



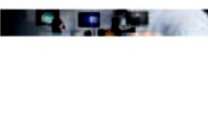
Lo storage as a service è il motore di crescita di CTERA

BIG DATA



Come governare la discontinuità introdotta dal mercato digitale

MOBILE



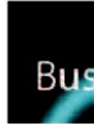
ENTERPRISE



Videointervista] Alberto Bullani, Country Manager,

Gli Speciali di ImpresaCity

RedHat Forum 2014 : Day, ancora un successo Open



Gli speciali di: IMPRESA city



Home Speciali Newsletter

Cerca sul sito...

Come conciliare Byod e accesso sicuro ai dati aziendali

Poiché anche in Italia ha ormai preso piede una certa accettazione dell'utilizzo di device personali anche per scopo di lavoro, il controllo degli accessi e una corretta amministrazione sono fondamentali.

di: **Roberto Bonino** del 01/04/2015 09:20

Mobility & Byod



Tweet 0 +1 0

Le anticipazioni del Rapporto **Assinform** 2015 (riferito all'anno passato) dicono, fra le altre cose, che la diffusione del **Byod** è stato uno dei fattori che ha favorito la crescita del business concentrato sull'**enterprise mobility**.

A livello globale, stando alle cifre diffuse da **Idc**, solo il 40% delle aziende autorizza i collaboratori ad accedere alle informazioni interne partendo da **terminali personali**, ma il 70% dei lavoratori indica di utilizzare comunque questi dati sui propri apparecchi, nonostante la presenza di direttive restrittive. In pratica, questo significa che **gli utenti aggirano i limiti imposti** e accedono alla rete aziendale spesso attraverso mezzi non sicuri o utilizzando **cloud storage**.

Al Cio spetta il compito di garantire la sicurezza, senza diffondere quella tipica percezione negativa che spinge a ignorare le regole interne e aggirare le barriere tecnologiche. Le due principali vie per prevenire comportamenti troppo rischiosi e gestire la circolazione dei contenuti sensibili appaiono il controllo degli accessi ai dati e l'amministrazione dei terminali mobili.

Il **Mobile Content Management (Mcm)** in genere deve rispondere alle esigenze di produttività e accessibilità, mantenendo i contenuti in **sicurezza** ovunque si trovino. Per i manager e i dipendenti, l'importante è sapere di poter accedere ai sistemi aziendali quando occorre e non perdere tempo nella ricerca delle informazioni. **Poter fornire ai clienti risposte più rapide e affidabili** rappresenta un guadagno concreto di produttività. In azienda, un sistema di condivisione dei file progettato per l'accesso remoto può autorizzare gli utenti in **Byod all'accesso dei contenuti attraverso un tunnel cifrato**. Inoltre, strumenti consolidati come **Active Directory** consentono agli amministratori di gestire l'accesso ai contenuti in ambienti eterogenei.

Il controllo dell'accesso ai dati con la gestione dei contenuti mobili

Poiché i collaboratori vogliono lavorare non solo con i documenti aziendali, ma anche con quelli personali, una soluzione di **Mcm** consente di controllare e segmentare correttamente i due ambiti. Ci sono, per esempio, diverse aziende che dispongono già di strumenti come **SharePoint**, su cui hanno investito anche significativamente. Questo strumento può essere sempre impiegato per il magazzino dei dati più importanti, ma gli amministratori possono affidarsi ad **Active Directory** per gestire e controllare gli accessi. Inoltre, non solo fornitori come **Ibm, Citrix ed Emc**, ma anche **Box e Dropbox** consentono di cifrare e controllare l'utilizzo di dati sensibili.

Oltre alla **consultazione mobile dei documenti**, gli strumenti collaborativi più robusti possono consentire la **modifica da remoto** su qualunque tipo di terminale. I sistemi di condivisione dei file che soffrono ancora di assenza di capacità di modifica e annotazione sono percepiti come restrittivi e possono stimolare l'utente a cercare in fonti non ben protette la soluzione. Naturalmente, le imprese devono poter controllare completamente i contenuti che circolano, per ragioni di sicurezza e compliance, ma i controlli necessari sono ormai largamente disponibili anche presso i fornitori di servizi di condivisione in modalità **cloud**.



Attualità



HP utilizza il Big Data per un'efficiente gestione delle App
Come accelerare l'esecuzione di ogni fase del ciclo di vita delle app



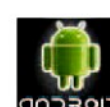
F-Secure controlla i parametri di connessione
Per contrastare le truffe online, Router Checker permette di impedire ...



Office 365 integra il mobile device management
Microsoft ha arricchito la propria suite cloud con funzionalità Mdm mutate ...



La mobility si coniuga ancora spesso con l'insicurezza
La maggior parte delle applicazioni mobili e i terminali che si



App e servizi Microsoft a bordo di Android
Disponibilità di OneNote, OneDrive e Skype sui nuovi Galaxy S6 e S6 Edge e ...

...continua

Opinioni e Commenti



Sicurezza e disponibilità nell'era dell'IoT
La tecnologia e i processi sono in grado di supportare le aziende nei ...

Byod, è fondamentale pianificare la sicurezza
Se dal punto di vista della produttività, i vantaggi del Byod appaiono ...

La gestione dei terminali mobili

Il Cio sanno che non possono aprire le maglie dei sistemi informativi a tutti i terminali, ma devono trovare un compromesso di fronte alla diffusione della mobility come prassi di connessione e sfruttamento di applicazioni. Un buon metodo per assicurare il successo di policy dedicate consiste nell'utilizzo di strumenti Emm (Enterprise Mobility Management).

Di fatto, queste piattaforme integrano soluzioni già presenti sul mercato su almeno tre dimensioni. La gestione dei terminali mobili (Mdm o Mobile Device Management) permette di controllare gli apparecchi e le loro configurazioni. A seguire, la gestione delle applicazioni mobili (Mam o Mobile Application Management) aggiunge il controllo sui programmi installati e installabili. Questi strumenti possono integrare controlli di sicurezza specifici, legati per esempio alla cifratura degli accessi remoti. Infine, il già citato Mcm consente di definire i contenuti dell'azienda accessibili, stabilire le condizioni e la modalità di utilizzo. L'organizzazione può anche specificare un livello di cifratura minima per i dati sensibili e confidenziali.

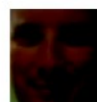
In base alle analisi di Gartner, specialisti come Airwatch, Good Technology e MobileIron affiancano per qualità delle soluzioni vendor più trasversali come Ibm, Citrix e Microsoft. Una volta implementato, l'Emm pone le basi necessarie per rendere i dipendenti più produttivi e soddisfatti. I rischi esistono e non devono essere trascurati, ma l'utilizzo di tecnologie affidabili e un'appropriata governance possono contenere il sotto-utilizzo delle applicazioni approvate e le vulnerabilità.

Scegli Tu! ▶ [Cloud ICT](#) ▶ [CRM Cloud](#) ▶ [IBM Cloud](#) ▶ [Cloud MDM](#)



Potrebbe anche interessarti:

[Cloud oggi, IoT domani. Ecco dove investire nell'Italia digitale](#)



Sicurezza delle password: un must per l'Enterprise Mobility, una spina nel fianco per l'IT
Tra le sfide da affrontare nei

App native o Web App?
La critica di Christian Heimann, Principal Developer Evangelist di ...

L'impatto del Byod sui network aziendali nel 2014
Un concetto da sempre associato a tablet e smartphone si sta estendendo ...

...continua

Cosa ne pensi di questa notizia?

Tweets Follow

PRESA **impresacity.it** @impresacity 40m
[Videointervista] Luca Zeriniani, Systems Engineering Manager, VMware Italia: L'offerta Software Defined Stora... bit.ly/1OXPBW

PRESA **impresacity.it** @impresacity 40m
Expo: siglato protocollo d'intesa con Ilycaffè: Ily

Tweet to @impresacity

ImpresaCity
Mi piace

ImpresaCity piace a 249 persone.

Plug-in sociale di Facebook

ImpresaCity

Segui +1

+ 81

[Home](#) [Redazione](#) [Copyright](#) [Pubblicità](#) [Privacy](#) [Newsletter](#) [Contattaci](#)



ImpresaCity e' un canale di B&Cty, testata giornalistica registrata presso il Tribunale di Como, n. 21/2007 del 11/10/2007 - Iscrizione ROC n. 15698

G11 MEDIA S.R.L.
Sede Legale Via NUOVA VALASSINA, 4 22046 MERONE (CO) - P.IVA/C.F. 03062910132
Registro imprese di Como n. 03062910132 - REA n. 293834 CAPITALE SOCIALE Euro 30.000 I.v.