SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Aprile 2014

Newsletter mensile di suggerimenti sulla sicurezza informatica

OUCH!

IN QUESTO NUMERO...

L'obiettivo sei tu!

Introduzione

Un errore che in molti commettono è di credere di non essere un obiettivo della criminalità informatica perché i loro dati non hanno alcun valore. Nulla potrebbe essere più lontano dalla verità. Se hai un computer, un tablet o uno smartphone, un conto online, un indirizzo email, una carta di credito o un'altra qualsiasi attività online, agli occhi dei criminali informatici hai anche un valore. In questo numero spiegheremo perché ognuno di noi è un obiettivo, come possiamo essere attaccati e cosa fare per proteggersi.

L'autore di questo numero

Eric Conrad è presidente e CTO di Backshore Communications nonché autore principale dei libri CISSP Study Guide, Seconda Edizione, e di "Eleventh Hour CISSP", Seconda Edizione. È anche co-autore dei corsi "Continuous Monitoring" e " Security Operations (SEC511)" del SANS Institute.

Perché ognuno di noi è un obiettivo

Crimini come le frodi, il furto di identità o l'estorsione esistono da quando esiste la civiltà; sono, purtroppo, parte integrante della nostra quotidianità. L'obiettivo di un criminale è sempre il medesimo: fare più denaro possibile, nel modo più facile possibile e con il minor rischio possibile. Si è sempre trattato di un'attività difficoltosa a causa delle limitazioni indotte dalla locazione geografica e dalla necessità di interazione fisica con le potenziali vittime. Questi fattori non solo limitavano i potenziali obiettivi, ma esponevano i criminali anche a una vasta gamma di rischi. Con l'avvento di Internet e delle tecnologie online, il crimine è cambiato radicalmente: i delinquenti possono facilmente considerare come loro obiettivo qualsiasi persona al mondo, con costi molto ridotti, quando non addirittura nulli, e con rischi molto bassi. Inoltre, gli hacker si sono uniti in organizzazioni molto efficienti, fattore che permette loro di essere più pericolosi che mai.

Essi sanno che il denaro che potranno raccogliere è direttamente proporzionale al numero di dati di carte di credito che riusciranno a rubare, al numero di conti in banca che avranno compromesso e alla quantità di password di cui saranno venuti in possesso. Tenteranno di attaccare chiunque sia connesso a Internet, te compreso. Sembra un lavoro improbo, ma è sorprendentemente facile grazie all'utilizzo di strumenti automatici che si occupano di svolgere tutte le attività al loro posto. Ad esempio, un gruppo di truffatori potrebbe costruire un database di milioni di indirizzi email e utilizzare uno strumento automatico per inviare messaggi phishing a ognuno

L'obiettivo sei tu!

di questi indirizzi. Inviare un messaggio ha un costo quasi nullo: per lo sporco lavoro vengono utilizzati altri computer già compromessi, forse anche il tuo. Questo è un altro motivo per cui anche il tuo computer ha un valore. Infine, ai criminali non interessa sapere chi cadrà vittima dei loro attacchi, ma sanno solo che più messaggi invieranno, più persone cadranno vittima dell'inganno. Un altro approccio utilizzato prevede l'analisi di ogni computer su Internet (usando, anche in questo caso, altri computer già compromessi), cercando computer o device che possono essere attaccati. Ricorda: chiunque può essere attaccato. Nessuno viene ignorato perché è speciale.

Potresti anche non rendertene conto, ma per i criminali informatici anche i tuoi dispositivi e le tue informazioni hanno un valore.

Come proteggersi

Quando i criminali informatici conducono i loro attacchi utilizzano metodi relativamente semplici. Per fortuna, utilizzando altrettanto semplici approcci, anche tu potrai proteggerti in modo adeguato.

- **Tu**: tu sei l'ultima linea di difesa contro il crimine informatico. Molti attacchi iniziano con un tentativo di inganno, chiedendoti di aprire un allegato infetto o facendoti rivelare la password al telefono. In questi casi, la miglior difesa è il buon senso: se qualcosa sembra sospetto o troppo bello per essere vero, sarà molto probabilmente un tentativo di frode.

- **Aggiornamenti**: assicurati che tutti i computer e i dispositivi mobili che usi siano aggiornati e vi siano state applicate le ultime patch. Non solo è importante per il tuo sistema operativo, ma per ogni applicazione o plugin installato. Tenendo il tuo sistema e le tue applicazioni costantemente aggiornati ti proteggerai meglio contro gli attacchi più comuni.

- **Password**: usa password forti e uniche per ognuno dei tuoi account. In questo modo, quando un sito web che usi subisce un attacco e le password di tutti gli utenti (compresa la tua) vengono compromesse, gli altri tuoi account sono al sicuro. Assicurati anche che i vari dispositivi siano protetti da una password forte e unica, da un PIN o da altri meccanismi di blocco. Per tener traccia di tutte le tue varie password ti consigliamo di far uso di un Password Manager.

L'obiettivo sei tu!

- **Carte di credito**: controlla sistematicamente i tuoi estratti conto, almeno una volta alla settimana. Non appena noti una transazione non autorizzata sulla tua carta di credito, comunicala immediatamente alla società che ha emesso la carta. Se la tua banca ti permette di configurare avvisi email o SMS relativi a transazioni insolitamente importanti o sospette, utilizzali per avere notifiche più velocemente.

- **La rete**: rendi sicura la tua rete Wi-Fi casalinga con una password forte per l'utente amministrativo e fai in modo che l'accesso ad essa sia consentito solo dopo l'inserimento di una password.

- **Social network**: più informazioni condividerai online, più facilmente ti metterai a rischio. Non solo ogni informazione pubblicata facilita ai criminali il lavoro di raccolta di dati sulla tua persona, ma ogni informazione pubblicata ti fa classificare come un obiettivo di un certo valore.

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

OUCH! Programmi di gestione password:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_it.pdf
OUCH! La sicurezza della rete di casa:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201401_it.pdf
OUCH! Email e phishing:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_it.pdf

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