SOPHOS

Come utilizzare i servizi cloud con Persistent Encryption

Protezione dei dati da personale non autorizzato e in-the-cloud

Di **Barbara Hudson**, Product Marketing Manager

Si ritiene che i servizi di cloud storage pubblici come Dropbox vengano utilizzati da più di 50 milioni di persone, fra dipendenti interni e road warrior, per condividere e trasferire i file. Sono convenienti e facili da usare, ma la loro accessibilità può mettere a repentaglio le policy di IT security quando si tratta di condividere dati di natura riservata. Molte aziende adottano un approccio estremamente restrittivo a queste tecnologie, implementando sistemi di Web filtering per prevenire l'accesso a servizi di Web storage, oppure utilizzando application control per impedire l'installazione di applicazioni di cloud storage.

Questo white paper indica come applicare la cifratura a qualsiasi scenario, per consentire agli utenti di gestire l'accesso al cloud senza mettere a repentaglio i dati o l'intera azienda.

I dati sono ovunque

Che cosa si intende per "cloud computing" e "cloud"? Per i media, il “cloud” è l'ultimissimo tormentone ed è un termine che viene utilizzato per descrivere lo storage virtuale remoto di ultima generazione.

Per gli esperti IT significa un modo per prelevare, archiviare, ridistribuire e gestire diversi zettabyte di dati.

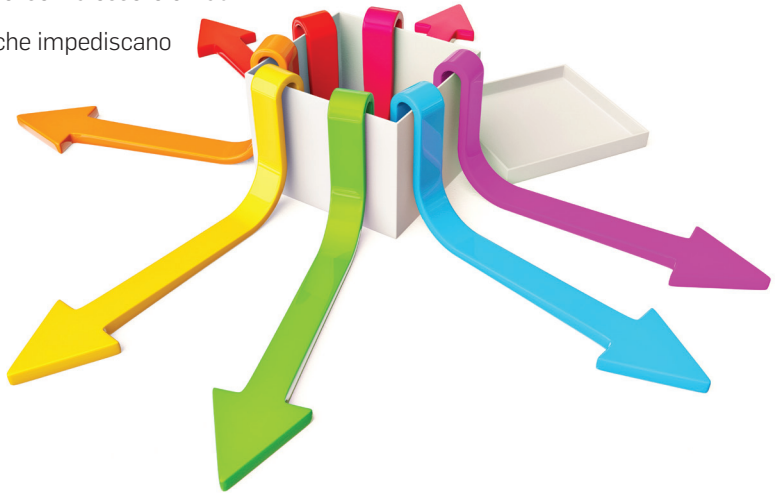
I servizi di cloud storage come Dropbox, che vanta più di 50 milioni di utenti, Egnyte o Microsoft SkyDrive sono utili strumenti che consentono di accedere ai propri file da qualsiasi dispositivo o luogo geografico. Questi servizi sono anche flessibili, scalabili e facili da installare. In quanto applicazioni SaaS (Software-as-a-Service), sono semplici da aggiornare e disponibili a chiunque desideri accedervi. Tuttavia, una maggiore accessibilità dei dati significa anche una più elevata vulnerabilità ai criminali informatici.

Oggi gli utenti possono lavorare da qualsiasi luogo geografico; è quindi fondamentale che la protezione dei dati sia altrettanto mobile e all'altezza della situazione. I dati sono già in circolazione su più dispositivi e infrastrutture e il numero di utenti che vi accede supera qualsiasi cifra mai raggiunta in passato. Vengono continuamente passati di mano in mano. Può darsi infatti che i vostri utenti stiano già utilizzando cloud pubblici senza vostro consenso o approvazione.

Di conseguenza, il tradizionale approccio alla sicurezza del perimetro di rete basato sul "sistema" non è più abbastanza. Il nuovo perimetro deve basarsi sui dati, e va protetto ovunque tali dati siano in circolazione, sia che vengano archiviati internamente, nel cloud pubblico, oppure che vengano visualizzati da dispositivi mobili.

Quando si pensa alla sicurezza in-the-cloud, è necessario considerarne le implicazioni per i dati aziendali e porsi le seguenti domande:

- Come viene gestita la complessità delle password per gli utenti che dispongono di account Dropbox?
- State adottando adeguate misure di sicurezza volte a limitare l'accesso degli utenti a dati che non sarebbero dovuti neppure essere caricati nel cloud pubblico?
- I file vengono trasferiti su servizi cloud pubblici senza essere cifrati?
- State esplicitamente implementando policy che impediscano ai dipendenti di scaricare sul proprio desktop un servizio di cloud storage?



Acquistare familiarità con il cloud

I dati non sono una risorsa statica. Aumentano, si modificano, e influiscono sulla curva di successo della vostra azienda sia nel presente che nel futuro. Per questo motivo i dati hanno bisogno di sicurezza, protezione e riservatezza. Inoltre, la loro funzione è quella di essere condivisi – con dipendenti, partner, dirigenti, consiglio di amministrazione, e chiunque abbia investito nella performance della vostra azienda.

L'aumento dell'uso di smartphone e PC tablet rappresenta una rivoluzione nel modo in cui avvengono le varie collaborazioni. Fornendo tali dispositivi in dotazione ai vostri dipendenti, o anche consentendone l'uso come parte delle vostre policy "Bring Your Own Device" (BYOD), spalancate le porte a enormi opportunità di comfort e incremento della produttività per gli utenti.

È risaputo che al giorno d'oggi dati e proprietà intellettuale siano fra le risorse più importanti per la maggior parte delle aziende. Difenderne sicurezza, integrità e riservatezza diventa quindi una questione di primissima priorità, che ne abilita il valore e il vantaggio competitivo.

In ultima analisi, si tratta di sfruttare le varie possibilità. Il business ha bisogno di informazioni, e per soddisfare tale esigenza queste informazioni devono essere accessibili e applicabili alla creazione di valore. Troppa sicurezza potrebbe privarvi di opportunità. Troppo poca rischia di provocare la perdita di importanti lead.

Non si può dare niente per scontato. Fin quando vi saranno dati pronti per essere visualizzati e condivisi, si troveranno anche servizi esterni che permettano agli utenti di farlo. Quando si tratta di svolgere il proprio lavoro e ottimizzare la produttività, è facile che gli utenti trascurino procedure che ritengono troppo severe e che quindi limitano, piuttosto che incoraggiare, le best practice.

4

milioni di record violati

solamente nel 2010,

secondo il report Data Breach Investigations del 2011, a cura di Verizon.

$7,2

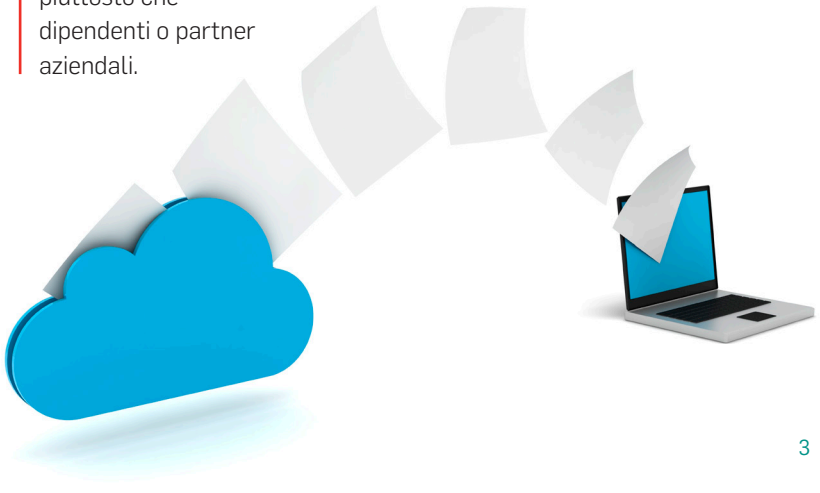
milioni di dollari per caso di violazione dei dati

Il costo a cui ammonta un caso di perdita dei dati corrisponde a $214 per record compromesso.

92

percento delle violazioni avviene per mano di hacker esterni

piuttosto che dipendenti o partner aziendali.



Applicare la cifratura dei dati ovunque

Spesso le informazioni di natura sensibile archiviate in un determinato database o applicazione sono protette, ma perdono qualsiasi difesa una volta trasferite altrove. Ne sono tipici esempi i fogli elettronici di Excel e i file dei clienti trasferiti tramite dispositivi USB non cifrati, privi di protezione, o ad alto rischio di furto o smarrimento. Tutto ciò può aprire la porta ad attacchi che rischiano di compromettere e violare i dati.

Negli ambienti IT moderni, i dati vengono cifrati solamente se un'applicazione dichiara esplicitamente di utilizzare la cifratura. In assenza di applicazioni che cifrino i dati, questi ultimi rimangono in chiaro e sono quindi vulnerabili. Con la cifratura, i dati che vengono lasciati "sparsi in giro" su condivisioni dei file o cloud, oppure all'interno della rete, rimangono inaccessibili agli utenti non autorizzati. In pratica, i dati risultano non protetti per default.

Persistent encryption – ovvero proteggere i dati mentre sono in transito, nel cloud o all'interno della rete – è il modo migliore per difendersi dal rischio di violazione dei dati. Si tratta di un approccio all'IT security radicalmente diverso da quello utilizzato al giorno d'oggi. Persistent encryption è anche un concetto semplice e trasparente per gli utenti. I dati rimangono sempre e comunque cifrati per gli utenti con diritto di accesso ai file.

Se un criminale informatico riesce a prelevare i dati ma non possiede la relativa chiave di cifratura, tali dati perdono qualsiasi valore. E il loro business model basato su furto e rivendita di informazioni di natura sensibile diventa sempre meno vantaggioso.

Come funziona la Persistent Encryption?

Una soluzione end-to-end per la gestione diretta della cifratura dei dati archiviati localmente o in-the-cloud consente agli utenti di impostare, gestire e conservare chiavi di cifratura per la messa in sicurezza di determinati file.

Gli utenti possono accedere ai dati in qualsiasi momento, sia che siano protetti dal firewall o che si trovino nel cloud. SafeGuard Encryption for Cloud Storage mantiene cifrati tutti i file archiviati nel cloud, sia che vengano copiati, sia che vengano trasferiti su altre unità, reti o dispositivi; esempi di tali situazioni sono dipendenti che prima di licenziarsi prelevano informazioni aziendali di natura riservata.

La cifratura viene effettuata sul client prima della sincronizzazione dei dati, in modo da garantirvi pieno controllo sulla sicurezza delle vostre informazioni. Ciò significa non avere nessuna preoccupazione legata a un'eventuale violazione della sicurezza del vostro servizio di cloud storage. Le chiavi centralizzate garantiscono a gruppi e utenti l'accesso ai file. All'addetto alla sicurezza aziendale viene concesso il diritto di accedere a queste chiavi, per poter a sua volta garantire a chi di dovere l'accesso in qualsiasi momento.

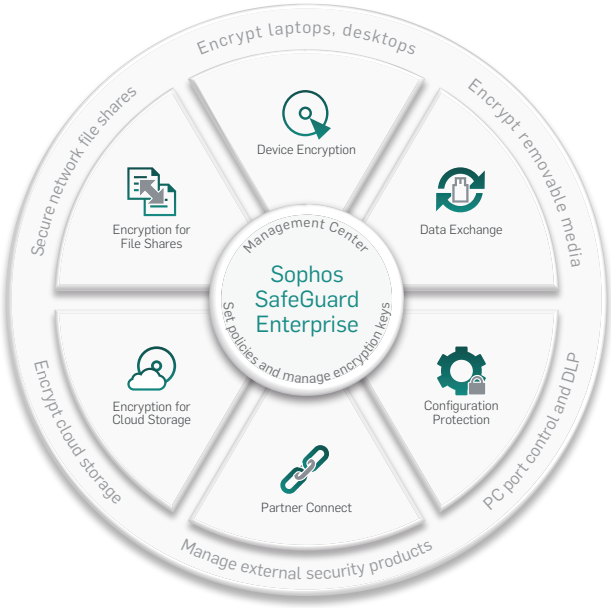
Proteggere i dati, ovunque si trovino

Con SafeGuard Encryption for Cloud Storage, non importa da dove venga effettuato l'accesso ai file sul servizio di cloud storage: computer domestici, laptop aziendali, oppure, verso la fine del 2012, lettori di file per iOS (ad es. iPhone, iPad) e dispositivi Android.

Nota: su questi dispositivi, i contenuti cifrati sono visualizzabili ma non modificabili.

Sophos SafeGuard Encryption

Solamente Sophos è in grado di offrire cifratura per computer, cartelle condivise e supporti rimovibili degli utenti, nonché anche per i dati archiviati in-the-cloud. Tutta questa versatilità viene abilitata con un unico agente e una singola console di gestione. La nostra è una soluzione di cifratura certificata che pone un freno alla violazione dei dati, facilitando il rispetto della compliance senza interferire con le consuete attività lavorative. E vi permette di risparmiare tempo prezioso, grazie alla sua semplicità di gestione.



Scegliete i moduli che si addicono alle vostre esigenze

Management Center

Un unico punto centrale di gestione per tutta la cifratura – anche in ambienti IT misti. Chiavi e le policy di gestione possono essere implementati nell'intera azienda.

- Monitoraggio di computer Windows e Mac
- Gestione centralizzata delle chiavi da un'unica console
- Opzione di self-help locale per il recupero delle password

Device Encryption

Cifratura trasparente dei dati presenti su laptop, desktop e supporti esterni, con protezione degli utenti contro accesso non autorizzato e perdita o furto dei dati.

- Cifratura trasparente e completa del disco
- La Power-on Authentication protegge i dispositivi già in fase di avvio
- Gestione completa di policy e chiavi di gestione per questo ed altri moduli dal Management Center

Data Exchange

Scambio sicuro dei dati fra clienti e partner commerciali per mezzo di supporti rimovibili, anche in mancanza di un'applicazione di cifratura.

- I supporti rimovibili possono contenere sia dati cifrati che non cifrati
- Monitoraggio dei file copiati o trasferiti su dispositivi di memorizzazione rimovibili
- Cifratura e decifrazione in background trasparenti

Encryption for File Shares

Protezione dei dati sulle unità locali e sui server di rete a livello di file e directory.

- Gli amministratori sono in grado di gestire i file senza dover accedere a informazioni di natura sensibile.
- Chiavi gestite in maniera centralizzata per consentire l'accesso a utenti o gruppi
- Ideale per team e gruppi di progetto

Encryption for File Shares include anche

Encryption for Cloud Storage

Cifratura dei file caricati sul servizio di cloud storage da computer gestiti, con abilitazione dell'accesso da altri tipi di dispositivo.

- Cifratura automatica per Dropbox, Egnyte e Microsoft SkyDrive (l'esecuzione immediata è possibile anche con diverse altre soluzioni)
- Cifratura dei file prima della loro sincronizzazione con il cloud
- Sono ora disponibili visualizzatori dei file su Dropbox compatibili con iOS e Android

Partner Connect

Gestione dei dispositivi cifrati con BitLocker dalla stessa console utilizzata per tutti gli altri tipi di cifratura.

- Amministrazione centralizzata per tutte le soluzioni di cifratura, incluse quelle per disco, condivisioni dei file, cloud e supporti rimovibili
- Policy di IT security omogenee, anche in ambienti misti, ovvero con o senza BitLocker
- Agevoli funzionalità di recupero, grazie al backup centralizzato delle chiavi e appositi meccanismi di emergenza

In sintesi

I dati sono ovunque. E anche cifrare gli hard disk non basta più a garantire la sicurezza, indipendentemente da dove siano archiviate le informazioni. Controllare l'utilizzo dei dati è essenziale, altrimenti si rischia che possano essere trasferiti su cloud, dispositivi mobili, o addirittura PC personali. La persistent encryption garantisce che questi dati non generino falle nei vostri sistemi di data security, ed evita che eventuali errori umani rischino di mettere a repentaglio le vostre informazioni.

Tempi più rapidi a vantaggio del business, grazie ai servizi di cifratura Sophos

I servizi di cifratura Sophos vengono descritti qui di seguito, insieme a un tipico programma di implementazione.

Giorno 1	‣ Panoramica della soluzione e pianificazione ad alto livello ‣ Installazione dei componenti del server ‣ Progetto pilota di installazione per un massimo di 5 computer client
Giorno 2	‣ Formazione per amministratore, addetti alla sicurezza, helpdesk ‣ Pianificazione di policy e delivery
Giorno 3	‣ Assistenza e supporto per il delivery

Osservatela in azione

Richiedete una prova gratuita di SafeGuard Encryption for Cloud Storage

Vendite per Italia:
Tel: (+39) 02 911 808
E-mail: sales@sophos.it

Boston, USA | Oxford, Regno Unito

Whitepaper Sophos 10.12v2.dNA

SOPHOS