SecLab
laboratorio di idee sulla sicurezza ICT
Newsletter di Secure Edge - your safety .net

Anno I - numero 1 - 17 gennaio 2003

Wireless LAN: pros and cons

di Sandro Fontana - sfontana@secure-edge.com

Come vi sentireste se il responsabile della rete aziendale vi mostrasse con orgoglio alcuni socket RJ45, connessi direttamente al vostro cabling aziendale, opportunamente predisposti nel parcheggio davanti al vostro ufficio e nel bar dietro l'angolo? Non trovate che sarebbe comodissimo navigare sulla vostra rete, inviare la posta e magari connettersi a Internet da questi luoghi?

Se qualche vostro collega vi dicesse una cosa del genere è probabile che cerchereste la telecamera nascosta. Dopotutto nessuno è così pazzo da fare cose di questo genere, vero?
In linea teorica no, ma dal punto di vista pratico non c'è nessuna differenza tra uno scenario come quello appena descritto ed installare una WLAN nella vostra azienda senza chiedere il parere al vostro Security Officer ed al vostro amministratore di rete.

La sicurezza intrinseca dello standard IEEE 802.11b è praticamente nulla ed in questo modo voi state per mettere la rete della vostra azienda a disposizione di chiunque abbia a disposizione un kit di ricezione.

Da un anno a questa parte, cioè da quando la tecnologia ha iniziato la sua diffusione a livello consumer e da quando sono iniziati i dibattiti e le dimostrazioni [1] sulla intrinseca mancanza di sicurezza di questo protocollo, non è cambiato praticamente nulla: installare una wireless LAN equivale ancora a cablare il parcheggio pubblico di fronte all'ufficio direttamente con la vostra rete interna.

Anche il WEP [Wired Equivalent Privacy] algorithm ha mostrato la sua piena debolezza [2], ed è quindi oggi una tesi accettata che le WLAN costituiscono un rischio molto serio alla sicurezza ICT.

E quale è il problema? Buttiamoci l'IEEE 802.11x, il WiFi, gli AP [Access Point], il WEP e gli altri acronimi relativi a queste tecnologie dietro le spalle e torniamo al nostro lavoro.

Spiacenti, ma non sarà così facile, o meglio non sarà possibile: un altro vaso di Pandora è stato aperto e richiuderlo non servirà a molto.

Come molte altre tecnologie potenzialmente pericolose per la sicurezza ICT, anche questa presenta una serie di vantaggi e benefici a cui gli utenti ed ahimè, anche noi stessi non vorremo rinunciare:

- Mobilità: accesso alle informazioni in tempo reale da qualsiasi posto (e non solo) dell'Azienda. La mobilità è a supporto della produttività e ad opportunità di servizi non erogabili tramite le reti wired.
- Facilità di installazione: installare una WLAN è facile e veloce (anche troppo) e naturalmente elimina la necessità di far passare cavi nell'edificio.
- Flessibilità: la tecnologia wireless permette alla rete di andare anche dove i cavi non potrebbero o comunque di farlo a costi vicini allo zero.
- Costi minori: anche se l'investimento iniziale di hardware necessario ad una WLAN è superiore al costo necessario ad una rete wired, i costi legati alle spese di installazione, gestione e manutenzione possono essere significativamente più bassi, specialmente se teniamo presente la nostra sempre crescente propensione agli ambienti dinamici, che richiedono frequenti variazioni della rete.
- Scalabilità: gli amministratori di rete possono configurare i sistemi di WLAN in varie topologie per adeguarsi alle specifiche installazioni ed applicazioni. La capacità di configurazione si applica bene a partire dalle reti peer-to-peer con pochi utenti ad importanti infrastrutture di rete con centinaia o migliaia di utenti.

Quello che rimane da fare è imparare a convivere con le WLAN, il che significa capirne le ragioni, le potenzialità e le possibilità di gestione.

Suddividiamo di massima due tipi di necessità:

1. Gateway di accesso ad Internet: tipicamente un servizio che può/potrà essere dato in aeroporti, alberghi, Internet Café, treni, teatri e cinema, ristoranti, stadi ecc. I visitatori esterni (i clienti) saranno i benvenuti ed il problema si sposterà sulle modalità di identificazione del cliente stesso e sul corretto billing dei servizi erogati: tipicamente la navigazione su Internet.
A rischio di apparire troppo semplicistico, penso che le problematiche sopra definite potrebbero essere risolte a livello applicativo, tramite un sistema di accesso tramite proxy-web basato su SSL ed identificazione tramite userid/password per l'autenticazione degli utenti/clienti, la gestione dei permessi di accesso ai servizi erogati e la loro contabilizzazione.

2. Gateway di accesso alla LAN aziendale: le potenzialità di esposizione a minacce esterne all'azienda sono enormi. La prima cosa da fare è sensibilizzare tutti sui rischi impliciti ed intrinseci della tecnologia e definire subito delle chiare policy che vietino il fai da te e che prevedano ispezioni ("probe") a sorpresa nelle aree aziendali (anche nelle vicinanze di queste) alla ricerca di WLAN non autorizzate.
La seconda cosa da fare è definire i requirements relativi ad una richiesta di WLAN. In prima istanza la soluzione sarebbe trattare questo gateway come un

ulteriore punto di ingresso untrusted alla pari di Internet, quindi posizionare gli AP sulla semi-DMZ, comunque su una delle subnet al riparo del firewall di frontiera.
In queste condizioni non ci sono differenze tra gli accessi che avvengono direttamente da Internet e quelli che arrivano dalla rete Wireless: tutte le difese necessarie sono state approntate e per quanto riguarda gli utenti abilitati, tutti i sistemi di autenticazione per accettare connessioni remote da Internet andranno bene anche in questo caso.
I client potrebbero quindi accedere tramite browser con la sicurezza fornita da SSL, ovvero dotarsi di un software per implementare una VPN basata su IPSec.

L'alternativa a questa configurazione è quella di avere un AP direttamente connesso alla rete interna tramite router, switch o hub; la definizione per questa architettura è WEL [WLAN-Extended LAN].
In questo caso gli AP agiscono come un hub, disponibile a chiunque, per un accesso Wi-Fi alla LAN aziendale, con tutte le conseguenze del caso.

Il minimo da fare è attivare tutte le features di sicurezza sull'AP, che come abbiamo detto sono scarse:

- Eliminare il brodcast dell'SSID [Service Set Identifier] e cambiarne il valore di default;
- Abilitare il WEP con chiavi di lunghezza 128bit (tenendo presente che i 128 bit non bastano a farci stare tranquilli [3]);
- Se il vostro fornitore l'ha implementato, utilizzare il controllo sull'indirizzo di MAC della scheda client, anche se questa tecnica è di pesante gestione; inoltre data la facilità di eavesdropping su questa rete, anche questo meccanismo di sicurezza non ha molto significato;

In pratica, quello che realmente dovremmo fare è non permettere l'installazione di una WEL, a meno di non avere a disposizione due cose:

- ragioni veramente particolari per questa architettura
- un investimento adeguato per aumentare il livello di sicurezza.

L'investimento dovrà riguardare l'EAP [Extensible Authentication Protocol], un'estensione del Radius che risiede nel layer 2 dello standard di autenticazione presente nell'802.1X e quindi è presente implicitamente negli apparati WLAN.

Con questa architettura i client che vogliono accedere alla LAN devono autenticarsi al server Radius tramite una coppia userid/password o meglio ancora tramite una implementazione challenge/response; il server Radius fornirà una chiave WEP di sessione, che verrà condivisa con l'AP, aumentando il livello di sicurezza rispetto alla chiave WEP statica

Una via equivalente a questa, che si sta diffondendo in attesa che l'IEEE emetta le specifiche 802.11i [4], è quella raccomandata dalla Wi-Fi Alliance, il WPA [Wi-Fi Protected Access].

Il sistema lavora usando l'EAP, ma la richiesta di autenticazione al server Radius viene attivata dall'AP, che agisce da engine-in-the-middle; il sistema prevede che il client e l'AP siano entrambi abilitati all'uso del WPA: la Wi-Fi Alliance dichiara che i prodotti certificati Wi-Fi avranno il WPA build-in a partire da febbraio 2003.

Il WPA permetterà un certo livello di sicurezza migliore del WEP anche per chi non vorrà/potrà dotarsi di un server Radius: in questo caso non ci saranno chiavi dinamiche WEP di sessione, in compenso ogni singolo client potrà comunque avere la sua chiave WEP univoca.

Il WPA non è comunque la perfezione; un white paper della Intel [5] ha già documentato la particolare vulnerabilità del WPA agli attacchi DoS (naturalmente tutti i sistemi WLAN sono comunque soggetti a DoS a livello degli AP).

Per concludere, se proprio non potete fare a meno di usare una WLAN, almeno mettetela nella semi-DMZ; se questo non è possibile datevi da fare per aumentare in qualcuno dei modi descritti in precedenza il livello di sicurezza finale.

Indipendentemente da questo, parlate chiaramente all'interno della vostra azienda dei pericoli delle reti wireless, fate cultura e magari stressate in una certa misura la situazione; dopo di che, procuratevi un War-Driving Kit, ed iniziate ad esplorare i dintorni della vostra azienda; fatelo spesso e naturalmente senza avvisare nessuno e se scoprite una rete presente, prima di urlare al fuoco, accertatevi che sia implementata da voi e non da qualche altra azienda.

❖

[1] War Driving by the Bay, 20 Apr. 2001, http://www.theregister.co.uk/content/8/18285.html
[2] Security of the WEP Algorithm,, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[3] http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
[4] L'IEEE 802.11 Task Force I sta decidendo su questo migliore e più sicuro standard per le WLAN: tra l'altro questo utilizzerà AES al posto di RC4; si attende la fine 2003 per la definizione ultima dello standard; l'ipotesi di delivery dei prodotti conformi all'802.11i è per metà del 2004
[5] http://www.wired.com/news/business/0,1367,56350,00.html