

## Godbiter

Kort og godt om IT-produkter og -teknologier vi finner spesielt interessante – smått og stort, gratis eller kommersielt. Nykommere på markedet og produkter vi har testet eller evaluert blir prioritert i den forbindelse, ved siden av produkter relatert til artikler i denne eller tidligere utgaver.

### Defragmentering og drift

«Defragmentering? Nei, det hører historien til. Vi bruker ikke Windows 9x og FAT-filsystemer lenger.» Ikke det? De fleste installasjoner av Windows 2000 Professional og NT 4.0 Workstation gjør faktisk det, uten at det ligger noen bevisst evaluering bak valget. Dessuten, og vel så viktig: Overgangen til et langt mer moderne og effektivt filsystem (NTFS) eliminerer ikke behovet for regelmessig defragmentering. For å fungere optimalt er regelmessig defragmentering en nødvendighet – på klienter såvel som på tjenerne. Sistnevnte gruppe er sjelden noe problem – vi har dem under tett kontroll og kan sørge for at filsystemer vedlikeholdes etter behov og jevnlig, uten tilsyn.

Langt verre er det med klientene, stasjonære som mobile: De er under brukernes kontroll, og vi har forlenget konstatert at å overlate driftsoppgaver til brukerne er det samme som å glemme dem. Det ligger ingen kritikk av brukerne i denne observasjonen. Svakheten er utelukkende å finne på systemsiden, der defragmentering er ett av en rekke forhold som fortsatt ikke er ivaretatt – selv etter å ha vært påpekt jevnlig overfor Microsoft i snart 15 år.

Problemstillingen er langt fra unik, snarere en regel – og en mulighet for entreprenører som ser utfordringene og vet bedre måter å løse dem på. Microsofts egne defragmenterings-verktøy er ineffektive, overlater alt ansvar til brukerne, og er til liten praktisk nytte. Selv avanserte verktøy fra andre leverandører har som regel den vesentlige ulempen at de må styres lokalt på maskinen det gjelder, dvs. av brukeren.

Derfor har problemet i det store og hele forblitt uløst: Systemene går saktere og saktere, stabiliteten reduseres, brukerne blir mer og mer misfornøyde, og kommer til slutt til driftsstøtte eller HELPDESK med maskinen for å få hjelp, eller en driftsperson logger seg på individuelle maskiner for å manuelt sette i gang en defragmentering.

Dette skalerer åpenbart ikke, men hjelpen er underveis: Verktøyleverandørene har omsider forstått problemet, og produkter som både kan fjernstyres, fjerninstalleres og kjøres automatisk dukker opp. Et godt eksempel er Defrag Commander, medlem av en familie interessante driftsverktøy fra Winternals Software i Texas, USA [[www.winternals.com](http://www.winternals.com)]. For noen hundrelapper per klient kan defragmenteringen fjernstyres, automatiseres og kontrolleres sentralt – en investering som er innspar i løpet av noen fattige uker ifølge våre kilder.

Vi har testet produktet i liten skala, og ser lett årsakene til entusiasme: Riktig angrepsvinkel og fornuftig prising – en effektiv løsning på et problem vi aldri skulle ha hatt i det hele tatt, og som må automatiseres bort snarest. Defrag Commander installeres på en hvilken som helst maskin i nettverket, fortrinnsvis en tjener som alltid er tilgjengelig. Deretter registreres klientene sammen med

tidspunkt og hyppighet for defragmenteringen. Et brukernavn og passord som gir de nødvendige privilegier på hver enkelt klient, må også oppgis. Resten går av seg selv. Ingen programvare-installasjon, intet vedlikehold på klientene. Rapporter etter hver kjøring forteller om resultatene. Dermed kan vi både verifisere at jobben er gjort og eventuelt justere hyppigheten i henhold til tallenes tale. Slik kan det gjøres. Enkelt, effektivt, skalerbart.

### Fjernstyrt viruskontroll

Apropos fjernstyring og forenkling: Viruskontroll er en annen side av samme sak – nødvendig, administrativt krevende fordi den må oppdateres kontinuerlig – og tilsvarende upålitelig fordi brukerne selv må involveres. En løsning er imidlertid i sikte også her: Fjerninstallert og fjernkontrollert viruskontroll er tilgjengelig, blant annet fra Network Associates [myCIO.com Virus Scan ASAP – www.mycio.com]. Produktet er fortsatt umodent – med få valgmuligheter og begrenset fleksibilitet, men er representativt for en viktig og attraktiv trend som fjerner brukerne fra sikkerhets-ligningen.

SOHO – Small Office, Home Office

Spesielt interessant er kombinasjonen Virus Scan ASAP og SOHO-brannmuren SonicWall: Brannmuren vil ikke åpne Internett-aksess uten at virusprogrammet er installert og i funksjon. At det også her finnes svakheter som kan gjøre det nødvendig å sette de rigide kontrollfunksjonene ut av spill, er naturligvis negativt, men igjen er det trendsignalene som er spesielt interessante: Bedre sikkerhet som er mindre synlig – og som fjernstyres.

### Stødige fremskritt for WINE

WINE (WINDows Emulator) har vaket på horisonten lenger enn vi kan huske, og har gitt Unix- og Linux-brukere tilgang til et voksende antall Windows applikasjoner siden midt på 90-tallet [se Mellvik-Rapporten nr. 59]. Utbredelsen har riktignok vært begrenset – først og fremst på grunn av krevende idriftsettelsesprosedyrer. Denne utfordringen er fortsatt betydelig, men WINE har gjort tilstrekkelige fremskritt de siste årene til å bli en naturlig del av ledende Linux-distribusjoner, fra blant andre RedHat.

Vi er kommet til et punkt der systemet kan installeres og settes i drift i løpet av noen få timer, uten bruk av kode, filer, fonter eller annet fra Microsoft, og dermed uten lisensmessige restriksjoner eller begrensninger. Etter idriftsettingen kan vi installere og bruke tusenvis av Windows-applikasjoner fra Solitaire til Office, med få begrensninger i forhold til deres naturlige miljø. Selv ytelsesmessig kommer dagens utgave av WINE akseptabelt ut, også for kompliserte og tunge applikasjoner som Adobe FrameMaker (som Mellvik-Rapporten skrives i). Fonter, drivere og printere representerer fortsatt betydelige utfordringer, men å bringe omgivelsene til et rimelig standard Windows-nivå er svært så overkommelig.

Det betyr ikke at Windows plutselig er truet av WINE/Linux, men at brukere og brukermiljøer som har kjørt 'dobbel' eller brukt flere systemer om hverandre, har fått en mulighet til å konsolidere. Den andre interessante observasjonen er at WINE emulerer Windows uten bruk av Microsoft-kode og uten tilgang til spesifikasjoner fra Microsoft. At utviklingsprosessen dermed tar lang tid, mye inn-

sats og alltid henger betydelig etter Microsofts nye systemer, er innlysende. Samtidig ser vi hovedårsaken til Microsofts totale vegring fra å publisere kildekode – for Windows og applikasjoner: Når en gruppe frivillige, som WINE-utviklerne er, kan komme så langt uten hjelpemidler, skal det liten fantasi til for å se at tilgang til mer informasjon om innsiden av systemene, ville skape en helt ny situasjon i markedet. Tilsvarende kan sies om andre Open Source produkter, for eksempel SAMBA, se Mellvik-Rapporten nr. 20 og 60. Faren for en Windows-utgave som er bedre enn originalen ville vært overhengende – ugunstig for Microsoft og en drømmesituasjon for markedet.

Noen reell åpning av kildekode eller spesifikasjoner fra Microsoft forblir med andre ord godt snakk i overskuelig fremtid. I mellomtiden fortsetter WINE, SAMBA og andre prosjekter å gi tallrike miljøer et alternativ, samtidig med at de fungerer som en korreks til Microsoft og andre kommersielle programvareleverandører i markedet: Når 'amatører' kan komme så langt på egen hånd, hva må være rimelige krav til de 'proffe' og ressurssterke?

### Sikker epost: HushMail

Under overskriften "Hvor ble det av sikker epost" i Mellvik-Rapporten nr. 90, nevnte vi avslutningsvis 4 eksempler på sikre epost-produkter – med ulik løsning og vinkling, men med samme målsetting. HushMail er nummer 2 i denne rekken (se presentasjonen av ZixMail i nr. 91).

Sikker epost er teknisk enkelt og praktisk vanskelig – i hovedsak fordi standardene er mangelfulle og mekanismene for utstedelse av 'digitale identifikasjons-papirer' fraværende. Derfor utpeker Web-baserte løsninger seg som det minste felles multiplum, en aksessmekanisme som de fleste kan bruke, og som på en effektiv måte kan dekke over de ufullstendigheter og inkompatibiliteter virkeligheten byr på.

Samtidig ligger det i kortene at løsningene ikke kan bli perfekte: Sikker alle-til-alle meldingsutveksling ligger et godt stykke inn i fremtiden, mens å utveksle transportsikret og signert epost mellom parter som har erkjent behovet, og tatt skritt for å legge forholdene til rette, er forholdsvis trivielt.

I dette bildet er HushMail et av de enkleste alternativene. Selskapet tar mål av seg til å bli sikker eposts svar på hotmail.com, og leverer en gratis epost-tjeneste til hvem som helst, og en betalt tjeneste til brukere som vil ha mer plass, større spennvidde og flere tjenester. I motsetning til ZixMail, er HushMail basert på åpne standarder – med OpenPGP som fundament. Videre er HushMail i sin helhet sentrert rundt selskapets egne tjenere. Meldinger fra tilfeldige sendere til vår HushMail konto, eller fra vår HushMail-konto til tilfeldige mottakere, kan ikke sikres. I sistnevnte tilfelle kan den signeres, hvilket har betydelig verdi dersom vi velger å stole på identiteten som er registrert hos HushMail. I og med at selskapet – som tilfellet er for andre gratis Internett-tjenester, ikke krever noen form for legitimasjon fra brukeren, kan hvem som helst registrere seg som Jan Petersen eller Kjell Magne Bondevik. For betalende brukere må det riktignok registreres både navn, adresse og kredittkortinformasjon, men legitimasjonsverdien er fortsatt tynn.

Problemstillingen er ikke unik for HushMail, men blir ikke mindre viktig av den grunn, og understreker forutsetning nummer én for generell utveksling av sikker epost i dag: Vi må vite at mottaker/avsenders adresse er korrekt og pålitelig.<sup>12</sup> For forretningskontakter og andre kontakter vi omgås daglig eller ofte, er dette forholdsvis uproblematisk, hvilket gjør at tjenester som HushMail er nyttige og gir betydelig sikkerhet.

Vi ser på HushMail primært som et godt eksempel på hva som kan oppnås med relativt enkle midler. Tjenesten er for begrenset og for lite raffinert til å ha betydelig nytteverdi i en større sammenheng, men ivaretar lett konkrete behov i liten skala. ■

<sup>12</sup> Vi diskuterer denne problemstillingen i detalj i neste utgave, i artikkelen om digitale signaturer og PKI, se baksiden for detaljer.

## Velkommen til Mellvik-Web!

*Referanser, kommentarer og pekere til utfyllende materiale i forbindelse med artikler i Mellvik-Rapporten, er Web-tjenestens hovedoppgave. Den tekst-baserte søkemotoren gjør det lett å finne frem til artikler og referanser basert på uttrykk eller termer. Videre gir Web-tjenesten anledning til å sende kommentarer, forslag og andre tilbakemeldinger, samt å bestille spesialrapporter eller nye abonnementer. Sist, men ikke minst oppdateres innholdsoversikten regelmessig med titler og temaer for artikler i fremtidige utgaver!*

Referansesiden for herværende utgave finner du på Mellvik-Rapportens forside: <[www.mellvik.no/MR/MR](http://www.mellvik.no/MR/MR)> (legg merke til at store og små bokstaver er signifikante) – eller direkte på forsiden under 'MR Referanser'.

**Følg med, og la oss få høre dine meninger!**