OUCH! | Ottobre 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Sicurezza in 4 punti

Introduzione

La tecnologia ha conquistato un ruolo sempre più importante nelle nostre vite, ma al contempo è aumentata anche la sua complessità. A causa del suo rapido tasso di crescita, diventa sempre più difficile restare aggiornati, anche per quanto concerne la sicurezza: vengono pubblicate continuamente nuove guide che illustrano come comportarsi in modo corretto, ma sebbene le modalità di protezione possano cambiare nel tempo, ci sono alcuni elementi fondamentali che potete sempre mettere in pratica per agire in sicurezza. I seguenti cinque passi chiave sono indipendenti dalla tecnologia. Potrete approfondire gli argomenti nella sezione “Risorse” al termine di questa newsletter.

L’autore di questo numero

Ryan Johnson prepara le azienda a rispondere alle inevitabili violazioni e insegna ”Advanced Network Forensics” al SANS Institute. Potete seguire Ryan su Twitter: **@ForensicRJ**.

1. **Voi**. Come prima cosa, tenete presente che la tecnologia, da sola, non può proteggervi. I criminali informatici sanno che il miglior modo per scavalcare la maggior parte delle misure di sicurezza è attaccare chi ne fa uso. Se vogliono le vostre password o il vostro numero di carta di credito, la cosa più semplice è di ingannarvi per fornir loro queste informazioni. Potrebbero, ad esempio, impersonare un tecnico di supporto Microsoft e comunicarvi che il vostro computer è stato infettato da un virus, mentre in realtà vogliono solo che voi concediate loro l’accesso ai vostri dati. Oppure potreste ricevere un messaggio email che vi comunica che il pacco che stavate aspettando non può essere recapitato, e vi viene richiesto di cliccare su un link per confermare il vostro indirizzo, mentre in realtà vi vogliono costringere a visitare un sito web maligno che consentirà loro di accedere al vostro computer. Gli attacchi come il Ransomware e la frode del CEO iniziano esattamente in questo modo. In conclusione, siete voi la miglior difesa contro un attacco: siate cauti e vedrete che con il buon senso individuerete e fermerete la maggior parte dei tentativi di attacco.

2. **Le password**. Il passo successivo nell’opera di protezione prevede di utilizzare una password forte e unica per ognuno dei vostri dispositivi, delle utenze online e delle applicazioni. Le parole chiave sono due: forte e unica. Una password forte non può essere facilmente indovinata dagli hacker e dai loro programmi automatici. Siete stanchi di

Sicurezza in 4 punti

password difficili da ricordare e da digitare? Provate a usare una passphrase, cioè un insieme di parole facili da ricordare, come ad esempio “Dov’è il mio caffè?”. Più una password è lunga, più sarà forte. Unica significa che è necessario utilizzare password diverse per dispositivi o utenze diverse. In questo modo se una password venisse compromessa, il resto dei vostri account sarebbe al sicuro. Non riuscite a ricordare tutte queste password? Non disperate, nessuno è in grado di farlo. Per questo motivo raccomandiamo l’uso di un password manager, ovvero un’applicazione ideata per memorizzare in modo sicuro le vostre password in formato protetto da crittografia.

Seguendo questi cinque suggerimenti sarete in grado utilizzare in sicurezza anche le tecnologie più recenti.

Infine, è importante proteggere gli account con la verifica in due passaggi. Le password da sole non sono infatti sufficienti a proteggere gli account, per cui abbiamo bisogno di qualcosa di più forte, come questo tipo di verifica che aggiunge un secondo passo, costituito da qualcosa che vi caratterizza (biometria) o qualcosa in vostro possesso (come un codice inviato al vostro smartphone o un’app in grado di generarlo). Abilitate questa opzione su ogni account che avete, incluso il password manager. La verifica in due passaggi è probabilmente il passo più importante che potete adottare per proteggere voi stessi. Ed è molto più facile di quanto pensiate.

3. **Gli aggiornamenti**. Assicuratevi che computer, dispositivi mobili, App e qualsiasi altro dispositivo connesso alla rete sia aggiornato all’ultima versione di software. I criminali informatici sono alla costante ricerca di nuove vulnerabilità nelle tecnologie che usate. Quando scoprono queste debolezze, fanno uso di programmi speciali in grado di sfruttarle ed avere accesso alla vostra rete, al computer e allo smartphone. Al contempo, le aziende produttrici delle tecnologie che usate lavorano strenuamente per mantenerle aggiornate. Configurando i vostri sistemi per installare gli aggiornamenti, renderete la vita più difficile agli hacker. L’aggiornamento deve essere automatico, laddove possibile. Questa regola si deve applicare a ogni tecnologia connessa in rete, inclusi i dispositivi TV connessi a Internet, i monitor per i neonati, i router di casa, le console di gioco e, in futuro, anche la vostra auto. Se il sistema operativo del vostro computer, del dispositivo mobile o di un’altra tecnologia non è più supportato e non sarà più in grado di ricevere aggiornamenti, vi raccomandiamo di sostituirlo con una nuova versione che lo sia.

Sicurezza in 4 punti

4. **I salvataggi**. A volte, indipendente da quanto siate cauti, uno dei vostri dispositivi o account online potrebbe venire compromesso. Spesso, in questi casi, l'unica opzione per verificare che il dispositivo sia libero da malware è di cancellarlo completamente e ricostruirlo da zero. L'hacker potrebbe anche impedirvi l'accesso ai vostri file personali, alle foto e alle altre informazioni conservate. L'unica opzione, a questo punto, è di ripristinare tutte le informazioni dai salvataggi. Assicuratevi di salvare regolarmente le informazioni importanti e verificate di poterle ripristinare. La maggior parte dei sistemi operativi e dei device mobili supporta i salvataggi automatici. Vi raccomandiamo inoltre di conservare i vostri backup sul cloud oppure offline, per proteggerli dagli attacchi.

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

securingthehuman.sans.org/ouch/archives

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

Il Phishing:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_it.pdf
I Password Manager:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_it.pdf
La verifica in due passaggi:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_it.pdf
Le passphrase:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_it.pdf
Salvataggi e ripristino:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_it.pdf

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