OUCH! | Gennaio 2014

Newsletter mensile di suggerimenti sulla sicurezza informatica

# OUCH!

IN QUESTO NUMERO...

- La tua rete wireless
- OpenDNS
- I dispositivi

# La sicurezza della rete di casa

## Introduzione

Fino a non molti anni fa, le reti casalinghe erano relativamente semplici: nulla di più di un punto di accesso wireless e uno o due computer usati per navigare in Internet o giocare online. Nel corso degli anni, alcune reti sono diventate più complesse: non solo possono ospitare un maggior numero di dispositivi, ma il loro utilizzo si è esteso anche ad altri scopi. In questo numero parleremo di alcuni concetti di base che ti permetteranno di rendere più sicura la tua rete.

### L'autore di questo numero

Kevin Johnson è CEO di Secure Ideas, gestisce MySecurityScanner.com ed è istruttore senior del SANS Institute. Potete trovare maggiori informazioni su **www.secureideas.com**.

## La tua rete wireless

La maggior parte delle reti casalinghe è wireless (reti Wi-Fi) Una rete Wi-Fi permette di collegare senza fili a Internet ogni tuo dispositivo, dai laptop ai tablet, dalle console di gioco alla televisione. Perché ciò accada, la tua rete necessita di ciò che viene denominato un punto di accesso (access point). Si tratta di un dispositivo fisico che ti connette al router Internet (a volte è inserito all'interno dello stesso router) e che è in grado di comunicare con i dispositivi che vi si connetteranno. Una volta collegati al punto di accesso, questi dispositivi potranno sia accedere ad Internet sia comunicare tra loro. Il punto di accesso diventa quindi una componente essenziale della rete casalinga, per cui ti raccomandiamo di seguire i seguenti suggerimenti per renderlo più sicuro.

- Per la maggior parte dei modelli di access point l'utente e la password di amministrazione sono ben conosciuti e spesso pubblicati su Internet. Per questo motivo devi cambiare la password dell'amministratore non appena installi il dispositivo. È inoltre opportuno che questa password non venga utilizzata per altri account.
- Una seconda opzione da configurare è il nome della rete (denominato SSID). Questo è il nome che i tuoi dispositivi vedranno nella fase di ricerca di una rete wireless locale. Assegna alla rete un nome che sia unico, in modo da poterlo identificare facilmente, e che al contempo non contenga informazioni personali. Configurare una rete come nascosta (o non-broadcast) non offre una grande protezione: molti strumenti di analisi della rete e tutti gli hacker mediamente esperti sono in grado di scoprire facilmente i dettagli di ogni rete nascosta.

© The SANS Institute 2013

# La sicurezza della rete di casa

- Il passo successivo consiste nel fare in modo che solo persone di fiducia possano collegarsi e usare la tua rete, e che i collegamenti siano protetti dalla crittografia. Se vuoi essere sicuro che vicini ed estranei non possano collegarsi devi abilitare la sicurezza forte sul punto di accesso. Attualmente il modo migliore è l'impiego di meccanismi come il WPA2: attivandolo, farai in modo che per ogni collegamento alla tua rete di casa venga richiesta una password. Le connessioni stabilite, una volta autenticate, saranno anche cifrate. Non utilizzare protezioni vecchie e superate come il WEP e non lasciare la rete aperta senza protezione alcuna: così facendo permetteresti a chiunque di collegarsi senza dover inserire la password di accesso.

*Per proteggere la tua rete di casa configura le opzioni di sicurezza , usa OpenDNS o un servizio simile e verifica che tutti i dispositivi connessi siano aggiornati.*

- Assicurati che la password utilizzata per collegarti alla rete sia forte, difficile da indovinare e che sia diversa da quella di amministrazione. Ricorda che questa password dovrà essere inserita una volta sola per ognuno dei tuoi dispositivi, poiché verrà conservata nella loro memoria interna.
- Molti punti di accesso wireless supportano la cosiddetta "rete per gli ospiti" (guest network). Questo tipo di rete permette appunto a ospiti o visitatori di sfruttare il tuo punto di accesso per connettersi ad Internet, senza però potersi collegare ai tuoi dispositivi personali connessi alla rete casalinga. Se aggiungi una guest network, ricorda di abilitare la protezione WPA2 e utilizza una password diversa da quella della rete principale.
- Se non riesci a ricordare le diverse password,usa un password manager per conservarle in modo sicuro.

## OpenDNS

Una volta che la tua rete wireless è operativa, ti raccomandiamo di configurarla per fare in modo che il servizio DNS si appoggi a OpenDNS (o a un servizio simile, come Norton ConnectSafe for Home). Quando digiti un indirizzo nel tuo browser viene utilizzato il servizio DNS per capire a quale server su Internet collegarsi. I servizi come OpenDNS identificano i siti web infetti e impediscono a ogni device collegato alla tua rete di visitare accidentalmente questi siti. Inoltre, questo servizio ti permette di filtrare e bloccare siti web dai contenuti sgradevoli o offensivi. Ciò che rende questo approccio efficace è che non è necessario installare nessun software sui device, poiché tutto si basa sulla modifica di un parametro di configurazione del punto di accesso.

© The SANS Institute 2013

# La sicurezza della rete di casa

## I tuoi dispositivi

Il prossimo passo consiste nel sapere che cosa è collegato alla tua rete casalinga e assicurarti che ogni dispositivo sia sicuro. Dovrebbe trattarsi di un compito semplice, perché non sono molti i dispositivi collegati, sebbene oggi siano sempre di più gli oggetti che possono connettersi a una rete wireless: non solo computer e tablet, ma anche televisori, console di gioco, monitor per neonati, termometri, ecc. Una volta identificati tutti i dispositivi sulla rete di casa, potresti essere sorpreso da quanti sono. Il miglior modo per renderli sicuri è di verificare che siano sempre aggiornati all'ultima versione del loro sistema operativo. Imposta gli aggiornamenti automatici dove possibile. Se non lo dovesse essere, aggiorna manualmente ogni mese il dispositivo. Infine, visita il sito del tuo Internet provider poiché potrebbe offrire strumenti e servizi gratuiti per rendere più sicura la tua rete.

## Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
http://www.securingthehuman.org

## Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

## Risorse

OpenDNS: http://www.opendns.org

Norton ConnectSafe: http://dns.norton.com/dnsweb/dnsForHome.do

Network security scanner: http://www.sophos.com/it-it/products/free-tools/network-security-scan.aspx

Password Manager: http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

OUCH! è pubblicata dal progetto Securing The Human del SANS Institute e viene distribuita con licenza Creative Commons BY-NC-ND 3.0.
Sei libero di distribuire questa newsletter o utilizzarla nei tuoi programmi di awareness senza però modificarne i contenuti.
Per traduzioni o ulteriori informazioni, contatta ouch@securingthehuman.org.

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis