La newsletter mensile sulla sicurezza informatica per gli utenti di

OUCH!

IN QUESTO NUMERO...

- Introduzione
- Scegliere un fornitore
- Mettere al sicuro i dati

Usare il Cloud in modo sicuro

Introduzione

Il Cloud è una tecnologia che sia le aziende sia i privati stanno adottando sempre più diffusamente. Il termine "Cloud" può assumere diversi significati, ma noi considereremo quello più diffuso ovvero l'utilizzo di un fornitore di servizio su Internet per conservare e gestire i propri dati. Uno dei vantaggi del Cloud non risiede solo nella possibilità di accedere e sincronizzare le informazioni dai vari device di cui disponiamo e da ogni parte del mondo, ma anche nel poter condividere le informazioni con chiunque desideriamo. La ragione per cui questo servizio è stato denominato "Cloud" (nuvola) risiede nel fatto che spesso non è possibile sapere dove i dati sono conservati fisicamente. Tra gli esempi di Cloud computing troviamo la gestione di documenti con Google Docs, la condivisione di file con Dropbox, la possibilità di configurare un proprio server su Amazon Cloud e la memorizzazione di musica e immagini su Apple iCloud. Sebbene questi servizi online ci permettano di essere più produttivi, sono purtroppo caratterizzati da una serie di rischi piuttosto peculiare: in questa newsletter vi spiegheremo come utilizzare il Cloud in sicurezza.

L'autore di questo numero

James e Kelli Tarala (@isaudit / @kellitarala) sono principal consultans presso Enclave Security, nonché autori di diversi corsi SANS tra cui "SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls" e "MGT 415: A Practical Introduction to Risk Assessments".

Scegliere un fornitore

Il Cloud non è la panacea a tutti i problemi e nemmeno qualcosa di cui aver paura: è solo uno strumento per svolgere un compito, sia al lavoro, sia a casa. Quando usate un servizio Cloud state affidando i vostri dati privati a degli estranei, aspettandovi che vengano mantenuti al sicuro e sempre disponibili. Per questo motivo dovete operare delle scelte adeguate: per ciò che riguarda l'ambito professionale, riferitevi al vostro superiore per verificare la possibilità di utilizzare servizi di Cloud computing. Nel caso sia possibile, chiedete quali servizi Cloud sono disponibili quali siano le policy che li regolano. Se invece state pensando al Cloud per un uso personale, dovete considerare i seguenti punti:

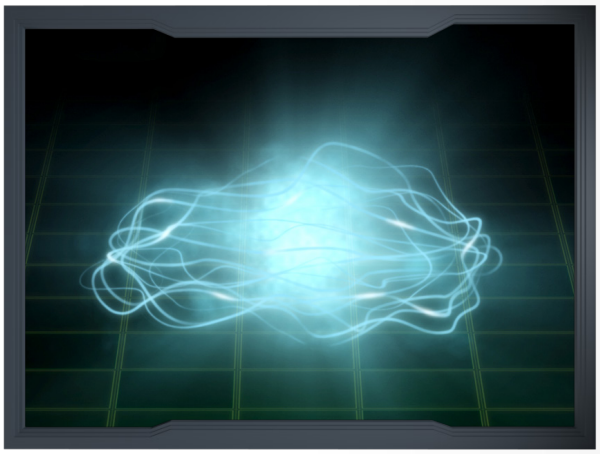
1. **Il supporto**. È facile ottenere aiuto o delle risposte alle proprie domande? Esiste un numero di telefono o un indirizzo email a cui riferirsi? Esistono altre possibilità di supporto, come i forum pubblici o una serie di FAQ?
2. **La semplicità**. Il servizio è semplice da usare? Più un servizio è complesso, più facilmente si possono compiere errori e quindi esporre o perdere incidentalmente le proprie informazioni. Usate un fornitore di Cloud

© The SANS Institute 2014

Usare il Cloud in modo sicuro

che trovate semplice da utilizzare e configurare.

3. **Sicurezza**. Come vengono trasmessi i vostri dati dal computer al Cloud? La connessione è protetta da crittografia? Come vengono conservate le informazioni? Sono cifrate? In caso affermativo, chi le può decifrare, oltre a voi?
4. **Termini di servizio**. Leggete i Termini di servizio (non preoccupatevi, a volte sono sorprendentemente semplici). Verificate quali siano i vostri diritti legali e chi possa avere accesso ai vostri dati.



Il Cloud può rendere i vostri dati più accessibili e aiutarvi a essere più produttivi: siate però cauti nel conservare e condividere le informazioni.

Mettere al sicuro i dati

Una volta che avrete selezionato il vostro servizio di Cloud, il passo successivo consiste nell'utilizzarlo in modo appropriato: come accedete e condividete i dati può infatti avere effetti positivi o negativi sulla sicurezza dei vostri file. Ecco alcuni degli elementi da considerare.

1. **Autenticazione**. Usate una password forte e dedicata per autenticarvi al vostro account sul Cloud. Se il fornitore mette a disposizione la verifica in due passi, vi raccomandiamo di farne uso.
2. **Condivisione di file e cartelle**. Il Cloud facilita la condivisione, a volte anche troppo. In uno degli scenari peggiori, potreste rendere i vostri file o le vostre cartelle disponibili pubblicamente all'intero pubblico di Internet. Il modo migliore per proteggervi è di impostare di default di non condividere nessun file con nessuno. Potrete quindi specificare quali persone o gruppi di persone potranno accedere a file o cartelle specifici, sulla base della necessità di sapere. Quando qualcuno non avrà più bisogno di accedere ai vostri file, rimuovetene il permesso. Il vostro fornitore di Cloud dovrebbe fornire un modo semplice per tracciare chi ha accesso a file e cartelle.
3. **Condivisione di file e cartelle con un link**. Una caratteristica comune di alcuni servizi Cloud è la possibilità di creare link che puntino a file o cartelle, permettendovi di condividerli con chi volete semplicemente fornendo un URL. Questo approccio però è molto poco sicuro poiché chiunque conosca questo indirizzo potrà avere accesso ai vostri file personali. Immaginate di inviare il link a una sola persona: questi potrebbe decidere di condividerlo con altri che potrebbero fare lo stesso e così via fino a comparire nei risultati di un motore di ricerca. Se condividete dati usando un link, assicuratevi di disabilitarlo una volta che non è più necessario o proteggetelo con una password, se possibile.
4. **Configurazione**. Dovete cercare di capire le impostazioni di sicurezza offerte dal vostro fornitore. Se, ad

Usare il Cloud in modo sicuro

esempio, condividete una cartella con qualcuno, questi ha la possibilità di condividerla con altri senza che voi lo sappiate?

5. **Antivirus**. Assicuratevi di avere l'antivirus sempre aggiornato sia sul vostro computer, sia su ogni dispositivo che utilizzate per condividere i vostri dati. Se un file che condividete viene infettato, anche gli altri computer che vi hanno accesso potrebbero contrarre a loro volta lo stesso virus.
6. **Salvataggi**. Anche qualora il vostro fornitore di Cloud effettuasse il salvataggio dei vostri dati, è necessario che anche voi facciate lo stesso con regolarità: non solo li proteggerete nel caso il servizio a cui vi appoggiate non fosse disponibile o cessasse le sue attività all'improvviso, ma renderete più semplice il compito di recuperare grandi quantità di dati andate perdute. Informatevi presso il vostro fornitore sulla frequenza dei salvataggi e sul loro mantenimento e non dimenticate di verificare la possibilità di recuperare versioni precedenti dei file.

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

Usare password forti:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_it.pdf
Programmi di gestione password:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_it.pdf
Il salvataggio dei dati:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_it.pdf

OUCH! è pubblicata dal progetto Securing The Human del SANS Institute e viene distribuita con licenza Creative Commons BY-NC-ND 4.0.
Sei libero di distribuire questa newsletter o utilizzarla nei tuoi programmi di awareness senza però modificarne i contenuti.
Per traduzioni o ulteriori informazioni, contatta ouch@securingthehuman.org.

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus