GUIDA ALLE BEST PRACTICE PER MOBILE DEVICE MANAGEMENT E MOBILE SECURITY

SOMMARIO

BERSAGLI MOBILI: MOBILE DEVICE MANAGEMENT E MOBILE SECURITY

1. APERTI 24 ORE SU 24

L'accesso alle informazioni e applicazioni aziendali vitali da dispositivi mobili consente di migliorare la produttività dei dipendenti e di accrescere l'agilità e la flessibilità delle aziende.

La mobilità, tuttavia, ha un prezzo. Le stesse funzioni che rendono i dispositivi smart così utili per i dipendenti li trasformano in oggetti attraenti per gli hacker, i ladri di dati, i distributori di malware e altri criminali. Negli ultimi 12 mesi, il 51% delle organizzazioni di tutto il mondo ha subito una perdita di dati a causa della scarsa sicurezza dei dispositivi mobili.[1]

Ma il problema non è solo il malware: la tendenza a incoraggiare le iniziative BYOD (Bring Your Own Device) nelle aziende di tutte le dimensioni contribuisce a una diffusione sempre più complessa di dispositivi al loro interno. Al tempo stesso, i confini tra uso aziendale e uso personale diventano sempre più indefiniti e ciò contribuisce a rendere più difficoltoso il compito degli amministratori IT alle prese con la gestione e il controllo delle risorse aziendali.

Com'è possibile supportare le iniziative BYOD senza troppi problemi? Come fare a controllare le attività dell'utente finale che scarica applicazioni in una stanza di albergo, in un altro fuso orario? Cosa succede se l'utente dimentica lo smartphone sul sedile del taxi? È possibile esercitare un controllo con facilità, da un'unica postazione centrale? La gestione dei dispositivi mobili offerta da Mobile Device Management (MDM) può rispondere alla maggior parte di queste domande.

2. MOBILE DEVICE MANAGEMENT - IN COSA CONSISTE?

Grazie a Mobile Device Management, il personale IT può estendere criteri e strategie di sicurezza dei dispositivi cablati a tutti i dispositivi, in qualsiasi luogo. L'uso del software MDM permette ai responsabili IT di automatizzare in maniera conveniente attività vitali di gestione e controllo, quali la configurazione dei dispositivi, gli aggiornamenti del software e i processi di backup e ripristino, garantendo al contempo la sicurezza delle informazioni aziendali sensibili in caso di furto, perdita o abuso da parte degli utenti finali.

3. COME SCEGLIERE LA GIUSTA SOLUZIONE MDM

3.1 Supporto multipiattaforma

Android, BlackBerry, iOS, Symbian, Windows Phone... Chi supporta le iniziative BYOD conosce fin troppo bene la necessità di proteggere più piattaforme e gestirle.

Una soluzione MDM multipiattaforma non è solo economicamente conveniente, ma elimina anche l'esigenza di gestire più sistemi. Garantisce inoltre elevata flessibilità, supportando sia i dispositivi posseduti oggi dalla vostra azienda sia i marchi e i prodotti che sceglierete in futuro.

1 Fonte: Ponemon, The Cost of a Lost Laptop (2009)

4. PRASSI DI MDM EFFICACI

4.1 Criteri solidi

È necessario creare criteri specifici per la mobilità che definiscano chiaramente, tra l'altro, quanto segue:

- Modalità di implementazione del dispositivo
- Quali dati saranno accessibili ai lavoratori mobili
- Autorizzazioni di utilizzo delle reti aziendali e per quali attività
- Procedure da implementare in caso di perdita o furto del dispositivo

È necessario definire e applicare i criteri in modo granulare e flessibile, ovvero applicando criteri diversi per utenti e gruppi diversi, in base alle specifiche esigenze. Questo livello di granularità deve estendersi ai dispositivi, impedendo, ad esempio, l'utilizzo di un apparecchio smarrito o in altro modo compromesso per l'accesso ai dati aziendali oppure eseguendone il blocco in remoto, aggiungendo in tal modo un ulteriore livello di sicurezza.

4.2 Containerizzazione

L'89% di chi usa i dispositivi privati per lavoro dichiara di accedere a informazioni aziendali di importanza vitale. Il 41% ammette di utilizzare i dispositivi privati in ufficio pur non disponendo della debita autorizzazione.[2]

Anche gli utenti più coscienziosi possono inavvertitamente mettere a rischio i sistemi e i contenuti della loro azienda scaricando applicazioni di consumo o accedendo a contenuti personali con il loro dispositivo.

La containerizzazione rappresenta una semplice soluzione a questo problema, poiché consente di tenere separati i contenuti aziendali da quelli personali presenti sul dispositivo. In tal modo il personale IT riesce a mantenere il controllo completo sui contenuti aziendali, proteggendoli dai rischi insiti nell'utilizzo privato e senza peraltro compromettere i dati personali. Con la containerizzazione i reparti IT possono applicare i criteri di sicurezza e protezione dei dati a un "container" presente su un dispositivo privato o di proprietà dell'azienda, garantendo un vantaggio particolarmente importante negli scenari BYOD.

4.3 Crittografia

Tra le best practice per MDM deve figurare anche la crittografia dei dati sensibili contenuti nel container, che consente di ottimizzare le strategie contro i furti. L'applicazione forzata di questa tecnica sui dati consente, ad esempio, di ridurre gli eventuali ritardi derivanti dalla cancellazione dei dati presenti su un dispositivo perduto o rubato.

Garantendo che solo i dati crittografati possano uscire dal container di un dispositivo, le organizzazioni possono ridurre il rischio di fuga di dati e rispettare i requisiti di conformità relativi alla protezione dei dati. La tecnologia di crittografia MDM di Kaspersky Lab può essere automatizzata e resa completamente trasparente per l'utente finale, assicurando in tal modo una stretta conformità ai criteri aziendali di sicurezza.

4.4 Protezione contro i furti e sicurezza dei contenuti

È quasi impossibile bloccare fisicamente dispositivi ultramobili di piccole dimensioni, ma è possibile bloccarne i contenuti e controllare cosa succede quando non sono più nelle mani del legittimo proprietario.

La soluzione MDM di Kaspersky Lab include funzioni di protezione contro i furti e per la sicurezza dei contenuti, da attivare in remoto per impedire l'accesso non autorizzato ai dati sensibili. Tra le funzioni ci sono le seguenti:

- **Controllo della SIM:** consente di bloccare un telefono perduto o rubato, anche in caso di sostituzione della SIM, e di inviare il nuovo numero al legittimo proprietario.
- **Localizzazione/tracciabilità del dispositivo:** consente di localizzare la posizione del dispositivo tramite GPS, GSM o Wi-Fi.
- **Cancellazione remota/selettiva:** consente di cancellare tutti i dati memorizzati su un dispositivo oppure solo le informazioni aziendali sensibili.
- **Blocco remoto:** impedisce l'accesso non autorizzato a un dispositivo, evitando l'esigenza di cancellare i dati

2 Fonte: Juniper Networks, Trusted Mobility Index 2012.

in esso contenuti.

4.5 Protezione antimalware per i dispositivi mobili

Avete bisogno di una strategia per gestire in maniera efficiente i dispositivi perduti o rubati, tuttavia i dispositivi sono esposti a rischi anche con gli utenti autorizzati. Molte organizzazioni si impegnano per implementare soluzioni antimalware e antispam sulle reti aziendali fisse, mentre fanno ben poco per impedire che i dispositivi mobili introducano virus o altro malware nella rete.

Le tecnologie per la sicurezza dei dispositivi mobili di Kaspersky Lab includono una soluzione antimalware mista, che affianca tecnologie proattive assistite da cloud al tradizionale rilevamento basato sulle firme, migliorando i tassi di rilevamento e offrendo una protezione antimalware in tempo reale. Le scansioni on-demand e programmate garantiscono la massima protezione, mentre gli aggiornamenti OTA automatici sono essenziali in qualsiasi strategia MDM.

4.6 All'insegna della semplicità: controlli centralizzati

Le tecnologie di Kaspersky Lab consentono agli amministratori di utilizzare una console centralizzata per gestire i dispositivi mobili, gli endpoint e la rete aziendale, per eliminare la complessità generalmente associata a soluzioni separate e all'uso delle numerose console, spesso incompatibili. L'espansione incontrollata della tecnologia complica a dismisura un lavoro già di per sé alquanto difficile.

Semplificando e automatizzando la configurazione sicura di più dispositivi, non solo si riduce il carico di lavoro dell'IT, ma si incoraggia l'uso di best practice per la sicurezza dei dispositivi mobili. Una volta stabiliti i vostri criteri e regole di base, il controllo centralizzato può essere ottenuto con un semplice clic, sia che i dispositivi da gestire siano 10 oppure 1.000.

4.7 Giusto equilibrio

Avete bisogno di una soluzione che consenta di implementare, gestire e proteggere il vostro ambiente IT mobile in maniera semplice e conveniente. La soluzione MDM di Kaspersky Lab semplifica e velocizza la configurazione sicura dei dispositivi mobili, mentre un agente mobile installato nei dispositivi vi garantisce la protezione necessaria per contrastare le minacce odierne. Gli amministratori IT hanno la certezza che tutti i dispositivi mobili vengono configurati con le impostazioni necessarie e sono protetti in caso di perdita, furto o uso improprio da parte degli utenti.

Non importa quanto grande sia un'azienda: se non gestiti adeguatamente, i dispositivi mobili si trasformeranno presto in un altro consumo di risorse, senza parlare dei rischi di sicurezza e di perdita dei dati. Indipendentemente dal fatto che intendiate ridurre i costi con il supporto di un'iniziativa BYOD o con l'attuazione di un rigoroso programma per i dispositivi mobili aziendali, i rischi da affrontare alla fine restano gli stessi: un crescente volume di dati aziendali sensibili resta in mano ai dipendenti, può essere abbandonato nei taxi oppure rubato o perduto.

L'ideale sarebbe poter disporre di mobilità, maggiore produttività e semplicità senza dovervi preoccupare di sicurezza e protezione dei dati. E ci riuscirete, grazie alle avanzate tecnologie per la sicurezza mobile e la gestione dei dispositivi mobili di Kaspersky.

5. CONCLUSIONI

Le organizzazioni necessitano di tecnologie di sicurezza intelligenti per proteggere i loro dati, oltre che di strumenti IT intuitivi e non complicati. I 2.500 dipendenti di Kaspersky Lab hanno il compito di soddisfare tali esigenze per gli oltre 300 milioni di sistemi da loro protetti, nonché per i 50.000 nuovi sistemi che si aggiungono ogni giorno a questa cifra.

Kaspersky MDM è un componente di Kaspersky Endpoint Security for Business. Grazie all'abbinamento di antimalware pluripremiato, strumenti di applicazione dei criteri IT, gestione centralizzata e protezione assistita da cloud, i prodotti Kaspersky per la sicurezza aziendale sono la scelta giusta per la vostra organizzazione. Parlate con il rivenditore per scoprire come Kaspersky può aggiungere la configurazione sicura alla vostra implementazione di endpoint mobili e molto altro ancora!

Kaspersky Lab ZAO, Mosca, Russia
www.kaspersky.it