

ALLARME WIFI: IL 70% DELLE AZIENDE CHE UTILIZZANO WIRELESS E' ESPOSTO ALLE INTRUSIONI.

Lo rivela un'indagine dell'Osservatorio Nazionale per la Sicurezza Informatica

Autore: Quirisparmio

Il rischio è anche che il proprio indirizzo IP sia utilizzato da malintenzionati per compiere malefatte. E' quanto emerge da una indagine compiuta dall'Osservatorio Nazionale per la Sicurezza Informatica, struttura no profit promossa dalla trevigiana **Yarix** in collaborazione con altre aziende del settore.

La tecnologia **wireless** sta ormai dilagando, complice il costo dell'hardware sempre più basso e la semplicità di installazione, però pochi tengono conto che le reti wireless se non correttamente configurate sono assai più vulnerabili del classico cavo.

Yarix insieme all'Osservatorio ha condotto un'indagine nelle principali città del veneto per scoprire quanti "spot" , **ossia quante connessioni senza fili, sono aperti e utilizzabili da chiunque voglia agganciarsi.** Questa tecnica, usata anche dagli **hacker**, è detta "**Wardriving**" e consiste appunto nello scansionare con attrezzature di facile reperibilità spot wifi "aperti". Gli spot aperti sono porte aperte sulle aziende o sui PC dei privati: permettono con estrema facilità di entrare nella rete e nei PC, di intercettare dati sensibili come le password dei conti bancari o i codici delle carte di credito. Il panorama che è emerso dall'indagine è preoccupante: a Treviso Centro Città 27 hot spot wireless completamente aperti e vulnerabili (1 è anche di una nota banca del centro città); a Belluno 12 hot spot ; a Venezia 32; Vicenza 28 Verona 26.

In totale il 68% degli "spot" trovati sono aperti o comunque facilmente accessibili. "Questa situazione è molto grave - ha dichiarato Mirko Gatto dell'Osservatorio - Immaginiamo non solo cosa possa significare entrare liberamente nella rete di una banca, ma anche quali pericoli corrono gli ignari utenti: qualcuno potrebbe utilizzare il loro IP (la carta di identità di chi naviga su internet) per commettere reati, scambiare file illegali, commettere truffe.

Qualcosa si è cercato di fare con il famoso decreto Pisanu Decreto Legge 27 luglio 2005, n.144 Misure urgenti per il contrasto del terrorismo internazionale, ma questo decreto riguarda solo gli enti pubblici che forniscono connettività ai propri clienti. Tutti gli altri devono fare da soli e fare pure in fretta".

[2007-05-24 15:39:57]