problémákat gyökerüknél kell kezelni, így e pont mögött mindenkit megvédhetünk.
Ezt a stratégiát követő szervezeteket minden erőforrásukat egyetlen helyre összpontosítják, mégpedig általában a levelező kiszolgálóra.
A kiszolgáló alapú megoldások azonban ritkán olcsók. A legtöbb ilyen termék esetében levelesládánként kell fizetni, legyen szó levelezőkiszolgáló bővítményről vagy önálló tartalomszűrő alkalmazásról. Ezek a megoldások dollárezrekbe is kerülhetnek és gyakran a vírus- és spam-minták frissítéseiért is éves díjat szednek.
Ebben a cikkben az ***amavisd-new*** nyílt forráskódú tartalomszűrő rendszerrel ismerkedhetünk meg, valamint a projekt egyik hatékony kiegészítésével a ***Maia Mailguard***-dal.

amavisd-new

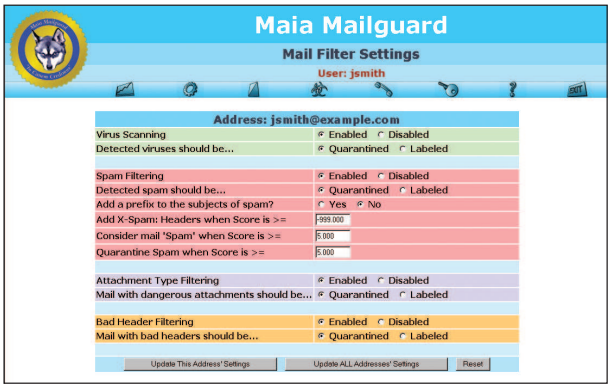
Az ***amavisd-new*** lényegében levelező-szűrő – leveleket fogad a levelezőkiszolgálótól, megállapítja hogy tartalmaznak-e spam-et vagy vírusokat, majd ennek megfelelően karanténba helyezi, elutasítja vagy kidobja a szabálysértő elemeket végül a maradékot a kézbesítést végző másik levelezőkiszolgálóra irányítja. Gyakorlatban az ***amavisd-new*** gyakran található két azonos gépen futó levelezőkiszolgáló között, hiszen, különösen a kisebb helyek esetében, a levelezőkiszolgálót és a tartalomszűrőt praktikus lehet azonos gépen elhelyezni. A nagyobb helyek külön tartalomszűrő gépre telepíthetik az ***amavisd-new***, ***SpamAssassin*** és vírusirtó programjaikat. Még nagyobb helyeken ilyen gépek terheléseloszlásos hálózatát érdemes felépíteni.
Az ***amavisd-new Perl*** nyelven, a biztonságot és megbízhatóságot szem előtt tartva készült és lényegében minden ***UNIX*** rendszeren jól üzemel. Magja az ***RFC***-nek megfelelő levélkezelő, amelyet úgy terveztek, hogy soha ne veszítsen el egyetlen levelet sem. Ennek érdekében az ***amavisd-new*** mindaddig nem veszi át véglegesen a levélelemet amíg az alatt elhelyezkedő levelező kiszolgáló át nem veszi tőle azt. Ez annyit jelent, hogy ha bármilyen hiba történik a levél szűrése közben, a levél nem veszik el, hiszen a felső levelezőkiszolgáló sorában megmarad. Az ***amavisd-new*** négyféle szűrési lehetőséget kínál: virus/malware keresés, spam szűrés, veszélyes csatolmányok és érvénytelen fejlécek tiltása.

Víruskeresés

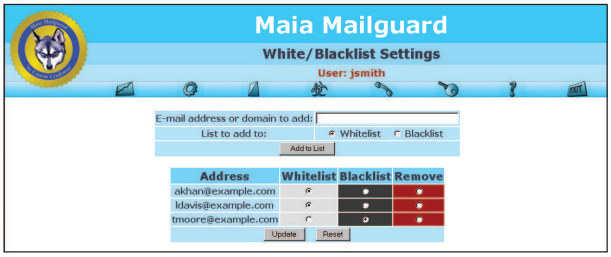
Az ***amavisd-new*** nem víruskereső; inkább egy keretrendszer, amely egy vagy több víruskereső meghívására képes. Több mint 30 népszerű víruskeresőt támogat,többek között olyan üzleti termékeket is mint a ***Sophos***, ***Symantec*** és ***Network Associates***, és persze a nyílt forráskódú ***Clam Antivirus***-t.
A parancssoros és démon-alapú víruskeresők egyaránt támogatottak. Persze a démon alapú keresők sokkal hatékonyabbak mint parancssoros rokonaik. Amennyiben a levelezőkiszolgálónk nagy mennyiségű levelet dolgoz fel, nem valószínű, hogy szívesen töltenénk be a memóriába egy parancssoros víruskeresőt minden egyes levélhez, amit aztán eltávolítunk onnan. A démon alapon futó víruskeresők csak egyszer töltődnek be, végig a memóriában maradnak, így az egész folyamat sokkal gyorsabb.
Amennyiben több víruskeresőnk is van, elsődleges és másodlagos csoportokba sorolhatjuk őket. A másodlagos csoporthoz akkor nyúl a rendszer, ha egyik elsődleges kereső sem érhető el.

Spam szűrés

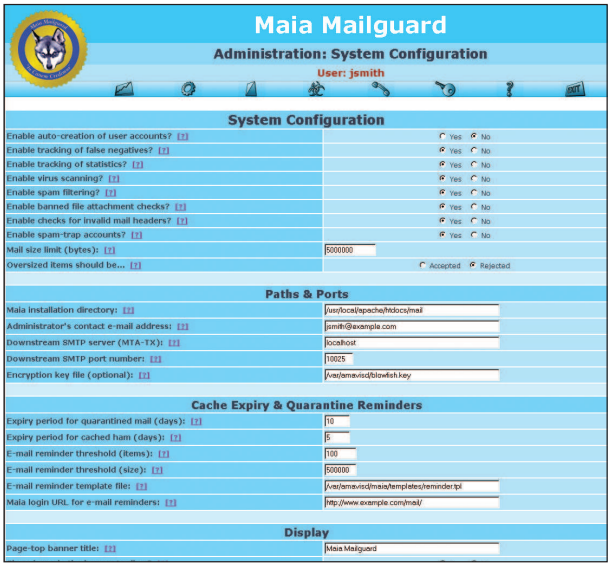
Az ***amavisd-new*** a spamszűrést a ***SpamAssassin*** beépítésével végzi. Az ***amavisd-new*** a címzettek számától függetlenül minden egyes levélhez egyszer hívja meg a ***SpamAssassint***, így a levelezőlisták vizsgálata sem foglal több erőforrást mint az egy címzettel rendelkező levelek.
A ***SpamAssassin*** a spamszűrő módszerek széles skáláját vonultatja fel: képes jellegfelismerésre, ***DNSBL*** és ***SPF*** keresésre, kezeli a ***együttműködésen alapuló jelentési hálózatokat (collaborative reporting networks)*** és a ***Bayes***-féle tanuló



1. ábra Minden e-mail cím saját tartalomszűrő beállításokkal rendelkezik

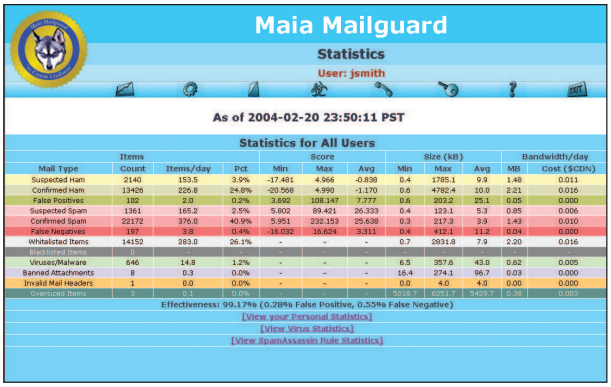


2. ábra A felhasználók saját fehér- és feketelistákat tarthatnak fenn

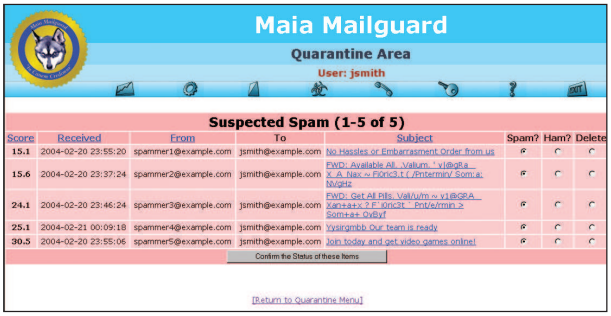


3. ábra A rendszergazda a legtöbb teljes körű beállítást elérheti a webes felületről

módszert. Minden teszt megállapít valamilyen számszerű értéket, amelyet aztán levelenként összegezünk, a felhasználók pedig tetszőleges határértéket állíthatnak be, ezáltal eldöntve, hogy mit tekintenek spam-nek és ham-nek. (A „ham" szó spamszűrő körökben a nem-spam levelet jelenti azaz a spam ellentéte, a *Monty Python* féle spam (löncshús) mintájára. a *fordító*) Ez elég hatékony megoldás, hiszen az egyik módszer gyengéit a többi módszer javítja. A jellegfelismerő a levél fejlécét és a levéltestét vizsgálja olyan nyomok után kutatva, melyeket az emberek spam vagy ham (nem-spam levél) jellegzetességeknek



4. ábra A szűrők által látottakat statisztikák foglalják össze



5. ábra A felhasználói karantén a spam-pontszám szerint rendezett

tartanak. Az a tény például, hogy a levél ***Date:*** fejléce 12 órával a jövőbe mutat vagy, hogy a levél szöveget nem, csak képet tartalmaz, könnyen utalhat spam jelenlétére, míg egy több mint ezer szót tartalmazó levél valószínűsíthetően ham.

A ***SpamAssassin*** képes ellenőrizni a csatlakozó levelező-kiszolgáló vagy ügyfél IP címét, majd ellenőrizni szerepel-e valamelyik ***DNS***-alapú tiltólistán (***DNSBL***), így képes meghatározni, hogy a küldő esetleg ismert spam forrás.

A ***DNSBL*** listák hagyományos alkalmazásával szemben azonban a ***SpamAssassin*** nem feltételezi, hogy a listán való szereplés önmagában végzetes bizonyíték; egyszerűen csak megnöveli a levél teljes pontszámát. Ez sokkal rugalmasabb megközelítés és lehetőséget ad arra, hogy külön beállítsuk valamennyi ***DNSBL*** pontszámát, attól függően mennyire bízunk meg listában és karbantartóinak rendszabályaiban.

A hamarosan megjelenő ***SpamAssassin 3.0*** már támogatja a ***Sender Policy Framework (SPF)*** kereséseket, amely megpróbálja azonosítani, hogy a kapcsolódó gépnek van e joga levelet küldeni az adott tartomány neve alatt.

Az együttműködésen alapuló jelentési hálózatok, mint a ***Vipul Razor***-ja, ***Pyzor*** és a ***Distributed Checksum Clearinghouse (DCC)*** egy másik tájékozódási forrást kínálnak a ***SpamAssassin*** részére. Az alapötlet az, hogy miután a spam leveleket fogadók millióinak küldik el, mire megkapjuk a nekünk szólót, rengeteg ember kap többé kevésbé hasonló leveleket. Amennyiben elég sok ember jelezte hogy az adott levél spam a mi spamszűrőnk is felhasználhatja ezt a tényt saját döntésfolyamatában.

Végül, de természetesen nem utolsósorban, a ***SpamAssassin Bayes***-féle tanuló mechanizmust is tartalmaz, amely lénye-

6. ábra A levélnézegetővel biztonságosan megvizsgálhatjuk a gyanús leveleket

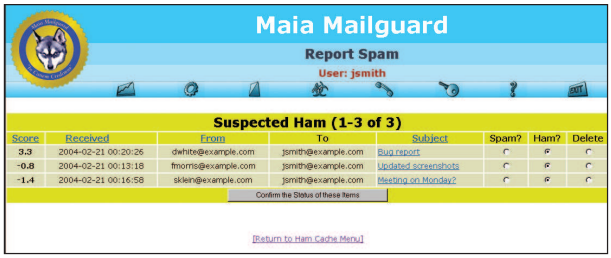
gében automatizált jellegfelismerő. Míg a korábban ismertetett jellegfelismerő rendszer az emberekre bízza a spam és ham közötti felismerhető különbségek azonosítását, a ***Bayesian*** megközelítés magától próbálja meg felderíteni ezeket a jellegzetességeket a korábban kapott spam és ham levelek vizsgálata alapján.

Veszélyes csatolmánytípusok tiltása

Üzembiztossági megfontolásokból gyakran jó ötlet megakadályozni a végrehajtható csatolmányokkal érkező leveleket, még ha a víruskeresőink szerint tiszták is. Végül is a víruskeresők sem tökéletesek, ráadásul a legfrissebb gonoszságok könnyen elérhetik a rendszerünket még mielőtt az anti vírus forgalmazó elkészítené a felderítéséhez szükséges új vírusmintát. Az ***amavisd-new*** lehetővé teszi, hogy megadjunk fájlkiterjesztés listákat, tartalomosztályokat és ***MIME***-típusokat, amelyeket karanténba szeretnénk zárni, elutasítunk vagy törölni kívánunk.

Érvénytelen levélfejlécek kezelése

Az ***RFC 2822*** szabvány szerint, a levélfejlécekben nem szerepelhet semmilyen 127-nél nagyobb értékű karakter, ***NULL*** vagy önmagában álló soremelés. Ezen a tartományon kívüli karakterek különleges kódolásúak lehetnek, így a világ különféle levelezőprogramjai probléma nélkül tudják értelmezni őket. Ha érvénytelen fejléccel érkező levelet kapunk, az lehet egy gyengén megírt levelezőügyfél hibája is, de igen gyakran olyan egyedi tervezésű program terméke, amilyeneket a spammerek használnak a tömeges levelezéshez. Az ilyesfajta, úgynevezett ***ratware*** (rat=patkány) készítői általában angol anyanyelvűek, és többnyire nem is gondolnak rá, hogy programjukat más nyelveken beszélők is használni fogják. Amikor a spammerek megpróbálják ezekkel a programokkal elküldeni a leveleiket, a ratware nem kódolja a különleges karaktereket, így hibás levélfejléceket készít. Az amavisd-new programban eldönthetjük, mit kívánunk tenni az érvénytelen fejlécű levelekkel: karanténba zárjuk, elutasítjuk, elvetjük, vagy keresztülengedjük.



7. ábra A ham gyorstár segítségével a felhasználó egyszerűen jelezheti az átcsúszott elemeket

Tartalomszűrő házirend beállítása

Az ***amavisd-new*** segítségével a rendszergazdák rendszer szintű tartalomszűrő rendszabályokat készíthetnek, ám ezeket a szabályokat tartomány illetve felhasználói szinten felülbírálhatjuk. Vannak felhasználók akik szeretnék átvizsgáltatni leveleiket mind a négy gyanús tartalomtípus (vírusok, spam, tiltott fájlok és érvénytelen fejlécek) szerint, mások viszont inkább kikapcsolnák valamelyik vagy akár valamennyi ellenőrzést. Az egyik felhasználó szeretné, ha az 5.0 vagy ennél nagyobb értéket elérő levelei a karanténba kerülnének, míg mások inkább azt részesítenék előnyben, ha a ***Subject:*** fejléc bővülne egy speciális előtaggal (például ***SPAM***), amennyiben a pontszám eléri a 4.0-t és csak akkor blokkolnák, ha 8.0-at is meghaladja. Ez a fajta finom felbontású vezérlés a teljes szűrőfolyamat alatt lehetővé teszi, hogy a rendszergazdák eltérő igényekkel rendelkező felhasználók széles körét szolgálják ki.
Ezen felül az ***amavisd-new*** mindhárom szinten fehér és feketelistákat tárol. Ezáltal a rendszergazdák rendszerszintű listákat hozhatnak létre; míg a rendszer másik végén a felhasználók saját egyedi listákat hozhatnak létre.

Karantén és figyelmeztetési lehetőségek

Előre meghatározhatjuk milyen lépéseket végezzen el az ***amavisd-new*** amikor megállít egy e-levelet. A levelet tárolhatjuk a karantén könyvtárban vagy levelesládában, vagy akár felhasználónkénti külön levelesládákban (pl. jozsi+spam). Választhatjuk az is, hogy az ***amavisd-new*** utasítsa el a levelet, azaz vagy ne fogadja el a felette elhelyezkedő kiszolgálótól vagy csendben dobja ki azt. Amennyiben a szervezeti szabályzatunk előírja, hogy a felhasználókat figyelmeztetni kell a blokkolt levelekkel kapcsolatban, az ***amavisd-new***-ban ez is beállítható. Ez azonban vitatott téma. Manapság sok ember a vírusfigyelmeztetéseket és spam reklamációkat inkább idegesítőnek mint hasznosnak tartja , különösen amióta a levelek feladója általában hamisított. Amennyiben mégis kellene küldenünk vírusfigyelmeztetéseket, az ***amavisd-new*** tartalmaz egy listát azokról a vírusokról, amelyek bizonyítottan meghamisítják a levélfejléceket így ilyenkor nem küld figyelmeztetéseket sem. Ezt a listát kézzel kell karbantartanunk és meg kell egyeznie azokkal a nevekkel, melyet az általunk használt víruskereső visszaad. Amennyiben egyszerűbbnek találjuk felsorolni azokat a vírusokat, amelyek nem hamisítanak címet, használhatunk inverz listát is.

Maia Mailguard

A ***Maia Mailguard*** egyszerű ***amavisd-new*** webes felületként született pályafutását, amely lehetővé teszi a felhasználóknak, hogy egy kényelmes felületen keresztül változtassák meg tartalomszűrő beállításaikat és kezeljék karanténjüket. A projekt egyre népszerűbb lett az ***ISP***-k, ***Web-mail*** szolgáltatók és a lapon kívüli szűrést kínáló cégek körében, így ezek a nagyobb igényű felhasználók hatására a ***Maia Mailguard*** hamarosan sokkal kifinomultabb rendszerré alakult.

A ***Maia Mailguard*** teljes értékű spam és vírus kezelő rendszer, amely ***PHP***, ***SQL*** és ***Perl*** parancsfájlokat, ***MySQL*** vagy ***PostgreSQL*** adatbázist valamint természetesen az ***amavisd-new***, ***SpamAssassin*** rendszert és egyéb támogatott víruskeresőket tartalmazhatja. Több Tartalomszűrő kezelhető egyetlen ***Maia*** csatolófelületről, amelyek egyazon ***SQL*** adatbázison osztoznak. Tekintve, hogy a tartalomkezelés, a karantén karbantartás és spamjelentések leegyszerűsítésére tervezték, a ***Maia Mailguard*** sok szempontból új eszköz a levelező felhasználók kezében.

Webes felület

A ***Maia*** web-alapú felülete több forrás szerinti azonosítást is lehetővé tesz, használhatunk ***POP3*** vagy ***IMAP*** kiszolgálót, ***LDAP*** kiszolgálót, külső ***SQL*** adatbázist vagy a ***Maia*** saját belső adatbázisát. A felhasználókat a rendszergazda felveheti kézzel vagy is felkerülhetnek amikor olyan levél érkezik helyi címre melynek címzettjével a ***Maia*** még nem találkozott azelőtt.

A felhasználóknak több e-mail címe is tartozhat egyetlen azonosítóhoz, de minden e-mail cím saját tartalomszűrő beállítással rendelkezik (*1. ábra*). A felhasználók a webfelületen keresztül címeket adhatnak hozzá és távolíthatnak el a fehér- illetve feketelistáikról (*2. ábra*), míg a rendszergazdák egy másik weblapkészleten tartomány illetve rendszer szintű beállításokat módosíthatják (*3. ábra*). Az amavisd-new mind a négy levéltípusáról statisztikák készülnek, nem különben a fehér- és feketelistára kerülő elemekről, túlméretes elemekről, ***hamis találatokról (false positives)*** és ***átcsúszásokról (false negatives)*** (*4. ábra*). Más táblázatok típusonként nyomon követik az egyes vírusokat valamint azt is, hogy mely ***SpamAssassin*** szabály hány alkalommal aktiválódott. Az adatokból valós időben grafikus ábrák készíthetők vagy adott időközönként statikus lapként elmenthetők.

Annak köszönhetően, hogy a ***Maia*** a karanténkezelést és a tartalomszűrő vezérlést egyenesen a felhasználók kezébe helyezi, a rendszergazdáknak nem sok naponta elvégezendő munkájuk marad. A ***Maia*** adott időben lefutó ***Perl*** parancsfájljaival kiegészítve, melyek jelentik a felhasználók által jóváhagyott spam leveleket és kezelik a lejárt karantén elemeket, a rendszer szinte önmagát működteti.

Karanténkezelés

Felhasználói szemszögből igen fontos, hogy amikor egy levél a karanténba kerül, könnyedén el tudjuk érni azt. A ***Maia*** a felhasználói karanténjában megtekinthetjük az elemek listáját, mégpedig spam pontszám szerint rendezve. Tehát azok az elemek amelyek a legnagyobb valószínűséggel tévedésből kerültek ide – azaz a hamis találatok – a lista tetején foglalnak helyet, így könnyebb észrevenni őket (*5. ábra*).

Amennyiben a fejléc alapján nem tudjuk eldönteni, hogy egy levél kívánatos-e vagy sem, a címre kattintva megtekinthetjük azt a ***Maia*** levélnézegetőjében (*6. ábra*). A levélnézegetőt bármilyen típusú levélen biztonságosan használhatjuk, ugyanis a legtöbb csatolmányt nem dekódolja, viszont letiltja a távoli képeket és kiszedi azokat a ***HTML*** tagokat amelyek más lapra irányíthatnának át bennünket. A levelet dekódolt vagy nyers formában is megtekinthetjük, valamennyi eredeti levélfejléccel együtt.

Amennyiben úgy döntünk, hogy a levél végül mégiscsak kívánatos, egy kattintással kimenthetjük a karanténból és elküldhetjük magunknak. Ezzel egy időben a ***Maia*** értesíti a ***SpamAssassin***-t a hibáról, így a ***Bayesian*** tanulórendszer kisebb valószínűséggel követi el még egyszer ugyanezt a hibát. A ***Maia***-t úgy is beállíthatjuk, hogy az ilyesfajta kimenekítések esetén a küldő címét automatikusan felvegye saját fehér listánkra.

A karanténon kívül a ***Maia*** rendelkezik egy úgynevezett ***ham gyorstárral*** is, amelyben tulajdonképpen a mostanában kapott elfogadott leveleink találhatók (*7. ábra*). A ham gyorstár célja, hogy könnyedén jelenthessük a szűrőn átcsúszott spam leveleket (false negatives). Ezeket az elemeket helyesen spamnek kijelölve taníthatjuk a ***SpamAssassin Bayes***-féle szűrőjét. A karantén és a ham gyorstár egyaránt a kapott levelek állapotának hitelesítésre szolgál. Ezzel nem csak a ***Bayes***-féle tanuló rendszert oktatjuk, hanem egyúttal lehetővé tesszük a spam levelek helyes beazonosítását is, hiszen az intézkedést ember hagyja jóvá.

Spam jelentés

A legtöbb spamszűrő csak a spam támadások kivédésre koncentrál és nem sokat, vagy egyáltalán nem törődik azok megelőzésével. Minthogy a ***Maia*** lehetővé teszi felhasználóinak, hogy spam-ként azonosítsák a leveleiket miközben az eredeti levélfejléceket nem módosítja, a spam több különféle módon is jelenthető. A ***Maia*** következő verziói képesek lesznek részletes fejlécanalízist végezni és félautomata jelentéseket küldeni az ***ISP***-k részére. Ezek a jelentések segítenek másoknak hatékonyabban kiszűrni a spam leveleket végül egyfajta büntetést jelenthetnek a spammelő számára.

A színfalak mögött a ***Maia*** automatikus parancsfájljai szabályos időközönként feldolgozzák a karantént, jelentik a helybenhagyott spam leveleket a ***SpamAssassin*** által használt együttműködésen alapuló hálózatoknak (***Vipul's Razor***, ***Pyzor*** és ***DCC***). Azzal, hogy megosztjuk az információt ezekkel a hálózatokkal, valamit adunk is és nem csak nyerünk mások jelentéseiből.

Hatékony, teljes körű megoldás

Végül, szóljunk pár szót arról ami a leginkább számít, vajon mennyire hatékony az ***amavisd-new*** és a ***Maia Mailguard*** a spam levelek elfogása terén, és milyen eséllyel kerülik el ham leveleink a karanténba kerülést? Saját helyem statisztikáiból ollózva, ez az érték szimpatikus 99.22%, 0.26% hamis találati (false positive) és 0.52% átcsúszó levél (false negative) értékkel. Ami a legjobb, ezeket a hamis találatokat könnyedén kigyűjthetjük a karanténból míg az átcsúszott leveleket jelenthetjük a ham gyorstárban.

A vírusok és egyéb rossz szándékú küldemények terén a hatékonyság még figyelemreméltóbb: 100%. Az alatt a hat hónap alatt amióta ezt a tartalomszűrő megoldást telepítettem, az asztali gépekre feltett víruskeresők semmit sem fogtak ami átcsúszott volna a tartalomszűrőn. Persze ebben nagy szerepe van annak is, hogy az ***amavisd-new*** több eltérő gyártótól származó víruskereső együttes használatát is lehetővé teszi – amit az egyik kereső elhibáz a másik általában elkapja.

Ha a teljesítményt nézzük, minden tartalomszűrő megoldás lelassítja valamilyen mértékben a levélfeldolgozást. Gyakran előfordul, hogy a nagyobb sebesség érdekében engedményeket teszünk a szűrő hatékonyság rovására, és inkább kikapcsolunk néhány szűrőt és tesztet ezzel növelve az átviteli teljesítményt. A nálam mért 99.22%-os hatékonyság eléréséhez például valamennyi szűrő bekapcsolt állapotban volt, ennek megfelelően 1–3 másodpercre volt szükség minden egyes levélelem átvizsgálásához egy közepesen terhelt dual-PIII 733MHz-es gépen 1GB memória mellett. Egy elfoglaltabb helyen elképzelhető, hogy ekkora késlekedés már nem elfogadható. Ők vagy kikapcsolják az időigényesebb teszteket, vagy gyorsabb processzort és több RAM-ot vásárolnak a tartalomszűrőhöz esetleg terheléselosztáson alapuló hálózatot építenek több tartalomszűrőből. Ettől függetlenül több mint 50.000 felhasználónak helyet adó rendszerek is használnak ***Maia Mailguard*** és ***amavisd-new*** párost, ahol több mint 350.000 e-levelet kezelnek naponta, tehát a megoldás skálázható, amennyiben elegendően jó alkatrészek állnak rendelkezésünkre.

Mint azt valószínűleg sokan megfigyelték, a spam és vírusok elleni harcban éppen a nyílt forrású eszközök a legjobb fegyverek. Az ***amavisd-new***, ***Maia Mailguard***, ***SpamAssassin*** és a ***Clam Antivirus*** segítségével hálózatunknak elsőrangú védelmet adhatunk anélkül, hogy hatalmas költségekbe vernénk magunkat.

Linux Journal 2004. december, 128. szám

Robert LeBlanc a Renaissoft elnöke (www.renaissoft.com), a Maia Mailguard szerzője, és az AnswerSquad spam-harcos guruja (www.answersquad.com). Amikor éppen nem a spanyolviaszt találja fel vagy még jobb egércsapdákat fabrikál, általában négy Alaszkaija Klee Kai, Zorro, Sikari, Piyomi és persze a Maia társaságában található.

KAPCSOLÓDÓ CÍMEK

- www.ijs.si/software/amavisd
- www.renaissoft.com/maia
- www.spamassassin.org
- www.clamav.net
- razor.sourceforge.net
- pyzor.sourceforge.net