

SPAM: Synlig progresjon

Når begge sider tror de vinner krigen, er det åpenbart at noe er galt. Slik er imidlertid situasjonen på SPAM-fronten – mens vi nærmer oss utgangen av 2004. Hvem tar feil?

Alle vinner, ingen taper?

SPAMmerne – underlig nok vet vi i stor grad både hvem de er og hvor de holder til – mener å være på offensiven både teknologisk og med hensyn til volum. Slik verden ser ut fra deres ståsted, har verken leverandører eller marked klart å komme frem til effektive mekanismer for bekjempelse av SPAM, og mengden epost de sender ut er større enn noen sinne. De har utvilsomt rett på begge punkter.

Samtidig opplever mange av oss at vi får mindre søppelpost. For enkelte er forbedringen marginal, men merkbar – for eksempel 20 meldinger i stedet for 25 per døgn. For andre er søppelposten praktisk talt borte. For egen del er vi nede i 1-3 per døgn, hvilket er 5% av *worst case* nivået fra 2001.

Ute av syne, ute av sinn ...

Dette er faktiske forhold. Kan en slik selvmotsigelse være mulig? Den virkeligheten vi snakker om, er ikke mer komplisert enn følgende analogi: Da Fjellinjen under Oslo ble tatt i bruk, ble trafikkforholdene i byen vesentlig bedre – færre biler, mindre kø, mindre kaos. Trafikken var imidlertid ikke mindre, kanskje snarere tvert imot. Den var flyttet ut av syne. Omtrent det samme er tilfelle med SPAM. Vi har ikke lykkes med generelle mekanismer for å stoppe ondet ved roten, men har kurert en del av symptomene. Det er et viktig fremskritt i seg selv fordi millioner av brukere dermed kaster bort mindre tid på uproduktiv søppelhåndtering. Nærmere en virkelig løsning er vi imidlertid ikke, et forhold vi skal komme tilbake til nedenfor.

Og SPAMmerne har sitt på det tørre: De sender virkelig flere meldinger enn noen gang, og har verken mulighet til eller interesse av å registrere hvor mye som kommer frem til en bona fide mottaker. Lykkelig uvitende om sin reduserte gjennomslagskraft, legger de beslag på en jevnt voksende del av Internettets kapasitet, for ikke å snakke om hundretusenvise av epost-tjenere verden over.

Vi har ved tidligere anledninger påpekt hvordan sistnevnte belastning kan reduseres dramatisk, og sannheten er at hver enkelt system/epost-administrator har mange og gode muligheter til å stoppe en vesentlig del av søppelposten på en slik måte at avsenderen **må** oppdage at den ikke kommer frem. Det skal imidlertid både verktøy, innsikt, interesse og tid til – innsatsmidler de aller fleste virksomheter mangler flere eller alle av.

Med lov skal land bygges ...

Dermed hanger vi videre, mens ekspertisen krangler om standarder og mekanismer for å stoppe elendigheten. Samtidig krangler leverandører, politikere og jurister om hva som er riktige tiltak fra den kanten. En rekke land – og enkelte stater i USA – har allerede innført lover – med de beste intensjoner, men som regel bommer de helt eller delvis på målet.

USA, EU og Australia fikk i løpet av 2003 lover som regulerer bruken av epost som markedsføringskanal, alle med sine sterke og svake sider. Den amerikanske (kjent som CAN-SPAM⁸) har blant annet den svakhet at den tillater én henvendelse til en vilkårlig mottaker, mens flere henvendelser forutsetter godkjenning fra mottakeren. Dersom avsenderen skifter navn ofte nok, representerer loven med andre ord ingen beskyttelse. EU-loven er bedre på flere områder, men beskytter kun privatpersoner. Postkasser hos en arbeidsgiver er ikke dekket, og dermed er vi omtrent like langt. Best ut kommer – ifølge ekspertene – den australske loven, som dekker SMS i tillegg til epost, og forlanger godkjenning fra mottakeren før en eneste melding sendes.

Det ingen lovgivning kan gjøre noe med, er imidlertid det faktum at SPAM kan ha opprinnelse hvor som helst i verden. En amerikansk SPAMmer som sender fra Kina eller India – hvilket er trivielt i teknisk forstand – ramler med andre ord utenfor enhver vestlig lovgivning. At slike lover nå er på plass, forventes derfor ikke å føre til noen merkbar reduksjon, men en flytting av 'kildene'. Ifølge en rapport fra FNs konferanse om handel og utvikling, kom over halvparten av all SPAM i 2003 fra USA, et tall som ventelig vil være vesentlig lavere i år.

... men uten teknologi har vi tapt

Dermed kan det argumenteres for at lovene allerede har hatt positiv effekt, og det hersker ingen tvil om at slik lovgivning er et nødvendig bidrag for å få utviklingen under kontroll. I en digital verden uten fysiske grenser, der ordensmyndigheten har beskjeden kompetanse og ditto ressurser, er det imidlertid innlysende at lover alene kommer til kort. Den mest effektive angrepsvinkel er å ta ondet ved roten – å sørge for at det ikke lønner seg å bedrive SPAM. Dette er lettere sagt enn gjort, fordi å sende en million eller ti SPAM-meldinger koster så godt som ingen ting. Så lenge tilstrekkelig mange brukere responderer på markedsføringen, forblir virksomheten lønnsom. Og 'dumme' brukere kan ikke reguleres bort – verken med lover eller på andre måter.

Det innsatsmidealet vi da sitter igjen med, er det samme som SPAMmerne benytter: Teknologi. Og det er nettopp om teknologi ekspertene har kranglet så busta fyker de siste to årene. Som vi har vært inne på i tidligere diskusjoner om temaet, finnes det en rekke metoder og mekanismer som hver for seg eller sammen kan bidra til å redusere – i noen tilfeller blokkere – SPAM. Dessverre har de fleste av dem bivirkninger som gjør dem uinteressante utenfor spesielle omgivelser. Høy kompleksitet er den hyppigst forekommende innvendingen, mens det i

8 CAN-SPAM: CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING.

andre tilfeller er påliteligheten som ikke holder. Sjansen for blokkering av legitime meldinger blir rett og slett for stor. Klientbaserte løsninger – såkalte SPAM-filtre – gjør god nytte for seg, spesielt i privatmarkedet, men er like fullt for bandasjering å regne. For det første blir det for komplisert for den enkelte bruker å engasjere seg i SPAM-kontroll, og for det andre skalerer ikke slike mekanismer. Belastningen på nettet og postkassene blir ikke påvirket, og vi er (nesten) like langt.

SPF til unnsetning

I 2003 ble SFP – *Sender Policy Framework* – lansert som en potensiell løsning på problemet. Mekanismen (beskrevet i Mellvik-Rapporten nr. 114 side 34) benytter Internettets navnetjeneste som formidler av kontrollinformasjon, og påvirker ingen eksisterende protokoller eller mekanismer. Den representerer en sammenbygging av flere tidligere forslag og ideer, og fikk umiddelbart stor interesse i epost-kretser.

Kjeeper i hjulene ...

Også Microsoft stilte seg opprinnelig positive til SPF, men ombestemte seg plutselig ved siste årsskifte og lanserte i stedet sitt eget forslag. 'Sender ID' kombinerer ideene i SPF med et tidligere forkastet forslag fra Microsoft – 'Caller-ID'.

Teknisk sett er Sender ID greit nok i den forstand at det tar vare på og utvider de attraktive egenskapene i SPF. Imidlertid viser det seg at Microsoft har tatt ut patent på deler av Sender-ID, slik at leverandører som vil ta teknologien i bruk, for det første må lisensiere den fra Microsoft, og for det andre risikerer å måtte betale lisensavgifter i den forbindelse. Dette forholdet – sammen med det faktum at Microsoft har vært uvillige til å opplyse om hvilke deler av forslaget de har søkt patent på, var årsaken til at Sender ID ble forkastet som standardforslag av Internettets standardiseringsorgan IETF i september.

Det betyr imidlertid ikke at Sender ID er borte fra scenen. For det første er draft-spesifikasjonen fortsatt tilgjengelig via IETF eller fra Microsoft, og er – interessant nok – det inntil videre gjeldende referansedokument for SPF. Dessuten fikk vi i slutten av oktober vite at Microsoft ikke har tenkt å gi seg. Selskapets advokater og teknikere har brukt en måned på å massere forslaget, og blant annet gjort det fullt bakover-kompatibelt med SPF. Samtidig har tunge krefter vært i sving i markedet, og America OnLine stiller seg igjen positive til Sender ID, etter å ha vendt ryggen til forslaget tidligere i høst. Det nye forslaget er innlevert til IETF for nye evaluering. Parallelt med dette går Microsoft videre med implementering av Sender ID i sine produkter – og i Hotmail.com. Forventningen synes å være at markedet kan tvinges til å bruke mekanismen, og det kan ikke utelukkes at metoden vil lykkes. Reaksjonene fra markedet er imidlertid unisone: Dette smaker av misbrukt markedsrett.

Situasjonen er fortsatt uavklart, men forventningen er at klokkene ringer tilstrekkelig kraftig til at amerikanske og/eller europeiske myndigheter griper inn. Sin enorme styrke til tross, skal det godt gjøres at Microsoft har nok politisk lobby-kraft til å påtvinge markedet en slik

patentert løsning, spesielt når alternativer finnes og er marginalt forskjellige i såvel teknologi som effektivitet. At selskapet nylig ble utpekt som kilde til SPAM i avisen The Washington Post, bedrer ikke oddsene.⁹ Sist, men ikke minst sørger Microsofts manglende vilje til å spille med i stedet for mot markedet, for å kaste ytterligere skepsis i retning av hvor genuint selskapet egentlig arbeider for bedre sikkerhet. En forverring på denne fronten har selskapet ikke råd til.

Microsofts 'sjanghaiing' av SPF har medført en forsinkelse i arbeidet mot SPAM på nærmere 12 måneder, og kan føre til at aktører som ikke allerede har tatt i bruk SPF eller andre mekanismer, sitter på gjerdet til en oppdatert spesifikasjon for SPF kommer nærmere årsskiftet.

Status

Til tross for denne nedturen er status på SPAM-fronten forsiktig optimistisk. Tiltakene virker – om de er aldri så mye kurerende av symptomer, og sjansene er store for at vi i løpet av 2005 får omforenede kontrollmekanismer som på sikt vil føre til at ressursødingen i Internettet blir redusert. Her er det viktig å huske at de mekanismene vi snakker om (først og fremst SPF) også har en sikkerhetsmessig viktig effekt. Når en slik mekanisme er på plass, blir det vesentlig mer komplisert å sende epost med falsk avsender.¹⁰

En annen positiv nyhet er at ISPene omsider begynner å føle presset fra markedet om å ta ansvar. Det beste eksemplet kommer fra amerikanske Savvis.com, en av verdens største ISP-er. Etter kraftig press fra blant andre antispam-organisasjonen Spamhaus, gikk Savvis i september med på å terminere tjenestene til nærmere 150 kjente SPAM-ere. Selskapet, som blant annet betjener 100 av verdens største banker og mange av de store finansinstitusjonene på Wall Street, hadde store inntekter fra SPAM-kundene, og vegret seg i det lengste for å terminere dem. Først etter at en frustrert eks-ansatt lekket informasjon om størrelsen på selskapets inntekter fra SPAM-kildene, ble belastningen for stor for Savvis.

Det er naturligvis frustrerende å se hvor langt inne det sitter for ISP-er i sin alminnelighet å velge bort inntekter for å holde sin sti ren. Tilsvarende frustrasjoner kan anføres for offentlig sektor og myndigheter – ikke minst her hjemme, som har markedsrett nok til å kreve ryddighet fra sine leverandører, men som kun unntaksvis gjør det. SPAM er et av svært få områder hvor offentlig sektor i kraft av sin størrelse som kunde virkelig kan utøve et påtrykk for å snu en negativ utvikling. Vi har kontaktet Samferdselsdepartementet ved flere anledninger i den forbindelse, men aldri fått noen respons. Mon tro om de ikke forstår problemet? ■

9 Microsofts toppsjef Steve Ballmer sendte tidligere i høst ut et 'executive letter' via epost til en liste på mange millioner, hvor han blant annet diskuterer hvor feil det er at Windows er usikkert og at Linux er bedre. Mens ingen benekter at dette er markedsføring, hevder Microsoft hardnakket at det ikke er snakk om SPAM. [Se www.washingtonpost.com/ac2/wp-dyn/A26555-2004Nov4]

10 En annen viktig side av epost-sikring er autentisering av sender og mottaker, og integritetskontroll av innholdet. Mens dette er temaer vi har diskutert en rekke ganger tidligere i Mellvik-Rapporten, er tiden moden for en revisitering og oppdatering. Den kommer på nyåret. Følg med!

Mer om SPAM i Mellvik-Rapporten

I 1. kvartal 2005 skal vi se nærmere på *Open Source*-produktet Mail-Sweeper, en interessant kombinasjon av ulike *Open Source*-verktøy som til sammen gir oppsiktsvekkende resultater, ikke bare i kampen mot SPAM, men for bedre epost-sikkerhet i sin alminnelighet.