



Stort test: Watchguard • Halon • Cronlab Symantec • Microsoft • Cleanmail

Ren e-post med

Skräppost är ett stort problem för både it-avdelning och användare. Det finns hjälp, kraftfulla system för e-posttvätt, men vilken produkt passar bäst för just dig? Vi har testat sex alternativ och satt betyg. Häng med!

De flesta företag använder e-posttvätt för att hindra sina anställda från att besväras av skräppost. Generellt fungerar produkterna bra tack vare att flera tekniker blandas – ofta görs en bedömning av avsändarens trovärdighet, en analys av e-postprotokollen och slutligen en innehållsanalys.

För att undersöka hur väl e-posttvätt fungerar har vi testat sex aktuella produkter – två boxar och två molntjänster har jämförts mot den inbyggda skräpposthanteringen i Microsoft Exchange 2010 samt en enklare lösning byggd kring Spamassassin, ett fritt tillgängligt Perl-

program för e-posttvätt baserad på innehållsanalys.

Tjänsterna varierar

Det som skiljer produkterna åt är förutom förpackningen vilka kringtjänsterna som stöds, hur lätta de är att använda och hur väl de kan konfigureras. Samtliga produkter fungerar som ett tillägg till en befintlig e-postmiljö och låter posten passera genom e-posttvätten. Man kan låta lägga in en text som visar om breven undersökts och genom webblänkar kan användarna undersöka brev som stoppats eller ändra enklare inställningar.

Funktionen i e-posttvätt kan jäm-

föras med inloggning i ett känsligt datorsystem, där man ju aldrig talar om ifall det är namnet på användaren eller lösenordet som är fel när inloggningen nekas. På samma sätt talar e-posttvätten inte om för avsändaren om det är adressen, mottagaren eller innehållet som orsakade att brevet räknades som skräppost. Om e-posttvätten är tveksam kan den uppge ett tillfälligt fel eller dröja med svaret för att se hur avsändaren betar sig.

Användarna behöver inte känna till hur e-posttvätten fungerar. För e-postadministratören är det däremot nödvändigt att förstå tekniken för att kunna göra justeringar, för att kunna felsöka och för att kunna anpassa sig gentemot andra e-postsystem.

Det finns en risk att brev ska komma bort, men oron för det är i regel obefogad. En avsändare kan begära mottagningskvitto och läskvitto och



Läs fler tester på
[www.techworld.se!](http://www.techworld.se)

rätt tvätt

mottagande system kan genom re-turkod eller svarspost meddela om mottagaren var okänd.

Du vågar ge besked

Effektiv e-posttvätt gör det också möjligt att i större utsträckning våga ge besked om mottagaren är okänd – tidigare har man tvingats vara restriktiv med det eftersom man riskerar att dra på sig ännu mer skräppost.

Spamhaus är ett internationellt samarbetsprojekt mot skräppost som via webbplatsen spamhaus.org levererar svartlistor. Med listorna ska kunna stoppa 80 procent av all skräppost genom att kontrollera avsändarens adress, ip-adressen och den förmedlande e-postservern. Minst 98 procent kan filtreras bort på grund av suspekta länkar som finns i brevet. Verkningsgraden för de här två metoderna tillsammans blir cirka 99,5 procent.

Utöver det här kan minst 95 procent av skräpposten filtreras bort på grund av övrig innehållsanalys, till exempel klassiska formuleringar som ofta återfinns i bedrägliga brev. Men när man lägger ihop alla tre metoderna blir verkningsgraden ändå bara marginellt bättre, cirka 99,6 procent, på grund av att varje enskild metod hittar samma brev.

Testerna som vi gjorde i samband med den här artikeln baserades på historiskt skräppost och kunde därför inte dra fördel av svartlistor. Den praktiska erfarenheten från testerna är dock att även verktyg med Spam-assassin i botten rensar bort 90–95 procent av all skräppost.

Fällor för skräppost

Leverantörerna av e-posttvätt har egna honungsfällor för att fånga skräppost. Det innebär att det inte

Scenario

Ett medelstort företag plågas av skräppost. Problemet växer och situationen är ohållbar, särskilt då det också drabbar användarnas mobiltelefoner. Man har bett it-avdelningen att hitta en effektiv och prisvärd lösning för att tvätta bort skräpposten.

Företaget har cirka tvåhundra anställda och en it-avdelning på fem personer. All personal använder e-post internt och får skicka och ta emot extern post enligt företagets e-postpolicy. Man använder Outlook e-postklient och Exchange 2010 som e-postserver.

Så gjorde vi testet



Vi satte upp alla produkterna för att hantera var sin e-postdomän som kunde skötas via en befintlig Exchange 2010-server. Först gjorde vi enkla tester för att se hur e-post kunde skickas och hur feladresserad e-post behandlades. Därefter provade vi ett arkiv med tidigare katalogiserad e-post som delats i skräppost och icke-skräppost. Samtidigt provade vi även hur e-postlistor och reklamutskick hanterades.

uppstår någon integritetsrisker i form av att en kunds brev plockas ut för en analys.

Produkter för e-posttvätt har ofta ett stöd för att hantera ett fullskaligt utbrott när man märker att en ny adress börjar skicka stora mängder brev. Mängden förfrågningar gör att trovärdigheten för sändaren minskar och tills ett brev hunnit passera en honungsfälla används till exempel temporära fel för att vinna tid och pröva användaren. Ibland spärras adressen tillfälligt i den server som normalt är den prioriterade e-postservern för att se om avsändaren är beredd att pröva nästa e-postserver, vilket riktiga e-postserverar normalt gör, i motsats till skräppostprogramvaror.

Snabbt igång

Vi bedömer inte att någon av de testade produkterna kräver en onormalt lång inkörningsperiod. Enbart Symantecs lösning krävde en extra åtgärd i form av överföring av e-postadresser, och det arbetet kunde man slippa om man även använde lösningen för utgående trafik, då e- ▶



| Produkt | Watchguard Spamblocker | Halon VSP H/OS 2 | Cronlab Anti-Spam Filtering |
|--|--|----------------------|--|
| Produkttyp | Hårdvara | Hårdvara | Molntjänst |
| Skräppostfiltrering av både inkommande och utgående trafik | Ja | Ja | Ja |
| Inbyggd svartlistning av avsändaradresser | Ja | Ja | Ja |
| Inbyggd svartlistning av reklamadresser (dbl) | Ja | Ja | Ja |
| Detektering av skräppostutbrott | Ja, separat funktion | Ja | Ja |
| Innehållsanalys | Ja | Ja | Ja |
| Karantän | Ja, kan konfigureras | Ja, kan konfigureras | Ja, förkonfigurerat |
| Cirkapris | Spamblocker 1 800 kr/år exkl brandvägg | 11 220 kr/år/licens | 16 kr/användare och månad (återförsäljare) |
| Betyg | | | |
| Installation | 20 av 25 | 15 av 25 | 20 av 25 |
| Detektering | 15 av 25 | 20 av 25 | 20 av 25 |
| Säkerhet | 20 av 25 | 20 av 25 | 20 av 25 |
| Anpassning | 15 av 25 | 25 av 25 | 20 av 25 |
| Totalbetyg | 70 av 100 | 80 av 100 | 80 av 100 |

► postanvändarna registrerades i samband med utskicken.

Några av produkterna, särskilt den från Cronlab, förklarar utförligt för användarna vad som stoppats (med en låg skräppostvarning), varför stoppet skett och erbjuder slutligen användaren en "detta är inte skräppost"-funktion för att avlasta administratören. Andra produkter kan tvinga it-administratören att leta fram en förklaring i de fall användarna begär det.

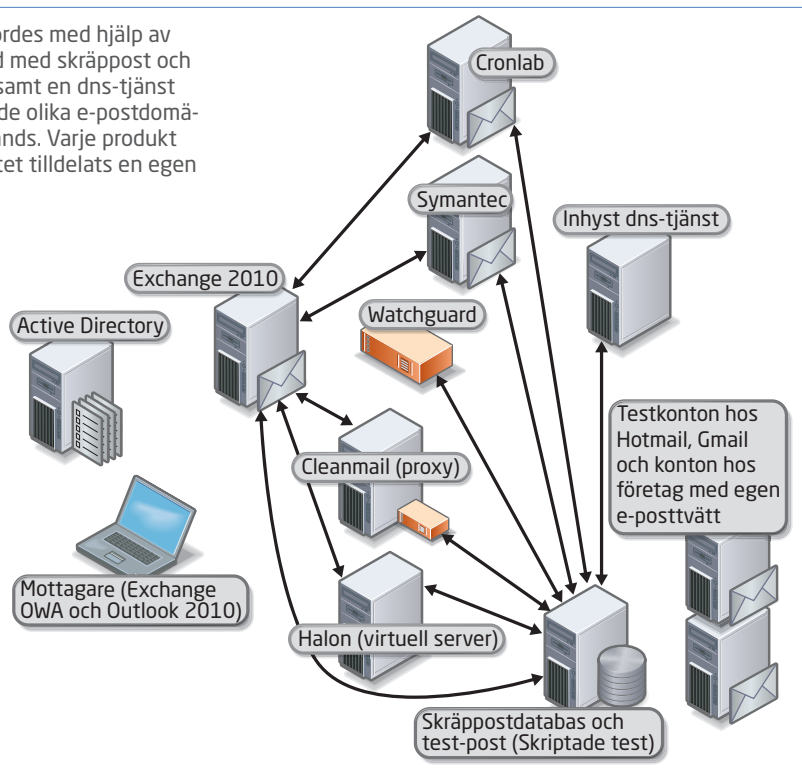
Produkterna från Watchguard och Cleanmail fungerar som proxylösningar, och utnyttjar möjligheten att låta den riktiga e-postservern förmedla kommunikationen och ge sina svar.

Tjänst, låda eller program

Ett e-postfilter kan hanteras som en tjänst via internet, som en hårdvara likt en brandvägg eller som ett program som körs i en server eller i användarens egen dator. Vilken produkttyp som passar bäst beror på företagets behov och krav på e-posthantering. Mindre företag har ofta en brandvägg som även innehåller e-posttvätt. Större företag har ofta en separat produkt eller en inköpt tjänst.

Både inkommande och utgående post kan tvättas. Skäl att granska ut-

Testet genomfördes med hjälp av en databas fylld med skräppost och icke-skräppost samt en dns-tjänst som pekade ut de olika e-postdomänerna som används. Varje produkt hade under testet tilldelats en egen e-postdomän.



gående post kan vara att kontrollera bilagor, spridning av interna dokument eller känslig information.

E-posttvätten börjar normalt med att kontrollera varifrån

anropet kommer samt vem mottagare och avsändare är. Om de här uppgifterna är rimliga tas brevet emot och innehållet kontrolleras.

Ett antal egenskaper i brevet bedöms enligt



| Symantec Message-Labs Email Security | Microsoft Exchange 2010 med Edge | CleanMail 4 | Spamhaus |
|---|-------------------------------------|--|------------------|
| Molntjänst | Mjukvara | Mjukvara | Datafeed |
| Ja | Ja | Ja | Inte tillämpligt |
| Ja | Ja | Nej, enbart dnsbl | Ja |
| Ja | Ja | Ja | Ja |
| Ja | Nej | Nej | Inte tillämpligt |
| Ja | Nej | Ja | Inte tillämpligt |
| Ja | Ja, begränsad funktionlitet | Ja, begränsad funktionlitet | Inte tillämpligt |
| 5 kr/användare och månad (återförsäljare) | Skräpposthantering ingår i Exchange | 9 100 kr/år första året, därefter rabatt | 10 700 kr/år |
| 20 av 25 | 15 av 25 | 15 av 25 | 20 av 25 |
| 20 av 25 | 15 av 25 | 15 av 25 | 15 av 25 |
| 20 av 25 | 20 av 25 | 15 av 25 | 0 av 25 |
| 20 av 25 | 10 av 25 | 15 av 25 | 0 av 25 |
| 80 av 100 | 60 av 100 | 60 av 100 | 35 av 100 |



olika kriterier. Till exempel kan enbart stora bokstäver i ärenderubriken ge en poäng, och att datum saknas ge en poäng. Om den totala poängsumman blir högre än en viss gränsvärde betraktas brevet som skräppost. Ofta finns flera gränsvärden i två steg, där den högre nivån innebär att brevet kastas direkt.

På samma sätt justeras poängen ned om produkten upptäcker vad som bedöms vara goda egenskaper hos brevet. Ett företag i läkemedelsbranschen släpper gärna fram brev som innehåller medicinska termer, medan en myndighet kan ta hänsyn till om brevet innehåller kända nyckelord och fraser, till exempel "ansökan om".

Fyra saker bedöms

Följande fyra bedömningsgrunder har beaktats i vårt test:

- installation (inklusive anslutningar, dokumentation och kontohantering)
- detekteringsförmåga och riktighet
- säkerhet i sändning (meddelar produkten korrekt om brev stoppas eller förmedlas?)
- anpassning – förmågan att hantera skräppost, virus, egna tester och rapporter.

Ingen produkt var signifikant långsammare än någon annan, med undantag för helt avsiktliga fördröjningar eller krav på omsändningar.

»E-posttvätten börjar normalt med att kontrollera varifrån anropet kommer samt vem mottagare och avsändare är.«

Normalt används inte e-posttvätt i situationer där prestanda spelar en roll, det vill säga internt inom ett företag eller då en användare läser sin inkorg eller söker information i den.

► Watchguard Spamblocker Produkttyp: Hårdvara

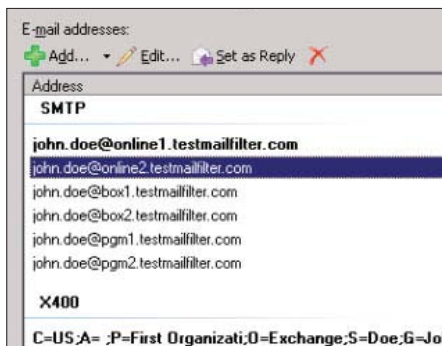
Watchguard gör brandväggsåldrar som innehåller en särskild funktion för e-posttvätt, Spamblocker. Den funktionen kräver ett separat abonnemang.

Beroende på hur ett brev har identifierats kan olika åtgärder vidtas. Den enklaste åtgärden är att brevet tillåts och därmed skickas vidare. En annan åtgärd är att brevet modifieras genom att rubriken ändras, till exempel kan texten "SPAM" läggas in först i rubriken, innan brevet skickas vidare. En tredje åtgärd är att brevet läggs i karantän. Ytterligare en åtgärd är helt enkelt att brevet stoppas och en returkod ges till avsändande e-postserver.

Normalt lägger Spamblocker även på extra sändningsinformation (mail headers) för att visa e-postprogramvaran och administratören hur kontrollen gått.

Proaktiva mönster

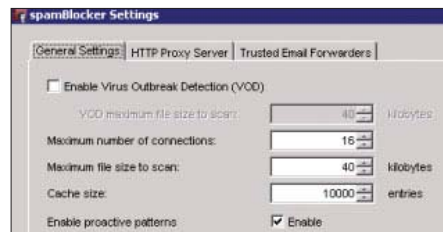
Kontrollen av skräppost utförs om Spamblocker är aktiverat och funktionen Enable proactive patterns är aktiverad. Varje brev jämförs med ett fingeravtryck av aktuell skräppost, alltså kombinationer av avsändare och karakteristiska textelement som lagras i minnet likt virussignaturer. Funktionen liknar den teknik andra leverantörer använder som analyserar svartlistor, sändningsinformation och textinnehåll, men den konstruerar alltså signaturer som utnyttjar ►



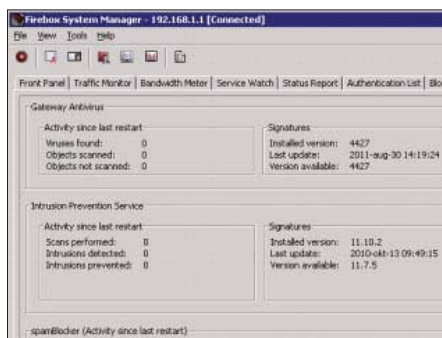
Som ett gemensamt testkonto använde vi i testet en fiktiv användare som hade en e-postadress i varje testad mejldomän.



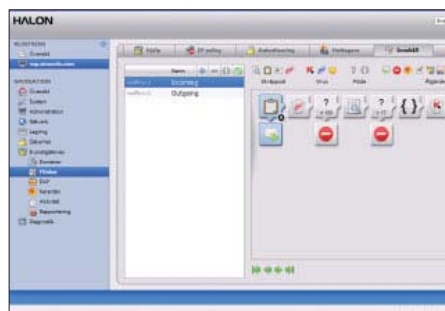
Watchguard har en enkel meny för Spam-blocker där man aktiverar tjänsten och anger hur olika typer av skräppost ska hanteras. Vanligast är att blockera det som helt uppenbart är skräppost och massbrev, men tillåter brev som bara är misstänkta att passera, eventuellt med en tillfogad varning i ärenderaden.



Watchguard SpamBlocker har olika inställningar om man vill skanna efter e-post som kan härröra från misstänkta virusutbrott respektive e-post som har kännetecknen på att vara skräppost (Enable proactive patterns). Båda alternativen bör väljas om man vill ha maximalt skydd.



Watchguard SpamBlocker ger i likhet med övriga produkter en översikt över hur mycket e-post som har hanterats.



Halons produkt har en arbetsyta där man kan definiera de olika kontroller som ska göras i ett flöde och vilka åtgärder som ska vidtas.



Cronlab Anti-Spam Filtering ger användaren enkla karantänrapporter där man ser vilka brev som har stoppats och har en möjlighet att hämta dem. Man kan även flagga för enskilda brev om de är oönskade.

► alla element samtidigt.

Watchguard ger i likhet med övriga produkter en översikt över hur många brev som hanterats som skräppost respektive stoppats. Efter som SpamBlocker fungerar som en proxy kommer de brev som stoppats som skräppost att orsaka loggposter i den interna e-postserverns loggar. Det kan förefalla oväntat för administratören.

► **Halon VSP H/OS 2**
Produkttyp: Hårdvara

Halon levererar både boxar och en tjänstlösning. Vi valde att testa VSP H/OS 2, en virtuell server som körs under VMwares hypervisor.

Det finns både fördelar och nackdelar med att använda en virtuell serverlåda. För ett företag som är vant vid virtualiseringslösningar, har rätt typ av hårdvara och använder VMware är det enkelt. Är man däremot ovan vid VMware eller kör denna produkt under ett vanligt operativsystem kan nätverkskopplingar och

liknande bli svårhanterade.

Logiken i Halons lösning är enkel att förstå och presenteras pedagogiskt. Om ett inkommande brev finns på en vitlista godkänns det direkt, annars går det igenom ett par tester som kan underkänna brevet. Slutligen görs ett par viruskontroller. Varje moment kan justeras upp eller ner efter administratörens önskemål.

Halon använder normalt inte sin karantänlösning utan låter hellre avsändaren få besked att meddelandet inte kommit fram. Om brevet var viktigt är det mer sannolikt att avsändaren reagerar på att ett svarsmeddelande att meddelandet inte tagits emot än att mottagaren skulle titta bland sin skräppost.

► **Cronlab Anti-Spam Filtering**
Produkttyp: Molntjänst

Cronlab levererar både hårdvara och molntjänst med i princip samma innehåll. Boxarna används främst av större kunder och onlinetjänsten av mindre kunder och då

tjänsten har sålts via en återförsäljare.

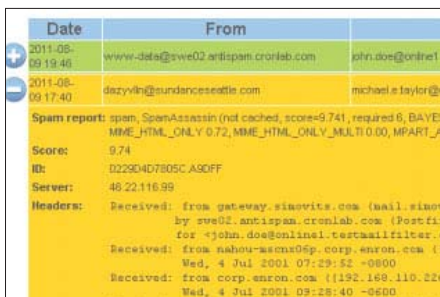
All e-post som inte är uppenbar skräppost sparas i lösningen. E-postadministratören samt varje användare har möjlighet att söka i sin stoppade e-post via ett webbgränssnitt med en inloggning kopplad till det egna e-postkontot.

Användaren har möjlighet att agera genom att rapportera att ett mottaget meddelande är skräppost genom att klicka på en länk som läggs i det mottagna meddelandet (funktionen kan stängas av och är konfigurerbar). På samma sätt kan hämtning av ett meddelande från karantänposten vara en indikation på att meddelandet kanske borde ha släppts fram.

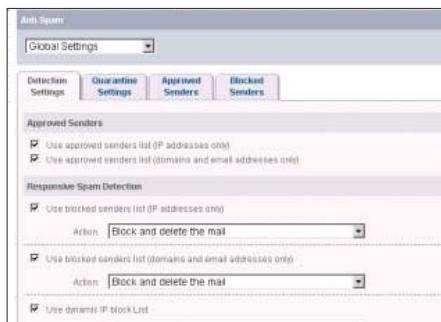
► **Symantec Messagelabs Email Security**
Produkttyp: Molntjänst

Symantec levererar en molntjänst som liknar den från Cronlab, men har ett extra stöd för att hantera policymässiga inställningar för

textinnehåll,



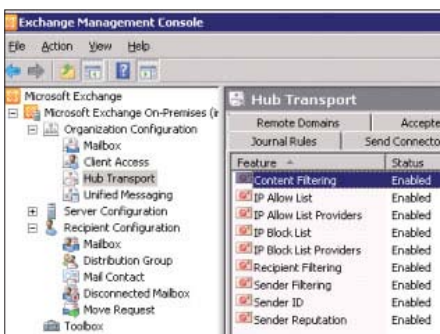
När användaren går till sitt meddelandecenter talar Cronlab om mer utförligt varför ett brev bedömdes vara skräppost. I det här fallet framgår värderingen som gjorts med hjälp av Spamassassin.



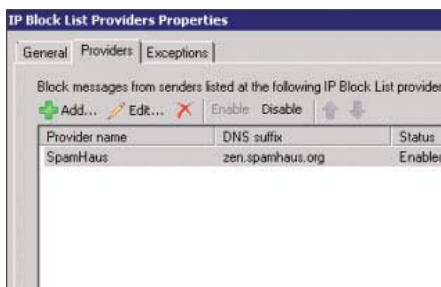
Symantec Messagelabs Email Security ger i likhet med övriga produkter en möjlighet att avgöra vad som ska ske med ett brev beroende på exakt hur det detekterats som skräp.



Symantec ger även stöd för en innehållsfiltrering, vanligen använt för utgående e-post. Filtreras man inkommande e-post efter vilket språk och vilka uttryck de innehåller så kan man låta en utsedd person ta hand om en viss typ av brev.



Även Microsoft Exchange innehåller skräppfilter som fungerar tillfredställande när alla funktioner är aktiva.



I Exchange kan man själva ange vilka svartlistor man vill använda. Vanligast är att man betalar för en svartlista från Spamhaus, men det finns även gratisjänster som kan vara aktuella.



Cleanmail innehåller i princip samma filtermöjligheter som övriga produkter. Det vi saknar är flera olika typer av svartlistor.



dokumenttyper och bilder. I likhet med de flesta andra lösningar för e-posttvätt ingår viruskontroll i produkten.

Symantecs lösning skiljer sig delvis från andra produkter vad gäller registrering av godkända användare. Om man använder både in- och utgående trafik via Symantec registreras en användare då e-post skickas ut, i annat fall måste tillåtna användare inom företaget registreras som mottagare. Tekniken har fördelar, men administratören måste komma ihåg att hantera eller informera nya användare. Den främsta vinsten är att interna adresser inom ett företag kan

hållas fria från skräppost – det är bara en mejladress som behöver kunna kommunicera mot externa användare som kan ta emot extern e-post.

Den normala inställningen är att skräppost från svartlistade adresser och med länkar till skräppostservers blockas. Däremot kan e-post som enbart analyserats innehållsmässigt släppas igenom.

Filter på utgående post

Symantecs produkt har även ett stöd för innehållsfiltrering. Det används typiskt för utgående brev eftersom man inte vill att känslig in-

formation ska läcka ut ur företaget.

Det finns en funktion för att granska bilder, som kan användas på olika nivåer. I vissa länder vill man ha en kontroll på vilka logotyper som används i brev, i andra länder vill man ha kontroll på om innehållet kan anses som stötande. Det är möjligt att lägga upp ett bibliotek med tillåtna bilder (logotyper, produktbilder), otillåtna bilder (gamla logotyper), vilken grad av stötande bilder som tillåts och vilken åtgärd som ska vidtas.

Innehållskontrollen kan utformas på liknande sätt – man kan lägga in ord som typiskt ska ge en varning eller stoppa ett utgående brev, till exempel olika sekretessmarkeringar som används inom företag och som normalt inte ska kunna ingå i utgående brev. Det finns även stöd för att hitta olika sifferserier, till exempel kredit- ▶



För- och nackdelar

Watchguard Spamblocker

- Enkel produkt
- Innehåller både brandvägg, vpn och e-posttvätt
- Stöd för detektering av skräppostutbrott och signaturigenkänning
- Stöd för detektering av virusutbrott
- Egen låda, inga problem med installation eller underhåll
- Spamblocker måste köpas som en separat tjänst
- Funktionen Enable proactive patterns måste aktiveras separat och kräver minnesutrymme
- Virusutbrottsdetekteringen utför inte en

vanlig signaturbaserad kontroll på virus

- Ingen kontroll av godkända e-postdomäner eller kontroller mot tillåtna e-postserverrar för den uppgivna domänen (via spf)

Halon VSP H/OS2

- Stöd för detektering av skräppostutbrott
- Kan köpas som box, virtuell box eller som tjänst
- Kan konfigureras mycket detaljerat
- Kan lagra brev i karantän lokalt i boxen
- Bra dokumentation
- Tekniskt krävande för administratören

Cronlab Anti-Spam Filtering

- Användarvänlig
- Bra information om stoppade brev
- Fullt stöd för att detektera skräppostutbrott
- Alla serverar och karantänpost kan hanteras inom Sverige
- Bra dokumentation
- En standardinställning gör att man inte får information om att brev stoppats

Symantec Messagelabs Email Security

- Användarvänlig
- Fullt stöd för att detektera skräppostutbrott

Långt ifrån perfekt filter, men få verkliga fel

I vårt jämförande test hamnade resultaten långt ifrån den filtrering på 99,5 procent som kunde förväntas. Detta beror i huvudsak på att det höga resultatet bara kan uppnås i en verklig situation där det finns kända skräppostare och giltiga svartlistor. Vårt test kom därför enbart att testa innehållsanalysen.

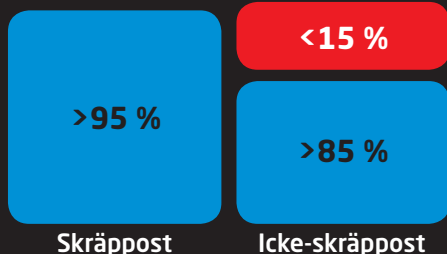
Enbart innehållsanalys bör för engelsk text få bort 90-95 procent av all skräppost, och det klarade alla de testade produkterna, även om Spamassassin hade vissa problem.

Med ett par hundra testbrev kunde vi inte hitta något enda brev som klart och tydligt hanterades fel av någon produkt. Däremot skilde sig resultatet med någon procent mellan dagens värdering av skräp och den värdering som gjordes när våra testbrev kategoriserades.

Även ålder och inaktualitet är egenskaper som Spamassassin betygsätter. I vårt test flyttade detta gränsen mellan skräp eller inte skräp i flera fall. Det som skenbart gjorde att produkterna från Cronlab, Halon och

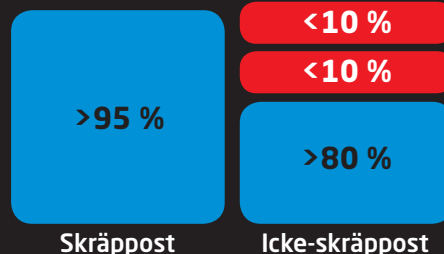
Symantec inte träffade rätt på en gång är deras metod att fördröja mottagningen av tveksam e-post. Den andra röda rutan nedan till höger är den mängd e-post som tillfälligt stoppas innan man är mer säker på avsändaren och hur avsändaren kommer att reagera på fördröjningen, till exempel genom att försöka anropa en annan sändningsväg. Vi märker att det är vanskligt att mäta produktens effektivitet mot varandra, och att man som köpare i första hand ska se till att produkten möter ens övriga önskemål.

Watchguard, Cleanmail och Exchange



Blå ruta: Korrekt hantering. **Röd ruta:** Tveksam varning - behövde kontrolleras, men bedömdes som godtagbar avvikelse

Cronlab, Halon och Symantec



Blå ruta: Korrekt hantering. **Röd ruta 1:** Tveksam varning - behövde kontrolleras, men bedömdes som godtagbar avvikelse. **Röd ruta 2:** Tveksam fördröjning/tillfälligt fel - behövde kontrolleras, men bedömdes som godtagbar avvikelse.

► kortsnummer eller personnummer.

Ordlistor för olämpligt språk finns på engelska, tyska och franska. Man kan själv komplettera listorna. Vi vill dock påminna om att det är bättre att utbilda användarna i hur man formulerar sig korrekt än att förlita sig på att e-postfilter ska hitta annat än de allra grövsta övertrampnen.

► **Microsoft Outlook/Exchange Edge**

Produkttyp: Mjukvara

Både Exchange 2010 och Outlook 2010 kan användas för e-posttvätt. Eftersom många företag har de här produkterna som grund för sitt e-postsystem kan de användas för att hantera skräppost utan

hänsyn till om ytterligare någon produkt används för samma ändamål.

Exchange 2010 tillåter ett företag att ange domäner eller ip-adresser som ska vit- eller svartlistas. Det finns dessutom innehållsfiltrering för e-postrubriker där bra och dåliga ord kan anges. För blockeringen kan ett företag hyra listor med adresser som ska blockeras



- Bra tilläggfunktioner vad avser innehåll i brev
- Bra dokumentation och utbildningsverktyg
- Omständligt att lägga in eller hantera tillåtna e-postmottagare

Microsoft Outlook/Exchange Edge

- Finns redan på plats hos många
- Fullt stöd för svartlistor
- Hittar också skräppost utan svartlistor
- Separat Edge-server behöver sättas upp mot en dmz
- Funktionen installeras inte som

standard på en Exchange-server med alla roller

- Separata licenser kan krävas för Spamhaus eller andra leverantör av svartlistor

Cleanmail med Spamassassin

- Enkla menyer och funktioner
- Ger god insyn i Spamassassin
- Funktionen att tvinga avsändaren att vänta på svar är inte intuitiv
- Installationen kräver teknisk kunskap
- Separata licenser för svartlistor kan krävas



nen är lite mer komplicerad än andra produkter eftersom bland annat Perl måste finnas på plats.

TechWorlds slutsats

För många organisationer kan det innebära gott anseende att kunna visa upp att utgående post har kontrollerats. För andra organisationer kan det vara viktigt att ha kostnadskontroll över sina it-tjänster, och då kan en tydlig rapport från e-posttvätten visa på vilket arbete som verkligen utförs.

Vilken produkt som du ska välja bestäms av din organisations behov och om du vill kunna hantera både e-posttvätt, viruskydd och e-postpolicy för de egna användarna med en och samma produkt. Alla testade produkter klarar att hitta skräppost på en godtagbar nivå, men vi tycker att de specialiserade produkterna är lite mer effektiva, lite enklare att använda och ger mer funktionalitet.

Nästa fråga är vilken produkt som är mest prisvärd. Det här beror givetvis på om du redan använder en annan produkt eller tjänst från någon av leverantörerna, och om du till exempel behöver viruskydd eller en innehållsfiltrering av utgående e-post. Den extra kostnaden för en tjänstlösning behöver också vägas mot det egna arbetet med att installera och drifta en box eller en programvara.

Vi utser Halon till vinnare i det här testet, även om de får samma poäng som tvåan och trean. Tvättlösning i en egen server innebär att e-posten skyddas rejält – man slipper behöva lita på en molntjänst, vilket kan ha betydelse till exempel för myndigheter. Dessutom ger produktens programmerbara gränssnitt administratören stor frihet för egna anpassningar. ■

Mikael Simovits & Tomas Forsberg

... är konsulter och skribenter inom it-säkerhet. Du når dem via
▶ mikael.simovits@techworld.se



av till exempel Spamhaus. Om det är ett litet företag kan man använda en gratisprenumerering av Spamhaus, men man får då ha högst 300 000 förfrågningar om dagen, inklusive skräppost och adresser inne i breven.

Det finns inga skäl att inte använda skräpposthanteringen i Exchange. Orsaken att de kommersiella leverantörerna brukar rekommendera att funktionerna i stort sett slås av är att undvika en överlappning som kan bli besvärande vid felsökning.

I Outlook ökar möjligheterna att låta användaren hantera skräppost beroende på rubriker och avsändare, särskilt då brevlådan inte är direkt ansluten mot Exchange-servern.

Det är värt att notera att Exchange saknar särskilda funktioner för att kunna hantera virus och bilagor.

Krävande administration

Det krävs förhållandevis goda kunskaper i Exchange för att använda funktioner som skräppostfiltrering. Det förutsätts också att administratören satt upp en Exchange-miljö där de yttre serverna (edge-serverarna) gör skräppostfiltrering, eller att administratören installerat komponenterna för skräppostfiltrering på en Exchange-server som har samtliga serverroller. Normalt görs en viss skräppostfiltrering i Exchange, exempelvis att feladresserad skräppost hanteras med det som kallas för en tar pit (tjärgrop, alltså ett par sekunders fördröjning innan ett nekande svar ges) och att innehållet inte läses ner på disk.

► Cleanmail med Spamassassin Produkttyp: Mjukvara

Spamassassin är ett välkänt program för e-posttvätt med öppen källkod. Det går att installera Spamassassin på både Linux- och Windows-serverar och produkten används då som komplement till en befintlig smtp-server.

För vårt test använde vi Cleanmail som smtp-proxy. Installationen gjordes på mindre än en timme. I jämförelse med övriga produkter var Cleanmail mer känslig för fel i smtp-protokollet och vägrade därför skicka vissa brev. En produkt som Spamassassin kan antas fästa större vikt vid metadata som saknas eller är felkonstruerade, jämfört med en produkt som även har tillgång till aktuell information om vilka ip-adresser som för stunden är aktiva skräppostavsändare eller vilken skräppost som för tillfället sprids.

Det uppstår också lätt en svårighet att avgöra var felet ligger eftersom proxyn presenterar sig som den bakomliggande servern.

Stöd för svartlistor

Efter installationen väl var avklarad visade sig produkten vara relativt lättanvänd. Cleanmail har stöd för svartlistor på samma sätt som övriga produkter, men antalet typer av listor som kan hanteras kan dock variera. I Cleanmails produkt anges enbart dns-baserade blockeringslistor (dnsbl).

Det krävs normala sysadmin-kunskaper för att veva igång Spamassassin, men installatio-

