

Kampen mot SPAM: En oppdatering

“SPAM forblir et voksende problem for både sluttbrukere og organisasjoner i 2004.” “SPAM og virus smelter sammen og representerer vår største sikkerhetsmessige utfordring i det nye året.” Ingen tvil om at det er tid for spådommer og projeksjoner for fremtiden, og SPAM får enorm oppmerksomhet. Årsaken er ikke bare problemets omfang, men også at politikere og lovgivere de siste månedene har vært svært så aktive på banen. De ønsker å regulere bort problemet. Hvorvidt dette er en farbar vei, diskuterer vi nedenfor.

Lys i tunnelen?

Mens spådommene – i tråd med tradisjonene – er like sprikende som de er tallrike, har de en felles undertone for SPAMs del: De er negative. Det skal bli verre. Innstillingen er naturlig, om ikke nødvendigvis riktig. Situasjonen ble verre i fjor og likedan året før. Dermed er sannsynligheten stor for å spå riktig når vi antar at det samme gjentar seg også i 2004. God gammeldags saueflokk-mentalitet med andre ord – med enkelte hederlige unntak som grunngir sine spådommer på faglig solid grunnlag.

Det finnes imidlertid også faktorer som peker i riktig retning. Unntaket – når vi først er inne på spådommer – fra regelen kommer fra ekspernten Michael Osterman i amerikanske Network World, som sier: *“Spam will continue to be a problem for many enterprises, but the problem will wane from practical perspective for most enterprises because of the widespread deployment of good spam-blocking tools.”*

Ser man det. Her synes det jo å være grunnlag for optimisme. Samtidig med at det uten tvil vil flyte mer SPAM rundt på Internettet og i tallrike

interne nettverk i 2004, vil synligheten bli mindre fordi verktøyene er blitt bedre. Dessuten er vi, det vil si markedet, blitt flinkere til å sette i drift disse verktøyene.

Ved siden av optimismen har Osterman et annet viktig poeng. SPAM forsvinner ut av syne for brukere flest. Årsaken til at nettopp dette er viktig, er at vi i hovedsak har to valgmuligheter når SPAM skal blokkeres. Vi kan involvere brukerne ved å sette mistenkelig epost i karantene og la den enkelte bruker rydde opp,

Kan vi regulere oss bort fra SPAM?

Hektisk aktivitet blant lovgivere og politikere i USA, Australia, EU og en rekke andre land bringer spørsmålet opp med økende hyppighet: Er det mulig å bruke lover til å stoppe SPAM? At politikerne tror det, forandrer ikke den virkelighet Internettet representerer, som gjør det mulig å flytte seg hvor som helst og når som helst med marginale kostnader. Staten New York fulgte nylig etter California med strenge lover og ditto straffer, og vil gå hardt ut mot det de mener er verstingene. I kulissene står Microsoft som støttespiller, og vil “plukke opp restene dersom det er noe igjen når statsadvokaten er ferdig.”

Det hersker ingen tvil om at disse aktivitetene og tiltakene er positive – fordi de opprettholder og videreutvikler mediebildet på SPAM som problem, og fordi de fortrenger SPAMmerne fra enkelte områder. Samtidig er vi realistiske nok til å erkjenne at effekten neppe vil bli spesielt merkbar, og sjansene for at resultater skal stå i forhold til forventninger, er minimale.

Det er med andre ord publisiteten – og holdningene den skaper – som er viktigst. På lengre sikt kan det være håp om at holdningsendringen påvirker en av de mest grunnleggende kvalifikasjonene for SPAM: At mottakerne faktisk kjøper produktene som tilbys. Dessuten er fokuset på oppdatering av lover og forskrifter nyttig for å redusere SPAMmernes muligheter til å saksøke ISP'er og andre som filtrerer søppelet på vegne av sine kunder.

eller vi kan filtrere meldinger som etter våre kriterier med høy sannsynlighet er SPAM. Anbefalingen er klar: Den siste varianten er den eneste som virker utenfor tekniske miljøer med egen ekspertise innen meldingsformidling. Dersom brukerne skal involveres, går både tiden og de tekniske ressursene til spille i alle fall.

Videre er frykten for 'falske positive', avvisning av legitime meldinger, i de fleste tilfeller overdrevet. Visst er det fare for at artikler fra CNN eller New York Times med uttrykk som 'gay sex' eller 'lesbians' vil bli avvist, men noe stort problem blir det neppe. Legitime avsendere som får meldinger i retur, vil observere hva som har skjedd og gjøre det som skal til for å rette problemet, for eksempel å ringe til mottakeren.

Årsak og virkning

Verktøy gir beskyttelse, men reduserer ikke det underliggende problemet – at SPAM øder store ressurser til ingen nytte, og Internettet flyter over av søppel. Vi deler ikke sikkerhetseksperter Marcus Ranums bekymring for at SPAM og virus skal kvele Internettet fullstendig, men det er all grunn til å arbeide videre også på et mer grunnleggende plan. Ute av syne betyr ute av sinn for brukerne, men for ISPer og nettverkseiere er ressursbruk og -misbruk fortsatt viktig. Å blokkere all nettverkstrafikk fra typiske 'SPAM-verstinger' som Kina, Korea, Latin-Amerika og Russland, er eksempler på tiltak enkeltorganisasjoner kan evaluere og sette i verk (og som benyttes av oss i Team Mellvik as). ISPer er imidlertid avskåret fra denne muligheten og må konsentrere innsatsen om aktiv filtrering og proaktivt samarbeid med SPAM-registrene vi har diskutert i tidligere utgaver.⁵

Vi har ved flere anledninger konstatert at SPAM og virus-problemene fortsetter å vokse, blant annet fordi markedet i sin alminnelighet kun

angriper symptomene, ikke årsakene. I den forbindelse har vi konsentrert oss om beskyttelsestiltak og hvor det er mest effektivt å sette dem inn. Om vi tar et skritt eller to enda lenger bakover, finner vi problemets grunnleggende – og temmelig opplagte – årsaker.

Den ene er kostnader: Det er praktisk talt gratis å sende ut millioner av meldinger, og å flytte seg fra den ene epost-kontoen til den andre

Microsoft: "Porto for epost er løsningen."

Et mer enn ti år gammelt forslag fra Microsoft om å innføre 'avsender-porto' for epost dukket av en eller annen grunn opp igjen rett før jul. Siden en slik mekanisme har fungert for det tradisjonelle post-systemet i et tresifret antall år, mener Microsofts forskere at det må gjøre susen også for epost, og bidra til å eliminere SPAM-problemet.

Det er en erkjent umulighet å innføre betaling for levering av epost inn i Internett-systemet. Ideen fra Microsofts forskere er at sendingen skal ha en belastningsmessig konsekvens for senderen. Via kompliserte algoritmer som beregner hvor mye kapasitet brukeren har å rutte med, skal en sofistikert mekanisme sørge for å belaste maskinen etter en forhåndsbestemt mal – som altså skal representere 'porto'. Maskinen går tregere i X antall sekunder for hver avsendte melding – eller deromkring.

Det skal minimal teknologisk innsikt til for å innse at ideen er ugjennomførbar og totalt verdiløs. Den eneste grunnen til å kommentere saken, er at alt som kommer fra Microsoft har en tendens til å bli tatt alvorlig av innsiktsløse teknologi-journalister. Enn om de stilte opplagte spørsmål – som 'hvem skal påse at hele verden innfører slike mekanismer', 'hvem skal fastsette portoen' eller 'skal vi kaste ufrankert post, uansett hvor den kommer fra'? Svarene gir seg selv, men siden katten er ute av sekken, ville det være kurant å få dem fra Microsoft selv. Det blir fra tid til annen hevdet at Microsofts forskere lever i en beskyttet verden, men kontakten med virkeligheten må forventes å være på et slikt nivå at de vet hva som skal til for å etablere en ny teknologisk verdensorden. Å introdusere mekanismer i henhold til disse forslagene i neste generasjon av Outlook og Exchange, er definitivt ikke tilstrekkelig.

⁵ Se Mellvik-Rapporten nr. 106 og 107.

etterhvert som de blir sperret. Den andre årsaken er at SPAM virker. Når en døgnflue-leverandør av Viagra, pornofilmer eller universitetsgrader sender ut sine millioner av kostnadsfrie epost-meldinger, får de typisk svar fra tilstrekkelig mange av mottakerne til at det hele blir glimrende forretning.

Den tredje årsaken er teknisk: Protokollen som transporterer epost er over 20 år gammel og laget for en verden som så totalt annerledes ut enn i dag. Enkelhet var viktigere enn sikkerhet og fleksibilitet var viktigere enn autentisering. Denne hjelpsomme, positive og etterrettelige verden har forlenget gått over i historien, mens protokollen lever videre. Derfor er det trivielt for hvem som helst å gi seg ut for å være noen andre. Ønsker du å sende epost til statsminister Bondevik fra president Bush, kan du gjøre det – uten å bruke mye tid på oppgaven og med minimale sjanser for å bli oppdaget. Derfor kan SPAMmere benytte hva som helst som avsenderadresser – fiktive eller reelle.

Alle tre årsakene er vanskelige å angripe. Den lave kostnaden er en grunnleggende suksessfaktor for Internettet. At mottakerne faktisk kjøper fra disse leverandørene kan best forklares ved å sitere en politimann fra Dagsrevyen for en tid siden: "Det er fortsatt lov å være dum." Og den gode, gamle SMTP-protokollen fungerer fortsatt aldeles utmerket til oppgaven den opprinnelig skulle løse. Å introdusere tilleggsfunksjonalitet som reduserer SPAM-problemet uten å gå på akkord med kompatibilitet, har så langt ikke vært mulig.

Her aner vi riktignok en lysning på horisonten. En tilleggs mekanisme med betegnelsen SPF (*Sender Permitted From*) er under utvikling og evaluering hos Internettets standardiseringsorgan IETF, og er allerede tatt i bruk i en del miljøer. Resultatene er oppløftende – sågar oppsiktsvekkende, ifølge enkelte eksperter, og kan komme til å gi positive effekter i større skala allerede inneværende år. [Vi skal gjennomgå SPF funksjonelt og praktisk i neste utgave.]

Aktivt forsvar, kurering av symptomer

Å angripe ondet ved roten er dermed en umulighet – i alle fall på kort sikt. Vi er tilbake til beskyttelsesmekanismer – ved siden av at vi kan ønske oss en langt mer aktiv holdning fra ISPer over hele verden. Mange bekker små gjør fortsatt en stor å, og det er en dårlig unnskyldning for en norsk ISP at deres kolleger i Thailand eller Nairobi ikke skjønner problemet. Et sted må vi begynne, og hvorfor skal vi i vesten kalle oss siviliserte hvis vi ikke engang er i stand til å holde grunnleggende orden i eget hus?

Kunnskap er makt. Vi vet årsakene til problemet og vi vet hva som er mulig og umulig. Dermed har vi et godt grunnlag for å vurdere hva som skal til for å forbedre situasjonen – hvilket bringer oss tilbake til diskusjonen om beskyttelsestiltak ovenfor: Vi kan ikke forby epost-brukere "å være dumme", men vi kan redusere eksponeringen overfor SPAM, hvilket er nettopp hva vi gjør – i profesjonell sammenheng. Privatmarkedet er en annen historie, og ingen andre enn ISPerne kan gjøre noe i den forbindelse. Med utgangspunkt i de ressursmessige for-

holdene vi diskuterte ovenfor, forblir det et mysterium at interessen for handling er så beskjeden. Selv giganter som AOL og MSN/Hotmail, som riktignok filtrerer bort millioner av SPAM-meldinger hver eneste time, er for myke i sin innstilling.⁶ De er redde for å miste kunder dersom filtreringen strammes inn, men burde være mer opptatt av å yte god service og eliminere kunder som misbruker tjenestene.

Frihet, fornuft og sensur

Her dukker naturligvis spørsmålet om frihet og sensur opp, og ingen vil hevde at problemstillingene er enkle. På den andre siden er sunn fornuft ikke bare en god målestokk, men også noe brukere flest kan forholde seg til. Åpenhet er alle restriksjoners beste venn, og for ISPene er det først og fremst åpenhet rundt tiltakene, motivasjonen og de positive konsekvensene for kundene som skal til for å komme et skritt videre. At noen vil være misfornøyde kan aldri unngås – “til lags at alle kan ingen gjera”.

Det er et underlig paradoks at de samme brukerne som klager over epost-filtreringen, henviser til menneskerettigheter og påberoper seg yttringsfrihet, uten å kny aksepterer rene husmannskontrakter fra programvareleverandørene og villig vekk betaler for programvare av tvilsom kvalitet. Dette mindretallet roper oftere og høyere enn flertallet, med den følge at det skal mot til fra leverandørsiden for å introdusere de riktige restriksjonene – til å bestemme hva som er akseptabelt og dernest formidle dette videre til kundene. Vi er ikke i tvil om at det samme flertallet vil se positivt på slike tiltak, gitt at de forstår både hva som gjøres og hvorfor. Dessuten er det intet stort teknisk problem å levere ufiltrert epost til brukere som insisterer på å få det.

Et annet forhold som taler for mer restriktiv filtrering, er at dagens epost-brukere kan være fra 5-6 år gamle og oppover. Mens voksne har forutsetninger for å se, vurdere og slette mye av søppelposten, er situasjonen en annen for mindreårige – som tvert imot blir formet av sine observasjoner og erfaringer.

Tid for konsolidering?

Markedet for SPAM-beskyttelsesprodukter har eksplodert i løpet av en 2-års periode, og antall leverandører likeså – til over 120 ved inngangen til 2004. Dette er et større kaos enn noen kan forholde seg til på kundesiden, og selv for leverandørene blir det etterhvert en umulig oppgave å distingvere seg i mylde-ret.

Derfor er det naturlig å forvente en konsolidering i segmentet i de to neste årene, med hovedvekt på inneværende år. De mest ressurssterke aktørene kjøper opp de som har best teknologi, mens de svakeste forsvinner – etter velkjente darwinistiske prinsipper.

På klientsiden vil sluttbrukere i voksende grad oppfatte ‘junk mail control’ mekanismer som forstyrrelser, i takt med at sentrale filtreringstiltak blir bedre – et forhold vi var inne på i forbindelse med omtalen av Outlook 2003 i nr. 111 (side 33).

Full krig

Vi snakket innledningsvis om å løfte blikket og ta et steg tilbake for å se de grunnleggende årsakene til SPAM. Samme metode er nødvendig for å få et forhold til den krigen som raser. Vi beskytter oss, arbeider med nye tiltak, vi filtrerer og lager lover. Men hva gjør den andre siden?

Noen av våpnene og taktikkene er innlysende: De finner kontinuerlig nye veier rundt

⁶ Det amerikanske selskapet Brightmail Inc., som er blant de største i verden på anti-SPAM løsninger, hevder å filtrere over 3 milliarder meldinger per døgn. En lang rekke kilder på Internettet monitorerer kontinuerlig mengden og utviklingen av SPAM. Et godt sted å starte for spesielt interesserte er hos ‘AntiSPAM-foreningen’ SPAMcon Foundation [www.spamcon.org].

våre filtre og beskyttelsestiltak. Langt mindre innlysende er det at også motparten arbeider med juridisk skyts. Ved en rekke anledninger har for eksempel ISPer og leverandører av epost-tjenester blitt saksøkt av SPAMmere for ulovlig sensur. Enkelte ganger har sågar søksmålene vunnet frem. Eksemplene er i hovedsak å finne i USA, der prinsippene om ytringsfrihet har en spesielt fremtredende plass i lovverket, og dessuten mer eller mindre kontinuerlig blir benyttet i rettsapparatet i ulike – i mange tilfeller pussige – sammenhenger. Dette understreker viktigheten av for det første å sørge for juridisk ryggdekning for tiltakene som settes i verk, og for det andre å arbeide for avklaringer fra myndigheter og lovgivere. Aktivitetene på politisk plan i mange land (se ramme på side 10) har størst effekt på nettopp dette forholdet: Å redusere mulighetene for juridiske motangrep fra SPAMmer-siden.

Forsvarsstrategi

Hvordan legger vi så opp forsvaret eller beskyttelsen mot SPAM? Vi gjennomgikk i nr. 106 og 107 en rekke praktiske vinklinger og råd i den forbindelse, som er like gyldige i dag. Den raske utviklingen på området betyr imidlertid at stadig nye alternativer kommer på banen, et forhold som ikke minst illustreres av leverandørtilveksten. At de 180+ leverandørene vi kjenner til i dag, trolig blir færre i løpet av de neste to årene, forandrer ikke det faktum at vi har fått flere muligheter – et større spekter å velge fra.

Fortsatt er segmentet fullstendig dominert av amerikanere, både på produksiden og på tjenestesiden. I og med at landegrenser har begrenset praktisk betydning i forbindelse med Internett-baserte tjenester generelt og epost-tjenester spesielt, vil dette vedvare i overskuelig fremtid. Derfor er det ingen umulighet at norske organisasjoner velger amerikanske tjenesteleverandører for kontroll og mottak av epost.

Outsourcing

For mange organisasjoner er nettopp *outsourcing* av eposten et optimalt alternativ. Jo bedre utbygget disse tjenestene blir, desto mer attraktive blir de. Mens epost utvilsomt kan karakteriseres som et virksomhetskritisk verktøy for organisasjoner flest, hører det til unntakene at teknisk epost-kompetanse er det vi kan kalle kjerneområde for en virksomhet. Bruken vokser, avhengigheten likeså og kompleksiteten blir større i takt med blant annet truslene – hvorav SPAM og virus er de viktigste. Videre har sending, mottak og arkivering av epost juridiske sider som må være under kontroll. Argumentene er mange og vektige for å overlate eposten til profesjonelle spesialister.

Programvare

Det er her vi finner den store mengden av aktører i anti-SPAM og anti-virus segmentene – av naturlige årsaker: Selvstendige filterprodukter, *plugin*-moduler for populære epost-tjenere, Open Source produkter og så videre. Evaluering og valg er tilsvarende vanskelig, men forenkles vesentlig av enkelte grunnleggende kvalifikasjoner basert på erfaring og sunn fornuft. *Plugin*-moduler til kompliserte epost-tjenere som

Notes (Lotus/IBM) og Exchange (Microsoft) er en dårlig idé. Om de er aldri så bra i seg selv, bidrar de til å komplisere allerede altfor komplekse og ineffektive produkter, med ustabilitet og økte driftsomkostninger som resultat.

Selvstendige produkter som gjerne kjører på dedikert hardware i en proxy-konfigurasjon, er optimalt – kostnadmessig, driftsmessig og effektivitetsmessig. Så sant kompetansen finnes, er det vel verdt å vurdere Open Source produkter som Sendmail, Qmail, Postfix, Procmail, Spamassassin – sistnevnte typisk i kombinasjon med en av de andre.

‘Sorte bokser’

‘Appliances’, ‘sorte bokser’ eller ‘nett-apparater’ – kjært barn har mange navn, og disse oppgavespesifikke boksene har forlenget funnet sin plass i markedet. De kan være smale eller brede i sitt nedslagsfelt, og for små og mellomstore miljøer som ikke ser *outsourcing* av epost som en mulighet, representerer slike produkter et attraktivt alternativ. Enkle, effektive og med pålitelige, automatiske oppdateringsfunksjoner.

Den britiske leverandøren Equinet, som vi har nevnt ved tidligere anledninger i Mellvik-Rapporten, har vært ett av svært få europeiske innslag i segmentet siden slutten av 90-tallet, og har naturlig nok en spesielt sterk posisjon i det britiske markedet. Andre eksempler som spesialiserer seg på epost er (amerikanske) Borderware, Corvio og Sendio.

Klientprogramvare

Siste gruppen i denne sammenhengen er klientprogramvare – typisk med utgangspunkt i viruskontroll-programmer som stadig får utvidet funksjonalitet, med kjente leverandørnavn som Symantec, McAfee/Network Associates, Trend Micro og så videre. Mens disse programmene kan være effektive nok, vil en slik angrepvinkel aldri kunne skalere, og vi anser derfor ikke gruppen for å være interessant i profesjonell sammenheng.

Progresjon

Mens vi vanskelig kan konkludere med at SPAM-situasjonen er under kontroll, setter beskyttelsestiltakene omsider merkbare spor etter seg. Dersom SPF-tillegget til Internettets epost-protokoll (som vi altså kommer tilbake til i neste utgave) blir en suksess, er det grunn til å tro at SPAM-bølgen vil være nedadgående om 3-4 år. I mellomtiden forblir SPAM- og virus-kontroll/beskyttelse viktige elementer på vår agenda.

[Flere produktpekere i tilknytning til denne artikkelen finnes på utgavens web-side, se side 35 for informasjon.] ■