

SPAM: Det nytter å slåss

SPAM er ingen ny problemstilling for Mellvik-Rapportens lesere. Allerede våren 1999 tok vi for oss fenomenet, som var en rimelig betegnelse på den tiden, i artikkelen "SPAM: Epost som dreper" (nr. 56).

Senere har vi fulgt opp ved en rekke anledninger i spaltene IT-revyen og Godbiter. Se MR *online* på vår Web-tjeneste for detaljer og pekere.

Fra irritasjon til problem

Søppelpost, SPAM, koster amerikanske organisasjoner over 10 milliarder USD i 2003, hevder analyse-selskapet Ferris Research. Uten å ta for hardt i kan vi estimere kostnaden å være noenlunde tilsvarende i resten av verden til sammen. To tredjedeler av all epost som traverserer store og små nettverk og fyller opp all verdens epostkasser er SPAM. Tiden er åpenbart overmoden for handling, men hva har vi å hjelpe oss med?

"Det største problemet er at spammerne er i ferd med å besudle selve funksjonen epost" skrev Tellef Øgrim – én av et fåtall oppegående teknologi-journalister her til lands – i Dagens Næringsliv nylig. Han fortsatte: "I noen jomfruelige år var epost en ny og vakrere form for kommunikasjon. Det kunne ikke vare. Like effektivt som fenomenet bilkø har fjernet mye av bilens glans av frihet, vil distributørene av elektronisk søppelpost ta glansen av eposten."

Han beskriver treffende følelsen mange av oss har etter å ha møtt en postkasse overfylt av søppel dag etter dag, kanskje måned etter måned. Ingen innsikt er bedre enn egen erfaring når det gjelder å forstå både problem og relaterte kostnader. Så lenge vi ble utsatt for en søppelmelding eller to per dag, var det knapt merkbart. Når over halvparten, kanskje så mange som 9 av 10 meldinger er SPAM, blir situasjonen en annen. At innholdet i meldingene antar stadig mer støtende former, bidrar til å forsterke følelsen av at nok er nok. Dessuten viser utviklingen ingen tegn til bedring. Fortsetter det slik, blir et sted mellom 90 og 100% av epost-meldinger søppel i løpet av maksimalt to år.

Kan det være så håpløst som Øgrim antyder? Finnes det intet håp om å bremse eller stoppe utviklingen? For mange av oss teller 'de jomfruelige år' med epost som 'ubesudlet og effektivt' verktøy godt over 20. I perioden har vi sett det ene teknologiske mirakel etter det andre. Kan det virkelig være så vanskelig å stoppe SPAM?

Det sterkt forenklete svaret er et kort og brutalt NEI. Men virkeligheten er ikke binær, sort/hvit: Selv SPAM-bekjempelse påvirkes av en rekke forhold, avveininger, prioriteringer og så videre. Hvilke forsakelser er vi villige til å akseptere for å komme problemet til livs? Hvilke kostnader er rimelige og hvilken SPAM-mengde er til å leve med?

SPAM og virus: To sider av samme sak?

Den viktigste erkjennelsen i første omgang er at problemet forlengst er blitt for stort til å kunne feies under teppet. Tallene fra Ferris Research er estimater på relativt løst grunnlag, men er skremmende selv om vi halverer dem én eller to ganger. SPAM er blitt et minst like stort problem som virus, og må behandles med tilsvarende alvor. De to plagene er sågar beslektet: De formidles på samme måte og har omtrent de

samme konsekvensene: Tapte tid, i noen tilfeller tapte data og i alle tilfeller tapte penger.

Videre ser vi at de mest utbredte bekjempelses-mekanismene er like ineffektive i begge tilfeller. Virusbeskyttelse for enkelt-klienter (PCer) er vel og bra, men skalerer for det første ikke og er for det andre notorisk upålitelige, ikke fordi produktene er dårlige, men fordi brukeren er en del av ligningen. Der det finnes brukere og PCer, finnes problemer. Så lenge virusbeskyttelse er avhengig av at brukeren holder fingrene fra fatet, blir effektiviteten langt under ønskelig nivå.

Situasjonen er enda verre for SPAM. For det første er skaden skjedd i det en melding når frem til brukerens postkasse. Selv om klienten (brukerens epost-program – Outlook, Netscape, Mozilla, Eudora etc.) kan foreta kontroll og eventuelt sletting av SPAM, er vesentlige ressurser allerede forbrukt. Meldingene er kommet inn i systemet, der de konsumerer båndbredde, lagringskapasitet, prosessorkraft og i de fleste tilfeller tid. Dessuten er en del av problemet ute av syne for alle andre enn spesielt oppmerksomme driftsansvarlige. Organisasjoner flest mottar daglig hundrevis eller tusenvis av meldinger til brukere som ikke finnes. At det er vanskelig å forstå meningen med å sende slike meldinger er uvesentlig. De kommer i store mengder¹ og de belaster våre systemer. Bedre blir det ikke av at 'epost-kontorene', programmene som mottar og distribuerer epost, er blitt ekstremt kompliserte og ressurskrevende i løpet av de siste 5 årene – en helt unødvendig utvikling som ikke gagnar andre enn hardware-leverandørene, og som forteller mer om dagens begredelige tilstand innen programvare og kvalitet.

Problemet har flyttet seg fra 'fraværende' til 'topp prioritet' på IT-lederes agenda i løpet av mindre enn 18 måneder, en forandring som har tatt de fleste leverandørene på sengen. Klient-verktøy er, som vi var inne på ovenfor, ikke bare feil angrepsvinkel, men i de fleste tilfeller bortkastet tid.

Til motangrep

Når problemet for alvor er blitt synlig, kommer spørsmålene: 'Hva gjør vi' og 'hvorfor har ingen gjort noe med det før'. Dessuten – symptomet er overfylte epostkasser, hva er det egentlige problemet – eller årsaken til problemet?

Den typiske første reaksjonen fra ledelsesnivå har vært 'kan vi ikke regulere bort problemet?', 'er dette lovlig?' og 'hvor får de adressene fra?'. Mens spørsmålene er naturlige, signaliserer de samtidig manglende forståelse for problemet:

- ✓ Det er ekstremt billig å sende ut millioner av epost-meldinger – en egenskap som følger med på kjøpet takket være Internettets beskaffenhet. Ulempen er fortsatt liten i forhold til fordelene.

¹ 1 perioder har 1 av 2 meldinger til mellvik.no tilhørt denne kategorien.

- ✓ Internettet er uregulerbart i tradisjonell forstand. En 'støykilde', som er en rimelig betegnelse på en 'SPAMmer', kan flytte seg fra land til land i løpet av sekunder, og er dermed utenfor rekkevidde for lovens arm uansett hvor lang den måtte være. At mange ISPer har satt en effektiv stopper for bruk av sitt nettverk som kilde til SPAM, er positivt, men kun en dråpe i havet.
- ✓ Våre epost-adresser brukes i utallige sammenhenger, både *on line* og *off line*. Det har vært gjort forsøk med å gjøre dem mindre tilgjengelige, gjennom for eksempel å underskrive med 'helge at mellvik dot no' i stedet for den aktuelle adressen. Resultatene har vært positive, men medisinen er for tungvint for alminnelige brukere.
- ✓ Å bytte epost-adresse er også effektivt – en stund, men upraktisk og vanskelig å gjennomføre i praksis.
- ✓ SPAMmere benytter ofte ikke-eksisterende adresser – et signal om at de kun kjenner domenenavnet (for eksempel mellvik.no), og prøver seg frem i blinde for å finne gyldige brukernavn/epost-adresser.

Det er innlysende at SPAM-problemet bør angripes så langt borte fra klientene som overhodet mulig. Dessuten indikerer analysen ovenfor at dersom vi på en effektiv måte kan få bukt med – eller drastisk redusert – SPAM-mengden, har vi samtidig redusert faren for virus. Riktignok er det ofte slik at virus sprer seg via interne epost-liste,² men sjansen for førstegangsinfeksjon reduseres vesentlig gjennom effektiv SPAM-kontroll.

All bekjempelse av SPAM hører hjemme i én av to kategorier: Den første er å forsøke å stoppe meldingene ved å finne frem til

Ut med eposten

SPAM-problemet er én av en rekke årsaker til at stadig flere organisasjoner vurderer å sette ut håndteringen av epost til tjenesteleverandører som spesialiserer seg på området. Dette er ikke bare en naturlig utvikling, men en utvikling som burde ha kommet for lenge siden. Misforståelsen at epost er enkelt og billig å håndtere er utbredt – og harmonisk med den uprofesjonelle holdningen organisasjoner flest har til epost.

Mens de fleste erkjenner at epost er et minst like viktig verktøy i hverdagen som tradisjonell post og telefaks, blir ikke erkjennelsen omsatt i profesjonell håndtering. Her er et stort lerret å bleke, og glimrende muligheter for leverandører som forstår problemstillingen og kan omsette forståelsen i effektive og kostnadsriktige tjenester.

Den amerikanske telecom-leverandøren Sprint har vært en foregangsfigur i denne utviklingen, og har i lang tid tilbudt det som kalles *managed e-mail services*. Mulighetene for tilleggstjenester utover grunnleggende SPAM- og viruskontroll er tallrike, og det er for de fleste organisasjoner unødvendig å håndtere epost i det hele tatt. Å la brukernes epostkasser befinne seg hos en tjenesteleverandør er like naturlig som at talepostkassen befinner seg hos telefoni-leverandøren.

At det er penger å spare på å flytte ut eposten, hersker det ingen tvil om. Spørsmålet her hjemme er først og fremst når det kommer leverandører som ser hvilket potensiale som ligger i profesjonelle epost-tjenester. Det handler om noe så unorsk som å ta ansvar. Markedet er enormt.

kilden og sørge for at våre adresser blir fjernet, eller at kilden i sin helhet blir borte. Å kontakte Internett-leverandøren som betjener senderen, er en naturlig angrepsvinkel, og fungerer i den forstand at tusenvis av SPAMmere årlig blir brakt til taushet på denne måten. Tausheten varer imidlertid ikke lenger enn til senderen har funnet seg en ny tjeneste-leverandør, innenlands eller utenlands. Uansett resultat er dette aktiv SPAM-bekjempelse.

² Problemet er først og fremst knyttet til funksjoner i Microsoft Outlook, og kan elimineres eller reduseres gjennom bytte av epost-klient.

Den andre varianten er etter beste evne å stoppe strømmen – så langt 'ute' i nettverket som mulig – fortrinnsvis ved grensen til vårt interne nettverk, eller enda bedre: Hos eller utenfor vår ISP. Dette er passiv SPAM-bekjempelse. Vi går løs på symptomene vel vitende om at selve problemet i beskjedne grad påvirkes. Imidlertid ser vi nyanser også her. Det er betydelig forskjell på å ta bryderiet med å registrere og 'anmelde' kildene og ganske enkelt å kaste dem, et forhold vi kommer tilbake til nedenfor.

Mens aktiv bekjempelse er nødvendig for å holde utviklingen til en viss grad i sjakk, er sistnevnte den eneste metode som gir umiddelbare, praktiske resultater. Søppel-strømmen må stoppes før den når frem til brukernes epostkasse, og jo lenger ute den kan stoppes, desto mindre ressurser ødes. Vi ser med andre ord bort fra klient-basert SPAM-kontroll, av årsaker vi allerede har vært inne på.

Hjelp til privatmarkedet: Mailblocks.com

Mens det på den ene siden er innlysende at typiske private PC-brukere har minimale forutsetninger for å beskytte seg mot SPAM, ville det på den andre siden være rimelig å forvente at deres Internett-leverandører hadde en generisk interesse av å stoppe søppelpost før den kom frem til brukerne. Leverandørene ville trolig ha gevinst av en slik tjeneste selv om den ikke kostet noe for brukerne. Videre er slike grunnleggende tjenester ypperlige som fundament for betalbare tilleggstjenester.

Igen har imidlertid ISPene vært lite flinke til å se potensialet og gripe sjansen mens den fantes. Resultatet er at brukerne har flyttet sin epost til leverandører som hotmail.com og yahoo.com, hvilket på den ene siden gjør livet enklere for ISPene, og samtidig redusere deres muligheter for salg av tilleggstjenester.

Dette er historie, og brukerne lar seg flytte på – dersom incentivene er gode nok. SPAM er et problem for de fleste, populære epost-tjenester foretar en viss filtrering av innkommende epost. De har også restriksjoner på utgående post, slik at de vanskelig kan misbrukes som utgangspunkt for SPAM. Dette er imidlertid ikke godt nok. Fortsatt rapporterer titusenvise av brukere at over 80% av deres innkommende epost er søppel. Det finnes rom for alternative leverandører som tar problemet på alvor.

Derfor opplever tjenester som Mailblocks [www.mailblocks.com] stor pågang i disse dager. I motsetning til Hotmail, Yahoo og mange flere, er Mailblocks en betalbar epost-tjeneste: USD 10 per år (12 MB) er i utgangspunktet en akseptabel pris, og med dagens 3-for-1 tilbud blir det hele praktisk talt gratis. Det viktige er imidlertid ikke prisen, men å bli kvitt SPAM, og Mailblocks har sin spesielle vri. Første gang vi sender epost til en Mailblocks-bruker, får vi melding tilbake med en Webpeker der vi 'autentiserer' oss. Mekanismen er ingen egentlig autentisering, men en måte å forsikre seg om at vi er en person, ikke en maskin. For våre pennevenner kan dette oppleves negativt, men mekanismen er enkel og resultatet er glimrende. Dessuten er vi kommet langt nok til at de fleste har en oppfatning av hva SPAM er og hvorfor det er viktig å beskytte seg. Siden de fleste av oss også er mottakere av høyst legitime 'ikke-personlige' meldinger – nyheter, abonnementer, hobbyer, fagstoff og andre ting, gir Mailblocks anledning til å opprette 'aliaser' som ikke kontrolleres på samme måte. Siden slike adresser svært sjelden oppgis, er de lite utsatt for SPAM. Dersom de imidlertid skulle bli kompromittert, har vi mulighet til å forandre dem når det måtte passe. Komplisert? Det kommer an på alternativene. Det viktigste poenget i denne sammenhengen er at det for det første finnes muligheter for brukere som er lei av SPAM, og for det andre arbeides intenst med mekanismer som reduserer eller eliminerer problemet. Tilsvarende finnes for profesjonelle brukere (organisasjoner), men da i en annen innpakning og et annet prisleie – fordi kravene er større og mer sammensatte.

Dessuten – og her er et viktig poeng – samvirker de to angrepsvinklene: Det finnes tjenester på Internettet som registrerer kilder til SPAM løpende, via egne registreringer og rapporter fra brukermiljøer. Listene – RBLs, *Realtime Black-hole Lists* på fagspråket – gjøres tilgjengelige for hvem som helst. Våre epost-agenter kan gjøre oppslag hos slike tjenester før de aksepterer innkommende eller utgående epost. Tjenestene er meget effektive, men benyttes fortsatt i altfor liten grad, fordi få kommersielle epost-agenter, for eksempel Microsoft Exchange, støtter slike tjenester. Sendmail, som fortsatt er den mest benyttede epost-agenten i Internettet, har imidlertid slik støtte. Vi kommer tilbake til hvordan problemet med manglende støtte kan omgås i avsnittet i praktisk SPAM-kontroll på side 10. RBL og MAPS, *Mail Abuse Prevention System*, diskuterer vi i en egen artikkel i neste utgave av Mellvik-Rapporten, se baksiden for detaljer.

Hvem og hvordan?

Neste spørsmål er hvem som skal gjøre jobben og hvordan den bør gjøres. Igjen har vi to muligheter: Å innføre funksjonelle tillegg til vår eksisterende (og i de fleste tilfeller interne) epost-tjeneste, eller å kjøpe kontroll-tjenesten eksternt. Sistnevnte vil i praksis si *outsourcing* – å la en ekstern tjenesteleverandør være mellomstasjon for inngående og/eller utgående epost – forutsetningsvis en leverandør med erfaring, ekspertise og verktøy – som kan ta ansvar for resultatet (se ramme på foregående side).

Slik *outsourcing* er åpenbart det enkleste, men hva koster det, hva får vi for pengene og hvor pålitelige er tjenestene? Det faktiske forholdet er at verken markedet eller leverandørsiden er moden, i alle fall ikke på våre kanter av verden og for det profesjonelle markedet. Nå er epost en ekstremt geografi-uavhengig tjeneste, slik at det rent praktisk spiller liten rolle hvor postkassene eller postkontorene befinner seg. Uansett skal vi imidlertid ha med en leverandør å gjøre, som for det første skal forstå våre behov og for det andre være behjelpelig med problemløsning, tilpasninger og løpende vedlikehold. Derfor er det naturlig å begynne søkingen på lokalplanet – blant ISPer, ASPer og aktører som leverer driftstjenester. Selv om ingen har gjort kontroll av epost til et fokusområde enda, registrerer vi at det finnes betydelig kompetanse på området hos enkelte av aktørene i markedet.

Mekanismer

Det kan i utgangspunktet høres trivielt ut: SPAM er epost, epost er meldinger og meldinger kan og må kontrolleres. Et filter i tilknytning til postkontoret eller 'epost-agenten' er alt som skal til.

Slik kan det gjøres, men det enkleste er ikke alltid det beste. I noen tilfeller er det tilsynelatende enkleste sågar umulig, mens det i andre tilfeller er lite lurt, fordi det finnes andre veier til målet som er både mer effektive og teknisk eller praktisk riktigere. Som vi har vært inne på utallige ganger tidligere, er første forutsetning for et godt resultat å forstå problemet.

Diskusjonen ovenfor legger et godt grunnlag for slik forståelse, og er utgangspunktet for følgende observasjoner rundt hvordan SPAM kan blokkeres:

- ✓ Så snart en sender kontakter vår epost-agent, konsumeres ressurser. Om de er aldri så små blir det merkbart når volumene blir store nok. Det blir de før eller siden – selv for virksomheter med noen få ansatte.
- ✓ Å blokkere utvalgte deler av verden fra kontakt med vår epost-agent kan se drastisk ut, men fungerer i praksis. Enkelte land og regioner er mer 'lovløse' i SPAM-sammenheng enn andre. For eksempel har det gitt gode resultater for mange miljøer å rett og slett blokkere all epost-trafikk fra land som Kina og Korea. India, Indonesia og Russland er også kandidater i så henseende – med mindre vi har legitime kontakter i disse landene.

- ✓ SPAMmere bruker utallige mekanismer for å komme rundt blokkeringer. Dette er et dynamisk område, akkurat som tilfellet er for virus. Å sørge for at epost-agenten foretar grunnleggende kontroller av sender og mottaker av meldinger, er en effektiv måte å kvitte seg med et betydelig SPAM-volum på. Eksempler er:
 - ✗ Stopp videresending til adresser som ikke er våre egne. SPAMmere er alltid på søken etter agenter som ukritisk videresender epost. Mens åpenhet for slik videresending var god takt og tone i Internettet for ti år siden, har misbruk sørget for at det er utillatelig i dag. Det kan sågar føre til at vi blir svartelistet som 'åpen for relaying', som det heter, en situasjon vi definitivt bør unngå å komme i.
 - ✗ Sending til eller mottak fra adresser som ikke har såkalte reversoppslag, det vil si som ikke har et offisielt navn i DNS-systemet, bør blokkeres. En kontroll av våre egne loggfiler viser at disse to punktene alene stopper ca. 12% av alle innkommende meldinger – og mer enn 20% av all SPAM.
 - ✗ Tilsvarende er det rimelig å blokkere sendere og mottakere som ikke oppgir et legitimt domenenavn som samsvarer med Internett-adressen som benyttes.
 - ✗ I den grad det er mulig, er det hensiktsmessig å kontrollere at mottaker faktisk finnes så tidlig som mulig i behandlingen av meldinger. Det er mye å spare på å kunne avvise meldinger til ukjente mottagere før selve meldingen overføres.
 - ✗ Å innholdsteste hver melding er en omfattende jobb som krever betydelige ressurser i forhold til resultatene: Mer enn 90% av dagens SPAM-strøm kan fjernes uten å gå så drastisk til verks. Derfor anbefaler vi å kombinere fullstendig innholdskontroll med viruskontroll, og å begrense den rene SPAM-kontrollen til 'Subject'-feltet, hvilket krever minimalt med ressurser. En annen mulighet er å innholdsteste meldinger under en viss størrelse, for eksempel 5 eller 10 kB, som erfaringsmessig dekker de fleste SPAM-meldinger.
 - ✗ RBL-tjenester er, som vi var inne på ovenfor, Internettets SPAM-politi. Å sørge for at vår epost-agent gjør oppslag i disse tjenestene for å avdekke 'uønskede' sender-adresser, er en effektiv måte å redusere SPAM-mengden på.

Avfallsbehandling

Et naturlig spørsmål på dette punkt er hva vi skal gjøre med SPAM-meldingene. Skal vi returnere dem, plassere dem i 'karantene' mens vi sender mottageren beskjed, eller bare kaste og glemme dem? Svaret er ikke innlysende. Umiddelbart er det mest fristende å returnere dem, hvilket på den ene siden må bli til plage for senderen, og på den andre siden gir legitime sendere anledning til å rette opp sine feil. Så enkelt er det imidlertid ikke. Med mindre vi har kontrollert meldingen skikkelig under 'innpasseringen' er sjansene store for at retur-adressen ikke finnes. Dermed blir returmeldingene liggende i en lokal kø der de consumerer ytterligere ressurser i stedet for å bli borte. Der adressen er legitim, viser den seg ofte å være hos en uskyldig tredjepart som har vært offer for et innbrudd eller en virus som sprer meldinger videre.

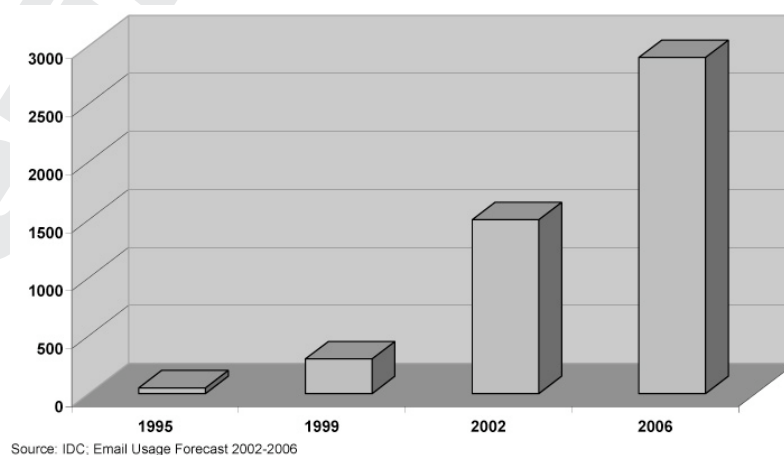
Karantene er en alminnelig opsjon i både frie og kommersielle verktøy, og fungerer typisk på den måten at meldingene blir midlertidig tatt vare på, mens mottageren får beskjed om deres eksistens og situasjo-

nen. Dermed får han eller hun mulighet til å akseptere, forkaste eller ignorere meldingen. I første tilfellet blir senderen registrert som legitim og fremtidige meldinger akseptert. I motsatt fall blir de automatisk forkastet neste gang. Metoden er effektiv, men forutsetter at volumet er overkommelig og brukerne velinformert for at de skal se på tiltaket som positivt.

Slik verden ser ut i dag, er det i mange tilfeller mest optimalt å forkaste meldingene og registrere avsender der det er mulig. Informasjonen evalueres av den lokale epost-ansvarlige, som eventuelt videresender til en av politi-tjenestene som vi diskuterer i neste utgave.

'Falske positive'

Det er ikke til å unngå at tiltakene fra tid til annen også vil blokkere legitime meldinger. Målsettingen er å holde antall slike 'falske positive' på et minimum, men å sørge for at de ikke forekommer er like umulig som å hindre trafikkulykker. Tilfeldigheter, feil, sløvheter og ulykker forekommer, og gir uforutsigbare resultater. Derfor er det ønskelig at noen i organisasjonen – eller hos tjenesteleverandøren – overvåker loggfilene, og avdekker slike falske positive. Interessant nok viser praktisk erfaring at selv store og antatt profesjonelle organisasjoner har betydelige svakheter i sine epost-systemer, og kan havne på blokkeringslistene våre fordi de rett og slett er for lite profesjonelle. En stor (amerikansk) leverandør av programvare for nettverkssikkerhet hører hjemme i denne kategorien. Deres nyhetsbulletin blir blokkert av vår SPAM-kontroll fordi senderen oppgir et domenenavn som høres fint ut, men som ikke er registrert i DNS. Når slikt skjer, bør IT-ledelsen hos vedkommende organisasjon kontaktes og gjøres oppmerksomme på forholdet.



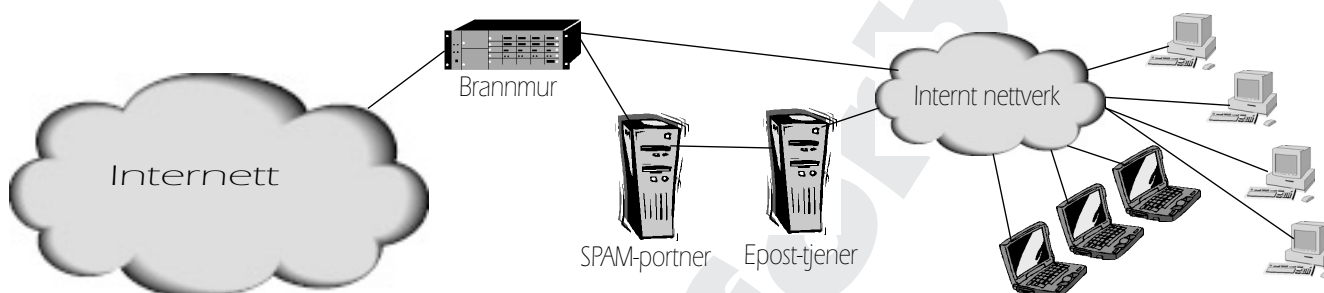
Figur 1 Analyse selskapet IDC forventer en dobling av SPAM-volumet fra 2002 til 2006.

Praktisk SPAM-kontroll

Som figur 1 viser, forventes SPAM-situasjonen å forverres vesentlig i løpet av de neste årene. Situasjonen er imidlertid ikke håpløs. Som vi har sett, finnes det en rekke virkemidler som på egen hånd eller sam-

let kan levere god beskyttelse mot det elektroniske søppelet. Dessuten – og dette er den gode nyheten i bildet – gir de enkleste virkemidlene de beste resultatene. Vi kan med enkle midler fjerne over 90% av SPAM-mengden, uten å få plagsomt mange 'falske positive'.

Følgende punkter oppsummerer en samling enkelttiltak vi har satt i verk for å begrense SPAM-trafikken rettet mot domener som kontrolleres av Team Mellvik as. Med god hjelp fra Torkel Hasle i Biblioteksystemer as og John Berntsen hos Pepco as, som har hatt beslektede tiltak i drift over lang tid, har vi oppnådd forbausende resultater.



Figur 2 En SPAM-kontroller plasseres i tilknytning til epost-tjeneren som behandler meldinger til og fra Internettet, enten integrert med denne tjeneren eller foran den, som en egen maskin eller prosess.

Investeringene er minimale – og de løpende kostnadene likeså. Tiltakene tar utgangspunkt i at innkommende epost passerer gjennom en Linux-maskin med Sendmail eller Postfix som epost-agent. Andre alternativer finnes, men disse to er mest utbredt, og har omtrent tilsvarende egenskaper i forbindelse med SPAM-kontroll. Hvilken som er optimal, avhenger av hva den lokale ekspertisen foretrekker. Også for miljøer som benytter Microsoft Exchange eller andre kommersielle løsninger som epost-sentral, er en tilsvarende løsning attraktiv: SPAM-portneren settes opp innenfor brannmuren, men utenfor dagens epost-sentral, og gjøres usynlig for den eksisterende løsningen – med minimale konfigurasjons-endringer, se figur 2.

Hvor mye ressurser som trengs, avhenger av trafikkmengden, gjennomsnittlig meldingsstørrelse og ikke minst hvilken grad av filtrering vi velger. For volumer under 10.000 meldinger per dag rekker en 500 MHz Intel PC med 512 MB hukommelse langt. Mekanismene vi har satt i verk, følger oppskriften ovenfor:

- ✓ Hent inn en liste over IP-adresser som skal blokkeres. www.ocean.com er en god start – med oppdaterte lister for adresser i Korea og Kina. Disse kan enten legges inn som blokkeringer i brannmuren eller i SPAM-portneren. Siden listene er omfattende (ca. 260 innslag for Korea+Kina), kan blokkering i brannmuren bli for tung å håndtere. Da er *IPtables* under Linux et godt alternativ.
- ✓ Gå gjennom konfigurasjonen av epost-agenten, sørg for avvisning av:

Mer om SPAM-kontroll i
 Postfix: www.postfix.org/uce.html
 Sendmail:
www.sendmail.org/antispam.html og
www.sendmail.org/tips/relaying.html

- ✗ Alle adresser som ikke har såkalte 'reverse navneoppslag' (ikke registrert i DNS-systemet).
- ✗ Adresser som er registrert hos 'SPAM-politiet' – de viktigste er relays.ordb.org, bl.spamcop.net, rbl.maps.vix.com, list.dsbl.org, relays.osirusoft.com, sbl.spamhaus.org.³
- ✗ Meldinger til brukere som ikke finnes.
- ✓ Legg inn automatiske rutiner for scanning av loggfiler, slik at den eller de ansvarlige kan finne falske positive og samle statistikker.

Trenger du spesifikke konfigurasjonsdetaljer? Send en epost til info@mellvik.no, og fortell hva du trenger – og gjerne litt om dine erfaringer – med andre tiltak, SPAM-mengder og annet!

Statistikkene er viktige for å kunne se effekten av tiltakene. En reduksjon på 60-90% er rimelig å forvente – i vårt konkrete tilfeller måler vi over 90%. Neste trinn er innholdsfiltrering – i første omgang på 'Subject'-feltet og eventuelt på meldinger under en gitt størrelse. Ord og uttrykk det bør filtreres på, fremkommer raskt ved å se på siste ukers SPAM-meldinger. Også slike tiltak er enkle å integrere med de nevnte epost-agentene, og bør gi en ytterligere reduksjon på minst 5%.

Konklusjon

SPAM er et like stort og alvorlig problem som virus, og er som vi har sett beslektet, siden leveringsmekanismen i de fleste tilfeller er den samme. Like viktig er observasjonen at et virusfilter også bør brukes som SPAM-filter. Det er ingen grunn til, og dessuten ineffektivt, å ikke slå begge fluer i en smekk. Dessuten finnes det, som vi har sett i denne artikkelen, enkle mekanismer som ikke bare reduserer SPAM-mengden vesentlig før filtrering tas i bruk, men som i samme slengen reduserer antall virus som banker på våre nettverksdører tilsvarende.

Tiden er overmoden for å ta disse enkle hjelpemidlene i bruk. Dersom vi besitter den nødvendige ekspertisen internt, er det lite annet enn omprioritering av tid som skal til. I motsatt fall er det oppportunt å vurdere hvorvidt kommersielle virkemidler med forenklete brukergrensesnitt skal tas i bruk, og om det er optimalt å sette hele utfordringen bort til spesialister. Vi har ingen problemer med å la tredjeparter ta hånd om våre talepostkasser, og det er ingen grunn til ikke å vurdere tilsvarende for epost.

Neste utgave

I neste utgave følger vi opp denne artikkelen med en gjennomgang av aktivitetene til 'SPAM-politiet', som ikke er noe regulært politi, men en håndfull organisasjoner som bruker store ressurser på å avdekke og gjøre tilgjengelig informasjon om SPAMmere. Derigjennom setter de oss i stand til effektivt å blokkere kildene – via lister og oppslagsmekanismer som har mye til felles med tilsvarende for virus. Vi skal også se på et *open source* verktøy for SPAM-kontroll: SPAMassassin – populært og effektivt i sin kategori. ■

³ Mer om disse i neste utgave, se baksiden.