EGOSECURE ENDPOINT SECURITY

C.A.F.E. PER IL CLOUD

prodotto distribuito da:

CoreTech

EGOSECURE

ENJOY DATA PROTECTION

CONCETTI PER L'USO IN SICUREZZA
DEI SERVIZI DI STORAGE BASATI SUL CLOUD

Il cloud è uno dei trend più forti del momento nel mondo IT. Senza dubbio offre vantaggi significativi per chi ha la necessità di avere a disposizione i suoi dati in qualsiasi momento, ovunque si trovi. Non dobbiamo dunque meravigliarci nello scoprire che – in un ambiente di lavoro sempre più flessibile e globale – molte aziende hanno deciso di adottare servizi cloud.

Purtroppo negli ultimi mesi una serie di notizie importanti provenienti dagli Stati Uniti ha reso molti responsabili aziendali particolarmente scettici rispetto alla reale sicurezza dei dati nel cloud. Stiamo parlando dello scandalo dell'NSA e degli altri servizi governativi segreti che si sono dimostrati particolarmente interessati ai dati altrui.

Ovviamente tutti i fornitori di servizi cloud ci tengono a presentare la loro offerta come sicura. In alcuni casi anzi mettono in primo piano la nazionalità stessa del cloud (italiano, piuttosto che tedesco o europeo) per dare perlomeno l'idea di una maggiore protezione dall'accesso indiscriminato delle citate agenzie americane.

Di solito i fornitori di servizi cloud tessono le lodi dei loro sistemi di cifratura presentandoli come un semplice meccanismo in grado di migliorare la sicurezza dei dati. Il problema è che sia le chiavi di cifratura, sia i dati, in questo caso si trovano di fatto nel cloud e sono dunque più facili da attaccare. La situazione cambia però quando le chiavi non sono disponibili né sono memorizzate on-line.

A dimostrazione di questo fatto basta far riferimento alle notizie legate allo scandalo Nsa: in alcuni casi il governo americano ha costretto i provider a fornire anche le chiavi di cifratura dei dati memorizzati sui loro server.

EgoSecure vi raccomanda di considerare l'approccio al cloud non ragionando solo sulla crittografia. Vi consiglia prima di tutto di partire da due semplici domande:

- Quali dati possono essere memorizzati nel cloud?
- Chi può effettivamente utilizzare il cloud per la memorizzazione?

Spesso basta rispondere a queste domande per capire quali elementi dell'azienda possono usufruire di questi servizi e quali limiti bisogna porsi, mantenendo sempre il controllo sui sistemi di crittografia dei dati che devono essere memorizzati online.

C.A.F.E. PER LA GESTIONE DELLA SICUREZZA NEL CLOUD

Il principio della gestione CAFE non tratta lo storage nel cloud in modo diverso da qualsiasi altra periferica di archiviazione presente in azienda. Il concetto di sicurezza è infatti omnicomprensivo e basta ragionare un attimo per capire che non c'è molta differenza tra una chiavetta Usb e un disco esterno, a parte qualche funzione specifica. L'obiettivo di una sicurezza completa ed effettiva può essere raggiunto solo dalla combinazione di queste funzioni (C.A.F.E.):

Controllo: definisce quale utente è autorizzato ad utilizzare un dato specifico. Solo i dipendenti che hanno la necessità di accedere a dati riservati per il loro lavoro devono averne effettivamente accesso.

Audit: tramite un processo di audit si possono tracciare le policy aziendali e – in caso di perdita dei dati – ci sono informazioni sufficienti per capire in che direzione muoversi.

Filtro: separare i dati critici da quelli non critici e bloccare l'accesso ai pericoli provenienti dall'esterno, come i cavalli di Troia.

Encrypt (crittografia): la cifratura rende inaccessibili i dati che si trovano al di fuori dell'azienda da parte di terzi o persone non autorizzate. Le policy devono essere scelte con cura e accettate e messe in pratica dagli utenti.

Management: la gestione di tutti i sistemi deve essere semplice e veloce e in particolare l'amministrazione deve essere user-friendly, per venire accettata da utenti e tecnici. Se la tecnologia di protezione non viene accettata non si può arrivare a una soluzione effettiva ed efficiente.

LE REGOLE PIÙ IMPORTANTI PER L'USO DEL CLOUD:

Le chiavi di cifratura non devono essere nel cloud ma devono restare entro le mura dell'azienda.

IMPLEMENTAZIONE PRATICA DEL PRINCIPIO C.A.F.E.

EgoSecure Endpoint è stato sviluppato in base al principio della gestione CAFE e fornisce tutte le possibili funzioni di una soluzione completa.

Il controllo permette di garantire l'accesso ai dati riservati soltanto a chi è effettivamente autorizzato. Non si possono memorizzare dati privi di diritti di accesso nel cloud.

L'Audit fornisce le informazioni di tipo forense che permettono di scoprire chi ha avuto accesso e a quali informazioni. Il tutto nel pieno rispetto dei diritti personali dei dipendenti. Il software può concedere l'accesso solo a 2 o 3 persone contemporaneamente, per avere la certezza che i file di registro non siano accessibili se non in seguito a un accordo.

L'**analisi dei contenuti** permette di filtrare tutto ciò che viene memorizzato nel cloud. L'**antivirus** protegge da virus e cavalli di troia provenienti dall'esterno. EgoSecure è una delle soluzioni più importanti del settore e vanta un livello di rilevamento dei virus particolarmente elevato. Il controllo delle applicazioni è una aggiunta perfetta che permette di bloccare anche i virus e i cavalli di Troia che ancora non sono riconosciuti dall'engine.

La **Cloud-Encryption**, la cifratura dedicata al cloud è effettuata al volo e in base ai file. Gli utenti non devono ricordarsi di svolgere azioni aggiuntive, tutto è automatico. Le chiavi di cifratura rimangono in azienda e non vengono mai trasferite nel cloud. I documenti sono dunque protetti da qualsiasi accesso non autorizzato.

Il pannello di gestione di EgoSecure Endpoint garantisce l'accettazione immediata da parte di amministratori e utenti. **L'installazione viene completata in poco tempo e offre già una protezione di base**. Non c'è bisogno di training dal momento che la soluzione è integrata nel workflow e non richiede azioni aggiuntive. Tutte le funzionalità sono controllate e monitorate dall'intuitiva console di management centralizzata.

+ EGOSECURE SI PAGA DA SOLO!

Vi state domandando qual è il costo di un soluzione per proteggere l'azienda dalla perdita dei dati? Grazie a un sistema integrato di gestione dei consumi la soluzione di EgoSecure costa pochissimo e si paga da sola.

EgoSecure permette di attivare la funzione di Green-IT non solo in modo centralizzato o in base a una pianificazione: garantisce la massima efficienza poiché il consumo energetico avviene solo quando i componenti del computer vengono effettivamente utilizzati. EgoSecure non dipende dal sistema operativo o dal software in uso, dunque è più efficiente dei pacchetti standard forniti dallo sviluppatore dell'Os.

In base all'hardware e ai costi locali dell'elettricità EgoSecure Green-IT permette di risparmiare dai 50 ai 100 euro all'anno a computer. Dunque si paga da solo in meno di un anno!

DICHIARAZIONI DEI CLIENTI

"Quello che ci piace davvero di EgoSecure è il suo concetto di funzionalità integrata come concetto generale. A differenza di altre software house che vendono una serie di singoli pacchetti separati, Egosecure offre una serie di componenti perfettamente integrati. In pratica il risultato è un consumo minimo di risorse per arrivare alla soluzione: semplicemente funziona. Per noi questo è importante dal momento che il pacchetto è sviluppato e migliorato con continuità e tutte le nuove funzionalità vengono immediatamente integrate nella soluzione in uso."

Jurgen Munk
Direttore IT di GroupM,
Dusseldorf

"EgoSecure non solo fornisce una serie di funzionalità particolarmente complete, ma lavora anche a stretto contatto con noi, con un livello di supporto decisamente sopra la norma"

Michael Kraemer
Pubblico ministero dell'ufficio per l'investigazione penale nella provincia di Saarland, Germania

"Grazie al suo eccellente livello di compatibilità EgoSecure è stata la prima soluzione a soddisfare le nostre esigenze."

Klaus Thomas
Comune della città di Baden