High-light

di **Silvia Beraudo**

SICUREZZA: IL 'TALLONE D'ACHILLE' DELLA MOBILITY

DI FRONTE ALL'USO SEMPRE PIÙ DIFFUSO DEI DISPOSITIVI MOBILI IN AZIENDA, I CIO DEVONO RIVEDERE GLI STANDARD DI COMUNICAZIONE, OTTIMIZZARE LE RETI E SOPRATTUTTO INNALZARE GLI STANDARD DI SICUREZZA

Il settore degli apparati mobili è in fortissima ascesa. I dati rilasciati da Gartner a inizio anno ritraggono un mercato dominato da tablet, smartphone, ultramobile e PC che dovrebbe attestarsi, nell'anno in corso, a circa 2,5 miliardi di unità, in aumento del 7,6% rispetto al 2013. I telefoni cellulari, pur continuando a rappresentare un 'must' per l'end user, continueranno a crescere, anche se a un ritmo più lento rispetto al passato (+5% con 1,9 miliardi di dispositivi), mentre una forte battuta di arresto è prevista per i PC tradizionali, che vengono considerati sempre più come uno strumento di creazione di contenuti condivisi, ma ormai troppo poco flessibili e leggeri per rispondere alle crescenti necessità di mobilità degli utenti finali.

L'ultramobile (tablet e ibridi), sempre secondo la società di analisti, costituirà il principale driver del mercato per il 2014 con una crescita prevista dell'ordine del 54%. La dirompente diffusione di strumenti di comunicazione Web 2.0 si sta verificando a livello sia domestico sia aziendale. Anzi, molto spesso capita di assistere alla supremazia dell'uso domestico della tecnologia rispetto quello aziendale, con dipendenti che utilizzano dispositivi mobili 'personali' al posto di quelli forniti dell'impresa a scopo di business. I vantaggi che derivano alle aziende dall'adozione di device mobili sono diversi e non si limitano alla riduzione dei costi hardware; riguardano soprattutto la maggiore flessibilità e produttività dei dipendenti che possono lavorare in mobilità, avendo accesso ai dati e alle applicazioni ovunque, aumentando le proprie prestazioni, garantendo così maggiore efficacia ed efficienza ai processi di business e quindi competitività all'impresa.


Fonte: www.dfki.de

Fonte: www.electronicproducts.com

La nuova piattaforma

Fenomeni come la 'consumerizzazione' dell'IT, app e Byod (Bring your own device) rappresentano oggi realtà di fatto inarrestabili e non più ignorabili, che impongono a IT manager e CIO di pensare nuove strategie e policy. Essi si trovano a dover rivedere i sistemi esistenti per adattarli a quelli dei nuovi dispositivi; a dover cercare nuove soluzioni in grado di soddisfare le esigenze dei lavoratori che necessitano di accedere alle risorse aziendali anche fuori sede attraverso mobile device, anche personali, e a dover avere un occhio di riguardo e maggiore cura per l'individuazione di soluzioni di sicurezza tali da contrastare i rischi legati alla fruizione dei dati attraverso la rete. Da qui l'adozione da parte di molti dipartimenti IT di soluzioni di 'Enterprise Mobility Management', una risorsa per l'innovazione e la sicurezza, nonché un'opportunità per il business. Il tasso di adozione di software di questo tipo per supportare ambienti mobili multi-piattaforma è raddoppiato tra le aziende nella seconda metà del 2012 (dati IDC). Solo in Europa occidentale la spesa per i software di enterprise mobility ha superato i 480 milioni di dollari nel 2012 e pare abbia superato i 660 milioni nel 2013. Il tasso di crescita medio annuo di queste soluzioni nel Vecchio Continente nel periodo 2012-2017 è stimato, sempre da IDC, intorno al 18%. E negli anni questi software si sono evoluti da singola soluzione tattica a vera piattaforma architetturale, con molte aziende che pongono proprio l'integrazione di soluzioni per la

mobilità nell'esistente infrastruttura IT come imperativo principale. Questo comporta considerazioni architetturali a più largo respiro, con i dipartimenti IT che stanno valutando quale stack di funzionalità implementare per realizzare una solida piattaforma mobile, in particolare ponendo l'attenzione su gestione e sicurezza dei device, sviluppo di applicazioni, integrazione con i sistemi di back-end, connettività e analytics. Per adeguarsi alla nuova realtà è quindi necessario un approccio strutturato e progettuale, che se da un lato implica la valorizzazione dei processi e delle strategie in uso, dall'altro necessita la loro integrazione con le nuove componenti mobili, una rivalutazione delle strategie di supporto agli utenti, della gestione e del controllo e, soprattutto, un ripensamento dei criteri legati alla sicurezza.

Il punto debole

La security è il principale punto debole della business mobility. Nel nuovo ambiente aziendale, dominato da connessioni wireless, da cloud e mobility, l'IT deve proteggere e gestire una moltitudine di dispositivi mobili e una serie sempre più diversificata di sistemi operativi.

Entro il 2017, secondo Gartner Group, il 90% delle aziende si troverà a dover gestire ambienti operativi multi-piattaforma, Windows, iOS e Android, un'eterogeneità di piattaforme che faciliterà l'operatività e la produttività aziendali, ma introdurrà nuove problematiche gestionali e in termini di servizi da offrire all'utenza interna.

Se fino a qualche anno fa le organizzazioni, i fornitori di software IT e i produttori di computer hanno affrontato il problema della sicurezza informatica con prodotti basati su un unico modello, dove protezione e sicurezza erano forniti dal sistema operativo e dal software in esecuzione su di esso, oggi questo modello non è più sufficiente. Si devono adottare sistemi di sicurezza multi-livello, in grado non solo di proteggere ogni perimetro della rete aziendale, ma anche di offrire il giusto livello di prestazioni al sistema e l'accesso alle informazioni in tempo reale per mantenere gli utenti produttivi e connessi. I 'mobile worker' possono collegarsi in qualsiasi momento e in qualsiasi parte del mondo attraverso laptop e smartphone: più dispositivi in esecuzione su più piattaforme e su sistemi operativi diversi creano maggiori rischi e complessità da amministrare da parte dell'IT. L'avvento della mobility ha reso più vulnerabili i dati sensibili delle imprese, consentendo ai malintenzionati di infiltrarsi con più facilità nelle reti aziendali, di mettere a punto attacchi informatici sui singoli servizi generando un aumento esponenziale di malware sempre più sofisticati. A complicare il tutto si aggiunge la permanenza nelle aziende di vecchi PC legacy, difficili da aggiornare, o di device personali che non dispongono di sistemi di sicurezza adeguati per proteggere i dati sensibili aziendali, quali indirizzi IP, informazioni su clienti o fornitori. Per arginare questi accadimenti l'approccio da adottare da parte dell'IT deve essere innovativo, tempestivo e capace di anticipare, prevedere e rispondere rapidamente agli incidenti quando si verificano, anche grazie alla possibilità di monitorare ogni singolo dispositivo in uso.

Fonte: www.dfki.de

L'uso di dispositivi mobile crea vantaggi alle aziende in termini di maggiore disponibilità e produttività della forza lavoro

'Save the data'

La protezione dei dati business critical sui dispositivi mobili costituisce un aspetto cruciale della strategia di sicurezza delle organizzazioni. Si tratta infatti dei componenti più a rischio di una qualsiasi soluzione di business mobility. Ogni dispositivo può contenere diverse informazioni, pubbliche o private, e potenzialmente fornire l'accesso alla rete aziendale a chiunque ne venga in possesso. Furto di identità, spionaggio industriale, violazione della privacy sono solo alcuni esempi delle conseguenze di una cattiva gestione della sicurezza.

Diverse e su più piani possono essere le strategie da mettere in campo per proteggere un dispositivo mobile. Prima tra tutte l'imposizione agli utenti, da parte degli amministratori IT, dell'uso di password individuali che diano accesso ai dati del dispositivo solo al legittimo proprietario e che, per molti sistemi, deve essere, oltre che robusta, con obbligo di re-settaggio schedulato.

Non sempre però questo basta. Le organizzazioni più avanzate per limitare i rischi richiedono, per esempio, accessi attraverso smartcard, sistemi biometrici, impronte digitali o tecnologie simili. Un altro aspetto basilare per l'IT che guarda alla mobility è l'uso di soluzioni wireless per abilitare da remoto qualunque client, identificare proattivamente i rischi potenziali per il sistema informativo aziendale ed effettuarne la cancellazione, completa o selettiva, in caso di smarrimento, furto o altri accadimenti (per esempio per la cessazione del rapporto di collaborazione con l'utente). Attraverso una corretta strategia di Mobile Device Management, e quindi una visione centralizzata di tutti i dispositivi, è possibile non solo configurare gli apparati mobili (tablet, smartphone, cellulari), ma anche permettere la distribuzione delle applicazioni e la protezione delle informazioni.


Fonte: www.ilprogettistaindustriale.it

Nel mondo di oggi, sempre più interconnesso, non si possono più ignorare fenomeni come 'consumerizzazione' dell'IT, app e Byod

Grazie a opportuni software diventa facile controllare e proteggere i dati e le impostazioni di configurazione per i dispositivi mobili della rete, bloccare gli apparecchi che non devono avere accesso alle informazioni aziendali ed eliminare i dati da remoto in caso di necessità.

Fonte: Gartner Group, IDC, BlackBerry