

IT-revyen

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

Sikkerhetspolicy for trådløse nettverk

Policy generelt og sikkerhets-policy spesielt er – med god grunn – blitt gjenganger i Mellvik-Rapporten. Turen er kommet til trådløse nettverk, også en gjenganger, og som mange lesere har påpekt de siste månedene – et mål i bevegelse. Vi finner en rekke referanser og eksempler på sikkerhets-relaterte WLAN-policyer på Internettet, men opplever at de skaper like mye forvirring som oppklaring. For eksempel hersker det sterkt sprikende oppfatninger om hva en policy skal inneholde – mens vår grunnregel er at den skal være så enkel som mulig, og ikke beskjeftige seg med praktiske prosedyrer eller tekniske detaljer. En policy skal i korte og konsise ordelag fortelle hva som gjelder, hvorfor, for hvem – samt ansvarsmessige forhold. Den skal være brukerorientert og brukervennlig – hvilket blant annet betyr at vi må ha et klart forhold til hvem brukerne er. En alminnelig IT-bruker fordrer noe helt annet enn en driftsperson – for eksempel. Og en sikkerhetspolicy kan være separat eller en del av et generelt policydokument – for WLAN og i andre sammenhenger.

Policy er ett av en rekke dokumenter som regulerer hverdagen – også for WLAN. Andre forhold som skal klarlegges, og som gjerne kan være referert fra et policy-dokument, er for eksempel prosedyrer for introduksjon av nye aksesspunkter, regler for deres plassering, teknologier som er godkjente, samt kontroll- og driftsprosedyrer.

En sikkerhets-policy for WLAN har lite med sluttbrukere å gjøre. For dem er nettverket YET ANOTHER INFRASTRUCTURE, og de forholder seg til tjenestene som tilbys, ikke nettverket i seg selv. Dermed blir en policy rettet mot teknisk personale, og kan inneholde elementer fra følgende liste:

- ✗ Kryptering og autentisering: Aksepterte mekanismer.
- ✗ Krav til standarder.
- ✗ Godkjente klienter/klienttyper/kategorier (PC, telefon, PDA, annet klientutstyr – fortrinnsvis ikke leverandører, som blir for detaljert i denne sammenheng).
- ✗ Godkjent nettverksutstyr (typer, kategorier) – inklusive antenner (og eventuelt krav til bruk av antenner for å redusere ekstern stråling). Igjen er det en målsetting, men ikke alltid gjennomførbart, å unngå leverandørspesifikk informasjon.
- ✗ Grad av åpenhet (tilgjengelig for gjester eller kun for interne – i siste tilfelle er filtrering på MAC-adresser aktuelt).
- ✗ Transportsikring (for eksempel VPN-type – det er hensiktsmessig å behandle WLAN-forbindelser som Internett-forbindelser).
- ✗ Sikkerhetskrav til klientene (kan henviser til policy for sikring av Internett-klienter).
- ✗ Krav til fysisk sikring av aksesspunkter og annet nettverksutstyr.
- ✗ Hvem som har ansvaret for WLAN-sikkerhet og hvordan policyen og tilstøtende dokumenter blir vedlikeholdt.

Utarbeidelsen av en slik policy fremtvinger avklaring av en rekke forhold som ofte blir liggende til de dukker opp som en overraskelse – gjerne av negativ art.

I neste utgave er vi tilbake med konkrete anbefalinger i den forbindelse – hvilke valg som er optimale for en WLAN-installasjon når sikkerhet står i høyet.

100 Mbps til 100 mill. brukere

Du har neppe hørt om “100x100 Consortium”, og ei heller et par andre grupperinger i amerikanske akademiske miljøer (for eksempel Carnegie-Mellon University og MIT) som arbeider med neste generasjons Internett. Betegnelsen 100x100 signaliserer ambisjonene – 100 Mbps til 100 millioner brukere, og enkelte tror dette kan realiseres i løpet av 2007. Om så ikke skulle skje, er forskningen likevel nyttig, mener amerikanske myndigheter, som ad ulike kanaler sponser disse grupperingene.

Med 100 Mbps frem til den enkelte abonnent er blant annet tradisjonelt kabel-TV i ferd med å få sin avløsning. Vi får det vi trenger (digital-TV), når vi trenger det, via en Ethernet-kontakt i veggen – eller mer sannsynlig, via vårt private trådløse nettverk med sentral i kjelleren eller i gangen. Men veien frem er brolagt med store utfordringer. Vel har Internettet vokst raskt og mye, langt utover hva selv optimistene trodde var mulig for 10 eller 20 år siden, men det er grenser for hvor langt dagens teknologi lar seg strekke. Nettverket knaker allerede kraftig i sammenføyningene, ikke så mye på grunn av trafikken som på grunn av den enorme kompleksiteten. Uansett teknologi er det mye som skal fungere effektivt når en halv milliard eller flere noder skal kunne kommunisere uten videre og når som helst. Det hjelper lite med en 100 Mbps Ethernet-forbindelse i veggen dersom Internettet bryter sammen under belastningen.

Gigantiske rutere, som i virkeligheten er store datamaskiner med flere titalls prosessorer og et antall gigabytes hukommelse, håndterer i dag dirigeringen av trafikk i Internettet. Deres størrelse og kompleksitet sørger for at kun et fåtall leverandører har ressurser til å utvikle dem. Listen blir stadig kortere, mens produktene blir mer kostbare. Og mens forskerne krangler om det meste, er de fleste enige om at dagens rutingteknologi ikke skaleres.

Derfor er disse forskningsprosjektene nødvendige forutsetninger for at utviklingen skal kunne fortsette. Amerikanske myndigheter bruker anslagsvis 100 millioner USD per år på slik forskning – vesentlig mer enn resten av verden til sammen. Observasjonen er interessant fordi debatten om amerikanernes dominante posisjon i Internett-sammenheng fra tid til annen dukker opp. Den er naturlig, og det er fritt for hvem som helst å bruke ressurser på å ‘oppdage/utvikle fremtiden’. Så lenge amerikanerne betaler regningen er det ikke unaturlig at de også forblir dominerende.

Vi er ikke i tvil om at 100x100 lar seg realisere, men 2007 er neppe noen rimelig tidsramme. 2010 er langt mer sannsynlig. I mellomtiden fortsetter Internettet sin vekst, i kapasitet, trafikk, kompleksitet, utstrekning og antall brukere. Videre kan vi observere at dødsdommene har sittet løst for en lang rekke teknologier som i dag er totalt dominante. Ethernet, x86-arkitekturen og TCP/IP er gode eksempler. Kan det hende at 100x100 likevel lar seg realisere ved å oppjustere dagens teknologi? Vi tror ikke det, men utelukke det kan vi ikke.

PDAfonen danker ut din laptop

Vi – og mange med oss – har drømt høylydt om det en stund: Færre duppedingser, en enklere hverdag. Paradoksalt nok er det jo slik at alle disse duppedingene – telefon, PDA, laptop, Pendrive, digitalt kamera, fjernkontroll, m.m. –

skulle gjøre livet enklere. Nå viser det seg imidlertid at vi bruker mer tid på synkronisering av data og å løse alskens brukerproblemer, enn vi sparer på deres eksistens. Her må noget gjøres, og trendene er klare: Lommeutstyret konvergerer – og overtar stadig flere av funksjonene vår laptop har hatt.

Og nå er de her – snart. Apples iPod er et nærliggende eksempel, og utstyr med tilsvarende funksjonalitet kommer fra den ene etter den andre av kjente teknologileverandører: Palm/Handspring (Treo 600), Sony (Clie), Dell og andre. Utstyr som begynte sitt liv som MP3-spillere eller PDAer, er allerede blitt universalverktøy – med telefon, radio, fotoalbum, adresseregister, epost, nettleser, trådløs konnektivitet, diktafon, kamera, filmavspilling – og vi kan fortsette. Det eneste som mangler er tastatur, mus, stor skjerm – og litt programvare. Med Bluetooth- eller WLAN-konnektivitet skal det fint lite til før også dette er på plass. Er det rart Microsoft stresser for å få sine operativsystemer inn i telefoner og PDAer?

Vi kan inntil videre fortsette å drømme, men i løpet av 18 måneder har vi de første PDAfonene som også erstatter laptop'en her. Samtidig blir de hoved- eller bi-komponenter i stuens underholdningsanlegg. Og det skulle forundre oss om ikke en av de første kommer fra Apple. Følg med!

Wireless VoIP: Rett rundt hjørnet

Men vi har da diskutert produkter som gjør dette i snart to år allerede? Javisst, men forskjellen er betydelig mellom hva som er mulig og hva som er lett tilgjengelig. Og WVoIP er fortsatt ikke lett tilgjengelig selv om leverandører som SpectraLink, Symbol, Proxim og Trapeze har levert produkter i en periode. Som vanlig er problemet knyttet til standarder. De kommer for sent og er i noen tilfeller utilstrekkelige når de kommer.

Problemstillingen er både innlysende og velkjent. WLAN brukes som resten av lokalnettet. Brukerne ser ikke annen forskjell enn at det går saktere, men opplever degraderingen som en akseptabel pris å betale for å slippe kablene. Å blande telefoni inn i ligningen uten samtidig å ha prioriteringsmekanismer tilgjengelige, er imidlertid like smart som å sende et ilbud ut i rushtrafikken. Derfor er det nettopp prioriteringsmekanismer leverandørene vi nevnte ovenfor har introdusert i sitt utstyr. I mangel av standarder å holde seg til, har de laget sine egne, som fungerer greit nok innenfor samme produsents utstyr, men forøvrig er uanvendelige.

Situasjonen er hemmende for utviklingen, men nå nærmer en IEEE-standard seg ratifisering, hvilket forventes å endre situasjonen dramatisk. 802.11e definerer QoS-mekanismer for alle typer 802.11-nettverk, og tar vare på både telefoni, videostreamer og vanlig dataoverføring. Leverandørene står nærmest i kø med produktannonseringer, og 2 års erfaringer med proprietære produkter sørger for at de verste barnesykdommene allerede er luket ut fra teknologien. Nettopp derfor spås WVoIP å komme til syne på radarskjermen for alvor allerede i andre halvår i år.

Om vi trenger flere telefoner? Slett ikke. Tvert imot trenger vi færre, og WVoIP kan bidra i så henseende. Mobiltelefoner (og PDAfoner) som i tillegg til GSM/GPRS også støtter 802.11, ble demonstrert ved flere store teknologimesser i 2003. Med 802.11e på plass kan disse kombinerte apparatene komme frem fra kulissene. Så gjenstår det å se hvordan markedet reagerer.

VoIP-utfordringer

Nei, vi tenker ikke på norske fylkeskommuner som tydelig har vært uheldige med sine leverandørvalg. Vi sier ingen ting på at de sitter igjen med den oppfatning at teknologien er umoden, men sannheten er at umodenheten primært er å finne hos leverandørene. For kunden spiller det imidlertid liten rolle hvor problemet er, og vi kan ikke annet enn undre oss over leverandørens selvdestruktive håndtering.

Våre øyne går imidlertid i motsatt retning. Den eksplosive utviklingen og akseptansen av VoIP i markedet skaper et sett nye problemer for internasjonale teleselskaper og offentlige organer som skal kontrollere dem. Ikke bare ser teleselskapene at inntekspotensialet i tradisjonell telefoni eroderer raskere enn noen hadde drømt om. I Japan er det blitt så ille at noe må gjøres i løpet av året om ikke Nippon Telecom skal havne under økonomisk tvangsadministrasjon. Like ille er det – sett fra de involvertes sider – at voksende deler av telefonien havner utenfor myndighetenes kontroll. I Internettet og raskt voksende private IP-baserte nettverk, er tjenestene uregulert og utenfor myndighetenes kontroll, og ingen har klart å finne ut hvordan de kan kontrolleres. På en konferanse for slike regulerende myndigheter og teknologileverandører i Sveits nylig, gikk diskusjonen høyt, men var lite produktiv. Som en observatør fra det vi kan kalle Internett-siden formulerte det: “Den gamle tele-skolen er ute av stand til å fatte at telefoni ikke lenger er linjer, abonnementer og apparater. Deres referanserammer – teknologisk og praktisk – dekker rett og slett ikke dagens virkelighet – at en hvilken som helst PDA, MP3-spiller eller PC også er et telefonapparat.”

Derfor kom de heller ikke til noen konklusjoner eller konkrete planer som kan bringe dem tilbake i kontroll. At det legges ned store ressurser fra den kanten for å få nettopp kontrollen tilbake, kan vi imidlertid ta for gitt. Det er ingen selvfølge at utviklingen får fortsette like fritt som den har gjort de siste 20 årene. Årsaken til at reguleringer ikke har lagt en klam hånd over Internettet for lenge siden, er dets internasjonale, grenseløse karakter. Tiltak som ikke alle er med på, vil automatisk falle i grus fordi de berørte partene så lett kan flytte seg til andre jurisdiksjoner. Filtrering og tvang er nytteløst fordi de fleste (i alle fall vestlige) land har grunnlover som setter en stopper for slike metoder.

Betydelig spenning knytter det seg imidlertid til fremtiden for generell telefoni – nasjonalt og internasjonalt. Sterke interesser og store penger er involvert, nye aktører truer med å forvise de tradisjonelle til statistroller, og veksten er stor – som illustrert av ferske resultater fra for eksempel Northern Telecom. Selskapet overrasket nylig markedet med gode tall, og anførte uventet sterk vekst innen nettopp VoIP som en av årsakene. Slikt blir lagt merke til.

AntiVirus-produkter: Notoriske SPAMmere

Har du noen gang fått epost fra et antivirus-program med beskjed om at din maskin er infisert? De fleste av oss har det, og vi tar slike meldinger på alvor. Det kan vi like godt slutte med. Vi kaster bort tiden. De fleste antivirus-programmer er notoriske SPAM-kilder som helt unødvendig fyller opp våre postkasser med reklame forkledd som advarsler om at vi har virus.

Mekanismene fungerer som følger: De fleste moderne virus bruker epost som spredningsmekanisme. Likeledes har de det til felles at de lager falske avsenderadresser og benytter tilforlatelige emnefelt som skal øke sannsynligheten for at naive brukere åpner vedlegget. Antivirus-programmene skal stoppe slike

meldinger så snart virus-signaturen er kjent, og gjør som regel det. Når et slik virus oppdages, sender programmet en advarsel tilbake til avsender av meldingen, med påstand om at vedkommende har virus og bør sjekke sitt system. Siden avsenderadressen er falsk, havner imidlertid denne returnmeldingen hos en helt annen enn den egentlige virus-sprederen, og er derfor både meningsløs og innholdsmessig feilaktig.

Og her begynner det å bli interessant: I antivirus-selskapenes beskrivelser av disse virusene står det i klartekst at de lager falske adresser. Likevel sender programmene ut sine advarsler – til de anerkjent falske adressene – der de i tillegg til påstander og advarsler, promoterer selskapets produkt. Dette er ikke noe annet enn SPAM, og det genereres millioner av slike meldinger hver eneste dag. Det hjelper lite at programmene har muligheter for å 'slå av' slike responser når de har 'på' som standardverdi, og brukere flest aldri finner frem til verken hvordan eller hvorfor de skulle forandre en slik innstilling. Dette er i beste fall useriøst. Så lenge situasjonen vedvarer er den riktige håndteringen av slik epost å registrere den som SPAM eller virus, og la den bli automatisk filtrert. Ironien blir komplett når produkter fra McAfee brukes til å filtrere sin egen epost, og tilsvarende for Symantec, RAV og så videre.

[En grundig analyse av problemet, med eksempler, er å finne på <http://www.attrition.org/security/rant/av-spammers.html>]. ■