

IT-revyen

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

Gamle problemer blir som nye ...

Vi undres – mens vi leser den ene historien etter den andre om PC-problemer av ulike slag, fra dokumenter som forsvinner til trådløse forviklinger, recovery-CDer som sletter alt, men ikke bringer utstyret tilbake til liv, om nettverks-forbindelser som kommer og går – kort og godt frustrasjoner. Ingen overraskelser, de fleste kjenner seg igjen i flere av scenariene. Årsaken til at vi undres er flommen av slike erfaringer som er å finne i alt fra dagsaviser til TV-programmer – for ikke å snakke om i sosiale sammenhenger.

Vi tviler ikke på at Windows-frustrasjonene er reelle, men de har neppe blitt så mye større det siste året som oppmerksomheten kan tyde på. Forutsetningsvis skal de tvert imot ha blitt mindre, i takt med at Microsoft forbedrer produktet. Oppsvinget i oppmerksomhet er med andre ord påtagelig. Det kan virke som om det plutselig er blitt akseptabelt for både journalister og brukere å fortelle om sine erfaringer og frustrasjoner, mens det tidligere har vært et poeng å holde dem for seg selv, for ikke å fremstå som mindre flink enn de andre, hvem nå det er. En variant av keiserens nye klær – som omsider er avslørt som ikke-eksisterende. I løpet av det siste halve året har et stort antall slike rapporter – mange av dem svært så velskrevne, og i enkelte tilfeller morsomme – dukket opp i våre hjemlige aviser og i trendsettende media som New York Times, Washington Post og LA Times. Et ferskt og glimrende eksempel av arten er å finne under overskriften "The iPod Shuffle" i The Washington Post (www.washingtonpost.com). Hyppigheten kan indikere at det blåser nye vinder på brukersiden i IT-markedet – en langsom erkjennelse av at visst er teknologi 'kult', men det er enda 'kulere' dersom den virker.

For egen del registrerer vi med interesse en voksende vegring mot å ta frem PCen. Tiden og frustrasjonene vi sparer på å holde oss til Mac'en og en sporadisk avstikker til Linux, er gull verdt – for oss. Den potensielle gevinsten er vel verdt et forsøk.

'Hyper-virus' underveis

Og mens vi først er inne på virkelighets-erkjennelse: Om vi ikke har gjort det før, er tiden overmoden for en porsjon ekstra refleksjon rundt sikkerhetsproblematikk i kjølvannet av ekspertenes snakk om 'UNCRACKABLE VIRUS'. De tror ikke, men mener å vite, at slike virus kan lages, og at 2005 er et sannsynlig år for deres 'inntreden i markedet'. Tidspunktet blir spesielt interessant fordi markedet nylig har fått erfare at selv de mest usannsynlige katastrofer virkelig inntreffer.

Et datavirus som ikke kan knekkes, er en alvorlig affære – på samme måte som tilsvarende biologiske virus alltid har vært det: Dødelig kort og godt. Vi trenger ikke bruke tid på å filosofere over konsekvensene av et slikt virus, og ei heller hvor lang tid det vil ta å finne veier å bli kvitt elendigheten på. La oss anta at det vil ta noen år. Hva gjør vi i mellomtiden? Det finnes kun én måte å forsikre seg mot en slik trussel på, og som ellers i sikkerhets-sammenheng er ingen sikring 100%. Glem antivirus-programmer og andre klient-baserte remedier, de vil per definisjon ikke fungere, og er i realiteten fullstendig verdiløse mot en slik trussel. Kun 'perimeter-beskyttelse' kombinert med velvalgte brukerverktøy har en

rimelig sjanse til å holde slike virus unna. Som de fleste av oss har erfart - direkte eller indirekte, er våre nettverks-verktøy – nettlesere og epost-klienter – takknemlige mekanismer for spredning av både virus og annet 'uønsket besøk'. I tillegg til å tette kontrollen av inn- og ut-passerende trafikk, er med andre ord valg av slike verktøy kritisk for vår grad av beskyttelse. Her har vi plenty å velge mellom, og hva vi velger bort er viktigere enn hva vi velger inn.

Det er innlysende at Internet Explorer og Outlook/Outlook Express må unngås. Ved å erstatte disse to med egnede alternativer, har vi allerede redusert vår eksponering med langt over 50%. For egen del har vi vært Windows-brukere siden Mellvik-Rapporten først så dagens lys i 1993, men har aldri installert anti-virus-programmer og heller ikke hatt virus – fordi vi har holdt oss unna de to nevnte programmer. Siden medio 2004 har vi tatt steget fullt ut og fjernet Windows i sin helhet fra daglig bruk. I tillegg har vi rigid epost-kontroll som vi har beskrevet ved tidligere anledninger. Om vi føler oss trygge? Ja, omtrent som når vi spenner på oss sikkerhetsbeltet i bilen eller flyet. Vi vet at uhell og katastrofer kan skje, men vi har gjort det vi kan. Har du?

Forandringens vind hos HP

De har gått forbausende upåaktet hen, men de er like fullt særdeles signifikante: De strategiske endringene hos HP i løpet av 2004 er intet mindre enn dramatiske, spesielt i et historisk perspektiv. Frikoblingen fra Intels 64-bits arkitektur er ett av symptomene. Merced-prosessen – som ble til Itanium – var Intels og HPs felles hjertebarn, og skulle erstatte HPs voksne og kostbare PA-RISC arkitektur (se Mellvik-Rapporten nr. 55) og selskapets øvrige prosessor-arkitekturer. Det gikk ikke slik. Itanium ble ikke det HP (og Intel) hadde håpet, og frikoblingen – som innebærer at alt engasjement og rettigheter overføres til Intel, legger veien åpen for HPs bruk av AMDs 64-bits arkitektur – som passer bedre og koster mindre. Når PA-RISC, Alpha, 32-bits Intel og andre tjener-arkitekturer skal fases ut, er sannsynligheten vesentlig større for at erstatningen blir AMD-basert enn Intel-basert.

Samtidig er konsument-markedet viktigere for HP enn noen gang, og samarbeidet med Microsoft har uten tvil vært nyttig for begge parter. HP har vært Microsofts største og viktigste partner i PC-markedet i et tosifret antall år. Derfor kom det som en overraskelse at HP gikk til Apple for å legge en MP3-spiller til sitt repertoar sist sommer. Siden den tid har Apples iTunes vært en selvfølge på alle selskapets PCer – til stor irritasjon for Microsoft.

Minst like overraskende kom nyheten rundt årsskiftet om at HP arbeider med en ny generasjon media-sentrerte produkter med Linux som operativsystem, og som etterhvert vil konkurrere med Microsofts Windows Media Center. Supplert med kunnskapen om at HP har beveget seg et langt stykke i retning av å anbefale Linux fremfor Windows på tjenersiden, og leker med mulighetene for en Linux desktop, er det ikke til å unngå at vi løfter et øyenbryn eller to. HP frikobler seg fra Microsoft og posisjonerer seg for et IT-sentrert konsumentmarked med større mangfold enn det vi har vært vant med de siste 10 årene, og der fokus flyttes fra tradisjonelle PCer til intelligente bokser med spesialiserte oppgaver.

HP har uten tvil et glimrende utgangspunkt for å videreføre sin sterke posisjon fra printer- og PC-siden til disse nye segmentene. Med større uavhengighet i forholdet til partnere har selskapet muligheter for å velge optimale teknologier i

stedet for kontraktsfestede produkter. Ingen bestrider fordelene med en slik frihet.

Tid for PCI-express

“PCI? Men det er jo hardware, og det overlater vi til ekspertene.” Uten tvil er optimalt valg for de fleste. Den tid er forbi da engasjement og detaljkunnskap på hardware-nivå var en nødvendig kvalifikasjon for både IT-ledere og driftspersonell. For sistnevnte gruppe er det riktignok fortsatt en fordel å ha god innsikt på hardware-siden, men å vite i detalj hva PCI betyr og hva som er forskjellen mellom PCI og PCI-express kan da ikke være nyttig?

Feil – enn så lenge. Teknologi – og i særdeleshet hardware-teknologi – forandrer seg løpende. Nye varianter kommer på banen, prøver seg, lykkes, blir etablert, blir en selvfølge – og går til slutt ut på dato, slik tradisjonelle serie- og parallellporter har gjort i alminnelig PC-utstyr.

PCI-express befinner seg helt i starten av en slik syklus, og er allerede dømt til å lykkes – fordi behovet er akutt og konkurrentene fraværende. Som navnet indikerer, er det snakk om en intern buss i maskinene, en mekanisme for kobling av periferiutstyr til selve systemet, regnekraften. Men hva er i veien med PCI-X, den oppgraderte utgaven av PCI som slett ikke er særlig gammel?

PCI-X ble tatt i bruk så sent som i 1999, og plages av en arkitektur som teknologisk og ytelsesmessig har gått ut på dato. Parallell overføring av data, som helt til årtusenskiftet ble ansett som hastighetsmessig optimalt, viser seg å ha begrenset skalerbarhet. Når hastigheten kommer over et visst nivå, blir det nærmest umulig å holde de parallelle datastrømmene i takt. Samtidig har både optisk og kabelbasert nettverks- (Ethernet-) teknologi demonstrert at serie-overføring har nærmest ubegrenset skalerbarhet. Diskteknologi – ATA kontra SATA, se IT-revyn i Mellvik-Rapporten nr. 111 – er et annet og nærliggende eksempel.

Situasjonen i dag er at PCI-X blir en flaskehals når Gigabit Ethernet og 10 Gigabit Ethernet tas i bruk. Nettverks-disker blir raskere enn interne, og tjeneren blir ute av stand til å ta i bruk kapasiteten. Samtidig fortsetter hastighetsøkningen for prosessorer og hukommelse, og prosessorfabrikantene snakker om opp til 8 prosessorer på samme brikke. Det sier seg selv at her må det en liten revolusjon til, og PCI-express har det som skal til, både i denne omgang og etter alt å dømme for overskuelig fremtid.

PCI-express er resultatet av et samarbeid mellom blant andre Intel, IBM, Dell, HP og Microsoft, og begynte sitt liv under navnet 3GIO (3. generasjons I/O). Teknologien har ingen ting til felles med tradisjonell PCI, som i tillegg til å være parallell også er en delt buss-arkitektur. PCI-express er for det første seriell, og dernest link-orientert, slik at hver enhet som kobles til, får sin egen ‘kanal’. På lavt nivå har nykommeren mye til felles med Gigabit Ethernet og FibreChannel, hvilket naturligvis har sørget for raskere vei fra design til konkrete produkter.

De av oss som har med anskaffelse av systemer å gjøre, har behov for kunnskap om disse forholdene. Produkter som anskaffes i dag, og som skal leve i mer enn 12-18 måneder, bør inkludere eller være forberedt for PCI-express. Intel startet leveringen av støttebrikker for PCI-express i juli i fjor. HP, IBM og Dell fulgte etter med servere i løpet av høsten. Vi snakker med andre ord ikke om fremtid,

men om teknologi som er tilgjengelig, som virker, og som løser akutte ytelsesmessige problemer.

Ikke overraskende var grafikkort-leverandørene (ATI, NVIDIA) først ute med støtte for PCI-express på periferisiden. Siden har annonseringene kommet jevnlig – SCSI-RAID-grensesnitt, SATA-grensesnitt og Gigabit Ethernet-grensesnitt. 2005 blir uten tvil året da PCI-express flytter seg fra kategorien 'lovende' til å løse reelle problemer på server-rommet. Det var på tide.

'Greylisting' mot SPAM

Kan det være mulig? Enda en metode for bekjempelse av SPAM? Hadde det ikke vært bedre å konsentrere innsatsen om å få de metodene vi allerede har til å fungere bedre? For utsiktene er – som vi var inne på i forrige utgave (side 29/30) – begredelige. Riktignok har en del av oss lyktes i å ta ondet praktisk talt ved roten, og er blitt kvitt det meste av elendigheten. Men for miljøer flest er SPAM-problemet like stort eller større enn noen gang – og fordrer enten handling eller kontinuerlig oppfølging.

Dette har vi verken tid eller ressurser til. SPAM er bortkastet tid for alle som er involvert, og vår søken etter nye og bedre eller enklere metoder tar derfor aldri slutt. GREYLISTING er ikke bare et glimrende eksempel i så henseende, men også den mest lovende mekanismen som har dukket opp siden SPF (se Mellvik-Rapporten nr. 114).

Mekanismen går i korthet ut på følgende: Når epost utveksles, kobler sender seg opp mot mottaker og avleverer først en avsender-adresse og en mottakeradresse, og dernest selve meldingen. Innebygget i protokollen for overføring av epost er en mekanisme som tar hensyn til overbelastede mottakere. Mottaker kan – etter å ha fått adresseinformasjonen velge å svare at den er for opptatt til å håndtere meldingen, hvilket betyr at sender må prøve igjen senere. De fleste legitime epost-agenter håndterer denne mekanismen med den største selvfølge, plasserer meldingen i kø og forsøker igjen senere, normalt i løpet av 1-4 timer.

Og her er vi ved rosinen i pølsen, som det heter: De fleste spam-kilder er 'roboter' som verken er protokollmessig robuste eller har tid til å håndtere køer med retransmisjoner. En midlertidig avvisning som beskrevet, vil dermed fungere som en de facto blokkering av useriøse aktører. Men er ikke dette for enkelt, og vil det ikke bidra til å forsinke legitim trafikk? Her kommer selve 'greylistingen' inn. Kombinasjonen avsenders IP-adresse, meldingens sender-adresse og mottaker utgjør en enhet som kan legges på en liste hos mottaker. En slik liste vil umiddelbart bli populert med de kildene vi vanligvis kommuniserer med, som dermed blir gjenkjent og alltid slipper igjennom umiddelbart. En melding som først er blitt forsinket, men som forsøkes levert en gang til – fra samme kilde, vil umiddelbart slippe igjennom og kombinasjonen blir merket som OK. Notoriske SPAMmere flytter typisk ofte på seg (dvs. de bytter adresse) og vil bli avvist også i neste forsøk dersom det skjer, fordi IP-adressen har forandret seg.

Det kan listes opp en hel rekke tekniske forhold som gjør greylistingen attraktiv, og en håndfull svakheter som for de fleste er til å leve med. Av sistnevnte kategori hører naturligvis forsinkelse av legitime meldinger fra nye avsendere til. I enkelte situasjoner kan hastigheten være kritisk, og greylistingen kan komme i

veien. Implementasjonene av mekanismen gir imidlertid betydelig rom for registrering av unntak, som kan håndtere slike singulariteter.

Og implementasjoner finnes. Til tross for at greylisting først ble foreslått så sent som i 2003, er mekanismen implementert på en lang rekke epost-agenter, av såvel Open Source som kommersiell kategori.¹¹ Og resultatene er overbevisende. Bibliotek-Systemer i Larvik, som vi ved en rekke anledninger har samarbeidet med i forbindelse med epost- og SPAM-prosjekter,¹² rapporterer at greylisting fjerner over 90% av all uønsket epost. At meldingene stoppes før de er levert, representerer en dramatisk reduksjon i belastningen på både epost-tjenere og infrastruktur forøvrig: Meldinger som stoppes så tidlig, vil aldri forlate senderens maskin.

Interessant? Vi skulle tro det. Web-stedet www.jgc.org (John Graham-Cumming) har dybdekunnskap om mekanismen og en lang rekke andre forhold knyttet til SPAM – et faglig eldorado for interesserte. ■

¹¹ Se projects.puremagic.com/greylisting/links.html for mer informasjon om slike implementasjoner.

¹² Se også artikkelen "Automatisert drift" i Mellvik-Rapporten nr. 111.