SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Agosto 2017

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Salvataggi e ripristino

Introduzione

Se utilizzate un computer o un dispositivo mobile per molto tempo, prima o poi qualcosa potrebbe andar storto, causando la perdita di file personali, documenti o foto: capita a volte di eliminare accidentalmente dei documenti, subire un guasto hardware, perdere un dispositivo o venire infettati da malware come il Ransomware. In momenti come questi, i salvataggi (detti anche backup) sono spesso l'unico modo per ricostruire la propria vita digitale. In questa newsletter, spieghiamo cosa sono, come eseguire il backup dei dati e sviluppare una strategia semplice adatta alle vostre esigenze.

L'autore di questo numero

Keith Palmgren è un esperto di Cybersecurity con oltre 30 anni di esperienza nel settore dell'IT Security. È istruttore senior di SANS e autore del corso SANS SEC301 "Introduzione alla sicurezza delle informazioni." Keith è consulente nell'ambito della sicuezza ed è presente su Twitter: **@kpalmgren**

Salvataggi: cosa, quando e come

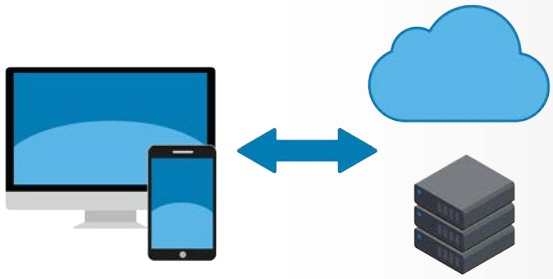
I backup sono copie delle vostre informazioni memorizzate in un luogo diverso da computer, smartphone o tablet, in modo che se doveste subire una perdita di dati preziosi, sia possibile recuperarli dai backup. Purtroppo, troppe persone non eseguono backup regolari, sebbene sia una procedura semplice e poco costosa. Il primo passo è decidere cosa si desidera salvare. Esistono due approcci: (1) dati specifici importanti; (2) tutto quanto, incluso l'intero sistema operativo. La maggior parte delle soluzioni di backup sono configurate (tramite impostazione predefinita) per utilizzare il primo approccio, memorizzando quindi i dati delle cartelle più utilizzate; nella maggior parte dei casi questo metodo è sufficiente. Tuttavia, se non siete sicuri di che cosa salvare o desiderate essere estremamente cauti, potete semplicemente scegliere di eseguire il backup di tutto.

In secondo luogo, è necessario decidere quanto spesso eseguire il backup dei dati. Applicazioni di backup di sistema come "Time Machine" di Apple o "Backup e ripristino" di Microsoft Window consentono di creare un programma di backup automatico. Le opzioni più usate permettono di eseguire il savataggio ogni ora, quotidianamente, settimanalmente, ecc. Altre soluzioni offrono una "protezione continua" con la quale vengono immediatamente eseguiti backup di file nuovi o modificati ogni volta che si salva un documento. Come misura minima consigliamo di eseguire backup automatici quotidiani.

Infine, dovete decidere come effettuare i salvataggi. Ci sono due modi: su supporti fisici o sul cloud. Ogni approccio ha vantaggi e svantaggi. I supporti fisici sono dispositivi sotto il vostro controllo, come ad esempio unità USB esterne o dispositivi

Salvataggi e ripristino

di rete accessibili via Wi-Fi. Il vantaggio dei dispositivi esterni è che consentono di eseguire il backup e il recupero di grandi quantità di dati molto velocemente. Lo svantaggio di un tale approccio è che se si viene infettati da malware, come il Ransomware, è possibile che l'infezione si diffonda nei backup. Anche un disastro fisico, come un incendio o un furto, può causare la perdita non solo del computer ma anche dei backup. Se quindi si utilizzano dispositivi esterni, è necessario disporre di un piano per memorizzare le copie del backup fuori sede in un luogo protetto. Assicurarsi che i backup memorizzati siano correttamente etichettati.



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

Le soluzioni basate su cloud sono servizi online che memorizzano i file su Internet. In genere, si installa un'applicazione sul computer che esegue automaticamente il backup dei file secondo una pianificazione determinata o successivamente alla loro modifica (normalmente ogni volta che un documento viene salvato). I vantaggi delle soluzioni cloud sono l'automatizzazione, l'accesso ai file da qualsiasi luogo e in molti casi la protezione mediante crittografia. Inoltre, poiché i dati risiedono nel cloud, i disastri domestici come fuoco o furto non influiscono sul backup. Gli svantaggi sono costituiti dal tempo richiesto per eseguire il backup, che può essere lungo, e dal recupero di grandi quantità di dati. La privacy e la sicurezza possono inoltre essere un problema se il provider di backup non utilizza la crittografia o non dispone di controlli di sicurezza elevati.

In ultimo, non dimenticate i dispositivi mobili: normalmente la maggior parte dei dati, come email, eventi di calendario e contatti, sono già memorizzati nel cloud. Tuttavia, le configurazioni delle app mobili, le foto recenti e le preferenze di sistema potrebbero non essere considerate. Se si esegue il backup del dispositivo mobile, non solo si conservano queste informazioni, ma è anche più facile trasferire i dati quando si effettua l'aggiornamento a un nuovo dispositivo. Un iPhone / iPad può eseguire il backup automatico di iCloud di Apple. Android o altri dispositivi mobili dipendono dal produttore o dal fornitore di servizi. In alcuni casi, potrebbe essere necessario acquistare applicazioni mobili sviluppate appositamente per effettuare i salvataggi.

Il ripristino

Una volta che avrete salvato i dati, siete giunti a metà del guado: per terminare il processo, dovete essere sicuri di poterli recuperare successivamente. Controllate periodicamente che i backup funzionino recuperando un file e verificando che sia quello che vi aspettate. Assicuratevi, inoltre, di eseguire un backup completo del sistema prima di un aggiornamento importante (ad esempio quando adottate un nuovo computer o un dispositivo mobile) o di una riparazione (come la sostituzione di un disco rigido) e verificate che sia ripristinabile.

Salvataggi e ripristino

Punti chiave

- A prescindere dalla soluzione utilizzata per il backup dei dati, assicuratevi di automatizzare i salvataggi e di controllarli regolarmente.
- Durante la ricostruzione di un sistema dal backup, assicuratevi di riapplicare le patch e gli aggiornamenti più recenti prima di utilizzarlo nuovamente.
- I backup obsoleti che non sono più necessari costituiscono un onere: distruggeteli per impedirne l'accesso da parte di persone non autorizzate.
- Se utilizzate una soluzione cloud, verificate politiche e reputazione del provider, e assicuratevi che soddisfi le vostre esigenze. Ad esempio, vengono crittografati i dati memorizzati? Chi ha accesso ai backup? Viene impiegata un'autenticazione forte come la verifica in due passaggi?

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
securingthehuman.sans.org/ouch/archives

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 Passphrase:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_it.pdf
La verifica in due passaggi:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_it.pdf
Usare il cloud in modo sicuro:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201611_it.pdf
La crittografia:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201606_it.pdf
Il Ransomware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201608_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley