

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.

Kildekode på vidvanke

Det besynderlige er at det ikke har skjedd tidligere. Microsoft er markedsle-dende, og har tusenvis av partnere som i varierende grad har tilgang til produk-tenes kildekode. Det betyr at spredningen er enorm, og det ville være besynderlig om ikke noen hundre eller tusen utviklere har sikret seg en kopi av koden 'til privat bruk'. På veien til markedsdominans har Microsoft dessuten ruk-ket å skaffe seg utallige fiender – som uten tvil kunne tenke seg å gjøre Gates & Co. et pek dersom anledningen skulle by seg.

Når store deler av kildekode til Windows NT og 2000 tidlig i februar dukket opp på Internettet, er det lett å anta at slike hensikter ligger bak. Vi er imidlertid ikke overbevist. Faktum er at vi stiller oss uforstående til at frislippet skulle være negativt for Microsoft eller markedet overhodet. Faktisk kan det ikke utelukkes at selskapet selv på en eller annen måte har orkestrert eller godkjent lekkasjen. Når konkurransen mot Linux tilspisser seg, ville det unektelig være praktisk for Microsoft å kunne si at Windows også er Open Source, om ikke i gavnet så i alle fall delvis i praksis.

Faren for at noen skulle utnytte koden til å lage en Windows-klone er minimal – til det er oppgaven for ressurskrevende og komplisert. Og skulle noen finne det for godt å gjøre seg kjent med koden, er kosekvensene utelukkende positive: Potensialet for avdekking av feil, overflødig kode og andre svakheter øker som kjent proporsjonalt med antall øyne som har sett koden.

Et annet scenario som har vært lansert i pressen, er at lekkasjen skal gjøre eldre utgaver av Windows 'upålitelige' i markedets øyne, og stimulere overgangen til nyere versjoner. Mens det ikke kan utelukkes at noen har tenkt tanken, har vi igjen vanskelig for å se at 'åpningen' skal gi seg slike utslag. Riktignok kan det hevdes at åpenheten vil gjøre det lettere for 'hackere' å finne feil som kan utnyt-tes, men SECURITY BY OBSCURITY gikk ut på dato for et tosifret antall år siden. Open Source produkter er påviselig sikrere enn tilsvarende med lukket kildekode, og effekten for Windows burde derfor være positiv, ikke negativ.

Det store 'kildekode-slippet' kan såvidt vi kan se, ha to potensielt negative kon-sekvenser for Microsoft. Dersom kodekvaliteten viser seg å være vesentlig dårli-gere enn det som er vanlig, vil det bidra til å redusere tilliten til Microsoft som leverandør. Likeledes kan det tenkes at koden avslører noen av selskapets hem-melige grensesnitt mot egne applikasjoner, hvilket avføder to komplikasjoner: For det første blir de dermed offentlige, slik at andre leverandører kan bruke dem. Og for det andre har Microsoft under eds ansvar i monopolrettssakene bevitnet at de ikke finnes. En slik avsløring ville med andre ord ha uoversiktlige konsekvenser for både pågående, historiske og fremtidige rettstvister.

Når støvet har lagt seg i løpet av mars måned, er sannsynligheten stor for at hele saken blir glemt. I løpet av et par måneder vil vi dermed vite om lekkasjen var overlagt eller et ulykkestilfelle. For markedet generelt blir konsekvensene mini-male uansett.

WLAN: Sikkerhets-anbefalinger

I løpet av et knapt år har WLAN-teknologi ristet av seg sitt tvilsomme rykte i sikkerhetsmessig forstand. Den profesjonelle delen av markedet vet at trådløse nettverk kan sikres – og aner hvordan det skal gjøres. I privatmarkedet er situasjonen mer nyansert, blant annet fordi det sjelden er trivielt å velge og idriftsette sikkerhetsmekanismene. Unntaket som bekrefter regelen er Apple, hvis Airport Extreme produkter har tatt en markedsandel som på ingen måte står i forhold til selskapets posisjon på systemsiden. Med over 20% av markedet for 11g-produkter – og et prisleie som ligger på ca. det dobbelte av de prisledende – har Apple demonstrert at kombinasjonen design og enkelhet kan skape suksess uten direkte kobling til pris også i dette segmentet. Enkelheten bidrar til bedre sikkerhet uansett markedssegment, og representerer dessuten et forbilde som andre leverandører bør bite seg merke i.

Mekanismer er viktige – og verdiløse om de ikke brukes. I større miljøer – med fra 30-40 til hundrevis av aksess-punkter, er trådløse svitsjer den eneste overkommelige måten å få et funksjonelt, stabilt og sikkert WLAN på. Er forholdene mindre, blir evalueringen mer sammensatt, men uansett vil følgende observasjoner være til hjelp for å bringe sikkerheten opp på et rimelig nivå:

- ✗ Alle WLAN-segmenter skal behandles som om de er eksterne, altså som Internettet, hvilket betyr at trafikken skal gjennom en brannmur, selv om den rent fysisk er aldri så intern.
- ✗ Kryptering skal være aktivisert, og det er en fordel om utstyret supporterer WPA.⁹ Imidlertid er 'gode gamle' WEP adekvat når vi for det første behandler nettverket som eksternt, og for det andre sørger for at brukerne benytter en kryptert VPN-forbindelse.
- ✗ Autentisering via 802.1x skal være – om ikke implementert, så i alle fall planlagt. Det betyr at utstyret må støtte denne standarden.
- ✗ Gjør bevisste valg med hensyn til klientutstyret (leverandører, type, egenskaper etc.), og registrér MAC-adressene slik at disse kan brukes i forbindelse med autentiseringen. Filtrering på MAC-adresse må også være støttet av svitsjene eller styringssystemet.
- ✗ Dersom nettverket skal være åpent for gjester, er det hensiktsmessig å skille de aksesspunktene som skal være tilgjengelige, i et eget VLAN eller segment. Åpen aksess for gjester bør port-filtreres, slik at kun nettleser og eventuelt epost-protokoller er tilgjengelige.
- ✗ Sørg for at aksesspunktene er godt sikret både fysisk og med passord. De kan med fordel plasseres ute av syne. Hold dem oppdatert med siste revisjon av programvaren (FIRMWARE) – fortrinnsvis automatisk.
- ✗ Sentraliserte styringssystemer for aksesspunktene kan utnyttes på utallige måter – for eksempel til å slå av aksesspunkter i perioder hvor de ikke skal brukes.
- ✗ Radioplanlegging er en kunst, og kan utnyttes til å unngå at dekningsområdet for WLAN strekker seg langt utenfor bygningen. Riktig utstyr og optimal plassering av antenner kan gjøre underverker i så henseende.
- ✗ Benytt intelligente overvåkingsverktøy ikke bare til å kontrollere kapasitet og dekning, men også til å finne ureglementerte aksesspunkter. Også andre

⁹ WPA-standardene har vært klar i et halvt års tid, og støttes etterhvert av de fleste nye WLAN-produkter på markedet. Imidlertid er det lenger mellom støtten på klientsiden, et forhold vi også har vært inne på tidligere.

mekanismer kan utnyttes positivt til dette formålet, blant annet løpende kontroll med hvilke MAC-adresser som ber om adresser fra hvilke porter. Ureglementerte (bruker-plasserte) aksesspunkter har de tre siste årene stått for en vesentlig andel av de sikkerhetsmessige katastrofene i tilknytning til WLAN.

WLAN: Se opp for proprietære utvidelser

Vi observerer at WLAN-markedet modnes så raskt at leverandørene – spesielt lokale forhandlere – ikke klarer å følge med. Disse leverandørene promoterer 'utrangert' 802.11b-utstyr til historisk høye priser, tilsynelatende uten å vite at verden forlengst har gått videre. Moderne produkter med støtte for sikkerhetsstandarden WPA og høyere hastighet via 802.11g i tillegg til den veletablerte B-standard, er ikke bare tilgjengelige, men koster sågar mindre enn de gamle produktene som 'PUSHES'. De 'gamle' produktene – som sjelden er mer enn 2 år gamle – er ikke verken unyttige eller uselgelige, men å selge dem til høyere pris enn siste modell synes i beste fall naivt.

At 802.11g-produkter har overtatt volum-markedet for WLAN-produkter betyr ikke at den veletablerte 11b-standard blir borte eller at produktene som støtter den blir verdiløse. Som vi har vært inne på tidligere, forblir 11b minste felles multiplum for slike produkter, og deres spredning fortsetter å øke – fordi de inkluderes i alt tenkelig utstyr fra kjøkkenmaskiner via musikkanlegg til PDAer, telefoner og kjøretøyer.

Og utviklingen fosser videre. På samme måte som 11b-standard relativt raskt ble utvidet med høyere hastighet fra 11g, som var under utvikling, ser vi i dag produkter som kaller seg 11g+ – eller i noen tilfeller 'Super-G', og som tilbyr 108 Mbps båndbredde og samme rekkevidde som før. Her er det imidlertid viktig å trå varsomt. At vi mangler en standard for den nye høyhastighetsvarianten, er en situasjon vi er godt kjent med. Risikoen med å anskaffe og ta i bruk prestandard produkter er velkjent og kalkulerbar, og kompenseres av at utstyret har relativt lav anskaffelseskostnad. Verre er det at enkelte utstyrsvarianter viser seg å ha betydelig forstyrrende effekt på andre trådløse nettverk i omgivelsene. Dette gjelder især produkter basert på en spesiell CHIP fra leverandøren Atheros, som viser seg å ha blitt sendt ut på markedet før den var skikkelig 'avluset'. Riktignok er vi vant med å både omgås og betale for 'lusbefengte' produkter i programvaremarkedet, men kravene vi stiller til hardware er heldigvis annerledes.

Vi skal unnlate å filosofere over denne åpenbare selvmotsigelsen, og holde oss til problemet: Alt har sin pris, og den nye båndbredden for WLAN-produkter kommer i hovedsak av en ny måte å kombinere kanalene i frekvensspekteret på. Kanalene er de som benyttes av 11b- og 11g-produktene, og nykommeren må ta hensyn til disse dersom de finnes. Ferske amerikanske tester viser at så ikke alltid skjer, med vesentlige forstyrrelser som konsekvens. Anbefalingen blir med andre ord å unngå Super-G og holde seg til etablerte standarder – i alle fall til implementasjonene bli mer modne. Det er en utvikling vi kommer til å følge nøye fremover sommeren og høsten her i Mellvik-Rapporten.

Avslutningsvis er det opportunt nok en gang å bringe på bane det faktum at de såkalte båndbreddene i WLAN-sammenheng i realiteten er bithastigheter (bit-rater). Videre er det slik at sameksistens av flere standarder automatisk medfører at den eldste blir retningsgivende ('minste felles multiplum'). Der hvor 11b-kl-

enter finnes, er det med andre ord snakk om en maksimal effektiv båndbredde per aksesspunkt på 6-8 Mbps, uansett hvor avansert aksesspunktet måtte være.

SSL-VPN: En oppdatering

Siden vår gjennomgang av kombinasjonen VPN og SSL i desember 2003 (Mellvik-Rapporten nr. 112), har etterspørselssiden utviklet seg raskere enn noen hadde drømt om. Fra å se på SSL som en mulighet – og kanskje som en årsak til å utsette beslutninger om teknologivalg, har et flertall av profesjonelle innkjøpere i nettverksmarkedet nå flyttet SSL-støtte opp som et ufravikelig krav for VPN-produkter. Erfaringene med eksisterende løsnings kompleksitet og tilhørende kostnader, sørger for at forenkling står øverst på prioriteringslisten for de fleste, og SSLs hovedattraksjon er nettopp enkelhet. I løpet av de siste 6 månedene har samtlige av de store aktørene innen kommunikasjons-sikkerhet presentert SSL-baserte VPN-produkter – enten med utgangspunkt i egenutviklet teknologi eller gjennom oppkjøp av ferske spesialiserte selskaper. F5, NetScreen og Symantec tilhører denne gruppen, mens Check Point, Nokia, Cisco og Nortel har utviklet sine egne løsninger.

Denne forandringen i VPN-markedet er et viktig steg fremover for IT-sikkerheten generelt. Misforståelsen at IPSec skulle løse alle tenkelige sikkerhetsproblemer for IP-nettverk har kostet store penger uten å gi god sikkerhet. Som vi var inne på i artikkelen i nr. 112, er ikke SSL-baserte VPN-løsninger noe dødsstøt for IPSec, men en god hjelp til å plassere teknologien der den hører hjemme: Sikring av nett-til-nett forbindelser.

Fjernaksess trenger enkle og effektive mekanismer som fordrer et minimum av administrasjon – og adekvat sikkerhet for alminnelige formål. SSL har disse egenskapene, og frigir tid til å fokusere på langt mer krevende utfordringer – for eksempel innholdskontroll. ■