SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Novembre 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Usare il cloud in modo sicuro

Introduzione

Il termine Cloud può assumere vari significati, ma quello più utilizzato definisce un servizio disponibile su Internet per conservare e gestire dati e/o sistemi. Un vantaggio del Cloud è la possibilità di accedere facilmente ai dati e poterli sincronizzare tra diversi dispositivi in qualsiasi parte del mondo e condividere informazioni con chiunque. Chiamiamo questi servizi "il Cloud" perché non è necessario sapere dove i dati sono conservati fisicamente. Ecco alcuni esempi di Cloud computing: creare documenti con Google Doce, condividere file con Dropbox, creare un server con Amazon Cloud, memorizzare dati dei clienti su Salesforce o archiviare musica e immagini su Apple iCloud. Si tratta di servizi online mirati ad aumentare la produttività, ma purtroppo caratterizzati da rischi peculiari. In questa newsletter scopriremo come poter ottenere il massimo dal Cloud con un occhio di riguardo sulla sicurezza.

L'autore di questo numero

Dave Shackleford (**@daveshackleford**) è un consulente professionale, fondatore di Voodoo Security e autore di diversi corsi SANS, tra cui "Security 579: Virtualization and Private Cloud Security" e "Security 524: Cloud Security Fundamentals".

Selezionare un fornitore

Il Cloud non è né il bene né il male: è solo uno strumento da usare sia al lavoro sia a casa per vari scopi. Quando usate i servizi Cloud state consegnando i vostri dati privati a qualcuno da cui vi aspettate che siano mantenuti al sicuro e sempre disponibili. Per questi motivi dovete assicurarvi di scegliere il Cloud in modo appropriato. Per ciò che riguarda i sistemi informativi del vostro lavoro o i dati aziendali rivolgetevi al vostro superiore per verificare che la vostra azienda permetta l'uso dei servizi Cloud. Se potete farne uso, verificate quali servizi possono essere utilizzati e quali policy ne regolamentalo l'utilizzo. Se state pensando al Cloud per un uso personale, considerate i seguenti punti.

1. **Il supporto**. È facile ottenere supporto o risposte alle vostre domande? Esiste un indirizzo email da contattare, un forum dove poter scrivere o una lista di domande frequenti sul sito?
2. **Semplicità**. Il servizio è facile da usare? Più un servizio è complesso, più è facile commettere errori, esporre le proprie informazioni o anche perdere. Selezionate un fornitore di servizi Cloud semplice da capire, configurare e usare.

Usare il cloud in modo sicuro

3. **Sicurezza**. Quali dei vostri dati vengono collezionati? Come vengono trasmessi i dati dal vostro computer al Cloud e come vengono conservati? Sono protetti da cifratura, e, se sì, chi li può decifrare?
4. **Termini di servizio**. Prendetevi un momento per leggere i Termini di servizio: spesso sono estremamente semplici da comprendere. Verificate chi può avere accesso ai dati e quali siano i vostri diritti legali, così come quali sono le vostre responsabilità e quelle che si assume il provider.

Il Cloud rende le vostre informazioni più accessibili e vi rende più produttivi, ma siate cauti su come accedete e condividete le vostre informazioni

Proteggere i propri dati

Una volta che avrete selezionato i vostri servizi Cloud, il passo successivo è fare in modo di utilizzarli in modo appropriato. Il modo di accedere e condividere i dati ha spesso effetti sulla loro sicurezza. Ecco alcuni degli accorgimenti che potete adottare:

1. **autenticazione**: usate una password forte e unica per autenticare il Vostro account. Se il fornitore permette l'utilizzo della verifica in due passi, vi raccomandiamo di abilitarla. Questo è uno degli elementi fondamentali per proteggere il vostro account;
2. **condividere file e cartelle**: il Cloud rende la condivisione fin troppo semplice. Nel caso peggiore, potrebbe capitarvi di credere di condividere i file solo con persone specifiche, mentre invece li avete resi disponibili pubblicamente a tutta l'Internet per errore. Il miglior modo per proteggervi è di impostare il default per non condividere i vostri file con nessuno e permettere solo a persone specifiche (o a gruppi di persone) di avere accesso a file o cartelle specifiche sulla base della necessità. Quando non sussiste più la necessità di accedere ai vostri file, rimuoveteli. Il fornitore dovrebbe fornirvi un modo semplice per tracciare chi ha accesso ai vostri file;
3. **condividere file e cartelle con un link**: una caratteristica comune di alcuni servizi Cloud è la possibilità di creare link web che puntino ai vostri file, in modo da poterli condividere in modo semplice fornendo un link a chiunque desideriate. Questo approccio però non è molto sicuro poiché chiunque conosca il link potrebbe aver accesso ai vostri dati personali. Anche se inviate il link a una sola persona, esso potrebbe venire condiviso con altri o apparire nei risultati di un motore di ricerca. Se condividete file in questo modo, assicuratevi di disabilitarlo una volta che non è più necessario, impostando una data di scadenza o proteggendolo con una password;

Usare il cloud in modo sicuro

4. **impostazioni**: esaminate le impostazioni di sicurezza del servizio Cloud. Ad esempio, se condividete un file con qualcuno, quest'ultimo può condividerlo a sua volta con altri senza il vostro consenso? Verificate anche che ci sia il modo di sapere chi ha condiviso i vostri contenuti e quando. Potete limitare la condivisione alla modalità "sola lettura" piuttosto che alla "lettura e scrittura"? (nel senso che anche altri possono modificare i file);
5. **antivirus**: assicuratevi di aver installato l'ultima versione dell'antivirus sul computer e su tutti i dispositive che hanno accesso ai vostri dati. Se i file che condividete vengono infettati, altri computer che accedono agli stessi file potrebbero infettarsi a loro volta.

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

La verifica in due passaggi:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_it.pdf
Le Passphrase:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_it.pdf
I Password Manager:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_it.pdf
Il Malware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_it.pdf

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