



SENTIRSI SICURI NELLA “NUVOLA”

di Eran Feigenbaum, Responsabile della Sicurezza per Google Apps

Con il progressivo trasferimento delle applicazioni dal desktop a internet, sono aumentate anche le preoccupazioni per la sicurezza. Se i nostri dati sono archiviati nei server di un'altra azienda (come avviene nel nuovo scenario del cloud computing), come possiamo avere la garanzia che siano al sicuro?

Potrà sembrare a prima vista paradossale, ma i dati salvati “nella nuvola” sono molto più sicuri di quelli nel nostro computer.

Il cloud computing, cioè il fatto di poter accedere a software e servizi IT via web attraverso un browser, implica un cambio di paradigma paragonabile al trasferire i propri gioielli dal cassetto di casa per portarli in una cassetta di sicurezza in banca. La banca sfrutta economie di scala: dispone di guardie, cassette di sicurezza, video sorveglianza: tutti servizi di cui normalmente un privato non dispone. La stessa cosa vale per i dati: i fornitori di servizi in modalità cloud, come Google, dispongono di strumenti per proteggere i dati di milioni di utenti ogni giorno, permettendo al cliente di usufruire di queste economie di scala a una spesa molto ridotta. Sono oltre 1000 le persone impegnate nella divisione Enterprise di Google, tra cui alcuni dei più famosi esperti di sicurezza al mondo, che lavorano per garantire che i dati dei clienti siano al sicuro.

È sufficiente leggere i titoli dei quotidiani per vedere ogni giorno notizie sulla perdita di dati: dati su chiavette USB, notebook e lettori MP3 persi o rubati...

Un rapporto pubblicato l'anno scorso da Credant Technologies ha rivelato che nel 2008 i passeggeri dei taxi di New York hanno dimenticato sui sedili 31.544 cellulari e 2.752 altri dispositivi portatili tra notebook, iPod e chiavette USB.

Le aziende dedicano una grande quantità di tempo e risorse alla protezione dei dati. Cos'è quindi che non funziona? Come ha riportato l'IT Policy Compliance Group l'anno scorso, il 75% dei casi di perdita di dati sensibili è dovuto all'errore umano. Quando ero responsabile della sicurezza in una grande azienda di servizi finanziari raccomandavo sempre al mio team di fare in modo di semplificare le procedure per la sicurezza per assicurarsi che gli utenti le seguissero. Spesso i dipendenti desiderano poter lavorare da casa per terminare le loro attività. Soprattutto ai dipendenti più giovani risulta strano lavorare dalle 9,00 alle 18,00 sempre alla stessa scrivania. Permettete loro di accedere a dati salvati e protetti nella nuvola in qualsiasi momento e da qualsiasi luogo e ridurrete automaticamente il rischio che li perdano. Io, ad esempio, ho scritto questo pezzo nel mio ufficio in California, l'ho modificato nel mio hotel in Europa usando un altro PC condiviso con i miei colleghi e poi l'ho pubblicato sul blog di Google dal notebook di un altro collega. Non ho mai dovuto inviarlo via mail, scaricarlo sul mio notebook o salvarlo in una chiavetta USB. È stato creato nel cloud ed è protetto nel cloud.

La nuvola offre altri importanti vantaggi per la sicurezza. Molte organizzazioni impiegano dai 30 ai 60 giorni per installare gli aggiornamenti per la sicurezza (le cosiddette “patch”) e già questo è un problema. Addirittura, molte aziende con le quali ho parlato hanno ammesso che spesso arrivano a impiegare anche dai 3 ai 6 mesi per installare gli aggiornamenti per la sicurezza. Questo significa che le applicazioni e i sistemi informatici tradizionali sono esposti al rischio di vulnerabilità per un lungo periodo. Noi invece gestiamo un ambiente informatico particolarmente omogeneo così quando è il momento di installare gli aggiornamenti lo possiamo fare in modo rapido e uniforme su tutti i nostri sistemi.

Infine, c'è la questione della sicurezza fisica dei nostri data center e dell'affidabilità dei nostri prodotti. In Google replichiamo i dati degli utenti in diversi data center, in modo che, dovesse succedere qualcosa a un data center, la nostra infrastruttura garantisce che i dati rimangano sicuri e accessibili. Mentre ero in Europa, è successo un fatto che supporta la bontà del nostro approccio: mi trovavo a Milano quando un'alluvione ha colpito il paese mettendo fuori uso alcuni importanti data center. Mentre una serie di aziende locali ne hanno subito le conseguenze, i clienti di Google non hanno avuto nessuna interruzione di servizio.

Bisogna ammettere che nessun sistema è sicuro al 100%. Talvolta i sistemi possono presentare problemi legati alla sicurezza. La questione è: quali persone, procedimenti o tecnologie abbiamo a disposizione per minimizzare l'impatto di questi eventi e quanto riusciamo ad intervenire tempestivamente nell'affrontare una criticità. Noi di Google Enterprise abbiamo creato i nostri sistemi pensando prima di tutto alla sicurezza e contiamo su un team al lavoro 7 giorni su 7 in grado di individuare nuove minacce e rispondere rapidamente. Oltre 2 milioni di aziende hanno già effettuato la migrazione a Google Apps e il numero sta crescendo in modo esponenziale, con 3.000 nuove aziende che ogni giorno passano a Google Apps.

Siamo convinti che il cloud sia il futuro della tecnologia informatica. Le soluzioni web sono vantaggiose in termini di costo, collaborative e molto spesso più affidabili. La Commissione Europea e la sua agenzia per la security [ENISA](#) stanno portando avanti almeno 3 studi sul cloud computing e con loro abbiamo discusso dei possibili modi per dimostrare a utenti aziendali e privati come rispettiamo la sicurezza e la privacy dei loro dati.

Spero di essere riuscito a spiegare perché la questione della sicurezza dovrebbe essere vista più come un vantaggio che come un fattore negativo nel passaggio al cloud computing.