

IT-revyen

Aktuelle nyheter og temaer i IT-markedet og bransjen forøvrig: Produkter, trender, erfaringer og observasjoner – med tilhørende kommentarer, anbefalinger og gode råd.

Er du en blogger, du også?

“Blogger? Jeg? Umulig – jeg vet jo ikke engang hva det er!” Til å ha vært en såkalt farsott på Internettet de siste to årene, har blogging – også kjent som **Weblogging** samt under et dusin andre navn – hatt en lav profil i IT-miljøer flest. Våre forsiktige og beskjedne forespørsler kvalifiserer riktignok ikke som empirisk grunnlag, men bekrefter i alle fall den oppfatningen vi startet med: Vi får sjelden noe annet enn hoderystelser og løftede øyenbryn tilbake.

Dermed fremstår det som enda mer underlig at blogging i antatt oppegående kretser blir hevdet å være en av Internettets største revolusjoner. “En frigjøring for millioner av IT-brukere over hele verden. Publisering for hvem som helst. Diskusjoner. Muligheter.”

Og her ligger naturligvis hunden begravet. Det viser seg at vi er en blogger likevel. Uten å vite det har vi deltatt i revolusjonen. Vi har lest nyhetsartikler på nett – for eksempel i PC Magazine, med etterfølgende kommentarer fra leserne, og vi har sågar bidratt med våre egne innspill. Dermed er vi en blogger.

“WHAT’S THE BIG DEAL?” Vi sitter igjen med en følelse av at det hele er en stor misforståelse. Vel er det utvilsomt riktig at en hvilken som helst hjemmebruker kan etablere sine egne Web-sider – hos seg selv eller hos en ISP, og med lett tilgjengelig programvare starte en Web-log, som i teknisk forstand er en mekanisme for å lese og levere kommentarer til et eller annet. Dette et eller annet er grunnlaget for ‘frigjøringen av massene’. Hvem som

helst kan publisere hva som helst når som helst, med ubegrenset tilgjengelighet, og med håp om at mange leser og kommenterer det som blir publisert. I enkelte tilfeller har slike blogger blitt temmelig store, med tusenvis av registrerte brukere og svært så livlige diskusjoner. Dette gjelder spesielt i tilfeller der kjente navn har vært involvert, forfattere, forskere, kjendiser og så videre. For menigmanns blogg, som det ifølge statistikkene finnes hundretusener av, er situasjonen en annen. Interessen er beskjeden utover nærmeste omgangskrets, og de har en tendens til å dø ut i løpet av noen måneder – i høyden et år. Det er innlysende at dersom folk flest publiserer sine egne blogger, blir det få som har nok tid til å lese og kommentere andres publikasjoner. Dessuten har de fleste store media-aktører forlenget kastet seg på bølgen, og trekker automatisk til seg betydelige leser-skarer – med åpenbare konsekvenser. Denne utviklingen er naturlig, men om den er positiv kan naturligvis diskuteres.

Disse forandringene – eller utviklingen, om vi vil – gjør ikke konseptet mindre nyttig. Noen revolusjon er det imidlertid knapt snakk om. Vi kjenner igjen både mekanismer og bruk fra tidlig på 80-tallet da Usenet – eller NETNEWS, som det også ble kalt – trådte sine barnesko. Usenet spredte seg som en farsott – først over USA, så Europa og etterhvert store deler av resten av verden, selv før Internettet ble generelt tilgjengelig. En rekke av funksjonene i NETNEWS var modell for Notes og andre såkalte gruppevare-verktøy, som dukket opp tidlig på 90-tallet.

The Joy of Tech... by Nitrozac & Snaggy



It wasn't too long afterwards, that Samantha started blogging someone else.

Usenet lever fortsatt i beste velgående, og er større enn noen sinne, men langt mindre bemerkelsesverdig i dagens vrimmel av Internett-baserte funksjoner og tjenester. Brukergrensesnittene har utviklet seg enormt i løpet av disse 20+ årene, og karakteristisk for tjenester basert på åpne standarder, finnes det mer enn 20 forskjellige brukerverktøy å velge mellom. En rekke av dem er nettleser-baserte, og til forveksling like det som kalles blogger og tilhørende brukergrensesnitt. Hvor grensen går mellom det ene og det andre, er ikke lett å si – sett fra brukersiden, og er egentlig ikke så viktig. Blogger er en videreføring og videreutvikling av Usenet som utnytter infrastruktur og tekniske muligheter anno 2000+. I løpet av de neste to årene vil de fleste interne portaler ha blog-funksjonalitet hvor medarbeidere diskuterer prosjekter, utfordringer – eller kanskje politikk, dersom virksomhetens ledelse finner det ønskelig å slippe diskusjonene helt løs. Mulighetene er ubegrensede ...

En trådløs tidsalder

“Vi går snart tomme for spektrum.” Tomme for hva? Spektrum! Hva er det? For de fleste av oss er ordene kjente, mens innholdet er verre å forklare. Ingen grunn til bekymring, dog. Spektrum er – sterkt forenklet – ‘kapasitet i eteren’, og for de fleste av oss er det like (u)interessant som lufttrykk-variasjoner i atmosfæren. Det berører oss, men nytteverdien av å forstå det som skjer og hvorfor, er beskjeden.

Noe er imidlertid alvorlig her: Vi har gjort oss avhengige av båndbredde i eteren, til våre mobiltelefoner, FM-radioer, trådløse nettverk, trådløse tastaturer og så videre. Kan det være tilfelle at ressursene er i ferd med å bli oppbrukt eller overforbrukt, og betyr det at utstyret kan slutte å fungere når som helst?

‘Tja’ er det beste svaret vi kan gi. Trusselen er i beste fall overdrevet, og minner til forveksling om IP-adresser i Internettet, som i ti år har vært en ‘truet’ ressurs, men som fortsatt har forbausende kapasitet tilgjengelig.

Advarslene fungerer mer som et varsko – til å øke bevisstheten omkring bruken av en endelig ressurs. En måling foretatt i sentrum av Washington DC nylig, et område med høyest tenkelig tetthet av trafikk i de fleste frekvensområder, avslørte at mellom 19 og 40% av spekteret (eteren) var belagt på noe tidspunkt i løpet av det vi kaller vanlig arbeidstid – vesentlig mindre enn forventet. Utenfor dagtid var belegget ubetydelig.

Årsaken til at observasjonene er viktige, er at vi omgir oss med stadig mer trådløshet. Vår avhengighet av trådløs kommunikasjon på ulike nivåer, øker raskt – alarmsystemer, nødsamband, politi-kommunikasjon, trafikkstyring, posisjoneringssystemer og så videre. Konsekvensene av deres bortfall eller redusert stabilitet er voldsomme og uakseptable.

Fordelingen av frekvensspekteret i eteren ble gjort for over 75 år siden, på et tidspunkt da eksperter og myndigheter oppdaget at vi sto overfor en endelig ressurs, og at det var nødvendig å regulere bruken av den. Grov-allokeringene har stort sett vært uforandret siden den tid, med justeringer og detaljreguleringer innen deler av frekvens-spekteret. Myndighetene har gjort seg til eiere av denne fellesressursen, og har i nyere tid auksjonert bort deler av spekteret til kommersielle aktører – til usannsynlige priser.

Andre deler av spekteret – vel å merke smale segmenter – er reservert for såkalt ulisensiert eller ‘fri’ bruk, hvilket vil si at hvem som helst kan bruke disse fre-

kvensene som de ønsker, så lenge de holder seg innenfor strenge grenser med hensyn til signalstyrke. Nettopp her finner vi mange av de populære nye anvendelsene av trådløs teknologi, et forhold vi har diskutert tidligere i tilknytning til trådløse nettverk. Disse områdene har fungert som rene magneter på nye, kommersielle anvendelser de siste årene, med en kolossal innovasjonsbølge som konsekvens. Ved hjelp av blant annet moderne digital signalprosesserings-teknologi har den ene barrieren etter den andre blitt forsert, med den følge at den effektive båndbredden og rekkevidden vi i dag kan trekke ut av et smalt spektrum med lav signalstyrke, har økt med flere størrelsesordener. Denne utviklingen begynte allerede ved overgangen fra analog til digital mobiltelefoni, og ventes ikke å stoppe med det første.

I sin tur betyr det at de båndbreddereservene som finnes i eteren i realiteten er mange størrelsesordener større enn tidligere antatt – nok en gang en nærliggende analogi til IP-adressene, som ved hjelp av CIDR og NAT har fått en tilsvarende økning. Innovasjonen i de relativt smale ulisensierte frekvensbåndene har fått myndighetene på gli med hensyn til å frigi deler av spekteret som tidligere har vært reservert, men aldri eller beskjedent benyttet. Dermed reagerer naturligvis mobiltelefoni-selskapene, som har betalt milliarder av kroner for rettigheter hvis verdi er i fritt fall.

Hvor dette ender vet ingen, men at innovasjon og utnyttelse av de frie ressursene vil fortsette, hersker det ingen uenighet om. Likeledes hersker det ingen tvil om at reservene i eteren vil fortsette å vokse, og at vår avhengighet av disse ressursene følger etter. En rekke nye ideer og teknologier med spennende potensiale har dukket opp de siste årene – fra forskningsinstitusjoner, akademiske institusjoner, militære prosjekter og kommersielle aktører. Nye antenner kombinert med smart programvare kan styre retningen på signalene på måter som ikke bare mangedobler rekkevidden, men som samtidig reduserer forstyrrelsene vesentlig. 'Rutenettverk' eller MESH NETWORKS utnytter nærliggende utstyr til å formidle signaler slik at enhver klient (for eksempel en LAPTOP eller en mobiltelefon) blir både basestasjon og klient. Alle hjelper alle og øker på den måten både rekkevidde og båndbredde – på bekostning av energiforbruk.

Smart programvare er nøkkelen til de fleste tilvekstene i dette spenstige feltet – ikke minst den siste vi skal sveipe innom i denne omgang. AGILE RADIOS, som vi i mangel av noe bedre kan kalle 'hoppende radioer', foretar kontinuerlige målninger av hva som er ledig i eteren rundt dem, og utnytter de beste frekvensbåndene. Siden de ledige områdene sjelden er sammenhengende, blir dette en kontinuerlig hopping mellom ulike frekvensbånd. Teknologien har militær opprinnelse, og selv om den er langt unna kommersiell utnyttelse, demonstrerer den at vår satsing på trådløshet i dag er en trygg investering i fremtiden. YOU AIN'T SEEN NOTHING YET.

CIDR – *Classless InterDomain Routing*

NAT – *Network Address Translation*

Microsoft sjanhaier standard for SPAM-bekjempelse

Når Microsoft foretar seg noe i IT-markedet, har det alltid konsekvenser. Noen ganger i praksis, og alltid med hensyn til oppmerksomhet. Media er interessert, markedet er interessert – med god grunn. Denne gangen handler det om SPAM. Formann Gates benyttet sin opptreden på RSA Securitys verdenskonferanse i slutten av februar til å annonsere selskapets nye teknologi for SPAM-bekjempelse. Under (det foreløpige) navnet Caller ID – amerikansk for nummervisning, og hentet fra telefoni-sektoren – har selskapet utviklet et forslag til en standard

for avsender-identifikasjon av epost-meldinger. Forslaget skal overleveres til Internettets standardiseringsorgan IETF, og Gates mener at dette er et stort og viktig steg i kampen mot SPAM.

Vi ønsker Microsoft velkommen på banen. Det er utelukkende positivt at selskapet omsider viser interesse for problemstillingen og signaliserer at de oppfatter problemet som alvorlig. Likeledes hersker det stor enighet blant eksperter i markedet om at avsender-identifikasjon er den mest nærliggende og dermed lovende veien å gå for å få SPAM-utfordringen under kontroll. Som vi diskuterte under overskriften “SPF: Nytt håp i SPAM-krigen” i Mellvik-Rapporten nr. 114 (side 34), har det i løpet av de siste årene dukket opp flere alternative forslag til hvordan slik avsender-autentisering kan gjøres, hvorav SPF (‘SENDER PERMITTED FROM’ eller ‘SENDER POLICY FRAMEWORK’) hittil er den mest lovende.

Det underlige med Microsofts forslag, som selskapet hevder å ha arbeidet med og testet internt det siste året, er at det ikke bringer noe nytt til bords. Caller ID teknologien setter sammen ideer og metoder som er kjente fra eksisterende alternativer. Videre har forslaget vesentlige svakheter i forhold til nettopp SPF. Dermed blir innspillet negativt i stedet for positivt. Det skaper forvirring der Microsoft hadde sjansen til å bidra til avklaring og fremgang, og vi har vanskelig for å se hva selskapets hensikt med initiativet kan være. Dersom målsettingen virkelig er å få etablert en åpen standard, slik selskapet selv hevder, ville det være naturlig å støtte et av forslagene som allerede foreligger – eller servere noe som er nytt og bedre.

Nasjonal strategi for informasjonssikkerhet

Handelsdepartementets “Nasjonal strategi for informasjonssikkerhet” (NSI) vakte berettiget og positiv oppmerksomhet da den ble presentert i fjor sommer. Endelig fikk vi noe å holde oss til fra myndighetene på IT-sikkerhets fronten. Siden er det blitt foruroligende stille – og vi har på oppfordring tatt for oss ‘strategien’ for å finne årsaken. Er det stille før stormen eller var dokumentet nok en papirøvelse?

Det er med betydelig skepsis vi gir oss i kast med en slik oppgave. Siden 1980 har vi vært igjennom et tosifret antall ulike IT-relaterte utredninger, planer og strategier fra regjeringshold, og vi har fortsatt til gode å bli imponert. Vi har til dags dato ikke sett et dokument som etter vår oppfatning har vært verdt summen av papiret det er skrevet på og innsatsen som ligger bak. Med fare for å overgeneralisere, er det vår oppfatning at slike dokumenter er notorisk løse i kantene, inneholder mange flotte mål og fine fraser, men lite konkret om hva som skal gjøres av hvem og når. Likeledes har vi til gode å finne et faglig nivå som står i forhold til målsettinger – og ikke minst i forhold til hva som er rimelig å forvente fra nasjonens høyeste hold.

NSI hever seg over denne faglige middelmådigheten. Gjennomgangen av problemstillinger, utfordringer og ansvarsforhold knyttet til IT-sikkerhet er relevant og utførlig, og samtidig kort og konsis. Videre annonserer dokumentet opprettelsen av flere viktige offentlige organer med ansvar for IT-sikkerhet, for eksempel Nasjonal sikkerhetsmyndighet (NSM) og Senter for informasjonssikkerhet (SIS). Utover dette er dokumentet etter vår oppfatning gjennomsnittlig. Det er fullt av fornuftige anbefalinger om hva som bør gjøres, men har få konkrete tiltak. I tilfeller der ‘bør’ er byttet ut med ‘skal’, mangler som regel hvem som har ansvaret, når tiltaket skal være gjennomført – eller begge deler.

Kort sagt sitter vi (nok en gang) igjen med følelsen av mye skrik og lite ull, mange gode intensjoner og lite substans. Her har myndighetene en enestående sjanse til å sette scenen, etablere kritiske fellestjenester, stille krav til markedet, sette normer og gå foran med et godt eksempel. I stedet blir det med det vi gjerne kaller 'godt preik'. Etablering av en nasjonal PKI-løsning for digitale signaturer er et godt eksempel. Tekniske løsninger og standarder finnes, og det er unødvendig for myndighetene å evaluere eller ta stilling til produkter. Det som trengs er en pålitelig tjeneste for utstedelse og administrasjon av digitale sertifikater – for enkeltindivider og virksomheter. Flere kommersielle aktører har forsøkt seg, uten suksess – først og fremst fordi dette er en samfunnsoppgave på linje med utstedelse av pass. NSI vier problemstillingen betydelig oppmerksomhet, men hvor blir det av handlingsplanen?

Likeledes ville det vært naturlig at våre myndigheter bestemte seg for hvilke krav det offentlige skal stille til sin egen og sine samarbeidspartneres sikkerhet, og som dermed blir en implisitt del av vare- og tjenesteleveranser fra næringslivet. En slik konkretisering og gjennomføring ville ikke bare styrke sikkerheten i det offentlige, men også ha store smitteeffekter i resten av samfunnet fordi leverandørsiden får konkrete krav og standarder å forholde seg til. Dette er et stort lerret å bleke, men det vil aldri bli bleket så lenge holdningen er at "spørsmålet om iverksettelse og dimensjonering vil måtte avvies mot kostnader gjennomføringen vil medføre." En slik 'se hvordan det går' innstilling kan aldri gi god sikkerhet og skaper feil holdninger i utgangspunktet. Enten mener myndighetene at sikkerhet er viktig og nødvendig, eller så er det ikke viktig. Vi kjenner til et dusin kommuner som har tatt IT-sikkerhet på alvor allerede, men vet at de fleste vil skyve slike utgifter nederst på prioriteringslisten inntil påbud foreligger fra øverste hold.

I forbindelse med gjennomgangen av regelverk for IT-sikkerhet presenteres noen enkle og fornuftige tiltak for å skaffe til veie grunnlagsinformasjon. Vi savner imidlertid en påpeking av at slike regelverk må holdes levende og kontrolleres/tilpasses til virkeligheten én til to ganger i året. Videre diskuteres felles sikkerhetsnormer for nasjonalt helsenett, med fokus på utarbeidelse av en sikkerhetspolicy "som innbefatter døgnskuttet overvåking av nettet, herunder tiltak for kriser og hurtig feilretting". Her etterlyser vi en referanse til det faktum at verken helsenett eller andre nettverk kan gis tilfredsstillende sikkerhet om de ikke i utgangspunktet har en arkitektur som tilgodeser sikring. Tiden er ute for sikkerhet i etterkant.

"Nasjonal strategi for informasjonssikkerhet" er lesverdig og informativ, men etter vår oppfatning lite verd som en strategi for nasjonal sikkerhet. Vi etterlyser noe som er mer handlingsorientert og som viser vilje til å stille krav, gjennomføre tiltak og bidra til å bringe Norge til et IT-sikkerhetsmessig nivå vi kan være tjent med og bekjent av. ■