Trend Micro Enterprise Security

La consumerizzazione delle IT.

Trend Micro, Incorporated

» *"Fatevi avanti!"* –
La consumerizzazione della mobilità aziendale

CHE COS'È LA “CONSUMERIZZAZIONE”?

La parola “consumerizzazione” indica la tendenza dei dipendenti a utilizzare dispositivi e applicazioni personali di fascia consumer per svolgere le attività aziendali. Questi dispositivi comprendono smartphone, pad e tablet dotati dei propri piani dati esterni.
La consumerizzazione sta avendo un enorme impatto sul modo in cui i reparti IT aziendali proteggono gli endpoint e tutelano i dati dell’azienda.

Questo movimento sta rapidamente trasformando il modo in cui i dipendenti e le aziende lavorano. Anche se non tutti i responsabili IT aziendali citano questa tendenza crescente con il nome di consumerizzazione, molti di essi hanno dovuto fare i conti con alcuni aspetti che la caratterizzano. Le implicazioni di un uso diffuso di dispositivi personali sul posto di lavoro stanno imponendo dei cambiamenti alle filosofie e alle prassi dei professionisti IT.

Molti dipendenti hanno oggi accesso a potenti sistemi informatici e a Internet ad alta velocità direttamente da casa. Così, mentre la tecnologia assume un ruolo sempre più importante nella loro vita privata, i dipendenti si abituano alla potenza e alla comodità delle applicazioni consumer Web 2.0, alla flessibilità dello scambio di dati con archiviazione in-the-cloud e Webmail e all'onnipresente connettività a Internet.

Con l’avvento di potenti dispositivi mobili personali, si sta verificando un significativo spostamento nel panorama dei dispositivi di client computing e nell’accesso ai dati aziendali. Il laptop Windows® messo a disposizione dall’azienda improvvisamente non è più l’unica opzione disponibile per i dipendenti. Ora, i membri del personale leggono le e-mail (sia private che di lavoro) tramite smartphone e dispositivi mobili capaci di accedere al CRM aziendale tramite tablet e memorizzano i dati aziendali sui propri laptop o netbook, non PC.

> In un sondaggio di Computerworld di settembre 2010, il 75% delle aziende sosteneva di supportare già l’uso dei dispositivi mobili di proprietà dei dipendenti.[1]

La consumerizzazione ha trasformato molti uffici in ambienti in cui i dipendenti possono dare libero sfogo a BYOD.

CHE COSA SIGNIFICA BYOD?

Il primo segnale dell'adozione della consumerizzazione delle IT da parte delle aziende si manifesta sotto forma dei programmi "Bring-Your-Own-Device": porta il tuo dispositivo. I programmi BYOD indicano che l'azienda non solo tollera l'uso di dispositivi di proprietà personale e sotto la responsabilità dell'utente, ma di fatto incoraggia e promuove tale uso.

Quando i dipendenti scelgono i propri dispositivi, e le aziende di grandi dimensioni forniscono un indennizzo o una sovvenzione per tali dispositivi, il risultato è vincente su tutti i fronti. I dipendenti ottengono i dispositivi che hanno il permesso di usare a fini personali e il reparto IT aziendale condivide e scarica in tutto o in parte il costo dell'hardware e del piano dati sui dipendenti. Inoltre, i dipendenti sono felici perché possono utilizzare i dispositivi che preferiscono, in un modo flessibile che consente di lavorare ovunque, e il datore di lavoro è felice perché può contare sulla maggiore produttività e soddisfazione dei dipendenti che ne consegue.

La tendenza del BOYD è sostenuta da altre tendenze, come il superamento attuato dagli smartphone sulla vendita di PC tradizionali[2], le esigenze dei dipendenti della Generazione X che cercano e si aspettano l'accesso ovunque e in qualsiasi momento alle informazioni e il forte numero di consumatori che si aspettano di utilizzare i propri smartphone per lavoro. (Statistiche e grafici riportati di seguito.)

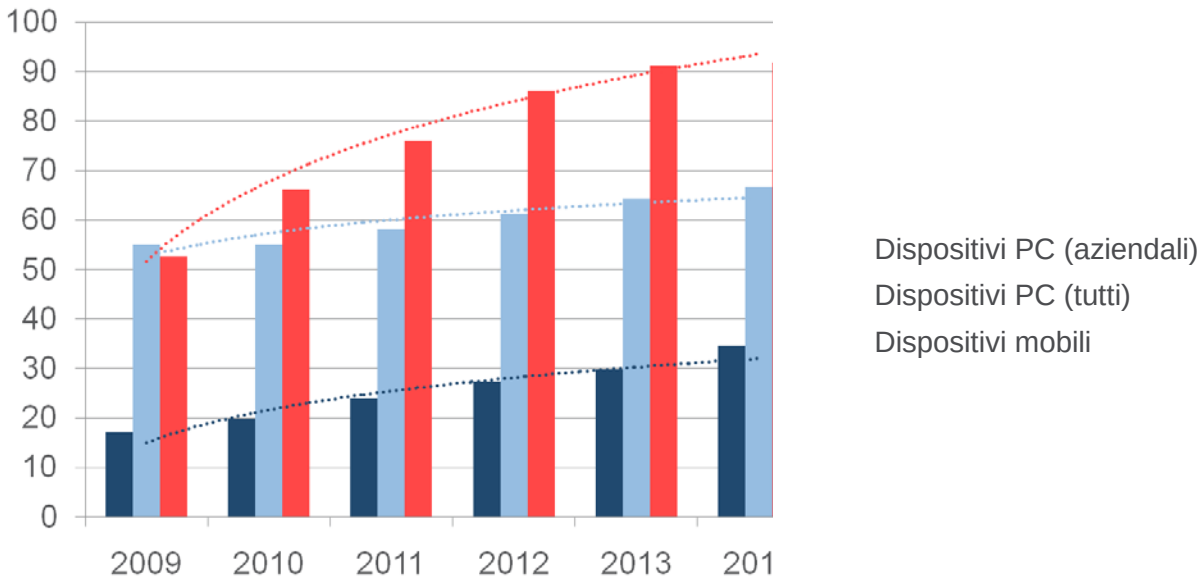

Figura 1: IDC segnala che la vendita di smartphone ha superato quella dei PC per la prima volta nel 2010

In un recente sondaggio condotto da Trend Micro, il 45% dei consumatori intervistati si aspetta di poter utilizzare il proprio smartphone privato anche per lavoro.

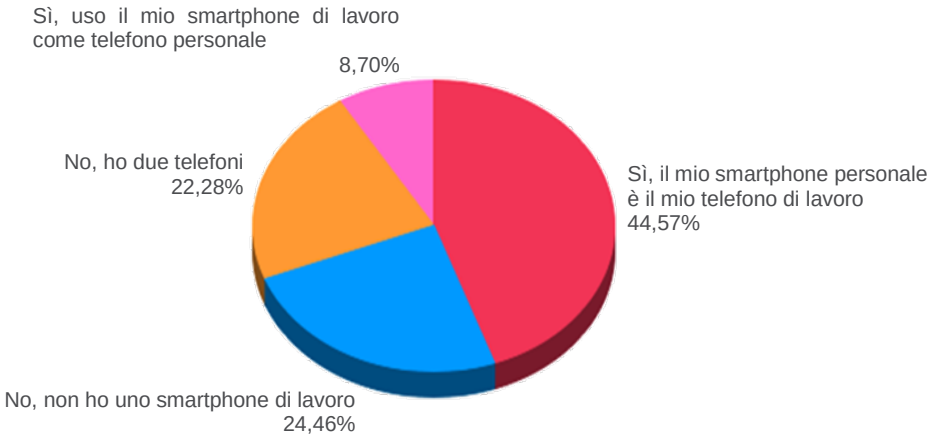

Figura 2: sondaggio sugli smartphone personali usati per lavoro

COME FA LA TUA AZIENDA A TRARRE VANTAGGIO DALLA CONSUMERIZZAZIONE?

I vantaggi aziendali derivanti dall'apertura dei dati e delle applicazioni aziendali ai dipendenti in movimento sono già chiari.

- La consumerizzazione consente ai dipendenti in remoto di essere più produttivi.
- Porta a una maggiore soddisfazione del cliente.
- Assicura che più dipendenti di talento decidano di restare.
- Può ridurre i costi IT di operazioni, hardware e licenze software.

Alcuni studi recenti indicano che quasi la metà della forza lavoro USA è già mobile e lontana dalla sede di lavoro principale per più del 20% del tempo.[3] In un recente articolo apparso su NetworkWorld.com, Jenny Englert, ingegnere cognitivo senior presso Xerox, in uno studio ha "scoperto che i dipendenti in movimento erano fuori dalla sede per circa l'80% della loro giornata lavorativa".[4] Tra i dipendenti in movimento si contano i cosiddetti "road warrior", specialisti sul campo, chi controlla la posta prima di recarsi in ufficio, chi viaggia per lavoro, telelavoratori e altri motori dell'economia basata sulle informazioni.

È probabilmente corretto affermare che i dipendenti aziendali, per lo più, sono già occasionali dipendenti in movimento, in quanto i confini tradizionali dell'ufficio si confondono con abitazioni, hotel, centri conferenze, aeroporti, autobus, treni, aeroplani e a molti altri luoghi commerciali come bar e centri commerciali.

L'abilità di un'azienda di essere competitiva dipende sempre più dalla possibilità concessa ai dipendenti in movimento di essere produttivi ovunque si trovino e di rispondere tempestivamente alle esigenze del mercato. Di fatto, secondo un sondaggio condotto da Yankee Group, i dipendenti affermano che "lavorare da casa è l'unico miglioramento davvero importante che le organizzazioni possono attuare per incrementare la produttività".[5]

La consumerizzazione può anche potenzialmente consentire di risparmiare tempo e denaro su costi operativi, hardware e licenze software. Secondo la rivista CIO, Avago, azienda

specializzata nel campo dei semiconduttori, spostando i propri dipendenti su Google Apps, ha risparmiato 1,6 milioni di dollari l'anno. Nel Regno Unito, l'impresa di costruzioni Taylor Woodrow, sostiene di aver risparmiato 2 milioni di dollari non molto tempo dopo aver implementato Gmail e abbandonato Exchange.[6]

COME FA IL REPARTO IT A GESTIRE E PROTEGGERE I DISPOSITIVI MOBILI DEI DIPENDENTI?

I reparti IT degli ambienti consumerizzati stanno affrontando una serie di problematiche connesse soprattutto all'acquisizione di visibilità e di un certo controllo sulla pletora di dispositivi sotto la responsabilità degli utenti.

- Gestione dei dispositivi sotto la responsabilità degli utenti

La gestione in questo caso ha un doppio fine. Per prima cosa, intende rendere l'esperienza dell'utente semplice e lineare al fine di ottimizzare la sua motivazione e produttività.
In secondo luogo, l'acquisizione di un certo grado di controllo sui dispositivi sotto la responsabilità degli utenti intende ridurre al minimo l'esposizione ai rischi per la sicurezza. Un dispositivo ben gestito, nella maggior parte dei casi, è un dispositivo più sicuro.

- Esposizione dei dati aziendali sensibili archiviati sui dispositivi

I dati aziendali sensibili possono essere esposti a terzi non autorizzati in diversi modi. Ogni anno vengono rubati milioni di cellulari e laptop. È necessario ritenere compromessi i dati sensibili archiviati sul dispositivo e, a seconda della natura di tali dati, è opportuno segnalarne la violazione alle autorità; il che comporta dei costi fino a 50.000 dollari per dispositivo esposto e danni d'immagine.

- Fughe di dati aziendali sensibili tramite applicazioni consumer

Poiché gli utenti utilizzano lo stesso dispositivo a fini privati e per attività lavorative, i dati sensibili possono essere facilmente trasmessi (con o senza intenzione dannosa da parte dell'utente) fuori dal dispositivo stesso. Possono essere spediti tramite Webmail o altri canali di comunicazione non aziendali.

- Introduzione di dati o software pericolosi

Le minacce informatiche possono venire introdotte nella rete aziendale in diversi modi. È possibile che un dispositivo sotto la responsabilità dell'utente venga infettato semplicemente navigando sul Web se non viene protetto o viene utilizzato in un ambiente non protetto.

Trend Micro, leader mondiale delle soluzioni di sicurezza in-the-cloud da oltre 20 anni, ha la soluzione che serve. Trend Micro crea un mondo sicuro per lo scambio di informazioni digitali grazie alla protezione dei contenuti Internet e alle soluzioni di gestione delle minacce per aziende e privati. Come pionieri della protezione dei server, offriamo una sicurezza di punta per client, server e cloud che si adatta perfettamente alle esigenze dei nostri clienti e partner, blocca più rapidamente le nuove minacce e protegge i dati in ambienti fisici, virtualizzati e in-the-cloud.

Basati sull'infrastruttura Trend Micro™ Smart Protection Network™, la nostra tecnologia e i nostri prodotti e servizi leader del settore per la protezione in ambito di cloud computing bloccano le minacce non appena si presentano, su Internet, e sono supportati da più di 1.000 esperti di minacce informatiche a livello globale.

Smart Protection Network garantisce una sicurezza più intelligente rispetto agli approcci tradizionali perché blocca le minacce più recenti prima che raggiungano la vostra rete. Sfruttando il cloud computing per tutte le soluzioni di sicurezza e i servizi Trend Micro, Smart Protection Network fornisce un'architettura in-the-cloud più solida che tutela la rete informatica e i dati aziendali riducendo al contempo la dipendenza dai lunghi tempi di download dei file delle definizioni.

L'esperienza di Trend Micro nella protezione degli ambienti aziendali vi consente di affrontare le problematiche della consumerizzazione della mobilità aziendale con la massima fiducia.

AUTORITÀ AZIENDALE E PRIVACY DEI DIPENDENTI A CONFRONTO

Sulla strada che porta alla consumerizzazione c'è un potenziale ostacolo di cui molti non hanno tenuto conto. Va da sé che quando un dipendente porta il proprio dispositivo e lo utilizza per lavoro, la potenziale conflittualità è enorme. Il conflitto emerge quando il reparto IT di un'azienda di grandi dimensioni ha l'esigenza di avere sufficiente controllo sui dispositivi mobili che accedono alle reti aziendali affinché siano protetti e deve al contempo soddisfare il desiderio dei dipendenti di mantenere riservati i dati personali sui dispositivi personali.

In due diversi sondaggi recenti di Trend Micro, vediamo gli interessi dei due gruppi che emergono e si bloccano potenzialmente nella tendenza verso la consumerizzazione. Alla domanda di Trend Micro, la stragrande maggioranza (91%) dei dipendenti aziendali ha dichiarato che non attribuirebbe al proprio datore di lavoro il controllo del proprio dispositivo personale per poter accedere alle applicazioni aziendali. Sempre nel corso del sondaggio, quasi l'80% delle imprese ha dichiarato che dovrebbe "avere l'autorizzazione o il controllo per obbligare all'installazione dei meccanismi di gestione sui dispositivi mobili." In altri casi è emerso che un numero sconcertante di responsabili IT ritiene che le aziende dovrebbero cancellare la memoria dei dispositivi personali (tutti) che si collegano alle reti aziendali.

È evidente che per i dipendenti essere in grado di proteggere i propri dati personali dalle invasioni aziendali è estremamente importante, mentre i professionisti IT ritengono di avere bisogno del controllo completo di qualsiasi dispositivo utilizzato per interagire con le macchine e i dati dell'azienda. Quindi qual è il metodo migliore per gestire le preoccupazioni di entrambe le parti?

In un rapporto recente, Cesare Garlati di Trend Micro consiglia di adottare "un approccio strategico ragionato nei confronti della consumerizzazione e di elaborare un piano organizzativo trasversale. L'informatica non può farlo in modo sommario e ha bisogno di coinvolgere i dirigenti, i responsabili dei settori di attività (marketing, vendite, risorse umane, sviluppo dei prodotti) nonché i clienti, i partner e i dipendenti che hanno adottato le nuove tecnologie."

“Durante la pianificazione dell’adozione della tecnologia consumer, i responsabili IT dovrebbero sottoporre dei sondaggi ai propri utenti più innovativi per capire quali dispositivi e quali applicazioni preferiscono e quali ritengono più utili per l’attività lavorativa. In questo modo, il reparto IT può realmente trarre vantaggio dall’esperienza degli utenti anziché promuovere le proprie opinioni presso la base.”

“La seconda fase prevede l’elaborazione di una solida serie di criteri che definiscono chiaramente quali dispositivi e applicazioni vengono considerati corporate-standard (completamente supportati dal reparto IT), quali sono tollerati (supportati congiuntamente all’utente) e quali non sono supportati (affidati completamente all’utente). Inoltre, il reparto IT deve definire il profilo dei dipendenti sulla base di caratteristiche fondamentali quali ruolo, settore di attività e sede. Deve inoltre elaborare una mappa delle tecnologie in base ai profili degli utenti e stabilire gli SLA per ogni intersezione.”

“La terza fase consiste nell’implementazione degli adeguati strumenti IT progettati specificatamente per proteggere e gestire la tecnologia consumer nell’azienda. Mentre alcune soluzioni si sono già materializzate sulla falsariga di specifici segmenti di prodotto, nessun fornitore da solo può fornire un’unica soluzione in grado di soddisfare i requisiti funzionali su tutte le piattaforme.”[7]

CONCLUSIONI

La “consumerizzazione” e la mobilità delle IT aziendali costituiscono un movimento reale, irreversibile e inarrestabile che necessita di attenzione immediata e di soluzioni innovative. Per poter continuare a contare su endpoint protetti, man mano che il potenziale delle violazioni aumenta, i reparti IT devono essere flessibili e inclusivi quando sviluppano i criteri, affinché i dipendenti siano incoraggiati a utilizzare i propri dispositivi mobili senza temere di perderne il controllo.

Se guidati e supportati dagli strumenti e dai criteri adeguati, i benefici della consumerizzazione possono essere notevoli per tutte le parti coinvolte, in quanto:

- *I dipendenti hanno la possibilità di scegliere e di lavorare con i dispositivi che preferiscono, nel momento e nel luogo in cui sono più produttivi.*
- *Il reparto IT non è sopraffatto da richieste di assistenza per i dispositivi, perché aiutato dalla conformità normativa e, di conseguenza, può concentrarsi su obiettivi di sicurezza più strategici.*
- *La dirigenza gode di dipendenti più soddisfatti e produttivi e di un vantaggio sulla concorrenza che cerca un modo per contenere l'inarrestabile.*

Trend Micro offre soluzioni che consentono di affrontare gli innumerevoli problemi fondamentali presenti negli ambienti aziendali consumerizzati e in mobilità, consentendo alle aziende di adottare e sbloccare in tutta sicurezza i vantaggi della consumerizzazione del proprio ambito IT.

PER ULTERIORI INFORMAZIONI: http://www.trendmicro.it/mobile-security

RISORSE

[1] Sondaggio ComputerWorld http://www.pcworld.com/businesscenter/article/210079/getting_it_set_for_mobile.html

[2] IDC Worldwide Quarterly Mobile Phone Tracker, gennaio 2011 e IDC Worldwide Quarterly PC tracker, gennaio 2011

[3] Yankee Group Study, “Maximizing Mobile Worker Productivity,” 2008

[4] Articolo NetworkWorld.com http://m.networkworld.com/news/2011/062711-desktop-doomed.html#mobify-bookmark

[5] Yankee Group, 2008 Blended Lifestyle Survey—U.S. Large Enterprise

[6] CIO Magazine: “Why Enterprises Are Moving to Google Apps, Gmail”, 10 giugno 2009

[7] “Why You Should Embrace Consumerization: Learn the steps to managing your workforce without limits” una relazione di Cesare Garlati, responsabile senior per la consumerizzazione e la Mobile Security, Trend Micro http://www.trendmicro.it/media/misc/consumerization-thought-leadership-it.pdf

TREND MICRO ITALY S.R.L.
Viale T. Edison 110 palazzo C
20099 Sesto San Giovanni (MI)
Telefono: +39 02/925931
Fax: +39 02/92593401
www.trendmicro.com.