

SPAM-politiet: Effektivt og tilgjengelig

Mens søppelpost, SPAM, er en beviselig kostbar plage, er det kun unntaksvis ulovlig i juridisk forstand å være 'SPAMmer'. I USA er det innført lover med varierende grad av stringens på såvel føderalt som delstatsnivå. Her defineres hvor grensene går og hvor ansvaret ligger, men i en globalisert verden uten grenser, har slik lovgiving beskjedent praktisk effekt.

Derfor finnes det heller ikke noe SPAM-politi i juridisk forstand. På den andre siden, og som vi diskuterte i forrige utgave av Mellvik-Rapporten, finnes det en lang rekke relativt enkle tiltak som kan settes i verk for å begrense strømmen av søppelpost. Tiltakene er beviselig effektive: Å eliminere mellom 50 og 90% av all søppelpost er en overkommelig oppgave.

At tiltakene er enkle for oss, betyr imidlertid ikke at de er trivielle i seg selv, eller er blitt til uten innsats. Internett-tjenester som registrerer SPAM-kilder og tilbyr effektive oppslagstjenester for oss som er brukermiljøer, er en hovedingrediens i beskyttelses-tiltakene.

Uten disse tjenestene ville vi stått maktesløse i kampen mot SPAM.

Videre er det slik at mens 80-90% blokkering kan høres tilfredsstillende ut i dag, vil bildet se annerledes ut om et år eller to dersom veksten opprettholdes. Målsettingen er å komme langt nærmere 100%.

SPAM er et mål i bevegelse: Kildene flytter seg, mekanismene forandres og metodene for å komme rundt mottiltakene er i kontinuerlig utvikling – på samme måte som tilfellet er for virus. Derfor kreves det en ytterligere fokusering på aktive tiltak – hvilket fordrer tid, ressurser og engasjement.

Hittil har markedet vært lite villig til å betale for slike tiltak. Mens dette forholdet

Rapport fra fronten

Vi har ved flere anledninger trukket frem likhetene mellom SPAM og virus – to sider av samme sak på mange måter. Jo mer vi arbeider med problemet, desto større blir likhetene. Mer eller mindre identiske spredningsmekanismer, konsekvenser, kostnader og bekjempelsestiltak forteller at det er meningsløst å behandle de to truslene separat. Tar vi den ene skal det ikke all verdens innsats til for å ta også den andre.

Samtidig observerer vi at SPAMmerne blir stadig mer utspekulerte: Etter samme mal som virus-'fabrikantene', finner de kontinuerlig nye veier for å omgå våre beskyttelsestiltak – og de lykkes. Ikke alltid, men ofte nok til at det vises. For eksempel registrerer vi – i forbindelse med vår egen praktiske SPAM-øvelse – at 'angrepene' forandrer seg i takt med våre beskyttelsestiltak.

Vår epost-tjener avviser epost fra titusenvis av potensielle SPAM-adresser, via mekanismer som vi diskuterte i forrige utgave. Som seg hør og bør har epost-tjeneren en *backup*, en reserve (to eller tre er alminnelig) som er registrert i DNS-systemet. Skulle hovedtjeneren være utilgjengelig, kan reserven kontaktes og vil motta og mellomlagre epost på våre vegne.

Mekanismen er nyttig og nødvendig. Samtidig introduserer den en bakvei forbi SPAM-kontrollen: Dersom én eller flere av reservene ligger utenfor vår egen kontroll, for eksempel hos en ISP, er bakveien et faktum. ISPenes SPAM-kontroll er typisk enten fraværende eller vesentlig mindre striks enn vår egen. Samtidig ligger det i sakens natur at reserve-tjeneren må kunne levere all mottatt post videre til oss – uansett hvor illegitim avsenderen måtte være sett fra vår side. Vi tar ikke først imot hjelp til midlertidig oppbevaring av post, for deretter å straffe hjelperen for jobben.

Denne bakveien er ikke bare tilgjengelig, men automatisk: Epost-tjenestene er bygget slik at de går videre til backup-tjeneren dersom de ikke kommer igjennom direkte. Den eneste måten å håndtere problemet på er å sørge for samme grad av kontroll på alle innpasseringspunkter. Dersom det betyr å selv ta ansvaret for reserve-tjenerne – eller å flytte hele ansvaret ut til en partner som også kan håndtere SPAM-blokkering, får det stå sin prøve. Ingen av delene er vanskelig verken teknisk eller på andre måter, og behovet for pålitelig, ubesudlet epost blir ikke mindre med tiden.

endrer seg i takt med problemets størrelse, er forståelsen fortsatt beskjedent hos det vi kan kalle 'bevilgende myndigheter' i små og store organisasjoner. Vi bruker gjerne penger på mekanismer og programvare som beskytter oss, men er vi villige til å bidra til organisasjoner og grupperinger som bekjemper problemet på et høyere nivå? I 99 av 100 tilfeller er svaret nei.

Ikke desto mindre finnes det et halvt dusin slike grupperinger i aktivitet, med resultater svært mange av oss nyter godt av allerede. I denne artikkelen skal vi se nærmere på hva de gjør, hvordan de overlever og hva de betyr for oss.

Nødvendig engasjement

Der loven ikke strekker til, er sunn fornuft og engasjement nødvendige forutsetninger for å bekjempe problemene. Byenes natteravnere er en glimrende analogi – med både bekjempende og forebyggende effekt. Hovedpoenget er at all verdens beskyttelse aldri kan bli god nok dersom ingen samtidig motarbeider selve problemet. Jo flere som engasjerer seg, desto raskere kommer resultatene.

For SPAM betyr det at vi som har teknologi-ansvar, ikke kan sitte med hendene i fanget og vente på at 'noen' skal få slutt på problemet. Denne 'noen' er oss, og det skal lite til for å yte et positivt bidrag. Nest etter å sette i verk minimale blokkeringstiltak for egen organisasjon, betyr det å være aktiv i rapporteringen av SPAM. Som vi skal se nedenfor, finnes rapporteringstjenestene, og koster liten tid. Neste trinn er økonomiske bidrag, som de fleste tjenestene er takknemlige for å motta, uansett størrelse.

Sløvheter er enhver SPAMmers beste hjelper. Som vi påpekte i forrige artikkel, var fri videreformidling av epost en selvfølge i Internettet på 80- og 90-tallet. Det var naturlig å hjelpe hverandre, et element i

alminnelig høflighet – inntil åpenheten ble offer for misbruk i stor skala. I dag er det motsatte tilfellet. Det er ikke bare god takt og tone å blokkere fri videreformidling, det blir betraktet som på grensen til kriminelt å ikke gjøre det. Tilsvarende gjelder for bruk av blokkeringsmekanismer og sporadisk kontroll av loggfiler og volumutvikling. Dette er grunnleggende oppgaver for driftsansvarlige. Finnes det ingen som har slikt ansvar – eller tid til å ta det, er tjenesten overmoden for utsetting til en ekstern tjenesteleverandør.

Likeledes vitner det om sløvheter og kompetansemangel å benytte ikke-registrerte Internett-adresser for levering av epost. At det er lovlig betyr ikke at det er akseptabelt, og stadig flere

40% SPAM i Storbritannia

En fersk rapport fra den britiske ISP-en BT Openworld, konkluderer med at over 40% av all epost til selskapets brukere i Storbritannia er SPAM. I seg selv er dette en lite oppløftende anerkjennelse for en ISP, og tallene ville neppe ha blitt publisert om ikke selskapet samtidig kunne fortelle hva de har gjort for å ta hånd i hanke med problemet. Anti-SPAM teknologi fra det amerikanske selskapet Brightmail (www.brightmail.com), som leveres av sikkerhetselskapet Symantec på våre breddegrader, overgår forventningene i henhold til rapporten. Løsningen er forøvrig den samme som Oslo Kommune i disse dager installerer som del av sin nye meldings-løsning, der programvare fra Critical Path (www.criticalpath.net) stakk av med kontrakten foran nesen på blant andre Microsoft og Oracle.

BT Openworld foretok sine målinger i perioden 17. til 23. mars, og kunne konstatere at over 11 millioner av totalt 25 millioner meldinger tilhørte kategorien SPAM. I samme periode samlet løsningen opp intet mindre enn 113.000 virusser.

Vel koster det penger å blokkere SPAM, men hva koster det å formidle dem, og hvor er norske ISP-er i bildet? Våre egne målinger viser at mer enn 1 av 10 SPAM-meldinger har vært innom en norsk ISP på sin vei til vår epost-tjener. Dette er en situasjon der ISP-ene skal gå foran og vise vei, ikke dilte etter og reagere når de blir tvunget til det!

mottakere blokkerer slike avsendere uten videre – eventuelt kombinert med automatisk informasjon til avsender om at så er tilfelle (se fakta-ramme om 'sløv epost-administrasjon').

Blokkerings-tjenester

Hvorfor får jeg SPAM?

En fersk rapport fra amerikanske *Center for Democracy Technology* kartlegger og forklarer hvorfor og hvordan våre epost-adresser havner på gigantiske adresselister – som i sin tur benyttes for SPAM.

Rapporten er tilgjengelig fra www.cdt.org/speech/spam/030319spamreport.html

Vi har konstatert at å stoppe SPAM på individuell basis er umulig. For det første angripes kun symptomene, og for det andre er mengden for stor og 'angrepene' for dynamiske til at individer og enkeltorganisasjoner har mulighet for å følge med og å være effektive. Vi er helt avhengige av fellesinnsats – tjenester som for det første kan samle inn informasjon om adresser og kilder til SPAM, og dernest levere mekanismer som forenkler forsvaret av brukermiljøene.

Et slikt politi har vært en del av det vi kan kalle antiSPAM bevegelsen siden siste halvdel av 90-tallet. Tjenestene de leverer, som vi skal komme tilbake til i detalj nedenfor, gjør det mulig for epost-agenter (som Postfix, Sendmail, Qmail med flere) å foreta raske oppslag før innkommende meldinger blir akseptert. Meldinger som forsøkes levert fra kjente SPAM-kilder kan dermed avvises allerede i oppkoblingsfasen, før data er utvekslet.

Sløv epost-administrasjon

SPAM-kontroll har bivirkninger. Én av dem er å avsløre hvor dårlig det står til med drift og administrasjon av epost-systemer generelt. Dette er åpenbart en venstre-håndsoppgave – også hos organisasjoner som burde vite bedre, for eksempel ISPer og selskaper som spesialiserer seg på IT-sikkerhet. I løpet av en periode på mindre enn to uker registrerte vi for eksempel mer enn 40 organisasjoner, de fleste norske, som leverer epost fra ikke-registrerte IP-adresser. Mens dette er fullstendig legalt, er det også dårlig kutyme og forteller om mangelfull fokusering og ditto krav til egne rutiner. Bedre blir det ikke av at mindre enn 1 av 20 responderer på henvendelser om forholdet. Og sist men ikke minst: Dette er kun én av en rekke feilkonfigureringer som plager tallrike epost-installasjoner, og bidrar til å redusere nytteverdien av mediet dramatisk. En annen er at systemene ikke reagerer på avvisningen, men gjentar leveringsforsøket med intervaller ned til 10 sekunder i flere dager. Selv om meldingene ikke kommer frem, blir det nettverkstrafikk og dermed ressursforbruk av slikt.

Denne 'gi blaffen' holdningen indikerer at epost ikke hører hjemme som intern oppgave i organisasjoner flest. Det finnes verken forståelse, interesse eller kompetanse til å ta seg av en så viktig kommunikasjonskanal hos organisasjoner flest. Oppgaven egner seg utmerket til bortsetting – som ikke bare ville heve kvaliteten for de aller fleste, men samtidig redusere kostnadene – ikke minst de skjulte.

Noen av organisasjonene som i løpet av perioden har havnet på denne listen er: Officeshop.no, Eurofoto.no, Sogn og Fjordane Energiverk, flere kommuner, Helly Hansen, XXL, utgiveren av ukebulletinen *Information Security News* (West Coast Publishing, Inc.), Internett-registrar Network Solutions Inc., PC Magazines digitale leveringstjeneste – og vi kan fortsette. En interessant observasjon er at mer enn halvparten av innslagene på listen lever av Internett- eller IT-relatert virksomhet. At epost-tjenesten fungerer og at meldingene kommer frem til kunder og leverandører er en livsbetingelse. Like fullt ignoreres grunnleggende 'service-behov'. Det blir som å leve av drosjetrafikk uten å vedlikeholde bilen.

Her er vi inne på et viktig poeng: Til tross for at vi gjerne kaller dem 'blokkerings-tjenester', blokkerer de ingen ting. De vedlikeholder kataloger (databaser) som er lett tilgjengelige for oppslag via standardmekanismer. Disse brukes i sin tur av hvem som helst som ønsker å blokkere trafikk fra registrerte SPAM-kilder.

Vår egen erfaring er at slike mekanismer typisk står for mellom 50 og 60% av blokkeringene – et høyt, men ikke forbausende tall som forteller i klartekst hvor effektive og nyttige disse tjenestene er.¹

Hvem og hvordan?

Hvem driver disse tjenestene og hvordan fungerer de? Her begynner den virkelig interessante delen av historien, både teknisk og sosialt. Tjenestene –

et halvt dusin av dem – drives etter idealistiske prinsipper, med

¹ Spesielt interesserte vil ha nytte av å vite at 30% av avvisningene har sin årsak i uregistrerte avsendere – systemer uten registrerte DNS-navn. Prosentene tar ikke hensyn til forbindelser som avvises i brannmuren (adresser i Kina og Korea, se forrige artikkel – Mellvik-Rapporten nr. 106).

UBE – *Unsolicited Bulk Email*

UCE – *Unsolicited Commercial Email*

Postfix mot SPAM

Epost-agenten Postfix er en solid og fleksibel (*Open Source*) plattform for både SPAM- og viruskontroll. Den er effektiv, enkel å installere og kurant å integrere sammen med andre epost-systemer, for eksempel som usynlig *front-end* for Microsoft Exchange. Postfix kan kjøres uten videre på de fleste tenkelige Unix- og Linux-systemer.

Vi har så langt konsentrert diskusjonen om SPAM. Samtidig har vi en rekke ganger konstatert at SPAM og virus er to sider av samme sak. I neste utgave – i spalten 'godbiter' – forteller vi hvordan Postfix enkelt og greit også kan brukes som virus-filter, uten å tenke på daglige oppdateringer av signaturer etc.

Mer om Postfix på www.postfix.org.

utgangspunkt i Open Source programvare og finansiert gjennom donasjoner og salg av tilleggstjenester. Så pussig det enn kan høres, er dette det best tenkelige utgangspunkt: Slike tjenester må per definisjon være uavhengige og uten andre interesser enn å bekjempe problemet.

Om vi har behov for flere? Definitivt. For det første angriper de ulike sider av problemet, for det andre har de ulike mekanismer for å velge hvordan SPAMmere registreres og listene oppdateres. Og for det tredje er det sunt med konkurranse – selv på gratis-tjenester. Dette handler ikke om penger, men om ego og faglig dyktighet hos aktørene. I likhet med andre (og mer alminnelige) former for konkurranse er dette utelukkende positivt innenfor rimelige grenser.

Hvor kommer dataene fra? Hvordan vet disse aktørene hvem som er kilder til SPAM, og hvordan kontrolleres de? Dette er rosinen i pølsen så og si: SPAM er langt fra alltid en sort/hvit eller av/på-situasjon, men et spørsmål om evaluering. Normalt (og noe forenklet) deler vi UBE/UCE i tre kategorier nettopp for å forenkle denne kategoriseringen:

- ✓ Åpenbar SPAM – som er lett å håndtere via tjenestene vi diskuterer her og mekanismer vi diskuterte i forrige artikkel.
- ✓ Gråsoner – som krever innsats fra den enkelte mottaker for evaluering og eventuell rapportering.
- ✓ Legitim masse-epost – fra leverandører der vi har registrert oss selv og akseptert å motta markedsføringsmeldinger.

Her er gråsonen den innlysende utfordringen: Vi kan irritere oss over

uønsket post, og det naturlige er å slette den og storme videre. Sannsynligheten er imidlertid stor for at en ny dukker opp fra samme avsender en time, en dag eller en uke senere. Så kan vi gjenta operasjonen, eller bruke de minuttene som skal til for å registrere meldingen hos en av tjenestene (se nedenfor), og dermed øke sannsynligheten for at strømmen stopper – fra denne avsenderen.

Anmeldelser og etterforskning

Det er med andre ord rapporter fra brukermiljøene, gjerne representert ved

Epost, SPAM og sunn fornuft

Enkelte ting kan aldri gjentas for ofte. Bruk av sunn fornuft – i alle sammenhenger – er et godt eksempel. Om årsaken er at det blir gjentatt for ofte vites ikke, men faktum er i alle fall at fornuften synes faretruende fraværende i forbindelse med epost. Her er et par eksempler til ettertanke:

- Over 40% av all intern epost er unødvendig. Mediet og verktøyene frister til misbruk. Meldinger som skulle ha vært sendt til én eller noen få mottakere, distribueres til en lang liste hvorav de fleste er helt uinteresserte i innholdet, eller det er dem uvedkommende. I enkelte tilfeller er det sågar gradert informasjon som overeksponeres på denne måten. Motivasjonen er som regel å få oppmerksomhet fra kolleger og overordnede, uten at noen vil innrømme det. Tilsvarende gjelder for vitser, bilder og filmsnutter av mer eller mindre humoristisk karakter, som ikke bare konsumerer betydelige tekniske ressurser, men kaster bort like mye tid for en gjennomsnittlig medarbeider som SPAM.
- Tilsvarende misbruk gjelder for 'svar'-funksjonen, der den opprinnelige meldingen med søkke og snøre (vedlegg etc.) sendes tilbake til avsender sammen med et svar som typisk er i størrelsesorden et par linjer. Og ikke bare avsenderen, men hele mottaker- og kopi-listen blir gjerne tilgodesett med denne uønskede kopien av allerede mottatte data.
- Mange, kanskje de fleste ekte SPAM-meldinger inneholder en 'mulighet' til å melde seg av listen. 'Trykk her dersom du ikke ønsker mer informasjon' er en typisk formulering. Dette er SPAMmernes mest effektive måte å samle legitime adresser på. Sørg for at alle epost-brukere er klar over at de aldri skal benytte seg av slike 'muligheter': De virker eksakt mot sin hensikt. [Ta en titt på www.spamhaus.org/global-remove.html for et glimrende eksempel.]

Enkel og effektiv SPAM-kontroll

På jakt etter en enkel og billig løsning for kontroll og blokkering av SPAM? Hvem er ikke det – og som vi konstaterte i forrige utgave av Mellvik-Rapporten, finnes det både billige og effektive løsninger. Vi har benyttet epost-agenten Postfix i en rekke løsninger (se ramme på foregående side) – en effektiv vei mot målet dersom vi har et passende system å installere programvaren på.

I motsatt fall – vi trenger et helt system – er **IMgate** [imgate.meiway.com] et interessant alternativ: Et komplett system, ferdig konfigurert til utelukkende å formidle epost, oppsatt med grundig SPAM-kontroll og gode muligheter for innholdskontroll. Sentralen i det hele er en Intel-basert PC med kapasitet som står i forhold til epost-volumet, og som i mange tilfeller kan være en avdanket Pentium-maskin. Operativsystemet er FreeBSD, og enkeltelementene må lastes ned og installeres hver for seg. Med en grundig rettleiding er dette relativt problemfritt.

Et annet alternativ er MessageWall [www.messagewall.org] – som ikke er en fullskala epost-agent, men en SMTP-proxy. Den installeres i forkant av den egentlige epost-agenten, som kan være hva som helst – fra Sendmail til Exchange. MessageWall har fordelen av å være spesialsydd for oppgaven, som gir høy effektivitet og enkel operasjon. Videre blir fleksibiliteten større med hensyn til konfigurasjon, der metode og grad av filtrering kan velges for hver enkelt mottaker – om ønskelig.

drifts- eller epost-ansvarlige, som er grunnlaget for tjenestene. Noe forenklet fungerer det på følgende måte: En melding som oppfattes som SPAM, videresendes til én eller flere 'politi-tjenester' – for eksempel Spamcop.org. Her registreres informasjon fra meldingens hode ('konvolutt')², som kryss-sjekkes mot eksisterende kunnskapsdatabase og returneres til rapportøren for verifikasjon. Dette kan ta fra noen minutter til noen timer avhengig av hvilken tjeneste som benyttes og hvordan belastningsbildet ser

ut. Kommersielle tjenester er gjerne noe raskere enn frie (Spamcop.org har begge deler), men forøvrig like.

Epost-tjenere som er åpne for fri formidling og kan misbrukes av hvem som helst (*open relay*), avsløres raskt på denne måten, og rapporteres til spesielle tjenester (se ordb.org nedenfor). I februar 1998 var 55% av alle epost-agenter på Internettet åpne for fri formidling. 18 måneder senere var tallet nede på 17% og anslås i dag til rundt 10%. Mens progresjonen er påtagelig, er det viktig å huske hvilken vekst vi samtidig har hatt i mengden tilgjengelige epost-agenter på Internettet. I praksis er antall åpne epost-agenter i dag marginalt mindre enn i 1998.

En gitt adresse eller avsender blir ikke registrert som SPAMmer (eller åpen formidler) før det er kommet 3-5 sammenfallende klager. For åpne formidlers vedkommende blir tilgjengeligheten kontrollert forlengs og baklengs av automatiserte rutiner og fra flere kontroll-punkter. Både avsender og alle steder som ifølge konvolutten har vært involvert i formidlingen, gjøres kjent med klagen og får anledning til å klage eller rette på feilene før endelig svartelisting finner sted. I praksis er de fleste slike advarsler til liten nytte. Adressene i konvolutten er ofte falske (de finnes ikke), eller de tilhører helt andre enn den virkelige avsenderen. De er imidlertid ikke dermed overflødige: De tjener for det første som sikkerhetsventil mot misbruk av svartelister, og for det andre som en legitim mulighet til å både avverge feilsituasjon og for seriøse aktører til å sette en stopper for misbruk av ressurser.

Å bli 'svartelistet' på denne måten er praktisk plagsomt og dessuten nedverdiggende for både organisasjonen og de teknisk ansvarlige. Seriøse organisasjoner sørger derfor typisk for å bli fjernet fra listen så snart de blir oppmerksomme på problemet – gjerne i løpet av få timer.

2 Det er viktig at slike meldinger videresendes med all hode-informasjonen intakt, ikke bare den korte versjonen som normalt er å se på skjermen.

Det betyr imidlertid ikke at listen er kort. For det første finnes det titusenvis av organisasjoner med egen epost-tjeneste, men uten å ha forutsetning til å drive den. Ingen leser meldingene til *postmaster*³ om at noe galt er fatt, tjenesten forblir åpen i måneder og år, mens brukerne undrer seg over at eposten fungerer stadig dårligere.

En kortfattet oversikt over de viktigste tjenestene følger nedenfor.

Spamcop.net – [www.spamcop.net] er vår foretrukne tjeneste for rapportering av SPAM. Etter å ha registrert vår epost-adresse og bekreftet denne gjennom en rask epost-transaksjon, får vi tildelt en spesiell adresse som skal benyttes når vi videresender SPAM-meldinger. Denne adressen inneholder en kode som identifiserer oss som avsender, og med denne i adresselisten er vi klare til å bli rapportør.

Spamcop analyserer meldingen vi har formidlet, finner alle adresser den har vært innom på sin vei, og gjennomgår innholdet på jakt etter adresser. Deretter sendes advarsler til administrative mottakere på disse adressene – det kan være fra 1 til nærmere 20 av dem i hver melding. Etter gjentagne rapporter og manglende respons fra de administrative kontaktene havner en adresse til slutt på svartelisten, der den blir værende til noen tar initiativ til å få den fjernet – sammen med indikasjoner på at problemet er fjernet.

Svartelisten er tilgjengelig via adressen bl.spamcop.net. Tjenesten er gratis, men kan suppleres av betalte tilleggstjenester – for eksempel filtrerte epost-konti (rettet mot privatmarkedet) eller større *outsourcings*-oppgaver via partnere.

Spamhaus.org – [www.spamhaus.org] konsentrerer seg om blokkering av de store SPAMmerne. Det er et faktum at overvekten av all SPAM i verden har sin opprinnelse hos én av mindre enn 200 såkalte *hardliners*, som flytter seg fra ISP til ISP over hele verden og sender ut SPAM til de blir stoppet, for så å flytte seg til neste. Spamhaus følger disse 'notoriske forbryterne' og vedlikeholder sin SBL, *Spamhaus Blocking List* – som vår epost-tjener kan gjøre oppslag i via DNS-mekanismer, på samme måte som tilfellet er for Spamcop.

Spamhaus følger disse SPAMmerne selv sammen med utvalgte ISPer, og er ikke avhengig av løpende rapporter fra publikum.

ORDB – Open Relay DataBase – [www.ordb.org] inneholder ikke SPAMmere med adresser til epost-agenter som ukritisk viderefremidler meldinger. Tjenesten er bortimot 100% automatisk: Brukermiljøer eller andre tjenester (for eksempel SPAM-registrene ovenfor) rapporterer inn mistenkelige adresser. ORDB tester dem, legger dem inn i databasen dersom de blir funnet å være åpne, og sender samtidig epost til administrative adresser hos den aktuelle epost-tjenesten. Her blir det

³ 'Postmaster' er en epost-konto som alltid skal finnes og være omdirigert til personen som er ansvarlig for driften – i henhold til standarden.

gjort oppmerksom på hvorfor registreringen er gjort, hvilke konsekvenser den har og hva som skal til for å fjerne registreringen.

Tjenesten er gratis, og mottar gjerne donasjoner.

DSBL – Distributed Server Boycott List – [www.dsbl.org] fungerer omtrent som ORDB ovenfor, men med andre innrapporterings- og kontroll-metoder. Oppslagsmekanismene er de samme og tjenestene kan med fordel brukes parallelt.

mail-abuse.org – er videreutviklingen av det som tidligere het MAPS RBL, *Mail Abuse Prevention System Realtime Blackhole List*. Tjenesten er i løpet av de tre siste årene konvertert fra å være ideell og gratis til å bli kommersiell – og langt mer omfattende. Samtidig er de grunnleggende tjenestene – tilgang til en *open relay* liste (relay.mail-abuse.org) og en blokkerings-liste (blackholes.mail-abuse.org) – fortsatt frie for alle. Videre er de fleste tjenestene fra MAPS tilgjengelig gratis for personlige brukere.

Andre 'svartelister' av interesse:

(Første adresse er til en informativ Web-side, den andre er til den tilhørende oppslagslisten.)

- www.njabl.org (dnsbl.njabl.org)
- blackholes.easynet.nl
(proxies.blackholes.easynet.nl)
- www.sorbs.net (dnsbl.sorbs.net)

Mail-abuse.org retter seg spesielt mot store aktører i markedet, ISPer og store organisasjoner, og legger vekt på opplæring av disse til å forstå sin rolle i SPAM-bildet. I forhold til denne målsettingen finner vi organisasjonens Web-sider kompliserte og vanskelige å finne ut av. Her er det uten tvil et lerret å bleke. Likeledes har vi hatt praktiske problemer med å få kontakt med organisasjonens tjenere ved flere anledninger.

Vanskelig valg?

Med alle disse mer eller mindre overlappende tjenestene, hvilke skal vi bruke og hvordan? Svaret er enklere enn mengden skulle tilsi. Med hensyn til rapportering av SPAM velger vi den enkleste, hvilket for tiden betyr Spamcop – med mindre vi har et betalt abonnement hos én av de andre.

Med hensyn til bruk av oppslagslistene, har vi anledning til å velge flere – gjerne samtlige. Dette er alminnelig, men ikke gratis i ytelsesmessig forstand. Alle oppslag tar tid,⁴ og 4 oppslag tar 4 ganger så lang tid som 1. Det betyr at en tungt belastet epost-tjener neppe bør utsettes for den ekstra forsinkelse dette vil medføre.⁵ Her er det viktig å være klar over at utfordringen er forsinkelse, ikke ytelse. Det nytter ikke å kaste Megahertz på problemet, det er parallellitet som hjelper. To gamle 486 maskiner vil i mange tilfeller gi høyere reell kapasitet enn én Gigahertz-maskin.

Videre finnes det andre måter å optimalisere på, for eksempel *caching* av oppslagslistene og optimalisering av svartelistenes rekkefølge. Epost-agenten vil avslutte behandlingen så snart den har funnet et

⁴ Et typisk DNS-oppslag over Internettet tar mellom 0,5 og 1 sekund.

⁵ De fleste Unix- og Linux-baserte epost-agenter har rikelig kapasitet i så henseende. Epost-volumer på noen få tusen meldinger per time er for beskjedne å regne i en slik sammenheng. For store organisasjoner, ISPer og andre tjenesteleverandører er situasjonen en annen.

innslag som forårsaker avvisning av en melding. Dersom én av listene gir flere treff enn de andre, utgjør det betydelig forskjell at denne kontaktes først. Hvordan dette gjøres i praksis kommer an på hvilken epost-agent som benyttes.

En alternativ vei rundt de ytelsesmessige utfordringene er å bruke en proxy – for eksempel MessageWall (se ramme på side 8).

Konklusjon

Vi leter kontinuerlig etter steder hvor vi kan kutte kostnader, øke produktiviteten – eller begge deler. SPAM-kontroll og blokkering ligger rett foran nesen vår, men angripes likevel kun unntaksvis. Det er fortsatt bemerkelsesverdig få som er oppmerksomme på hvor stort problemet er, hvor mye det koster og hvor enkelt det er å komme i gang med forsvars-tiltakene.

Dessuten – og like viktig – er det å vite at blokkering av SPAM er et effektivt tiltak også mot virus. Vi har gjennom egen erfaring verifisert at enkle innstillinger i tilknytning til epost-agenten Postfix kan fjerne virus som fortsatt ikke har fått en signatur hos antivirus-leverandørene. Denne muligheten – og mekanismene som brukes – skal vi komme tilbake til i neste utgave. Følg med! ■