SYBASE
An SAP Company

WHITE PAPER

I vantaggi della mobilità: perché proteggere i dispositivi mobili?

LA MANCANZA DI SICUREZZA NELL'AMBIENTE MOBILE — UN PROBLEMA OVVIO CHE TENDE AD ESSERE IGNORATO

Secondo gli esperti del settore, entro il 2013 i lavoratori mobili in tutto il mondo raggiungeranno una cifra pari a 1,2 miliardi.[1] Gli esperti stimano inoltre che entro il 2013 il 75% dei lavoratori negli Stati Uniti sarà "mobile"[2], ossia utilizzerà un dispositivo mobile per almeno il 20% delle proprie attività professionali.

Da un altro sondaggio emerge che il 36% dei proprietari di cellulare ha subito il furto o lo smarrimento del proprio telefonino.[3]

Questi dati suggeriscono che in un futuro imminente circa il 25% dei lavoratori avrà smarrito un dispositivo mobile che dà l'accesso ad informazioni confidenziali. Non sorprende quindi che la sicurezza dei dispositivi mobili sia un problema di grande attualità per qualsiasi azienda.

Eppure, nonostante il problema desti grande preoccupazione, sono poche le aziende che prestano la dovuta attenzione alla sicurezza mobile. I sondaggi mostrano che, sebbene la sicurezza mobile sia una questione della massima priorità e la violazione dei dati abbia interessato numerose imprese, le aziende che implementano una solida strategia di sicurezza mobile sono in minoranza.[4] Perché le organizzazioni non adottano una politica di protezione più aggressiva per i loro dispositivi mobili? Le ragioni sono diverse:

- La velocità con cui le nuove generazioni di dispositivi mobili sono giunte sul luogo di lavoro ha colto impreparate molte aziende;
- oggi la mobilità aziendale è dettata dai gruppi di lavoro e dai dipendenti, non dai responsabili aziendali della politica IT. Questo ha dato luogo ad un approccio frammentario nei confronti della sicurezza mobile;
- la mobilità di oggi è complicata dal fatto che i lavoratori utilizzano dispositivi di loro proprietà sia per scopi professionali che personali;
- il problema della sicurezza è ulteriormente aggravato dalla diversità in costante aumento di dispositivi mobili sul luogo di lavoro;
- le semplici modalità di accesso e la proliferazione di applicazioni mobili scoraggiano l'elaborazione di politiche di gestione della sicurezza.

Numerose aziende non hanno ancora implementato una strategia globale a livello di sicurezza mobile perché la ritengono troppo costosa e complessa. Nel frattempo, la mobilità continua a prendere sempre più piede nelle attività aziendali giornaliere e con essa crescono i costi associati alla violazione della sicurezza. Nel 2009 il costo medio per singolo episodio di violazione dei dati è stato pari a 6,75 milioni di dollari.[5]

La maggior parte delle aziende ha definito politiche di sicurezza. La sfida a cui devono far fronte include due problematiche:

1. Adattare le politiche di sicurezza all'ambiente di lavoro mobile;
2. Decidere quale tipo di tecnologia è necessaria per gestire i dispositivi e implementare le politiche.

Il primo passo nell'elaborazione di una strategia di sicurezza mobile è comprendere la natura della minaccia.

COMPRENDERE I RISCHI ASSOCIATI ALLA MOBILITÀ E I RELATIVI RIMEDI

Spesso i costi indiretti associati alle violazioni della sicurezza sono di gran lunga superiori ai costi diretti sostenuti per mitigare i danni. Oltre a porre rimedio alla violazione dei dati e alle possibili sanzioni dovute a violazioni delle norme in materia di conformità, la violazione della sicurezza può privare le aziende del loro vantaggio competitivo. Possono mettere in imbarazzo aziende o dipendenti chiave, creando una cattiva pubblicità e problemi legali. Possono causare la perdita di fiducia da parte di clienti e partner. In definitiva, le violazioni della sicurezza possono danneggiare il brand di un'azienda compromettendone la capacità operativa.

Con la diffusione sempre più marcata della mobilità nelle attività di routine, le aziende che intendono elaborare una strategia di mobilità devono far fronte al problema della sicurezza mobile. A tal fine, è importante comprenderne i fattori di vulnerabilità.

In senso lato, le attività aziendali mobili presentano quattro fattori di vulnerabilità:

- Dispositivi smarriti o rubati
- Accesso non autorizzato ai dati
- Rischi derivanti dall'uso di un unico dispositivo per fini professionali e personali
- Lacune nella gestione dei dispositivi e nell'implementazione della politica

Analizziamo singolarmente ognuno di questi fattori.

Rischi associati ai dispositivi smarriti o rubati

I dispositivi mobili sono facilmente smarribili e questa è un dato di fatto difficilmente modificabile. Insieme ai dispositivi viene persa una quantità significativa di dati.

Nonostante la mole di dati persi a causa del furto di dispositivi e la facilità con cui tali dispositivi vengono smarriti, in molti casi non si fa niente per proteggere concretamente i dati presenti sui dispositivi mobili. Lo stesso studio da cui è emerso che oltre un terzo dei proprietari di cellulari negli Stati Uniti ha subito il furto o lo smarrimento del telefonino ha rivelato un altro fatto sorprendente. Circa il 90% di quelle persone non disponeva di alcun mezzo per bloccare in remoto i dispositivi o cancellarne in remoto i dati. Inoltre, più della metà degli utenti di smartphone non utilizza protezioni tramite password sui propri telefonini.[6]

Questi dati suggeriscono quattro funzionalità che dovrebbero essere alla base di qualsiasi strategia di sicurezza mobile:

- **Autenticazione utente a livello di dispositivo** — I lavoratori mobili sono tenuti ad utilizzare password per effettuare il login e accedere alle applicazioni e ai dati aziendali.
- **Bloccaggio e cancellazione in remoto** — Questa funzione consente alle aziende di disabilitare in remoto i dispositivi mobili affinché nessuno possa utilizzarli, e di eseguire la cancellazione remota dei dati dai dispositivi.
- **Crittografia dati** — Nel caso in cui non ci si accorga subito dello smarrimento di un dispositivo, tutti i dati aziendali in esso contenuti dovrebbero essere crittografati.
- **Controllo dati** — Se un utente non si collega alla rete per un determinato periodo di tempo, il dispositivo elimina i suoi dati o blocca l'accesso alla posta elettronica aziendale.

Accesso non autorizzato ai dati.

Questa minaccia riguarda l'apparente uso autorizzato di dispositivi mobili per acquisire l'accesso non autorizzato ai dati. Non si tratta di un problema strettamente correlato alla mobilità. La stessa minaccia può provenire da qualsiasi sistema client all'interno di un'organizzazione. Gli strumenti di gestione della mobilità offrono soluzioni per estendere le politiche di sicurezza standard all'ambiente mobile.

I dispositivi mobili possono fungere da portali per l'accesso non autorizzato a informazioni riservate in tre modi:

- **Un utente non autorizzato potrebbe accedere ai dati con un telefonino smarrito o rubato** — L'autenticazione utente, il bloccaggio e la cancellazione in remoto, la crittografia dati e il controllo dati assicurano una protezione contro questa minaccia.
- **Utenti autorizzati ottengono l'accesso non autorizzato a informazioni riservate o ne fanno un uso inappropriato** — Si tratta di una minaccia comune a qualsiasi sistema client di un'organizzazione. Il rischio ulteriore in un ambiente di mobilità aziendale deriva dagli stessi benefici offerti dalla mobilità: accesso in qualsiasi momento e luogo, e praticità.

Le best practice in materia di sicurezza, incluse le politiche di gruppo e di restrizione dell'accesso, consentiranno di regolamentare l'accesso alle informazioni riservate in un ambiente di mobilità aziendale. Una strategia di sicurezza mobile è però in grado di garantire alcuni controlli aggiuntivi, tra cui:

- **Provisioning di applicazioni mobili** — Le persone autorizzate ad eseguire le applicazioni aziendali sono direttamente controllate dalle organizzazioni. In questo modo viene messo in atto un livello di controllo più rigido sull'accesso alle informazioni riservate.
- **Aggiornamenti alla configurazione in remoto** — La capacità di eseguire in remoto le impostazioni del dispositivo e le restrizioni "over the air" assicura l'implementazione delle politiche definite.
- **Monitoraggio e registrazione di eventi e attività** — Il monitoraggio e la registrazione di attività consentono di individuare rapidamente i problemi di sicurezza e di controllare automaticamente l'accesso ai dati aziendali.

Rischi associati all'uso di uno stesso dispositivo per fini professionali e personali.

La ragione per cui le aziende consentono ai loro dipendenti di utilizzare un unico dispositivo mobile per fini sia professionali che personali è legata ai vantaggi significativi che ne traggono.

I dipendenti che hanno la possibilità di usare i loro dispositivi preferiti sono più propensi ad utilizzare le applicazioni aziendali mobili semplicemente perché per loro è più pratico. Inoltre, consentendo ai dipendenti di utilizzare i propri dispositivi, le aziende possono ridurre in modo significativo i costi di aggiornamento hardware.

Questo, tuttavia, comporta anche rischi. Le aziende si preoccupano giustamente delle responsabilità in cui possono incorrere in caso di utilizzo inappropriato dei telefonini da parte dei dipendenti. Per di più, cosa accadrebbe a tutti quei dati se un dipendente lasciasse l'azienda o vendesse il suo vecchio cellulare su eBay?

ALCUNI DATI SORPRENDENTI

- Ogni anno vengono rubati circa 1,3 milioni di cellulari, solo nel Regno Unito[7]
- Le più importanti aziende statunitensi subiscono il furto di 1.985 memory stick USB, 1.075 smartphone e 640 laptop, ogni settimana[8]
- Ogni anno nei taxi di Chicago vengono lasciati 120.000 cellulari[9]
- Negli Stati Uniti vengono smarriti 113 cellulari al minuto[10]

Una strategia di sicurezza mobile che includa politiche e strumenti di gestione dei dispositivi può garantire i controlli necessari a risolvere questi problemi.

- **Separazione delle funzioni aziendali sul dispositivo mobile** — Gli strumenti per la gestione della sicurezza mobile consentono alle aziende di definire quali applicazioni e dati presenti sui dispositivi sono relativi all'attività aziendale e pertanto sotto il loro controllo.
- **Cancellazione dei dati in remoto** — Questa funzione consente alle aziende di applicare le politiche di smantellamento dei dispositivi. Ad esempio, se un dipendente lascia l'azienda, l'operazione sul suo dispositivo può essere eseguita in modo selettivo cancellando solamente le applicazioni e i dati aziendali, senza compromettere la funzionalità per "uso personale". La stessa capacità verrebbe sfruttata per l'applicazione delle politiche al fine di eliminare tutte le informazioni aziendali da qualsiasi dispositivo che viene ritirato dal servizio.
- **Fading dati** — I dispositivi non connessi in rete perdono automaticamente i dati dopo un determinato periodo di tempo.

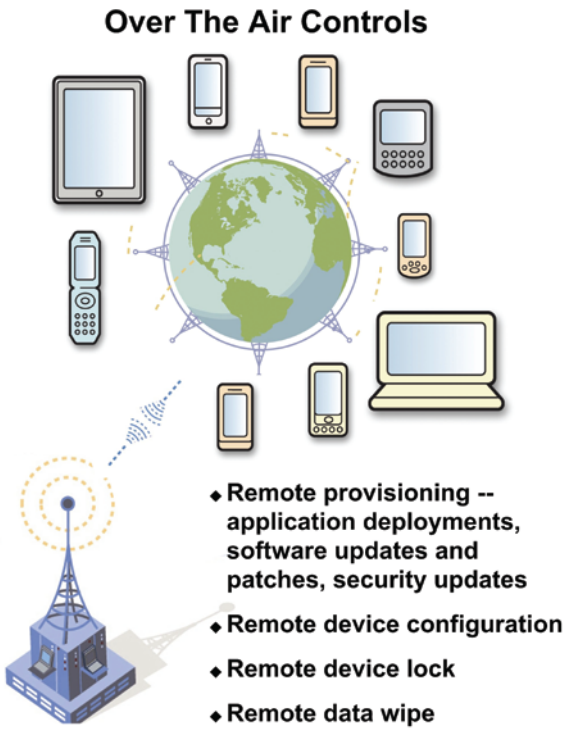
Lacune nella gestione dei dispositivi e nell'implementazione della politica.

La validità delle politiche di sicurezza è direttamente correlata alla capacità di un'organizzazione di implementarle. Inoltre, la mobilità aziendale odierna rende più complesso l'ambiente di implementazione a causa di una serie di fattori.

- Raramente i dispositivi mobili sono fisicamente presenti quando sorge l'esigenza di proteggerli;
- La maggior parte delle grandi aziende fa uso di numerosi e svariati tipi di dispositivi, come ad esempio smartphone, tablet, laptop, PDA e altri. Molti di questi dispositivi vengono eseguiti su sistemi operativi diversi; inoltre, sul mercato vengono regolarmente introdotti nuovi tipi di dispositivi mobili.
- Con il ricorso sempre più marcato della mobilità nelle attività di routine, le aziende tendono ad avvalersi di un maggior numero di applicazioni aziendali, ognuna con le proprie funzionalità di accesso ai dati e con protocolli di sicurezza specifici.

Nel tentativo di garantire il monitoraggio dei dispositivi e l'applicazione delle politiche di sicurezza, molte organizzazioni hanno adottato un insieme eterogeneo di strumenti di gestione e sicurezza. Questo approccio si traduce in livelli di protezione incongruenti.

- **Un'unica piattaforma di gestione della sicurezza** — Questa soluzione offre una console comune per la gestione della sicurezza in grado di supportare tutti i tipi di dispositivi e applicazioni che contraddistinguono un ambiente dinamico di mobilità aziendale.



Sintesi dei rischi e dei rimedi specifici...

RISCHIO	RIMEDI
Dati persi a causa di dispositivi smarriti o rubati	• Autenticazione utente a livello di dispositivo • Bloccaggio e cancellazione in remoto • Crittografia dati • Controllo dati
Un utente non autorizzato accede ai dati con un cellulare smarrito o rubato	• Autenticazione utente a livello di dispositivo • Bloccaggio e cancellazione in remoto • Crittografia dati • Controllo dati
Un utente autorizzato ottiene l'accesso non autorizzato a informazioni riservate o ne fa un uso inappropriato	• Politiche di sicurezza • Provisioning e impostazioni delle applicazioni mobili • Aggiornamenti alla configurazione in remoto • Monitoraggio e registrazione di eventi e attività
Rischi derivanti dall'uso di un unico dispositivo per fini professionali e personali	• Politiche di sicurezza • Separazione delle funzioni aziendali sul dispositivo mobile • Cancellazione dati in remoto • Fading dati
Lacune nella gestione dei dispositivi e nell'implementazione della politica	• Un'unica piattaforma di gestione della sicurezza

Tenendo ben presenti questi rischi e rimedi, è possibile pensare in termini strategici alla sicurezza mobile. In che modo, tuttavia, è possibile elaborare una strategia coerente a tutti i livelli dell'organizzazione dal momento che oggi la mobilità è caratterizzata da così tanti e diversi tipi di dispositivi mobili e scenari di utilizzo?

Un metodo valido consiste nell'organizzare le procedure di gestione della sicurezza basandosi sulle fasi del ciclo di vita di un dispositivo. Vediamo perché.

APPROCCIO AD UNA STRATEGIA DI SICUREZZA MOBILE BASATO SUL CICLO DI VITA

Le ragioni che spingono a considerare la sicurezza mobile globale dal punto di vista del ciclo di vita di un dispositivo sono più che valide: le diverse fasi del ciclo di vita offrono infatti opportunità concrete per l'applicazione delle politiche di sicurezza.

Tutti i dispositivi mobili hanno più o meno lo stesso ciclo di vita, che può essere suddiviso nelle seguenti fasi:

- **Fase di provisioning** — È il momento in cui un dispositivo viene adibito per la prima volta ad un uso aziendale. Che si tratti di un dispositivo di proprietà aziendale o personale, questa è la fase migliore per configurare le funzioni di sicurezza per il resto della vita utile del dispositivo. L'"inizializzazione" del dispositivo potrebbe includere la separazione delle funzioni aziendali e personali, l'installazione di software antivirus, la messa a disposizione di una serie di applicazioni aziendali di base, la fornitura di dati, la configurazione della posta elettronica aziendale, l'impostazione della protezione tramite password e la configurazione dell'accesso in rete. Tutte queste operazioni possono essere eseguite in remoto mediante controlli over-the-air.
- **Fase di produzione** — Una volta configurato correttamente, il dispositivo mobile è pronto per l'uso aziendale. A quel punto tenere aggiornato il dispositivo mobile con le ultime patch di sicurezza e software, installare o aggiornare le applicazioni in base alle necessità e monitorarne l'uso diventa una questione tecnica. L'utilizzo di controlli over-the-air per eseguire queste funzioni in modo più efficiente consente di gestire e proteggere i dati per l'intera vita utile del dispositivo.
- **Fase di smantellamento** — Si tratta del momento in cui un dispositivo viene ritirato dal servizio. Potrebbe coincidere con la sostituzione del dispositivo con un modello più nuovo, o con l'uscita di un dipendente dall'organizzazione, oppure con lo smarrimento o il furto di un dispositivo. Lo smantellamento comporta l'eliminazione di tutti i dati, le applicazioni e le funzionalità aziendali dal dispositivo. Anche questa operazione può essere eseguita in remoto tramite controlli over-the-air. È possibile configurare i dispositivi in modo che in determinate circostanze cancellino automaticamente i dati e le funzioni aziendali in essi contenuti, ad esempio in caso di mancato accesso ad una rete aziendale per un periodo di tempo prolungato.

Provisioning

- Definizione politiche di sicurezza
- Inizializzazione password
- Installazione e crittografia dati
- Installazione e configurazione software antivirus
- Installazione e configurazione controlli firewall e periferiche
- Installazione e configurazione applicazioni aziendali

Produzione

- Aggiornamenti software e configurazione
- Esecuzione back up dati sul dispositivo
- Applicazione aggiornamenti sicurezza e patch
- Applicazione politiche di sicurezza
- Monitoraggio e tracking di violazioni e minacce alla sicurezza
- Conformità registrazione attività

Smantellamento

- Disabilitazione dispositivo smarrito o rubato
- Cancellazione dati e applicazioni aziendali dal dispositivo
- Esclusione e blocco in remoto
- Blocco di violazione d'accesso
- Controllo dati
- Disabilitazione dell'accesso alla rete e all'applicazione

Il segreto per un'elaborazione e applicazione efficaci di una strategia di sicurezza mobile sta nell'usare il dispositivo e gli strumenti appropriati di gestione della sicurezza. Molte organizzazioni si sono create barriere a causa dell'approccio frammentario alla mobilità aziendale. Questo è comprensibile, ma esiste una soluzione migliore.

LA SICUREZZA MOBILE COME STILE DI VITA

Recentemente la nuova tecnologia mobile ha ispirato molte iniziative di mobilità aziendale. Fornendo informazioni migliori in qualsiasi momento e luogo necessario, la mobilità semplifica e accelera il processo di business, consente alle aziende di fornire un servizio migliore e offre notevoli vantaggi competitivi.

Questi vantaggi, uniti al costo ridotto e alla facilità di adozione di soluzioni specifiche "pronte all'uso", hanno dato origine a numerosi programmi pilota e adozioni a livello di gruppi di lavoro. Un indicatore della rapidità con cui la mobilità entra nei luoghi di lavoro è l'interesse dimostrato dalle aziende per l'iPad di Apple. A meno di un anno dalla release iniziale dell'iPad, l'80% delle aziende appartenenti alla classifica Fortune 100 stava testando o implementando questi dispositivi[11], rendendo l'adozione di questa tecnologia una delle più rapide in tutta la storia del business.

Molte applicazioni di mobilità aziendale riscuotono grande successo presso i lavoratori che, dopo avere iniziato ad utilizzarle, non possono più farne a meno. Troppo spesso, però, le buone idee in termini di mobilità aziendale si trasformano in deliri a livello di gestione. Qualche implementazione di successo scatena la richiesta di altre e ben presto i responsabili IT si trovano a dover fare i conti con molteplici applicazioni mobili eseguite su diversi tipi di dispositivi mobili, ognuno con la propria serie di strumenti di gestione e configurazione.

In assenza di un'unica piattaforma di sicurezza utilizzata per gestire tutti i dispositivi mobili (tablet, smartphone, laptop, PDA e altri dispositivi), non può esserci una strategia di sicurezza mobile coerente e di sicura applicazione. Ma quali sono le capacità chiave che deve avere una piattaforma di sicurezza mobile?

- **La piattaforma deve supportare un'ampia gamma di dispositivi mobili** — questa caratteristica è importante perché l'evoluzione della tecnologia mobile è in fase di accelerazione. Sul mercato vengono costantemente introdotti nuovi dispositivi con nuove funzionalità. Compaiono nuove configurazioni più idonee a determinate applicazioni aziendali (ad esempio tablet). Se le organizzazioni non vogliono porsi un freno utilizzando una tecnologia obsoleta o limitata, devono essere in grado di applicare le politiche di sicurezza ad un'ampia gamma di tipologie di dispositivi, senza fare eccezioni per le nuove tecnologie mobili.
- **La piattaforma deve supportare un'autenticazione utente efficace** — si tratta della principale difesa contro l'uso non autorizzato di dispositivi mobili.
- **La piattaforma deve supportare una crittografia efficace** — è uno degli strumenti più importanti per proteggere i dati sui dispositivi mobili.
- **La piattaforma deve avere la capacità di definire restrizioni all'accesso e politiche di sicurezza per tutte le applicazioni aziendali mobili** — questa caratteristica è essenziale per gestire e applicare la politica in modo uniforme, riducendo al minimo i fattori di vulnerabilità, per le attività aziendali mobili di tutta l'organizzazione.
- **La piattaforma deve supportare controlli "over-the-air" efficaci quali provisioning remoto, configurazione remota dei dispositivi, bloccaggio remoto dei dispositivi e cancellazione remota dei dati** — un requisito per il controllo dei dispositivi mobili che sono generalmente distribuiti su una vasta area geografica, non comodamente ripristinabili presso un centro di assistenza, e spesso smarriti o rubati.
- **La piattaforma deve avere sofisticati controlli di sicurezza e potenti funzionalità di monitoraggio dell'attività**— essenziali per supportare lo stesso livello di gestione dell'accesso basato su diritti di cui necessitano le grandi organizzazioni per i loro sistemi client mainstream.

L'implementazione di un'efficace strategia di sicurezza basata su piattaforma migliora la conformità di un'organizzazione alle norme in materia di tutela delle informazioni riservate, riduce l'incidenza dei reati di violazione dei dati mediante dispositivi mobili e semplifica la gestione della sicurezza.

Per ulteriori informazioni sulla creazione di soluzioni mobili sicure e gestibili, visita il sito: http://www.sap.com/italy/solutions/mobility/index.epx oppure contatta un rappresentante SAP.

NOTE

1 Garrestson, Rob. "IDC: Mobile Workers Will Pass 1 Billion in 2010." *CiO Zone*. 24 febbraio 2010.
2 Ibid.
3 Maurer, Allan. "More than a third of consumers have had cell phones lost or stolen." *TechJournal South*. 8 febbraio 2011.
4 Waltz, Martha. "Mobility Threats." *Mobile Enterprise.* 7 marzo, 2011; Info security. "40% of businesses looking to deploy mobile data encryption." 25 giugno 2010; Check Point. "Check Point Survey Reveals Growing Mobile Workforce Expected to Increase Security Complexity in 2011." 7 dicembre 2010.
5 Sinrod, Eric. "Data Security Breaches Cost Real Money." *FindLaw.* 2 febbraio 2010.
6 Garrestson, Rob. "IDC: Mobile Workers Will Pass 1 Billion in 2010". *CiO Zone.* 24 febbraio 2010.
7 Info security. "40% of businesses looking to deploy mobile data encryption." 25 giugno 2010.
8 Lennartsson, Kurt. "How to Use Data Encryption to Secure Mobile Business Data." *eWeek*. 14 gennaio 2010.
9, 10 MicroTrax (2011), "Alarming Statistics."
11 Dignan, Larry. "Apple's enterprise mojo by the numbers." *TechRepublic.* 19 gennaio 2011.

SYBASE, INC.
SEDE INTERNAZIONALE
ONE SYBASE DRIVE
DUBLIN, CA 94568-7902
U.S.A
1 800 8 SYBASE

www.sybase.com

Copyright © 2012 Sybase, Inc. Tutti i diritti riservati. Sono riservati i diritti sui materiali non pubblicati ai sensi delle leggi sul diritto d'autore degli Stati Uniti. Sybase e il logo Sybase sono marchi registrati di Sybase, Inc. o delle relative affiliate. * indica la registrazione negli Stati Uniti d'America. SAP e il logo SAP logo sono marchi o marchi registrati di SAP AG in Germania e in diversi altri paesi. Tutti gli altri marchi appartengono ai rispettivi proprietari.
02/12 L03333

SYBASE®
An SAP Company