Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di martedì 18 novembre 2014

SOLUZIONI TECNOLOGICHE

Wi-Fi pubblici, occhio alle reti non protette!

di **Teamsystem.com**

Chi viaggia spesso o partecipa a eventi e conferenze, considera sempre con grande favore la presenza di una **rete Wi-Fi libera** alla quale collegarsi e scaricare la posta, soprattutto quando ci si trova all'estero e non si vuole pagare una connessione in roaming con il proprio cellulare. Lo hanno capito anche i gestori dei locali pubblici che sempre più spesso offrono questo servizio ai clienti. In alcuni casi, però, l'ansia di offrire qualcosa in più si trasforma in un vero boomerang. È il caso di chi tiene la rete Wi-Fi "aperta", **senza prevedere una password per l'accesso**. Il collegamento è immediato, ma i rischi per la sicurezza sono altissimi. Chiunque, infatti, potrebbe intercettare le nostre comunicazioni.

A che cosa serve la password sul Wi-Fi

Esistono due ottimi motivi per usare una password per la rete senza fili. La prima è evitare il **collegamento agli sconosciuti** che potrebbero usare il Wi-Fi a nostra insaputa. Questa, però è solo la più ovvia delle conseguenze della protezione con password. La funzione più importante della password è invece quella di permettere la **codifica dei dati che vengono trasmessi**. Se non la usiamo, tutte le informazioni inviate e ricevute tra il dispositivo utilizzato e il router che ci collega a Internet risultano infatti **trasmesse "in chiaro"**, col rischio che qualche malintenzionato le intercetti e si impossessi di dati riservati.

Il problema è stato denunciato già qualche anno fa, quando ha fatto la sua comparsa su Internet **FireSheep**, un'estensione di **Firefox** disponibile gratuitamente. FireSheep permette di controllare le trasmissioni all'interno di una rete Wi-Fi e intercettare le informazioni di accesso a numerosi servizi, come **Gmail**, **Facebook** e molti altri. Per usarla non è necessario essere un **hacker** e nemmeno conoscere un linguaggio di programmazione. L'estensione si installa con facilità. Per usarla, basta accedere con il computer a una rete senza fili non protetta da password e aspettare. Ogni volta che qualcuno collegato alla stessa rete Wi-Fi si connette a un servizio online, **FireSheep intercetta i dati di accesso** (nome utente e password) **e li memorizza**.

Le società che gestiscono i vari servizi online hanno adottato alcuni accorgimenti per bloccare il fenomeno. Quasi tutti, infatti, hanno cominciato a usare **connessioni "sicure" basate sul protocollo SSL**, lo stesso utilizzato dai sistemi bancari online. Possiamo accorgercene facilmente controllando l'indirizzo nella barra del nostro browser. Quando all'inizio vediamo la sigla "**HTTPS**", sappiamo che si tratta di una connessione sicura. Anche se Facebook e Gmail sono più protetti, lo stesso non vale per molti altri siti e per altri dati che inviamo dal nostro

computer, per esempio le email. Molti servizi, infatti, non utilizzano un sistema di comunicazione sicura. Lo stesso vale per alcune chat e altri programmi. Il rischio, poi, è ancora più alto da quando **molti siti permettono di accedere ai propri servizi usando il nostro profilo di Facebook**. Anche se il social network ha introdotto il sistema di protezione HTTPS, un pirata che controlla la rete senza fili a cui siamo connessi può ottenere i dati di accesso a Facebook attraverso un altro sito o servizio.

Rischi sempre più elevati

Dai tempi di FireSheep è passato ormai qualche anno e su Internet sono comparsi numerosi programmi con funzioni simili o anche molto più efficaci. Esistono anche app per **Android**, come **Password Sniffer Spy 2.0**, che operano esattamente allo stesso modo. Nello stesso tempo, gli esperti di sicurezza hanno scoperto che il **protocollo SSL** ha delle vulnerabilità che potrebbero essere usate per decodificare le informazioni trasmesse al sito Web. Se un pirata informatico riuscisse a sfruttare questa debolezza, l'uso di connessioni protette non sarebbe più una garanzia sufficiente per evitare che qualcuno acceda ai nostri dati segreti. Ciò che ci protegge davvero, in realtà, sono **i protocolli WPA e WPA 2**. Si tratta dei sistemi di **codifica dei dati nelle reti Wi-Fi** che tutti i router permettono di attivare attraverso le impostazioni. Il problema è che, senza una password, questi protocolli non possono funzionare. Il loro scopo è codificare i dati trasmessi e ricevuti usando una **chiave crittografica** che viene creata, appunto, usando la password. Per proteggere la trasmissione dei dati è quindi indispensabile impostare una parola d'accesso. Come fare, allora, per consentire l'uso di Internet ai visitatori di un locale pubblico? Per fortuna, i sistemi di crittografia WPA e WPA 2 usano la password in maniera "intelligente". La codifica dei dati viene fatta attraverso complessi algoritmi e chiavi crittografiche aggiuntive. Questo significa che, anche se un pirata informatico conosce la password di accesso, non potrà comunque "leggere" i dati trasmessi all'interno di una rete senza fili. Anche usando software specializzati e un computer molto potente, **la loro decodifica potrebbe richiedere dei giorni o addirittura mesi**.

Chi gestisce uno spazio pubblico e vuole permettere a tutti di collegarsi alla propria rete Wi-Fi, potrebbe proteggere la rete con una password, magari indicandola chiaramente con un cartello ben visibile appeso nei locali che gestisce. In questo modo chiunque si potrà collegare proprio come se avesse a disposizione una rete aperta, ma le comunicazioni che viaggiano al suo interno saranno a prova di intercettazione. Se però ci accorgiamo che la rete Wi-Fi che stiamo per usare non ha una protezione, evitiamo semplicemente di collegarci. Il rischio sarebbe davvero troppo elevato. Molto meglio utilizzare il nostro traffico dati.