OUCH!

SANS SECURITY AWARENESS

La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per te

Sì, sei un bersaglio !

Introduzione

Molte persone credono, sbagliando, di non essere un possibile bersaglio per gli hacker, infatti pensano che loro stessi, i loro sistemi o i loro account non abbiano alcun valore. Questo, invece, è molto lontano dalla verità. Se usi la tecnologia al lavoro o a casa, fidati di noi: hai valore per i cattivi. Ma sei fortunato. Hai già la migliore difesa contro questi attacchi informatici: e questa difesa sei tu.

Perché sei un bersaglio

Oggi in Internet ci sono molti cyber criminali, tutti con motivazioni diverse. Allora, perché qualcuno di loro avrebbe necessità di attaccarti? Perché attaccando te riescono a raggiungere il loro obiettivo. Ecco due esempi comuni di cyber attaccanti e di motivi per i quali potrebbero prenderti di mira.

⚠ **Cyber Criminal:** Il loro scopo è fare più soldi possibile. Ciò che rende Internet prezioso per loro è il fatto che possono facilmente trovare chiunque, molto semplicemente, premendo un pulsante. E ci sono MOLTI modi in cui possono fare soldi attraverso di te. Ad esempio potrebbero operare un furto di denaro dal tuo conto bancario, oppure creare una carta di credito a tuo nome ed addebitare dei costi su questa, potrebbero utilizzare il tuo computer per hackerare altre persone o addirittura violare i tuoi dati dai social media o dagli account di gioco per poi rivenderli ad altri criminali. La lista di modalità attraverso le quali i cyber criminali possono fare soldi sfruttandoti è quasi infinita. Ci sono centinaia di migliaia di criminali informatici che si svegliano ogni mattina con l'obiettivo di hackerare quante più persone possibile, incluso te.

☆ **Targeted Attackers:** Si tratta di cyber criminali particolarmente qualificati, che spesso lavorano per gli enti governativi, per i sindacati criminali o per possibili concorrenti nell'ambito del tuo lavoro. Potresti pensare che il tuo lavoro non attiri molta attenzione ma in realtà rimarresti molto sorpreso di sapere che:

- Le informazioni che gestisci sul posto di lavoro hanno un valore straordinario per diverse aziende o governi.
- Gli attaccanti potrebbero prenderti di mira non per violare te, ma per hackerare uno dei tuoi colleghi o qualcuno nel tuo sistema conoscenze, attraverso di te.

- **Questo tipo di criminali potrebbe prenderti di mira al lavoro perché interessato ad altre società per cui lavori o delle quali sei partner.**

Ho un anti-virus, quindi sono al sicuro

Ok, quindi sono un bersaglio!!! Ma questo non è un problema! Installerò antivirus e firewall sul mio computer e sarò protetto, giusto? Beh sfortunatamente non è così. Molte persone pensano che installando alcuni strumenti di sicurezza saranno al sicuro. Sfortunatamente questo non è sempre vero. Gli hacker informatici continuano a migliorare e molti dei loro metodi di attacco attualmente aggirano facilmente le tecnologie di sicurezza. Ad esempio, creano spesso malware speciali che il tuo antivirus non è in grado di rilevare. Ignorano i filtri e-mail con un attacco di phishing personalizzato o ti chiamano al telefono e ti imbrogliano facendosi dare i dati della carta di credito, del denaro o le password. La tecnologia gioca un ruolo importante nel proteggerti, ma alla fine sei tu la miglior difesa.

Fortunatamente essere sicuri non è così difficile, in definitiva il buon senso e alcuni comportamenti di base sono la miglior difesa. Se ricevi un'email, un messaggio o una telefonata che è estremamente urgente, strana o sospetta, potrebbe trattarsi di un attacco. Per garantire la sicurezza dei tuoi computer e dei dispositivi, mantenendoli aggiornati, devi abilitare l'aggiornamento automatico. Infine, utilizza una passphrase valida e unica per ciascuno dei tuoi account. Essere consapevoli sui temi della cyber-security è in definitiva la miglior difesa. Non sai da dove iniziare? Prendi in considerazione l'iscrizione al mensile OUCH! newsletter a sans.org/ouch!

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)

L'autore di questo articolo

Matt Bromiley *(@mbromileyDFIR) fornisce analisi su incidenti di sicurezza informatica, è un esperto nell'analisi forense con oltre 8 anni di esperienza. Ha lavorato con organizzazioni in tutto il mondo gestendo incidenti di cyber security. Matt è inoltre un istruttore di "Digital Forensic" e "Incident Response", ed è docente per i corsi SANS FOR508 e FOR572.*

Bibliografia

Stop That Malware: https://www.sans.org/u/L1J
Social Engineering: https://www.sans.org/u/L1O
Phone Call Scams: https://www.sans.org/u/L1T
Passphrases: https://www.sans.org/u/L1Y
Poster - You Are a Target: https://www.sans.org/u/L23