SANS SECURING THE HUMAN ADVANCTION

OUCH! | Settembre 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

La verifica in due passaggi

Introduzione

Il processo di provare la propria identità (denominato "autenticazione") è un passo fondamentale per proteggere le informazioni: l'autenticazione forte cerca di assicurare che solo voi possiate accedere alle vostre informazioni, alle email, alle immagini e ai vostri conti online. Ci sono tre diversi modi per confermare la vostra identità: usare qualcosa che sapete (ad esempio, una password), qualcosa in vostro possesso (la vostra patente) e una vostra caratteristica fisica (una vostra impronta digitale). Ognuno di questi metodi ha vantaggi e svantaggi e, di questi, il metodo più utilizzato è la password, cioè qualcosa che sapete. In questa newsletter vi illustreremo come potete proteggervi con la verifica in due passaggi, un metodo molto più sicuro della sola password e molto semplice da usare. Per capire come funziona, dobbiamo partire dalle password.

L'autore di questo numero

Keith Palmgren ha più di 30 anni di esperienza nell'ambito della sicurezza delle informazioni. È un istruttore certificato SANS nonché autore del corso SANS SEC301, un'introduzione alla sicurezza delle informazioni. Quando non insegna, Keith si dedica a consulenza e progetti. Potete seguire Keith su twitter: **@kpalmgren**.

Le password

Le password provano chi siete sulla base di qualcosa che conoscete. Il problema delle password è che esse costituiscono l'unico punto di vulnerabilità: se qualcuno può indovinarle o avervi accesso, potrà spacciarsi per voi e accedere a tutte le informazioni da esse protette. Per questo motivo avete appreso vari metodi per proteggerle: utilizzare password forti e difficili da indovinare, usare password diverse per ogni account e non condividerle mai con nessun altro. Sebbene questi consigli rimangano sempre validi, nell'era moderna le password sono sempre meno efficaci. Le ultime tecnologie rendono la compromissione di una password un'attività sempre più accessibile ai criminali informatici. Ciò di cui abbiamo bisogno è una soluzione di autenticazione forte facile da usare e più sicura. Per nostra fortuna, questa soluzione è ora disponibile e prende il nome di "verifica in due passaggi".

La verifica in due passaggi

La verifica in due passaggi (chiamata a volte, autenticazione a due fattori) è una soluzione più sicura della sola password.

La verifica in due passaggi

Funziona richiedendo non uno, ma due metodi di autenticazione. Un esempio è la vostra carta bancomat. Quando ritirate del denaro da uno sportello, usate una forma di verifica in due passaggi poiché avete bisogno di due cose: la vostra carta bancomat (qualcosa che avete) e il vostro PIN (qualcosa che sapete). Nel caso perdiate il bancomat il vostro denaro sarà comunque al sicuro: chiunque trovasse la carta non potrebbe prelevare alcunché poiché non conoscerebbe il vostro PIN (a meno che non l'abbiate scritto sulla carta!). Un criminale deve possedere sia la carta sia il PIN per compromettere il vostro conto corrente. Questo è ciò che rende la verifica in due passaggi molto più sicura: poter fare affidamento su due livelli di sicurezza.

Usate la verifica in due passaggi quando disponibile, poiché è uno dei metodi più efficaci per proteggere le vostre informazioni.

Usare la verifica in due passaggi

La verifica in due passaggi è qualcosa che potete configurare per ognuno dei vostri account. Fortunatamente, molti servizi online ora la offrono e uno dei leader in questo ambito è Google. Gli account Google sono uno degli obiettivi primari poiché Google offre una vasta rosa di servizi online gratuiti a milioni di persone in tutto il mondo. Per questo motivo era necessario offrire un'autenticazione forte e l'azienda californiana fu una delle prime a rilasciare questo metodo di autenticazione per la maggior parte dei servizi disponibili. Se capirete come funziona la verifica in due passaggi di Google, comprenderete anche come funziona per tutti gli altri servizi come Twitter, Facebook, Apple, Instagram e molti e-banking.

Per prima cosa, abilitate la verifica in due passaggi sull'account Google e registrate il vostro numero di telefono cellulare. Una volta completato questo passaggio, l'autenticazione funzionerà nel seguente modo. Come prima cosa vi collegate al vostro account con nome utente e password. Questo è il primo dei due fattori: qualcosa che conoscete. Google invierà poi al vostro smartphone un messaggio di testo contenente un codice univoco costituito da una serie di sei numeri. Come fate con la password, inserite questi sei numeri quando vi viene richiesto dal sito. Questo è il secondo dei due fattori. Per accedere al vostro account dovete conoscere la password e possedere un telefono mobile per ricevere il codice unico. Anche se un attaccante avesse la vostra password, non potrebbe avere accesso all'account Google senza il vostro telefono. Per assicurare che l'account sia veramente sicuro, Google vi invierà un codice diverso ad ogni vostro collegamento.

La verifica in due passaggi

Una seconda possibilità utilizzabile sia con Google sia con altri servizi è offerta da un app installabile sul vostro smartphone da utilizzare in sostituzione dell'SMS. Questa app è in grado di generare il codice univoco ogni volta che volete.
L'utilizzo dell'app offre il vantaggio di non necessitare di un collegamento alla rete telefonica per ricevere l'SMS contenente il codice poiché è lo smartphone stesso che lo genera autonomamente. Inoltre, il codice prodotto non potrà essere intercettato, come potrebbe accadere con un SMS.

Ricordate: la verifica in due passaggi non è attiva per default, ma dovete abilitarla da voi. Sebbene questa operazione potrebbe sembrare onerosa all'inizio, vi raccomandiamo di utilizzarla sempre quando è possibile, specialmente per servizi critici come l'email, l'online banking o il salvataggio di file sul cloud. Questo metodo di verifica offre una protezione molto più efficace della semplice password.

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

Le passphrases: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_it.pdf
Siti che supportano la verifica in due passaggi: https://twofactorauth.org
La verifica in due passaggi di Google: http://www.google.com/landing/2step/

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