SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Novembre 2014

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Social Engineering

Introduzione

Pensando agli attacchi informatici, un errore comune che molti commettono è credere che vengano utilizzati strumenti e tecnologie estremamente avanzate per introdursi in computer, account e dispositivi mobili. Tutto ciò non corrisponde sempre a verità. I criminali informatici sanno che uno dei modi più semplici per rubare le informazioni o violare il computer di una vittima consiste semplicemente nel tentare di ingannarla. In questa newsletter impareremo come vengono attuati questi attacchi, chiamati di Social Engineering, e cosa potete fare per proteggervi.

L'autore di questo numero

Alissa Torres è istruttore SANS certificato, specializzata in Computer Forensics e risposta agli incidenti. Tra le sue esperienze figurano la gestione degli incidenti e la partecipazione a un team di sicurezza in qualità di investigatore specializzato in analisi forense digitale. Potete seguire Alissa su Twitter (**@sibertor**).

Il Social Engineering

Il Social Engineering è un tipo di attacco psicologico in cui un attaccante inganna una vittima per convincerla a fare ciò che egli vuole. Il Social Engineering esiste da migliaia di anni: l'idea di ingannare o truffare qualcuno non è affatto una novità. I criminali informatici sanno che usare questi metodi su Internet è estremamente efficace perché permettono loro di colpire milioni di persone in breve tempo. Il modo più semplice per capire come funziona il Social Engineering è osservare un esempio del mondo reale.

Supponiamo che riceviate una chiamata da qualcuno che si spaccia per un tecnico di un'azienda di supporto informatico, o del vostro provider o ancora del supporto tecnico Microsoft. La persona spiega di aver notato che il vostro computer si comporta in modo strano, poiché, ad esempio, sta inviando una grande quantità di spam, e crede che esso sia stato infettato da malware. L'azienda sta investigando il problema e vi vuole aiutare a renderlo sicuro. La persona al telefono userà vari termini tecnici e vi condurrà attraverso un percorso confuso per convincervi che il vostro computer è stato infettato.

Potrebbe chiedervi di verificare la presenza di determinati file nel vostro computer e guidarvi nella loro ricerca. Una volta riscontrata la presenza di questi file, il chiamante vi assicurerà che si tratta di segnali dell'infezione in atto, mentre in realtà essi non sono altro che comuni file presenti su ogni computer. Una volta che vi avrà fatto credere che il vostro computer è infetto, vi suggerirà di consultare al più presto un sito e comprare un software di sicurezza oppure, in alternativa, vi chiederà di permettergli l'accesso al vostro computer per poter

© The SANS Institute 2014

Social Engineering

rimediare al presunto danno. In realtà, il software che vi venderà sarà esso stesso un programma maligno: se lo acquisterete e installerete, non solo sarete stato ingannato, ma avrete anche pagato per esserlo.

Tenete a mente che gli attacchi di Social Engineering non si limitano alle chiamate telefoniche, ma possono essere effettuati con qualsiasi tecnologia, come il phishing via email, via sms o i sistemi di messaggistica, anche su Facebook, Twitter o chat online. L'importante è sapere cosa cercare.

Imparare a prevenire, individuare e bloccare gli attacchi di Social Engineering è uno dei modi più efficaci per proteggersi.

Individuare e bloccare gli attacchi di Social Engineering

Il modo migliore per difendersi da questo tipo di attacchi è usare il buon senso: se qualcosa sembra sospetto potrebbe costituire un tentativo di attacco. Alcuni semplici indicatori di Social Engineering sono:

- la creazione di un eccessivo senso di urgenza: se vi sentite sotto pressione per prendere una decisione in fretta, agite con cautela;
- qualcuno vi richiede informazioni a cui non dovrebbe avere accesso o dovrebbe già conoscere;
- vi viene proposto qualcosa troppo bello per essere vero. Un esempio classico è la notifica via email della vincita a una lotteria, alla quale non avete mai partecipato.

Se sospettate che qualcuno stia tentando di farvi cadere vittima di un attacco di Social Engineering, smettete di comunicare con quella persona. Se si tratta di una conversazione telefonica, agganciate. Se tutto avviene in una chat online, terminate la connessione. Se si tratta di una email, cancellatela. Se l'attacco ha a che fare con il vostro lavoro, comunicatelo al vostro helpdesk o al dipartimento sicurezza.

La prevenzione

Esistono precauzioni che è bene mantenere per evitare di esporsi ad attacchi di Social Engineering.

- **Non condividere le password con nessuno**. Nessuna azienda vi contatterà mai chiedendovi una delle vostre password. Se ciò dovesse accadere, si tratta di un attacco.

- **Non condividete troppo**. Se un attaccante conosce molte informazioni sul vostro conto, sarà più facile per lui trovarvi e ingannarvi per farvi fare ciò che vuole. Anche quei piccoli dettagli che condividete sulla vostra vita di tanto in tanto possono essere messi insieme per creare il vostro profilo. Meno

© The SANS Institute 2014

Social Engineering

informazioni condividerete pubblicamente, attraverso siti di social network, di opinioni su prodotti o forum pubblici, meno probabilmente cadrete vittime di attacchi.

- **Verificate i contatti**. A volte potreste ricevere una chiamata dalla vostra banca o dalla società che ha emesso la vostra carta di credito, dal vostro fornitore di servizi Internet o da altre aziende ancora. Se avete qualsiasi tipo di dubbio sulla legittimità delle richieste che vi vengono fatte, chiedete il nome della persona e il suo numero di telefono aziendale. Cercate poi il numero di telefono dell'azienda su una fonte di informazioni affidabile ad esempio sulle comunicazioni cartacee che avete ricevuto per l'estratto conto del conto corrente o della carta di credito, o ancora consultando il sito web dell'azienda, avendo poi cura di digitare l'indirizzo nel vostro browser. In questo modo, quando chiamate l'azienda, sapete che state veramente parlando con uno dei suoi dipendenti. Sebbene tutto ciò possa sembrare un problema, preservare la vostra identità online e le vostre informazioni val ben qualche sforzo aggiuntivo.

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
Social Network in sicurezza:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201303_it.pdf

OUCH! è pubblicata dal progetto Securing The Human del SANS Institute e viene distribuita con licenza Creative Commons BY-NC-ND 4.0.
Sei libero di distribuire questa newsletter o utilizzarla nei tuoi programmi di awareness senza però modificarne i contenuti.
Per traduzioni o ulteriori informazioni, contatta ouch@securingthehuman.org.

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