SANS SECURITY AWARENESS
ITALTEL
OUCH! | Gennaio 2018
La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per tutti

OUCH!

IN QUESTO NUMERO...

Come creare una casa cyber sicura

Introduzione

Diversi anni fa creare una casa che fosse sicura dal punto di vista informatico era semplice; La maggior parte delle case era costituita da non più di una rete wireless e alcuni computer collegati ad essa. Oggi la tecnologia è diventata più complessa ed è parte integrante delle nostre vite, dai cellulari e le console dei videogiochi ai termostati e forse i vostri frigoriferi. Di seguito troverete quattro semplici passi da seguire per creare una casa sicura.

L'autore di questo numero

Matt Bromiley è un esperto nella gestione degli incidenti informatici e aiuta i clienti di tutte le dimensioni a gestire le violazioni dei dati. È anche un istruttore SANS e insegna per FOR508 il corso "Advanced Digital Forensics and Incident Response. Segui **Matt@mbromileyDFIR**

La vostra rete wireless

Quasi tutte le reti domestiche iniziano con una rete wireless (o Wi-Fi). Questo è ciò che consente a tutti i vostri dispositivi di connettersi a Internet. La maggior parte delle reti wireless domestiche sono controllate dal vostro router Internet o da un access point wireless dedicato e separato. Entrambi funzionano allo stesso modo, trasmettendo segnali wireless; i dispositivi all'interno della tua casa si collegano tramite questi segnali. Questo significa che mettere in sicurezza la vostra rete wireless è un elemento chiave per proteggere la vostra abitazione. Di seguito vi raccomandiamo i passaggi per rendere sicura la vostra casa.

- Cambiate la password dell'amministratore predefinita del vostro router Internet o del vostro access point wireless, a prescindere da chi controlla la vostra rete wireless. L'account amministratore è quello che ti consente di configurare le impostazioni per la tua rete wireless.
- Assicuratevi che solo le persone di cui ti fidi possano connettersi alla tua rete wireless. Questo si ottiene abilitando delle funzioni che rendono più robusta la rete. Attualmente l'opzione migliore è usare il meccanismo di sicurezza chiamato WPA2. Una volta abilitato il WPA2 sarà necessaria una password per consentire alle persone di connettersi alla rete domestica e, una volta collegate, le loro attività online saranno cifrate.
- Assicuratevi che la password utilizzata per connettersi alla rete wireless sia complessa e che sia differente da quella dell'amministratore. Ricordate che dovrete inserire la password una sola volta per ciascuno dei vostri dispositivi, poiché questi ultimi memorizzano e ricordano la password che avete impostata.
- Molte reti wireless supportano quella che viene definita una rete ospite o Guest. Ciò consente ai visitatori di connettersi a Internet, ma protegge la rete domestica in quanto non possono connettersi a nessuno degli altri

Come creare una casa cyber sicura

dispositivi sulla rete domestica. Se aggiungete una rete ospite, assicuratevi di abilitare WPA2 e una password dedicata per questa rete.

Non vi sentite preparati per effettuare queste configurazioni? Chiedete al vostro fornitore di servizi Internet oppure controllate il loro sito web, controllate la documentazione fornita con il vostro router Internet o l'access point wireless o anche in questo caso fate riferimento al loro sito web.

Segui questi quattro semplici passi per creare una casa cyber sicura; proteggi la tua rete wifi, abilita gli update automatici, usa passphrase dedicate ed abilita i backup.

I vostri dispositivi

Il passo successivo è sapere quali dispositivi sono collegati alla rete domestica wireless e assicurarsi che tutti questi dispositivi siano sicuri. Questo approccio era semplice quando sulla rete era presente solo un computer o due. Tuttavia oggi quasi tutto può connettersi alla rete domestica, inclusi smartphone, TV, console di giochi, baby monitor, altoparlanti o forse persino la tua auto. Una volta identificati tutti i dispositivi sulla rete domestica, assicuratevi che ognuno di essi sia sicuro. Il modo migliore per garantire la loro sicurezza è garantire che ciascuno di essi abbia abilitati gli aggiornamenti automatici. I cyber criminali trovano costantemente nuovi punti deboli nei vari dispositivi e sistemi operativi. Con gli aggiornamenti automatici, il computer ed i dispositivi gireranno sempre sul software più aggiornato, il che rende molto più difficile l'accesso da parte di chiunque.

Password

Il prossimo passo è usare una password robusta e unica per ciascuno dei tuoi dispositivi e account online. Le parole chiave qui sono robusta e unica. Stanchi di password complesse difficili da ricordare e difficili da scrivere? Anche noi. Utilizzate invece una passphrase. Questo è un tipo di password che utilizza una serie di parole facili da ricordare, come "Dov'è il mio caffè?" O "sole-ciambelle-felice-perso". Più lunga è la passphrase, più sarà robusta . Una password univoca significa utilizzare una password diversa per ogni dispositivo e account online. In questo modo se una password viene compromessa, tutti gli altri tuoi account e dispositivi sono ancora al sicuro. Non riescite a ricordare tutte quelle password robuste e uniche? Non preoccupatevi, neanche noi. Ecco perché vi consigliamo di utilizzare un gestore di password, che è uno speciale programma di sicurezza che memorizza in modo sicuro tutte le tue password in una cassaforte virtuale cifrata.

Infine, attivate l'autenticazione a due fattori (2FA) ogni volta che è disponibile, in particolare per i tuoi account online. L'autenticazione a due fattori è molto più robusta. Questo meccanismo usa la tua password, ma aggiunge anche un secondo passo, come un codice inviato al tuo smartphone o un'app sul tuo smartphone che genera il codice per te.

Come creare una casa cyber sicura

L'autenticazione a due fattori è probabilmente il singolo passo , più importante, che potete fare per proteggervi online ed è molto più facile di quanto pensate.

Backup

A volte, non importa quanto voi possiate essere attenti, potreste comunque essere hackerati. In tal caso, spesso l'unico modo per recuperare le informazioni personali è il ripristino dei dati dal backup. Assicuratevi di eseguire backup regolari di tutte le informazioni importanti e verificate di poterle ripristinare se necessario. La maggior parte dei dispositivi mobili supporta backup automatici sul cloud. Per la maggior parte dei computer potrebbe essere necessario acquistare alcuni tipi di software o servizi di backup, che sono relativamente economici e semplici da usare.

PER SAPERNE DI PIU'

Iscriviti ad OUCH!, la newsletter mensile di sensibilizzazione alla sicurezza informatica, consulta gli archivi di OUCH! e approfondisci le soluzioni SANS per la sensibilizzazione alla sicurezza visitando il sito securingthehuman.sans.org/ouch/archives.

Versione Italiana

Italtel è una società multinazionale che progetta e realizza soluzioni e servizi di Information & Communication Technology basati su prodotti propri e di partner. Offre un ricco catalogo di servizi professionali di ingegneria, di servizi gestiti e soluzioni di Cybersecurity, collaboration, IoT, digitalizzazione delle reti e servizi di comunicazione.
Per maggiori informazioni www.italtel.com e seguici su Twitter (@Italtel)

Risorse

Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2017#september2017
Two-factor Authentication:	https://securingthehuman.sans.org/ouch/2017#december2017
Backups:	https://securingthehuman.sans.org/ouch/2017#august2017

Direzione Editoriale: Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
Tradotto da: Italtel Solutions Business Unit - Cyber Security