

IT-revyen

Mellvik-Rapporten er verken avis eller nyhetsmagasin, men vi er definitivt opp-tatt av det som skjer rundt oss. Under overskriften IT-revyen kommenterer vi aktuelle nyheter og temaer i markedet og bransjen forøvrig. Vi konsentrerer oss om emner og trender som faller inn under MRS naturlige fagfelt, og inviterer leserne til å komme med innspill.

Historieløse PCer

De er en pest og en plage, alle disse historiske tilkoblinger og enheter som har vært med våre PCer siden tidenes morgen: Floppy-enhet, parallell-port, serie-porter, musport, tastaturport og så videre. Umoderne kort og godt. Alt ville vært så mye enklere om vi kunne slippe denne historiske ballasten – i alle fall for leverandører av operativsystemer og PCer. USB/USB2, FireWire og nettverkstil-kobling dekker alle behov og får klare seg – mener Intel og Microsoft med flere. Ingen er overrasket over det: Kun markedet – dvs. vi som bruker utstyr som har fått noen år på baken og som fortsatt fungerer aldeles utmerket, er interesserte i å bevare situasjonen: Mottoet og logikken er: IF IT AIN'T BROKEN, DON'T FIX IT. Men uten forandring, ingen BUSINESS, og de teknologiske argumentene er overbevi-sendende nok.

De drømmer, disse leverandørene: Det er riktignok et faktum at USB har gjort vei i vellinga på en rekke områder de siste årene, men det tok 6 år før bitene falt på plass. Markedet trenger og forlanger stabilitet, og lite tyder på at vi vil aksep-tere historieløse systemer med det første. På den andre siden dukker det stadig opp nye anvendelsesområder der historiske enheter og tilkoblinger er verdiløse. Det betyr at nye, segment-tilpassede PC-varianter – Compaqs tynne klienter er gode eksempler, vil fortsette sin fremmarsj. I privatmarkedet og store deler av forretningsmarkedet ser vi imidlertid ingen tegn som indikerer at de antikvariske portene fra IBMs første PC i 1982 vil bli borte med det første. Nytteverdien er kort og godt for stor. Dessuten er tilleggskostnaden for produsentene minimal. Forandring til forbedringens fremme.

Verdiløse backups

Sikkerhetskopiering har mye til felles med forsikring: Kostbart og nødvendig, og noe vi håper å aldri få bruk for. Deres eksistens får oss til å føle en trygghet for at situasjoner er tatt vare på, skulle ulykken være ute. Først da finner vi ut hvor mye forsikringen er verdt, enten vi snakker om sikkerhetskopiering eller regulær skadeforsikring.

Sikkerhetskopiering er enkelt, en mengde data, en strøm av bits og bytes som kan gjenskapes når som helst. Det våre mer eller mindre avanserte backupverk-tøy ikke er hjelpelige med, er datakonvertering: Data blir gamle i den forstand at de innehar antikvariske formater. Som vi var inne på ovenfor, lever våre leve-randører av forandring: Det gir penger i kassen i form av oppgraderinger og nyanskaffelser. Forandringene gjelder ikke minst dataformater, noe brukere av Microsoft Word har fått stifte smertelig bekjentskap med de siste 5 årene.¹¹

¹¹ Det finnes unntak som bekrefter regelen: Vi har brukt FrameMaker (som Mellvik-Rapporten produseres med) siden 1988, og kan fortsatt åpne de eldste dokumentene uten problemer. At utseendet blir annerledes dersom riktige fonter mangler, er en ulempe, men ingen overraskelse.

Poenget er at all verdens backup-verktøy er til liten nytte dersom vi ikke også har hjelpemidler som kan lese dataene. Og når vi har problemer med 5-6 år gamle dokumenter, hvordan skal situasjonen være etter 10, 30 eller 50 år? Et argument for å gå tilbake til mikrofilm? Neppe, men i alle fall en problemstilling å være oppmerksom på: Data er verdiløse dersom de ikke kan brukes. Med andre ord bør også tilgang på verktøy være en del av vår policy for sikkerhetskopiering. Er den det?

Færre reiser, flere utfordringer

“Verden blir aldri den samme.” Vi hører det igjen og igjen, med referanse til 11. september 2001, og er hjertens enig. Men hva er konsekvensene? Hvordan blir verden annerledes? Svaret er ingen gitt å vite, og mange av oss oppdager nye sider ved fremtiden hver eneste dag. En av dem er konsekvensene av det faktum at folk nødig reiser. I stedet for å være reisevillige og sågar reisesøkende i arbeidssammenheng, er en hel verden blitt hjemmekjære på et nivå som nærmer seg siste verdenskrig.

Blant mange utfordringer i kjølvannet av denne holdningsendringen er behovet for mobil datakraft, for konnektivitet og såkalte Web-kameraer, som sammen med lett tilgjengelig programvare utgjør billigvarianten av Tandbergs video-telefoni. Men mobil datakraft, er ikke det selvmotsigende? Slett ikke: ‘Hjemmekjær’ er ment i bokstavelig forstand: I større grad enn noen gang blir folk gjerne hjemme og arbeider derfra – med mobiltelefon og bærbar PC. Dermed får vi en oppskalering i bruk av de ressursene som inngår i ligningen – pluss enkelte overraskelser: Flere bærbare systemer blir stjålet, skadet, ødelagt – eller får ulike programvareproblemer.

Er driftsavdelingen rustet for utfordringene? Finnes prosedyrene for regenerering av en disk som ikke vil starte, erstatning av en knust eller tapt maskin i løpet av noen timer, sikring av data slik at tap og tyveri blir et økonomisk, ikke et sikkerhetsmessig spørsmål – og så videre? Vi ser at utfordringene kommer, så hvorfor ikke ta forberedelsene mens det enda er tid?

Vaksine for infiserte systemer?

Vaksine er vi alle kjent med. Mange av oss husker sågar at de fleste vaksiner er fremstilt av eller ved hjelp av de samme bakterier eller virus den skal beskytte mot. Hukommelsen fra barndom og tidlig ungdom stimuleres av at noen i omgangskretsen ble syke av selve vaksinen.

Om vi overfører modellen til datavirus og strekker den videre til å dekke ormer og andre varianter av automatiserte, selvrepliserende programmer, fremkommer interessante ideer. Mekanismene som utnyttes av disse programmene – legitime kommunikasjonsmekanismer kombinert med hull, feil og svakheter i ulike programmer, fra applikasjoner til tjenester og operativsystemer – er like tilgjengelige for positive som for negative oppgaver. Med andre ord – hva er i veien for å utvikle og spre ‘vaksinerende virus’, virus som sprer seg i nettverket, finner og tetter hull og feil, og rapporterer tilbake til ‘sentralen’ – hva som har skjedd?

Tankene er verken unike eller nye. Slike 'virus' finnes og har vært i sirkulasjon – ikke bare for å tette hull, men for å fjerne farlige virus – som Code Red og Code Blue. Eksempelene har vist at det er mulig å lage og spre slik vaksine, og har dermed bidratt til å skape debatt om et overmodent tema: Hvor langt er det mulig – og riktig eller rimelig – å gå i vår søken etter å bedre sikkerheten? Det er et faktum at de fleste alvorlige angrep og skader kunne ha vært unngått dersom ofrene hadde hatt funksjonelle prosedyrer for å løpende oppdatere sine systemer.¹² Kommer vi nærmere en løsning ved å true med ukontrollerte og ukontrollerbare vaksinasjoner? Hvordan vet vi forskjell på godartet og ondartet? Kan vi sikre oss mot bivirkninger? I mange tilfeller må systemer omstartes én eller flere ganger i forbindelse med oppdateringer, hvordan skal dette ivaretas, tidspunktet velges og så videre?

Kort sagt – vi ser en mulighet og tallrike problemer. Idéen er imidlertid for god til å la ligge fordi den ser vanskelig ut. Hva om det fantes en internasjonal enhet som virkelig kunne utvikle, teste og garantere slike vaksiner? Kanskje også etablere standarder og akseptable nivåer for kvalitet og kontrollrutiner hos deltaende leverandører, og derigjennom bidra til å øke konkurransen og heve nivået på programvare generelt?

Vi har ikke løsningen eller svarene i dag, men vi er ikke i tvil om at det her ligger betydelige muligheter med potensiale til å gi bedre IT-sikkerhet på alle nivåer. Dessuten, og like viktig: Temaet diskuteres blant sikkerhetsekspertene og leverandører i disse dager. Vi venter spent på hva som kommer ut og når!

Content Delivery Networks

I en bransje som flommer over av uttrykk og forkortelser, er det lenge siden 'å være oppdatert' var det samme som å kjenne dem alle. Her må det leksikon og avansert søketeknologi til for å holde orden i kaoset: Vi slår opp når vi trenger det, og husker det som er viktig.

Det er med andre ord ingen grunn til å skjemmes om uttrykket CONTENT DELIVERY NETWORKS (CDN) er fremmed eller innholdsmessig ukjent. Det har riktignok eksistert en stund, men vært mest synlig langt inne i leverandørorganisasjoner – på produsentsiden, som Cisco/ArrowPoint og Nortel/Alteon, og hos tjenesteleverandører som Yahoo, Akamai og Digital Island. Konseptet er imidlertid tilstrekkelig spennende til å ta nærmere i øyesyn: Det handler om å øke ytelse og leveringseffektivitet for komplekse Web-transaksjoner, ikke nødvendigvis mot tusener eller millioner av personlige brukere, men like gjerne i forbindelse med handel og transaksjoner mellom virksomheter, B2B på fagspråket.

Det er nettopp innen siste segment CDN i disse dager opplever et oppsving, etter at forhåpningene til det generelle Web-markedet viste seg å være altfor optimistiske. Der inntektene mangler sitter investeringsmidlene langt inne, som seg hør og bør. Videre ser vi voksende interesse for bruk av CDN i store internasjonale selskapers interne nettverk.

¹² Vi overser her det åpenbare faktum at hele problemet ville vært minimalt dersom programvarebransjen hadde levert bedre kvalitet.

CDN er ikke et nettverk, som navnet kan indikere, men en mekanisme for å optimalisere leveringen av innhold til 'konsumentene', det være seg firmaer, ansatte eller private. Slik Internettet og andre store nettverk fungerer, påløper det gjerne store forsinkelser, belastningstopper og andre små og store driftsforstyrrelser som gjør levering av store datamengder over ditto avstander, til en høyst uforutsigbar affære. CDN sørger for å mellomlagre – CACHE på fagspråket – innholdet nær brukerne: Yahoo har sitt hovedsete i California, og store brukerskarer over hele verden. Disse betjenes ikke direkte av gigantiske Web-tjenere på hovedkontoret, men av CDN-utstyr som automatisk optimaliserer leveringen i nærheten av brukerne. Noe annet ville ha gitt uakseptable responstider og brukerne ville flyktet.

Et annet eksempel er supermarkedkjeden Safeway, som opererer over hele USA og i en rekke andre land: Praktisk talt all opplæring foregår via digitale videostrømmer til PCer lokalt der de ansatte arbeider. Datastrømmene formidles via satelitt og mellomlagres av CDN-utstyr på brukerstedene, for bruk når det passer. Responser blir god og forutsigbar, mens avhengigheten av konstant og pålitelig båndbredde i alle deler av nettverket er borte.

Selv med en kraftig økning i tilgjengelig båndbredde (se artikkel på side 13), er det liten grunn til å se for seg at behovet for slik optimaliseringsteknologi vil bli borte. Store avstander vil alltid gi forsinkelser og tilgjengelig båndbredde vil forbli en variabel ressurs, akkurat som fremkommeligheten på våre veier. Derfor er CDN – som kanskje vil bli kalt noe helt annet om et år eller tre – et viktig element i store nettverk, godt ute av syne for brukerne, og en essensiell mekanisme for kvalitetssikring sett fra innholdsleverandørens side.

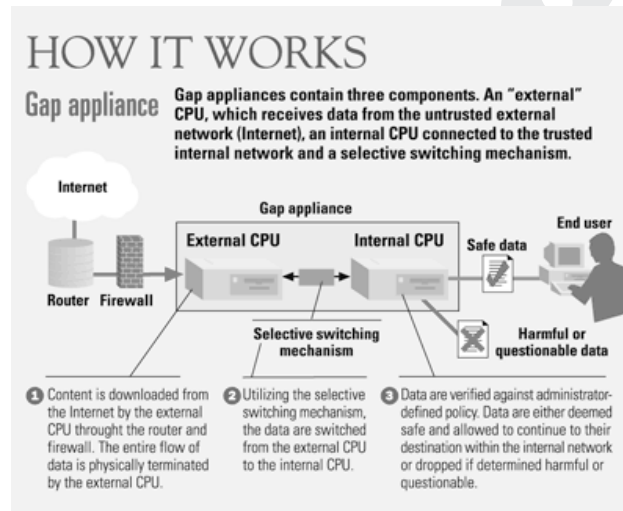
Gap Technology: Isolasjon fra nettet

Temaet dukker stadig opp – og hyppigere de siste månedene: Hvordan kan vi tilby eksterne tjenester på nettet og samtidig ivareta god sikkerhet innover? Det vanlige svaret er en demilitarisert sone (DMZ), et konsept vi har diskutert ved en rekke anledninger her i Mellvik-Rapporten: Et 'friorråde' som er innenfor vår første brannmur, men utenfor det interne nettverket.

Så langt er alt vel og bra, men hva med kommunikasjonen fra DMZ og inn i nettverket? Det kan være behov for transaksjonsbasert trafikk – til databaser og registre, oppdateringer av informasjon på de eksterne ressursene eller andre varianter: Utdfordringen er å sørge for at hullene som uvegerlig må lages i det indre forsvaret, blir så små og trygge som overhodet mulig.

En rekke varianter har vært prøvd og er i bruk i den forbindelse, alle med sine fordeler og ulemper. Siste skudd på stammen er såkalt Gap-teknologi – som etablerer en fysisk avstand mellom de to nettverkene som skal kommunisere. 'Fysisk' må oppfattes i overført betydning, men er en grei billedliggjøring: De to sidene er aldri forbundet direkte til hverandre, men til en svitsj som kobler fra det ene nettverket når det andre kobles inn og motsatt. Svitsjen terminerer trafikk fra begge sider, undersøker innholdet i henhold til definerte regler, og videre sender det som godkjennes. Figuren nedenfor, som er hentet fra nettmagasinet Network World Fusion, forklarer detaljene. Hver side har sin egen

prosessor som pakker ut og kontrollerer innkommende data, mens den pakker inn og viderefremidler utgående data. Kombinert med en sikker DNS-proxy for navneoppslag og takket være teknisk sett svært enkle oppgaver, er boksen i seg selv immun overfor angrep og svakheter i programvare.



Konseptet er interessant i sin enkelhet, og har potensiale til å gi sikring på et vesentlig høyere nivå enn tidligere har vært mulig. At verken denne eller andre kjente mekanismer kan stoppe DENIAL OF SERVICE angrep, som setter nettverk og tjenester ut av spill gjennom å konsumere alle tilgjengelige ressurser, må vi leve med. Slike angrep vil effektivt blokkere trafikkflyten, men vil ikke representere noen fare for det interne nettverket.

Aktive leverandører av GAP-teknologi er RVT Technologies (www.rvttech.com), Spearhead Security Technologies (www.sphd.com) og Whale Communications (www.whalecommunications.com). Vi vil komme tilbake til temaet her i Mellvik-Rapporten i løpet av 2002. ■