

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.

Over til Lindows

‘Navnet skjemmer ingen’ lærte vi i barneskolen. Ikke alltid like lett å akseptere, men utvilsomt prinsipielt og etisk korrekt. Navn kan imidlertid skape både irritasjon og forvirring, ikke minst i tilknytning til produkter. Lovverk og forskrifter i de fleste siviliserte land beskytter mot tilsiktede forvekslinger i den forbindelse, og håndheves med voksende hyppighet – og vanskelighet i en verden som blir stadig mer grenseløs.

I utgangspunktet skulle vi tro at generiske uttrykk som bil, vindu, maskin og så videre, ikke kunne beskyttes eller reserveres: Språket er felleseie og kan verken kjøpes eller eies av selskaper eller personer. Kreativ anvendelse av såvel lover som markedskrefter har imidlertid gitt oss en rekke eksempler på at slike selvfølgheter ikke lenger er like selvfølgelige. ‘Windows’ er det mest nærliggende eksemplet – kjent av de fleste og ‘eiet’ av Microsoft. Behovet for å eie eller kontrollere språket stopper imidlertid ikke der. Selskapet vil også ha kontroll over ord og uttrykk som ligner på deres store arsenal av reserverte produktnavn.

Her kommer Lindows inn: Et for de aller fleste fullstendig ukjent navn som ikke sto for noe som helst inntil nylig. Svarene vi har fått fra vår private lille rundspørning, er av typen “et eiendomsselskap?” og “et etternavn?”. Anonymiteten for Lindows er imidlertid over: Microsoft har saksøkt selskapet med samme navn for plagiering av produktidentitet og brudd på lovverket som beskytter navnerettigheter. Med andre ord må Lindows ikke bare ha noe med IT å gjøre, men ha eller representere et produkt som Microsoft anser for å være truende.

Dette er i seg selv grunn god nok til å undersøke nærmere hva Lindows er. Og når Microsoft først har styrt våre tanker i disse baner, skal det ikke stor fantasi til for å oppdage at Lindows gjerne kan være en sammensetning av Linux og Windows. En rask visitt til www.lindows.com forteller at selskapet – som ble startet i fjor av mp3.com gründer Michael Robertson – utvikler et Windows-kompatibelt operativsystem som skal kunne kjøre de viktigste Windows-applikasjoner, se ut som Windows, og være klart til levering i 1. kvartal – på engelsk for USD 99. Koblingen til Linux er uklar utover at selskapet proklamerer moralsk og lisensmessig støtte til Open Source.

Uansett er dette mer enn nok til å skape interesse – fra vår side og fra de fleste internasjonale media. Lindows har i løpet av de siste 3 månedene vært nevnt i NYT, CNN, Wired, CnetNEWS, MSNBC – og Finansavisen, for å nevne et knippe. Dessuten har en testversjon av systemet vært ute i noen måneder, og vi antar at kombinasjonen av testresultater og oppmerksomhet har vært tilstrekkelig til å trigge interessen fra Microsofts side.

Det lover unektelig godt, og vi venter i spenning på hva som kommer ut av de store ordene. Robertson har gode papirer med hensyn til å få ting til å skje. På

den andre siden er utfordringen han har gitt seg i kast med, formidabel – og velkjent: Mange har prøvd før, ingen har lyktes så langt. Vi minnes spesielt WABI, WINE, PetrOS, SoftWindows og SoftPC blant et dusin slike produkter gjennom 15 år.

Som John Dvorak i PC Magazine sier, er det først og fremst et spørsmål om å kjøre Office 97, 2000 og XP, og for vår del legger vi til Internet Explorer og Outlook Express. Er disse på plass og stabile, er Lindows langt på vei. Hvordan det stiller seg med lisenser og andre juridiske forhold, er også interessant. Imidlertid burde tilstrekkelig mange emulatorer og simulatorer av ulik alder og opprinnelse være i drift til at dette ikke representerer noen praktisk hindring.

Vi venter i spenning – ikke minst på Microsofts neste trekk ...

ZixMail: Sikker epost?

“Hvor ble det av sikker epost?” spurte vi i forrige utgave, og konstaterte at så lenge bevisstheten mangler, er sjansene små for at sikker epost finner veien ut fra nisjene. Alternativt må vi komme til et punkt der sikker epost er både usynlig og selvfølgelig, og ikke til bryderi for verken sender eller mottaker. Dit er det langt, blant annet fordi standardene er mangelfulle og kompatibilitet mellom ulike epost-systemer og -produkter tilsvarende problematisk.

Mens vi venter på at disse forholdene skal komme i orden, er det et faktum at de nisjene der behovet er tilstrekkelig aksentuert til å kvalifisere investeringer, vokser kontinuerlig. Dermed finnes det også leverandører som har funnet et marked i nettopp disse nisjene. Vi har nevnt en håndfull av dem de siste månedene – og får stadig spørsmål i den forbindelse. Derfor har vi tittet nærmere på noen av disse produktene – med spørsmålet: Hvor sikkert kan det bli og hvor vanskelig er det? Ingen praktisk evaluering, men en gjennomgang av hvordan utfordringene er angrepet og hvor enkelt eller vanskelig det er å folde løsningene inn i en eksisterende infrastruktur.

Hovedproblemet er ikke at markedet mangler eller har vanskelig for å se behovet for sikring av eposten, men at medisinen fortsatt betraktes som verre og mer kostbar enn sykdommen i de fleste miljøer: Vi mangler standarder og mekanismer som dekker over kompleksiteten en sikker epost-løsning nødvendigvis må ha: Signaturer, autentisering, sporing, kryptering under transport og lagring – for å nevne de mest grunnleggende elementene. Løsningsalternativene som finnes, har angrepet disse utfordringene på ulike måter, og er for det første inkompatible med hverandre. For det andre har de svært ulike karakteristika med hensyn til måten de folder seg inn i eksisterende infrastrukturer på.

Første kandidat ut er ZixIt Corp. og deres ZixMail, som har fått betydelig internasjonal oppmerksomhet de siste månedene. Produktet inneholder flere interessante konsepter og ideer utover å ivareta grunnleggende krav til sikkerhet. Sentralt i løsningen står selskapets egen tjener, som leverer transaksjonssertifikater og lagrer den offisielle halvpart av asymmetriske krypteringsnøkler, og dessuten ivaretar levering av meldinger til mottakere som ikke selv kjører ZixMail lokalt.

www.zixit.com

Denne avhengigheten er naturligvis et tveegget sverd: Den representerer en forenkling – OUTSOURCING om vi vil – av en komplisert del av sikkerhets-ligningen og gjør brukermiljøet uavhengig av en egen PKI-løsning, som både er kostbar og krevende å vedlikeholde. Gitt at selskapet har sunn økonomi og forøvrig er i god forfatning [forhold vi ikke har studert i denne forbindelse], er dette ikke bare en akseptabel måte å løse utfordringene på, men en nødvendighet – og i en rekke henseender optimal løsning.

Tjenestens andre og like viktige funksjon er levering av sikker epost til brukere som ikke selv kjører ZixMail – et problem for alle løsninger av denne typen: I og med at sikringsmetodikken er proprietær, er produktene kompatible kun med seg selv. Dette løser ZixMail ved å kun levere en 'hentelapp' i mottakerens postkasse, med en peker til hvor den egentlige meldingen kan hentes. Dette skjer via nettleseren og SSL-kryptering, som gir middels god sikkerhet i forhold til hva vi får når begge ender har samme sikringsprodukt. I forhold til usikret epost er imidlertid selv denne hybride løsningen for sikker å nevne, mens den aldri kan gi fullgode leveringskvitteringer (NON REPUDIATION).

Klientsiden håndteres enten med ZixMails egen klient, eller med plug-in moduler til Outlook eller Lotus Notes, en løsning som gir minimale synlige konsekvenser for de fleste brukermiljøer, men med spennvidde som begrenser seg til Windows.

Utover å ivareta sikkerheten og gi mulighet til å sende sikker epost til en hvilken som helst mottaker, er dette ZixMails viktigste attributt: Usynlighet for brukeren. Dermed kan en policy som forlanger bruk av sikker epost i organisasjonen realiseres i praksis. Faktorer som i tillegg må evalueres, er naturligvis kostnader, plattformer, brukeradministrasjon og ikke minst forholdet til eksisterende sikkerhetsløsninger (brannmurer, arkivmekanismer, sikkerhetskopiering og så videre).

■

I neste utgave gjør vi en tilsvarende gjennomgang av HushMail [www.hushmail.com].

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> (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!