OUCH! | Agosto 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

- Cosa salvare e quando
- Come effettuare un salvataggio
- Il ripristino
- I punti chiave

Salvataggi e ripristino

Introduzione

A chiunque, per quanta attenzione possa avere, potrebbe capitare l'inconveniente di perdere file personali, documenti o foto, per avere rimosso i file sbagliati, ad esempio, o per un problema hardware, perché avete perso il laptop o perché il vostro computer è stato infettato. In momenti come questi, l'unico modo per ricostruire la vostra vita digitale risiede nel salvataggio dei dati. In questa newsletter illustreremo cosa sono i salvataggi, come salvare i vostri dati e come sviluppare la strategia più corretta per le vostre esigenze.

L'autore di questo numero

Heather Mahalik è un esperto di analisi forense, specializzata negli smartphone. È co-autore di "Practical Mobile Forensics", editore tecnico di "Learning Android Forensics" e co-autore dei corsi "Advanced Smartphone Forensics" e "Macintosh Forensics" del SANS Institute. Potete seguire Heather su **Smarterforensics.com** e su Twitter: **@heathermahalik**.

Cosa salvare e quando

I salvataggi non sono altro che copie delle vostre informazioni che vengono memorizzate in un altro luogo in modo che quando perderete dati importanti, avrete la possibilità di ripristinarli dai salvataggi effettuati in precedenza. Purtroppo, non molti effettuano salvataggi, il che è un peccato perché si tratta di una procedura semplice ed economica. Per decidere cosa salvare potete usare due approcci: (1) salvare dati specifici e importanti; (2) salvare tutto quanto, compreso il sistema operativo. Il primo approccio rende più veloce l'operazione di salvataggio e consente di risparmiare spazio, mentre il secondo è più semplice e completo. Se non siete sicuri su cosa salvare, vi raccomandiamo di salvare tutto quanto.

Il passo successivo consiste nel decidere la frequenza del salvataggio: giornaliera, settimanale, ecc. Per il computer di casa, esistono programmi come Time Machine di Apple o Windows Backup e Restore di Microsoft che vi permettono di creare una pianificazione precisa dei salvataggi. Queste soluzioni archivieranno automaticamente i vostri dati durante il giorno sia mentre state lavorando sia quando non siete al computer. Altre soluzioni offrono una "protezione continua" mediante la quale i file nuovi o modificati vengono salvati immediatamente quando vengono chiusi. In ogni caso, vi raccomandiamo di effettuare salvataggi giornalieri. La domanda che dovete porvi per effettuare una pianificazione sulla base delle vostre esigenze è "Quante informazioni posso permettermi di perdere se devo ripristinare i dati da un salvataggio?"

Come effettuare un salvataggio

Ci sono due modi con cui potete salvare i vostri dati: media fisici o archiviazione sul cloud. Il primo mezzo è costituito da ogni tipo di hardware, come DVD, dischi USB o esterni. Qualunque media scegliate, fate attenzione a non salvare mai i

Salvataggi e ripristino

file sullo stesso dispositivo che conserva i file originali. Il problema con i media fisici è che in caso di incidenti dovuti a fuoco o furto potreste perdere sia il vostro computer sia i vostri dati. Per questo dovreste prevedere di memorizzare copie dei vostri salvataggi in un luogo sicuro. Se lo fate, però, ricordate di etichettare ogni salvataggio con il suo contenuto e la data e, per un ulteriore sicurezza, proteggetelo con la crittografia.

Salvataggi automatici e affidabili sono l'ultima linea di difesa nella protezione dei dati.

Le soluzioni basate su cloud hanno un approccio diverso: si tratta infatti di servizi con cui i vostri file vengono archiviati da qualche parte su Internet, disponibili spesso in modalità gratuita, per salvare un numero limitato di dati, e a pagamento, che vi consente l'archiviazione di notevoli quantità di dati. Installando un programma sul vostro computer, avrete la possibilità di salvare automaticamente i vostri file. Il vantaggio di questa soluzione risiede nel fatto che i vostri salvataggi sono nel cloud, per cui se dovesse accadere un incidente che porti alla perdita di dati sul vostro computer, i vostri salvataggi sarebbero comunque al sicuro. Potete inoltre accedere a essi da qualsiasi luogo, anche in viaggio. Lo svantaggio del cloud è che potrebbe essere più lento, specialmente nel caso dobbiate salvare grandi quantità di dati. Se siete indecisi nel scegliere una soluzione di backup fisica o su cloud, potete sempre adottarle entrambe.

Infine, non dimenticate i vostri dispositivi mobili: il vantaggio in questo caso è che la maggior parte dei vostri dati (email, eventi sul calendario, contatti) è già salvata nel cloud. Potreste comunque avere informazioni non salvate su cloud, riguardanti ad esempio le configurazioni delle app, le foto più recenti o le configurazioni di sistema. Effettuando un salvataggio dei dispositivi mobili, non solo preserverete queste informazioni, ma sarà più facile ricostruire il vostro dispositivo quando, ad esempio, lo aggiornerete con uno più recente. Un iPhone/iPad può salvare automaticamente su Apple iCloud, mentre i dispositivi Android o di altro tipo dipendono dal produttore o dal fornitore del servizio. In alcuni casi potrebbe essere necessario acquistare app specifiche per i salvataggi.

Il ripristino

Una volta salvati i dati siete solo alla metà del guado: dovete anche essere certi di poterli ripristinare. Controllate ogni mese che i salvataggi siano validi, ripristinando un file e verificando che sia corretto. Effettuate anche un backup completo del sistema prima di un aggiornamento importante, ad esempio quando adottate un nuovo computer o un nuovo smartphone, o prima di una riparazione, e verificate che sia ripristinabile.

Salvataggi e ripristino

I punti chiave

- Automatizzate i backup il più possibile e verificateli con regolarità
- Quando ricostruite un sistema completo da un salvataggio, applicate le ultime patch di sicurezza e gli aggiornamenti prima di utilizzarlo
- Salvataggi obsoleti potrebbero costituire una criticità e dovrebbero essere distrutti per prevenire che qualcuno vi possa avere accesso senza essere autorizzato
- Se usate una soluzione basata sul cloud, verificate che le policy e la reputazione del fornitore del servizio corrispondano ai vostri requisiti. Controllate, ad esempio, che proteggano i dati con la crittografia, chi può avere accesso ai vostri backup, se viene supportata la verifica in due passaggi, ecc.

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
La verifica in due passaggi:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_it.pdf
Usare il cloud in modo sicuro:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_it.pdf
La crittografia:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_it.pdf

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