OUCH! | Febbraio 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Proteggere la rete di casa

Introduzione

Fino a pochi anni fa, le reti casalinghe erano piuttosto semplici, costituite spesso da nulla di più di un hotspot wireless e uno o due computer per navigare in Internet, acquistare online e giocare. Le reti attuali sono molto più complesse: colleghiamo molti più dispositivi che usiamo per gli scopi più svariati. In questa newsletter capiremo come rendere sicura la rete di casa alla luce degli sviluppi degli ultimi anni.

L'autore di questo numero

Cheryl Conley guida il team di Security Education and Awareness in Lockheed Martin, azienda nella quale ha promosso una campagna di awareness per i 100.000 dipendenti, in cui sono previsti focus group e un programma di phishing globale. Seguite Cheryl su **@conleychera**.

La rete wireless

Ogni rete casalinga ha inizio con una rete, detta anche Wi-Fi, che vi permette, senza bisogno di cavi, di collegare a Internet ogni dispositivo, dal laptop ai tablet, dalla console di gioco alla televisione. La maggior parte delle reti wireless sono controllate dal vostro router, che è il dispositivo che il vostro fornitore di servizio Internet installa a casa vostra per collegarvi alla rete. La vostra rete può essere controllata da un sistema separato, chiamato Wireless access point collegato a sua volta al vostro router. Entrambi i dispositivi lavorano allo stesso modo, diffondendo segnali wireless. I vari dispositivi a casa vostra si connettono alla rete mediante questi segnali e, da lì, a Internet e anche tra di loro. Rendere sicura la vostra rete è una parte fondamentale nella protezione della vostra casa. A questo scopo, vi raccomandiamo di seguire le seguenti indicazioni.

- Cambiate la password di amministratore di default del router o dell'access point wireless. L'account di amministratore è ciò che vi permette di configurare la rete wireless. Il problema è che molti router Internet vengono installati con le credenziali di default, che sono ben conosciute e spesso pubblicate su Internet, dove diventano facile preda di istinti malevoli. Per questo motivo dovete impostare una password forte per l'amministratore
- Modificate il nome di default della vostra rete wireless, denominato anche SSID. Si tratta del nome che i vostri dispositivi vedono quando ricercano una rete. Battezzate la vostra rete con un nome facilmente identificabile,

Proteggere la rete di casa

ma assicuratevi che non contenga informazioni personali. Potete anche impostare la rete come nascosta (rete non-broadcast), sebbene esistano molti strumenti di hacking in grado di identificare anche le reti configurate in questo modo

- Fate in modo che solo persone di fiducia si possano collegare alla vostra rete, e che le connessioni siano protette da crittografia, abilitando la sicurezza forte. Attualmente, la miglior opzione è di usare il protocollo di sicurezza WPA2: attivandolo, verrà richiesta una password al momento del primo collegamento. Non usate metodi di sicurezza obsoleti come il WEP, o, peggio, nessuna sicurezza, che equivale a una rete aperta a tutti senza autenticazione
- La password usata per la connessione alla rete deve essere forte e diversa da quella dell'account di amministrazione. La userete una volta sola quando configurerete la connessione di rete per la prima volta sul vostro dispositivo: essa poi verrà conservata per i collegamenti successivi
- Molte reti wireless supportano la cosiddetta "Guest network", che permette ai visitatori di collegarsi a Internet attraverso una rete supplementare, proteggendo così la vostra rete principale da sguardi indiscreti. Anche su questa rete dovrete abilitare la protezione mediante WPA2 e assegnare una password diversa da quella della rete casalinga
- Disabilitate il Wi-Fi Protected Setup o altri meccanismi che permettono il collegamento di ogni dispositivo senza conoscere la password della rete e le impostazioni di configurazione
- Se avete difficoltà a ricordare tutte le vostre password, vi raccomandiamo di usare un password manager per conservarle al sicuro

Per proteggere la tua rete di casa, rendi sicura la rete Wi-Fi, aggiorna tutti i dispositivi e proteggili con una password.

Non siete sicuri su come agire? Chiedete pure al vostro fornitore di servizio, controllate la documentazione tecnica che accompagna il vostro router o l'access point o consultate il sito web del produttore.

I dispositivi

Il prossimo passo consiste nel sapere cosa è connesso alla rete di casa e rendere sicuro ogni dispositivo, operazione semplice quando si hanno pochi dispositivi, ma sempre più complessa nel nostro mondo "sempre connesso", in cui ogni

Proteggere la rete di casa

cosa è collegabile, ivi incluse le TV, le console di gioco, i monitor per bambini, i sistemi audio, gli elettrodomestici e anche la vostra auto. Un modo semplice per scoprire cos'è collegato alla rete è di utilizzare uno scanner come Fing: quest'app, che potete installare sul computer o sullo smartphone, esegue uno scan della rete per individuare ogni device connesso. Una volta individuati i dispositivi sulla rete, dovrete fare in modo che ognuno di essi sia protetto. Il miglior modo per farlo è che ognuno di essi abbia aggiornato il sistema operativo o il firmware. Se possibile, attivate gli aggiornamenti automatici. Se ognuno dei vostri dispositivi richiede una password, usatene una unica e forte. Consultate anche il sito del vostro provider: potreste trovare utili strumenti gratuiti per aiutarvi in questa situazione.

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

Le Passphrase:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_it.pdf
I Password Manager:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_it.pdf
Tablet e sicurezza:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_it.pdf
Proteggere la rete wireless:	https://www.navigaweb.net/2014/12/proteggere-la-rete-wireless-da.html

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