SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Ottobre 2014

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Sicurezza in cinque 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. Sebbene i dettagli delle 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.

L'autore di questo numero

Lenny Zeltser si occupa della protezione delle IT operation dei clienti di NCR Corp e, per il SANS Institute, tiene un corso di lotta contro il malware. Potete seguire Lenny su Twitter (**@lennyzeltser**) e leggere il suo blog sulla sicurezza su **blog.zeltser.com**.

Cinque punti chiave

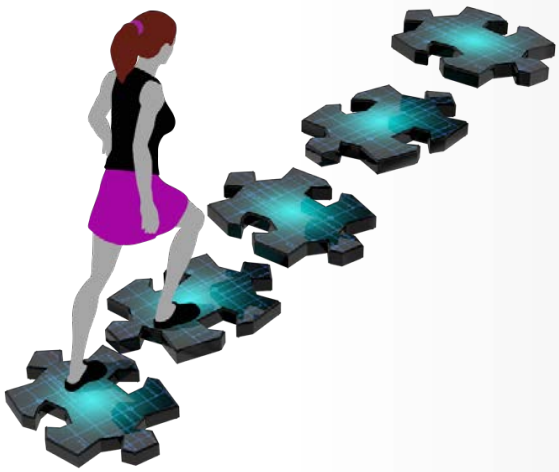
Ognuno dei punti che andremo a descrivere costituisce una semplice introduzione. Per approfondire gli argomenti, fate riferimento alla sezione "Risorse" al termine di questa newsletter.

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 tecnologie 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. 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. **L'aggiornamento**. 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 vulnerabilità nelle tecnologie usate. Quando scoprono queste debolezze, fanno uso di programmi

Sicurezza in cinque punti

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. Una volta che una vulnerabilità è conosciuta, creano una patch per porvi rimedio e la rilasciano al pubblico. Assicurandovi che computer e dispositivi vari siano aggiornati, ridurrete il numero di vulnerabilità conosciute, rendendo più dura la vita agli hacker. L'aggiornamento deve essere automatico, laddove possibile. Questa regola si deve applicare a quasi ogni tecnologia connessa a una rete, ivi 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, dispositivo mobile o 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.



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

3. **Le password**. Il passo successivo nell'opera di protezione prevede di utilizzare una password forte e unica per ognuno dei vostri dispositivi, utenze online e applicazioni. Le parole chiave sono due: forte e unica. Una password forte non può essere facilmente indovinata dagli hacker e dai loro programmi automatici: buona norma è utilizzare una frase o un insieme di parole, anziché una sola, contenente anche simboli e numeri. 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. Infine, se i vostri account supportano la verifica in due passaggi, vi raccomandiamo di abilitarla sempre, perché è uno dei modi più robusti per proteggerli.

4. **La crittografia**. Un passo ulteriore che raccomandiamo è costituito dall'impiego della crittografia, che consente solo a voi e alle persone di cui avete fiducia l'accesso alle vostre informazioni. I dati possono essere cifrati in due luoghi: a riposo e in movimento. Crittografare i dati a riposo significa proteggerli nei luoghi in cui vengono conservati, nei file all'interno dei vostri dischi o delle chiavi USB. La maggior parte dei sistemi operativi vi permette di crittografare automaticamente tutti i dati utilizzando caratteristiche come la Full Disk Encryption (crittografia dell'intero disco). Vi raccomandiamo di abilitarla quando è possibile. Cifrare i dati in movimento significa proteggerli con la crittografia durante la loro trasmissione dal vostro computer

Sicurezza in cinque punti

o da un dispositivo all'altro, come ad esempio quando accedete al vostro conto corrente online. Un modo semplice per verificare se la crittografia è attivata quando navigate in Internet è di verificare che l'indirizzo del sito che state visitando inizi con "https:" e che vicino ad esso ci sia l'immagine di un lucchetto chiuso.

5. **I salvataggi**. A volte, indipendentemente 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.

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

Email e Phishing:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_it.pdf
Rendere sicuro il tablet:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_it.pdf
Le Password:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_it.pdf
Programmi di gestione password:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_it.pdf
La verifica in due passaggi:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_it.pdf
La crittografia:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_it.pdf
Il salvataggio dei dati:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_it.pdf

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