SOPHOS

BYOD: rischi e vantaggi

Come mantenere protetti smartphone, laptop e tablet dei dipendenti

Di **Gerhard Eschelbeck**, Chief Technology Officer
e **David Schwartzberg**, Senior Security Engineer

Sia che siate utenti finali o amministratori IT, Bring Your Own Device (BYOD) sta diventando sempre più una regola e sempre meno un'eccezione negli ambienti di lavoro moderni. Sebbene BYOD sia una strategia estremamente pratica per i dipendenti, bisogna tenerne presente l'impatto sui modelli di sicurezza aziendali. Questo whitepaper descrive rischi e vantaggi di BYOD, indicando come si possa adottare BYOD sul posto di lavoro, pur mantenendo protetti i dati.

BYOD e l'impatto sul business

Oggi come oggi, i responsabili IT si trovano ad affrontare moltissimi problemi relativi alla sicurezza, con cambiamenti costanti e repentini. Come se non bastasse, devono fare di più con meno risorse. Devono fornire agli utenti finali accesso alle tecnologie più recenti e all'avanguardia, per garantirne la competitività. E hanno la responsabilità di proteggere i dati di azienda, clienti e dipendenti, contrastando nel contempo gli attacchi dei cybercriminali.

Le nuove tecnologie portano con sé nuovi modi di accedere ai dati, nuovi tipi di dispositivi e interessanti alternative alle tradizionali piattaforme PC. Non a caso Tim Cook, amministratore delegato di Apple, definisce questo periodo come "era post-PC"[1].

Queste dinamiche hanno generato una tendenza a utilizzare BYOD sul posto di lavoro: un trend che sta diventando sempre più comune.

BYOD include ben più che i semplici personal computer. Significa che per svolgere il proprio lavoro i dipendenti utilizzano smartphone, tablet, BlackBerry, ultrabook e molto altro ancora. Il concetto BYOD può essere esteso a software e servizi, in quanto gli utenti potrebbero adoperare servizi cloud e altri tool on-line.

I problemi di tecnologia che fino a pochi anni fa rendevano BYOD un'idea tutt'altro che realistica hanno favorito la vasta diffusione e l'ampio utilizzo di questi tool.

Tra di essi vi sono:

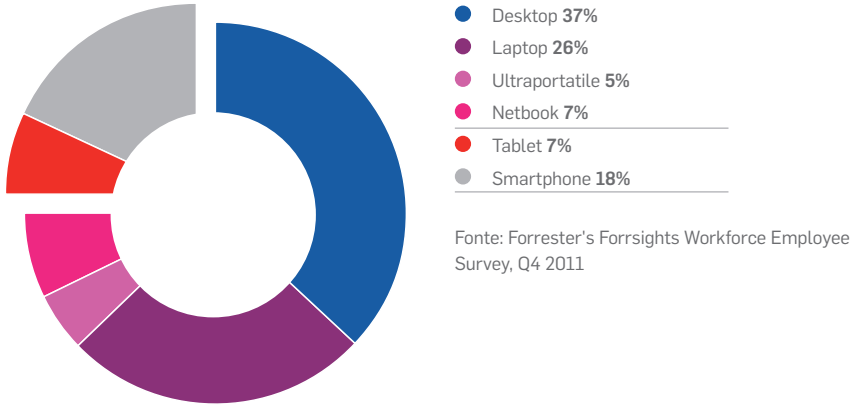
1. Web: Oggi come oggi il Web è praticamente l'unico modo per accedere ad applicazioni di qualsiasi genere: business, finanza, supporto clienti, vendite o tecnologia.

2. Wireless: Indipendentemente da dove vi troviate e dal dispositivo che utilizzate, potete accedere alle infrastrutture di back office grazie a reti Wi-Fi sempre più estese.

3. Dispositivi mobili: I dispositivi sono diventati strumenti molto più sofisticati, economici e portatili, con memoria e durata della batteria più elevate.

1. "The post-PC world is real and it's here", The Globe and Mail, http://www.theglobeandmail.com/technology/gadgets-and-gear/the-post-pc-world-is-real-and-its-here/article4098023/

Fra i dispositivi utilizzati per scopo lavorativo, uno su quattro è uno smartphone o un tablet.



Fonte: Forrester's Forrsights Workforce Employee Survey, Q4 2011

BYOD e l'impatto sulla sicurezza

È rischioso presumere che proibire l'utilizzo dei dispositivi personali possa risolvere il problema: i dipendenti continueranno a usarli, fuori dal vostro controllo e a prescindere dalle vostre policy di sicurezza.

Indipendentemente dalla vostra opinione su BYOD e dal modo in cui decidiate di implementarlo, i responsabili IT devono affrontarne l'arrivo esattamente come per qualsiasi altro tipo di tecnologia: con un delivery controllato e prevedibile.

Ponetevi le seguenti domande:

1. A chi appartiene il dispositivo? È una domanda che col passare del tempo ha ricevuto risposte diverse. In passato i dispositivi appartenevano alle aziende. Con BYOD, i dispositivi sono di proprietà dell'utente.

2. Chi gestisce il dispositivo? In passato, la risposta era semplice. Oggi come oggi potrebbe essere l'azienda, oppure l'utente finale.

3. Chi protegge il dispositivo? La responsabilità degli utenti non svanisce semplicemente perché i dispositivi appartengono a loro. Dopotutto i dati in essi contenuti sono di proprietà dell'azienda.

Rispondere a queste domande è essenziale sia per capire i rischi che per approfittare dei vantaggi di BYOD.

Tutte le aziende hanno la flessibilità, a seconda dei relativi requisiti normativi ed etiche aziendali, di utilizzare BYOD nel modo che ritengono più adeguato. Vi sono ad esempio aziende che hanno scelto di non implementare un programma BYOD, in quanto lo considerano un rischio troppo elevato.

Nel mese di maggio del 2012, IBM ha proibito ai suoi 400.000 dipendenti l'uso di due diffusissime applicazioni di consumo, per via dei rischi che avrebbero rappresentato per la sicurezza dei dati. L'azienda ha vietato l'utilizzo del servizio di cloud storage Dropbox e di Siri: l'"assistente personale" per iPhone di Apple. Siri risponde alle richieste vocali e invia query ai server di Apple, dove vengono decifrate e trasformate in testo. Siri è anche in grado di creare messaggi SMS ed e-mail da comandi a voce, ma alcuni di questi messaggi a fumetto possono contenere informazioni sensibili e di proprietà[2].

In ultima analisi, il successo di BYOD si misura in termini di disponibilità dei dipendenti a utilizzare i dispositivi mobili nel rispetto delle regole da voi impostate. Le procedure e le policy di sicurezza della vostra azienda devono stabilire se e come desiderate implementare un programma BYOD.

È necessario avere la possibilità di implementare policy di sicurezza a livello dei dispositivi e poter proteggere la proprietà intellettuale nell'eventualità di furto o smarrimento di un dispositivo.

Scaricate il whitepaper "Risolvere i problemi di Dropbox" da Sophos.it

BYOS: Bring Your Own Software

Le stesse tecnologie su cui si basa l'avanzamento della diffusione di BYOD consentono agli utenti di accedere anche a software diverso da quello aziendale. Tale fenomeno è noto come Bring Your Own Software (BYOS).

Gli utenti finali possono servirsi di fornitori di servizi cloud pubblici e gratuiti per agevolare la collaborazione e il trasferimento di documenti dalle dimensioni elevate. Tuttavia questi documenti possono contenere dati che rientrano nell'ambito regolato dalle indicazioni normative, rischiando di mettere a repentaglio i vostri dati.

È necessario valutare la metodologia di trasferimento e archiviazione dei file aziendali sui servizi di cloud storage. Ponetevi le seguenti domande:

- Come vengono cifrati i dati?
- Utilizzano una chiave unica per tutti i clienti?
- Chi possiede diritti di accesso alla chiave di decifrazione dei dati?
- Sarebbero disposti a cedere i dati alle autorità, nel caso in cui ne venga richiesta la confisca?
- In quali paesi sono situati i server su cui vengono archiviati i dati?
- La vostra azienda ha stipulato accordi con i clienti che proibiscono l'archiviazione dei dati in determinati paesi?

2 "IBM: Sorry, Siri. You're Not Welcome Here", InformationWeek, http://www.informationweek.com/news/security/mobile/240000882

Come proteggere i BYOD

La primissima e migliore strategia di difesa per i BYOD comincia con gli stessi requisiti applicabili ai dispositivi già connessi alla rete aziendale. Fra queste misure di sicurezza vi sono:

- Implementazione di passcode sicuri su tutti i dispositivi
- Protezione antivirus e prevenzione della perdita dei dati (DLP)
- Cifratura completa di disco, supporti rimovibili e cloud storage
- Gestione dei dispositivi mobili (Mobile device management, MDM), per eliminare i dati di natura sensibile in caso di furto o smarrimento di un dispositivo
- Application control

La cifratura va sempre applicata sia ai dati in transito che a quelli fermi. Proteggere i dispositivi con password sicure significa renderne estremamente difficile la violazione e il conseguente furto dei dati. Ma se per caso la password del dispositivo venisse violata, la cifratura dei dati in esso contenuti costituirebbe un secondo livello di sicurezza da espugnare, prima di poter accedere alle informazioni.

È consigliabile indurre gli utenti a considerare i livelli di sicurezza aggiuntivi come utili tool in grado di abilitare i dispositivi personali nell'ambiente di lavoro. Utilizzando una password per i dispositivi, gli utenti riconoscono di avere un certo grado di responsabilità nella protezione dei dati.

Oltre a dotare i dispositivi di passcode e sistemi di prevenzione antivirus, è necessario implementare un livello di application control ottimizzato per i BYOD. Se i dipendenti possono accedere alle applicazioni tramite la rete interna, è necessario che tale opzione sia disponibile anche quando lavorano in remoto, mediante VPN o software e-mail.

Per essere efficace, un programma BYOD deve permettere agli utenti di essere produttivi al di fuori dell'orario di lavoro, fornendo nel contempo la flessibilità di poter fare ciò che desiderano quando non lavorano (come ad es. aggiornare il proprio stato o dedicarsi a giochi interattivi).

Qualsiasi decisione prendiate per le policy di BYOD, accertatevi che siano implementabili e che consentano al reparto IT di effettuare il delivery del software in remoto.

Impostare standard per policy e compliance

Le policy vanno formalizzate, specialmente quando si tratta di BYOD. Ponetevi ad esempio le seguenti domande: le policy devono includere tutti i dispositivi attualmente disponibili? Intendete limitare l'uso dei dispositivi personali dotati di specifiche piattaforme hardware e software? Cosa intendete fare con i dispositivi che non sono ancora disponibili, ma che giungeranno sul mercato nei prossimi anni?

Il mercato dei dispositivi mobili palmari è in rapida evoluzione, con versioni e produttori sempre nuovi. Tenendo presente queste considerazioni, le policy di BYOD devono essere adattabili. È necessario stipulare policy strategiche per iscritto, in base alle vostre conoscenze attuali e a ciò che ritenete possa riservare il futuro. Occorre anche utilizzare tecnologie che implementino le policy scritte in modo da fornire gestione, modelli di verifica per gli audit, controllo e sicurezza.

Il delivery di una soluzione concepita per verificare la gestibilità remota dei dispositivi può rappresentare un valido aiuto nella sfida costantemente in corso: quella di far sì che le policy di sicurezza siano sempre adeguate e affidabili, specialmente se la vostra azienda opera in un ambito dai severi standard di compliance e audit.

Inoltre, conoscere i piani di servizio dei dipendenti vi può aiutare a fornire servizi più efficaci a minor costo. Utilizzare l'hotspot o le opzioni di tethering di un piano dati può risultare in una migliore esperienza complessiva per gli utenti finali. I piani "solo dati" per i dispositivi personali Wi-Fi possono essere una valida alternativa ai piani di servizio remoto e ISP per gli uffici domestici.

7 passi verso un piano di sicurezza BYOD

La coesistenza di sicurezza aziendale e BYOD è possibile. E comincia con la pianificazione. Ecco come:

1. Individuare i fattori di rischio introdotti da BYOD

- Quantificare il possibile impatto di tali rischi sulla vostra azienda
- Ove applicabile, cercare le normative corrispondenti ai fattori di rischio.

2. Istituire un comitato per l'adozione di BYOD e per comprenderne i rischi; fra i membri, includere:

- Stakeholder dell'azienda
- Stakeholder IT
- Stakeholder in ambito Information Security

3. Decidere la modalità di implementazione delle policy per i dispositivi che si connettono alla vostra rete

- Dispositivi mobili (smartphone)
- Tablet (ad es. iPad)
- Computer portatili (laptop, netbook, ultrabook)

4. Impostare un piano di progetto che includa i seguenti punti:

- Gestione remota dei dispositivi
- Application control
- Compliance alle policy e report di audit
- Cifratura di dati e dispositivi
- Potenziamento della sicurezza per il cloud storage
- Formattazione dei dispositivi disattivati
- Revoca dei diritti di accesso di un dispositivo quando il rapporto con l'utente finale passa da dipendente a ospite
- Revoca dei diritti di accesso di un dispositivo quando un dipendente viene licenziato

5. Valutare le varie soluzioni

- Tenere presente l'impatto sull'attuale struttura della rete
- Pensare a come ottimizzare le tecnologie di cui già disponete, prima di passare al punto successivo

6. Delivery delle soluzioni

- Cominciare con un gruppo sperimentale per ciascuno dei reparti degli stakeholder
- Estendere la sperimentazione ai vari dipartimenti, in base ai vostri criteri organizzativi
- Rendere il programma BYOD disponibile per tutti i dipendenti

7. Esaminare ed effettuare una valutazione delle soluzioni a intervalli regolari

- Includere vendor e consulenti di fiducia
- Esaminare i piani di sviluppo del periodo di valutazione successivo
- Considerare piani di gruppo rivolti al risparmio, se si tratta di un'opzione realistica

Se adeguatamente implementato, un programma BYOD può ridurre i costi, pur incrementando produttività e utili. Man mano che BYOD diventa sempre più diffuso nei reparti IT, la sicurezza deve diventare il concetto più immediato e importante sia per gli utenti che per gli amministratori IT.

Vendite per Italia
Tel: (+39) 02 911 808
E-mail: sales@sophos.it

Boston, USA | Oxford, Regno Unito

Whitepaper Sophos 06.12v1.dNA

SOPHOS