

Epost-filtrering: Enkelt, billig, effektivt

Det høres unektelig ut som et utklipp fra en annonse eller et stykke TV-reklame. Samtidig setter overskriften fingeren på et akutt problem – og et forslag til løsning. Markedsføring kan være så mangt. I utgangspunktet er jo all positiv oppmerksomhet om en tjeneste eller et produkt, markedsføring. Dersom historien eller påstandene som fremføres, i tillegg er sanne, hvilket dessverre langt fra alltid er tilfelle, får de reell verdi – for produkt, leverandør og et interessert mottakerapparat.

De fleste av oss trekker et skille mellom markedsføring og informasjon, men ingen er uenige i at informasjon kan være svært så god markedsføring. Når vi for eksempel her i Mellvik-Rapporten informerer om positive erfaringer med spesifikke produkter eller teknologier, er det både naturlig og ønskelig at interessen for objektet stimuleres.

Tid for handling

Vårt tema i denne sammenhengen er anti-SPAM-verktøy – i utgangspunktet verken spennende eller teknologisk interessant. Nød lærer imidlertid hvem som helst å spinne, og situasjonen tilsier at interessen i markedet burde være maksimal for slike produkter akkurat nå. Ikke bare ser vi at utfordringene knyttet til uønsket epost og virus fortsetter å tilta. Velbegrunnede regnestykker indikerer at denne kategori meldinger i inneværende år kan komme til å utgjøre mer enn 70% av all

Truende søvngjengere

Infiserte PCer har lange vært en av de største SPAM-kildene på Internettet. Et virus finner veien til en PC, skjuler seg godt og begynner sin oppgave som relé-stasjon – videreformidler av epost, til adresser den finner lokalt eller til adresselister den henter fra SPAM-kilden.

Om den er aldri så plagsom, er denne formen for SPAM håndterbar – fordi meldingene sendes direkte fra den infiserte maskinen. Adressen havner rimelig raskt på en svarteliste (RBL), og miljøer som arbeider aktivt med SPAM-bekjempelse, blokkerer adressen.

I minst samme takt som våre verktøy blir mer sofistikerte, blir også den andre siden – SPAMmerne – 'flinkere'. En ny variant av scenariet ovenfor demonstrerer denne 'progresjonen'. I stedet for å selv levere SPAM-meldingene direkte til mottaker-adressene, benytter de nye 'SPAM-botene' – som de gjerne kalles – seg i stedet av Internett-leverandørens epost-tjener for formidlingen. Dette er den normale veien for epost fra både private Internett-brukere og mange virksomheter. Meldingene leveres til ISPens epost-kontor, som deretter formidler dem videre til mottaker.

Vi skal hoppe over diskusjonen om hvorfor SPAMmerne ikke har benyttet denne veien tidligere, og i stedet se på konsekvensene av forandringen. Mens den infiserte PCens

adresse tidligere kunne svartelistes og derigjennom blokkeres, blir problemstillingen nå en helt annen. Visst kan online.no eller broadpark.no blokkeres i en svarteliste, men en slik blokkering vil berøre alle kunder av den aktuelle tjenesten, ikke bare de som har infiserte maskiner.

Det finnes en rekke eksempler på slike totale blokkeringer av store ISPer, med spanske Telefonica som primær eksponent. Uansvarlige ISPer er blitt 'straffet' gjentagne ganger på denne måten i løpet av de siste 4-5 årene. Slike blokkeringer har imidlertid tilstrekkelig dramatiske konsekvenser for epost som kommunikasjonsmedium, til at bruken av dem kan ha motsatt effekt, og føre til at brukermiljøene ser seg nødt til å droppe svartelistene i stedet for de ansvarsløse ISPene.

Det er både ironisk og begredelig at Internett-leverandørene med relativt enkle midler kunne ha stoppet denne SPAM-trafikken både etter den gamle og den nye modellen. Interessen fra den kanten har imidlertid vært låber (se kommentar om Telenor på side 30). Indirekte er det derfor ISPene som bærer hovedansvaret for at SPAM-problemet nå truer med å ødelegge epost som kommunikasjonsmedium. Det kan være fristende å si 'tilgi dem, for de vet ikke hva de gjør' – men de burde vite det, og vår medlidenhet er fullstendig fraværende.

epost som transporteres over Internettet. Dersom dette stemmer, og trenden fortsetter, er det reell fare for at SPAM kan kvele hele epost-mekanismen slik vi kjenner den i dag.

I begynnelsen av februar kom det dessuten signaler fra eksperthold om at en ny mekanisme for formidling av uønskede meldinger har dukket opp. Mekanismen truer med å gjøre mange av tiltakene som så langt har 'holdt oss i live' i den tiltagende strømmen av søppel, verdiløse (se rammen på forrige side for detaljer).

Behovet for å foreta en grundig gjennomgang av forsvarstiltakene er derfor akutt: Den løsning finnes knapt som ikke kan bli bedre – via konfigurasjon, optimalisering, tilleggsprodukter, plattformskifte eller på andre måter. Hvilken kompetanse organisasjonen besitter og i hvilken grad eksterne tjenesteleverandører er involvert i epost-infrastrukturen, avgjør hvilken angrepsvinkel som er optimal. Som vi også er inne på i kommentaren om kommersielle anti-SPAM verktøy på side 33, finnes det en lang rekke produkter av høy kvalitet som gjør en hederlig jobb, og som i mange tilfeller representerer riktige valg.

Utover formålet har imidlertid disse produktene også det felles at de er relativt kostbare. For oss som arbeider med slike problemstillinger, og dermed har forutsetninger for å se konsekvensene, kan kostnads-spørsmålet virke lite relevant i forhold til truslene. For de som sitter på pengesekken, ser det imidlertid gjerne annerledes ut, og kostnadene kan bli det vi kaller en showstopper. Dermed blir eksistensen av Open Source-verktøy spesielt interessant.

Open Source til unnsetning

Vi har tidligere ved flere anledninger diskutert hvordan Open Source-baserte epost-agenter som Postfix, Sendmail og Exim, kan gjøres til aktive medhjelpere i kampen mot uønsket epost. Disse egenskapene sammen med fleksibiliteten og robustheten som karakteriserer verkøyene, er årsaken til deres store popularitet.

SPAM, statistikk og pålitelighet

SPAM-statistikker er middels pålitelige. De er basert på reelle målinger, som i sin tur ekstrapoleres til å bli verdens-dekkende. Dette er mer enn godt nok både til å se utviklingen og til å få realistiske indikasjoner med hensyn til problemets omfang.

Tekniske detaljer og variasjoner sørger imidlertid for betydelig grad av forvirring med hensyn til belastningen denne SPAM-mengden representerer. Dersom vi kan stoppe en melding før den blir levert, for eksempel når avsender er svartelistet, eller dersom mottaker ikke finnes, blir belastningen per melding marginal – både for mottakersystemet og for nettverket. Meldinger som mottas for deretter å bli returnert, kanskje til en ikke-eksisterende adresse, representerer den motsatte enden av skalaen. Meldingen overføres gjerne 5 eller flere ganger før den omsider havner i et arkiv for ikke leverbar post.

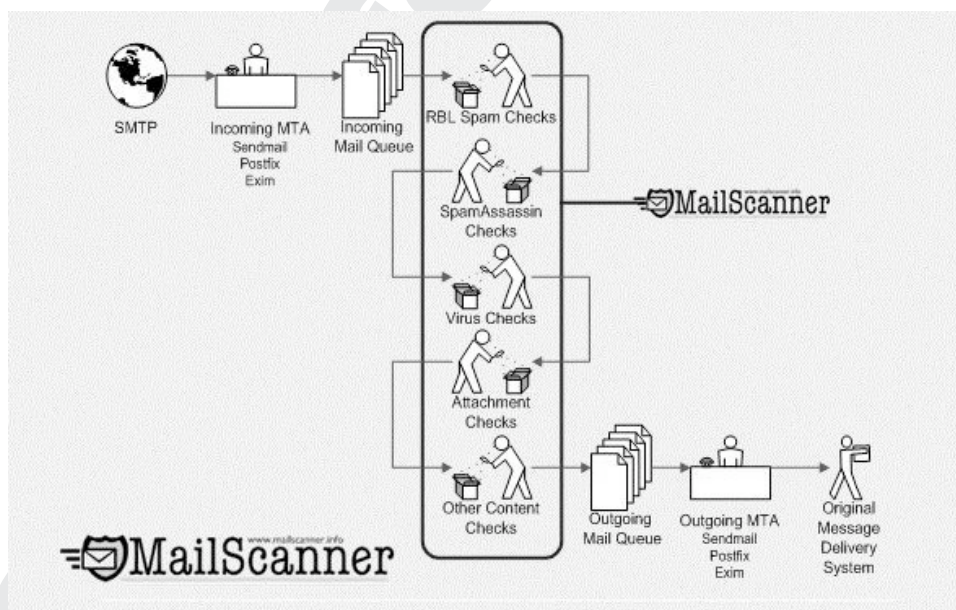
Denne spennvidden er et incentiv i seg selv til å gjøre maksimalt ut av mulighetene som finnes til å optimalisere epost-håndteringen, ikke bare ved å stoppe flest mulig meldinger i døra, men å holde de som kommer gjennom unna tunge og ressurskrevende mastodonter som Exchange og Notes/Domino.

Det er imidlertid grenser for hva selve epost-agenten kan klare på egen hånd, og utfordringen vokser parallelt med at spredningsmekanismene for SPAM virus blir mer sofistikerte. Her kommer Open Source-verktøyet MailScanner til unnsetning. Nærmest uansett hvordan epost-systemet ser ut i dag, kan MailScanner introduseres uten å komme i konflikt med den eksisterende infrastruktur. Dersom vi er så heldige å ha én av de nevnte Open Source epost-agenter i drift, blir oppgaven spesielt enkel, og MailScanner kan praktisk talt brukes 'out of the box'. Installasjonstider på godt under en halvtime

er ikke uvanlig i slike omstendigheter, en effektivitet som ikke engang de kommersielle verktøyene kan konkurrere med.

For andre epost-agenter – for eksempel Exchange eller Qmail – er installasjonsoppgaven mer omfattende, men langt fra avskrekkende for en kompetent og lesefør drifts- og epostansvarlig med Linux- eller Unix-erfaring. Oppskrifter og veiledninger finnes på nettet, om ikke i selve MailScanner-dokumentasjonen, som er omfattende i seg selv, og som dessuten teller to publiserte bøker.

Årsaken til at MailScanner tiltrekker vår oppmerksomhet, er – i tillegg til dens tekniske egenskaper og lave reelle kostnader – produktets utbredelse. MailScanner er installert og i bruk i over 40.000 organisasjoner³ over hele verden, betjener flere brukere enn Hotmail og AOL til sammen, og prosesserer mer enn en halv milliard meldinger per dag. Den er forbausende nøysom i sine ressurskrav⁴ i forhold til de fleste kommersielle verktøy, og har mer enn lang nok fartstid til å kunne påberope seg den pålitelighet som skal til for et virksomhetskritisk verktøy.

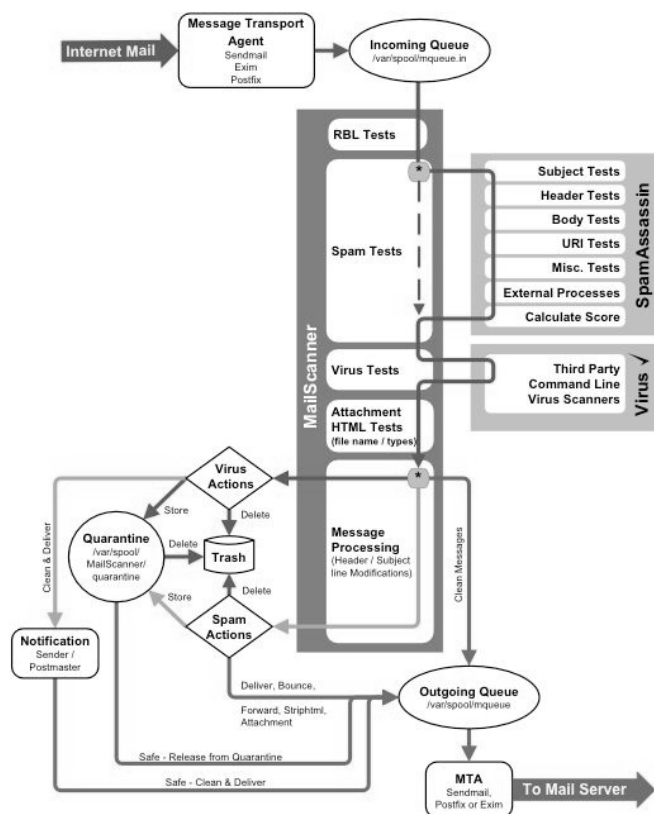


Figur 1 MailScanner tar imot en innkommende epost-kø fra en eksisterende epost-agent, og sender meldingene gjennom 5 prosesser før de eventuelt slippes inn og tilbake til epost-agenten for endelig levering.

Årsaken til at MailScanner i løpet av relativt kort tid (4 år) har fått en slik utbredelse, er at verktøyet bygger på og samarbeider med andre velrenommerte Open Source-verktøy. Produktet er på mange måter et rammeverk som kobler sammen SPAM-kontroll, virus-kontroll, innholdskontroll og andre kontrollmekanismer til en helhet som er over-

3 Blant de mest kjente navnene på 'kundelisten' finner vi Siemens, HP, US Navy, US Army, UCLA, Harvard, MIT. Se www.mailscanner.info for mer informasjon.

4 En velbestykt tjener med 2x2,4GHz Xeon/2GB hukommelse og 15.000 rpm SCSI diskler håndterer over 1,4 millioner meldinger per dag. En gammel Pentium-maskin med rikelig hukommelse er tilstrekkelig for de fleste små og mellomstore organisasjoner, og kan samtidig 'huse' selve epost-tjeneren.



kommelig å forholde seg til uten å kreve ekspertise i forhold til hvert enkelt verktøy.

Figur 1 ovenfor illustrerer hvordan MailScanner fungerer. Den overtar en inngående meldingskø fra epost-agenten, som for enkelhets skyld bør være Postfix, Sendmail eller Exim, og kjører hver enkelt melding gjennom en serie prosesser. Behandlingen resulterer til slutt i forkastelse, karantene eller klarering og overføring – enten til den samme epost-agenten eller til en annen.

Den tekniske prinsippsskissen til venstre synliggjør detaljene i prosessen, og viser at minst to av dem utføres av verktøy som befinner seg utenfor MailScanner. Produktet gir seg med andre ord ikke ut for å være best i alt, men limer – som vi var inne på ovenfor – sammen verktøy som egner seg best for oppgaven.

Punktene nedenfor kaster mer lys over hvert enkelt trinn i prosessen:

- ✓ RBL-tester: RBL står for *Realtime Blackhole List* (se Mellvik-Rapporten nr. 106), og kontrollen her består i oppslag via DNS i én eller flere slike svartelister. Dersom avsenders IP-adresse finnes i en slik liste, blir meldingen avvist. Det er imidlertid langt mer optimalt å la mottagende epost-agent foreta denne kontrollen – hvis det er mulig. Den kan gjøres før meldingen aksepteres og mottas, hvilket sparer enorme ressurser.
- ✓ SPAM-testene utføres av SpamAssassin, et velkjent og velrenommet Open Source-verktøy med enda større utbredelse enn MailScanner. Her får vi imidlertid SpamAssassin i en pakke som forenkler konfigurasjonen vesentlig og samtidig gir kontroll på flere nivåer med på kjøpet. Selv miljøer som i dag kjører SpamAssassin alene, vil ha fordel av å ta i bruk MailScanner.
- ✓ Også virus-skanningen utføres av eksterne programmer – ett eller flere. MailScanner har grensesnitt mot et tosifret antall antivirus-produkter, Open Source og kommersielle, og legger forholdene til rette for å kjøre flere av dem i serie. En typisk konfigurasjon er å kjøre ClamAV, et Open Source-produkt som har fått glimrende evalueringer fra en rekke kilder, og eventuelt spe på med én eller to i tillegg, som ekstra sikkerhet. Poenget med å involvere flere virus-skannere er å heve sannsynligheten for at vi får på plass signaturer for nye virus før de banker på døra. Det er samtidig innlysende at hvert til-

legg har en ytelsesmessig konsekvens, som varierer sterkt fra produkt til produkt, men som må være med i kapasitetsplanleggingen.

- ✓ Kontroll av vedlegg og HTML-kode, inklusive vedleggstyper og filnavn er neste trinn. Hvorvidt denne rekkefølgen er optimal eller ikke, kan diskuteres – i og med at forkasting av vedlegg ville ha forenklet viruskontrollen vesentlig. En del av denne kontrollen kan dessuten gjennomføres av epost-agenten, men siden MailScanner kan slå flere fluer i ett smekk, er det optimalt å samle prosesseringen her.
- ✓ Behandling: Siste punkt er en konsekvens av alle de foregående. Dersom ett eller flere av de trinnene finner noe å sette fingeren på, sørger den avsluttende behandlingen for å gjøre nødvendige endringer for at deler av meldingen likevel skal kunne leveres (fjerning av vedlegg for eksempel). Samtidig får mottaker beskjed om hvilke endringer som eventuelt er foretatt. Her genereres også logger og informasjonsmeldinger til epostansvarlig – som indikert i skissen på foregående side.

Etter fullført behandling sendes meldingen videre til epost-agenten, som kan være lik eller forskjellig fra den som først mottok meldingen. I mange tilfeller begynner prosessen med Sendmail eller Postfix, mens den avsluttende leveringen går til Exchange, en vesentlig optimalisering når Exchange først er med i ligningen.

Oppsummering

SPAM- og virus-problematikken kan angripes på mange måter og med god hjelp fra en lang rekke ulike produkter. Den eneste varianten som ikke fungerer, er å feie problemet under teppet. En slik uansvarlighet er uakseptabel, og eksistensen av verktøy som MailScanner, Postfix, Sendmail, Exim, Qmail, ClamAV og flere sørger for å gjøre terskelen over til en relativt sikker og søppelfri epost-hverdag, særdeles overkommelig.

Som de fleste av oss forlengst har brakt i erfaring, er det imidlertid ikke tilstrekkelig å finne en løsning som fungerer i det den settes i drift. Her forandrer slagmarken og våpnene seg løpende, og den som ikke er i stand til å tilpasse seg kontinuerlig, har tapt. MailScanner har i løpet av 4 år vist seg like god eller bedre enn sine kommersielle konkurrenter i så henseende, ikke minst fordi tilleggsverktøy som SpamAssassin og ClamAV har usedvanlig raske responstider i forhold til nye trusler.

Nærmest uansett hvilken virkelighet vi lever med i dag, skal det gode argumenter til for ikke å ta en nærmere titt på MailScanner. ■