ZEBRA

FORMULARE UNA POLICY ROBUSTA PER LA SICUREZZA MOBILE: i rischi principali e in che modo le imprese possono evitarli.

La sicurezza IT della mobilità aziendale viene spesso paragonata alla copertura assicurativa. Qualcosa di cui tenere conto semplicemente perché siete obbligati a farlo. Questa visione limitata, però, non affronta il vero problema. La sicurezza fornisce molto più che una semplice copertura in risposta a un evento specifico. Può fornire anche rassicurazione, consentendo alla vostra impresa di operare e innovare senza il rischio di violazioni di dati.

In questo libro bianco, esamineremo le considerazioni principali da fare per mettere a punto una policy robusta in materia di sicurezza mobile. Presenteremo i rischi principali e cosa potete fare al riguardo, in modo da poter mettere in moto nuove opportunità per migliorare produttività, efficienza e precisione nelle attività operative.

No a un approccio passe-partout

Persistono divergenze sul valore della sicurezza. Quello su cui tutti sono d'accordo è che si tratti di un argomento complesso che tocca numerosi ambiti dell'organizzazione. Quando prendete in considerazione l'ampio ventaglio di casi d'uso della mobilità, le metodologie delle applicazioni e le soluzioni di implementazione delle singole imprese, il valore complessivo della sicurezza, nonché la sua complessità, diventa maggiormente evidente.

In un negozio al dettaglio, il personale munito di tablet può servire i clienti rapidamente. Ma quegli stessi clienti vogliono essere certi che i dati personali forniti siano sicuri su tali dispositivi. Nell'ambito della produzione, c'è l'aumento delle tecnologie indossabili da prendere in considerazione. Questo cambiamento comporta il fatto di rendere sicuro il flusso di dati provenienti da un vasto numero di endpoint.

Le metodologie delle applicazioni variano inoltre a seconda del caso d'uso e del tipo di dispositivo. Dalle app basate sul web fino a quelle mobili native o addirittura ibride, ciascun esempio comporta esigenze specifiche in materia di sicurezza per l'impresa.

Le opzioni di implementazione mobile disponibili possono aggiungere un ulteriore livello di complessità. Se l'azienda promuove il BYOD (Bring Your Own Device) o utilizza una tecnologia di classe consumer, il team IT potrebbe trovarsi a dover impegnare ulteriori risorse. Quando i sistemi operativi mobili di classe consumer non forniscono i livelli di sicurezza richiesti, il team IT dovrà mettere a punto soluzioni di sicurezza internamente. Vi sono poi ulteriori preoccupazioni quando si tratta di proteggere l'attività di rete e la sicurezza per la connettività WAN o WLAN.

Le piattaforme di mobilità devono affrontare ciascuna di queste considerazioni in materia di sicurezza e allo stesso tempo soddisfare la richiesta aziendale di maggiore IT in movimento. L'obiettivo, per qualsiasi impresa, dovrà essere quello di preservare la sicurezza dei dati senza intralciare le attività operative quotidiane. Quali sono, quindi, le minacce principali e cosa dovrebbe includere una policy robusta in materia di sicurezza mobile?

C'È L'AUMENTO DELLE TECNOLOGIE INDOSSABILI DA PRENDERE IN CONSIDERAZIONE.

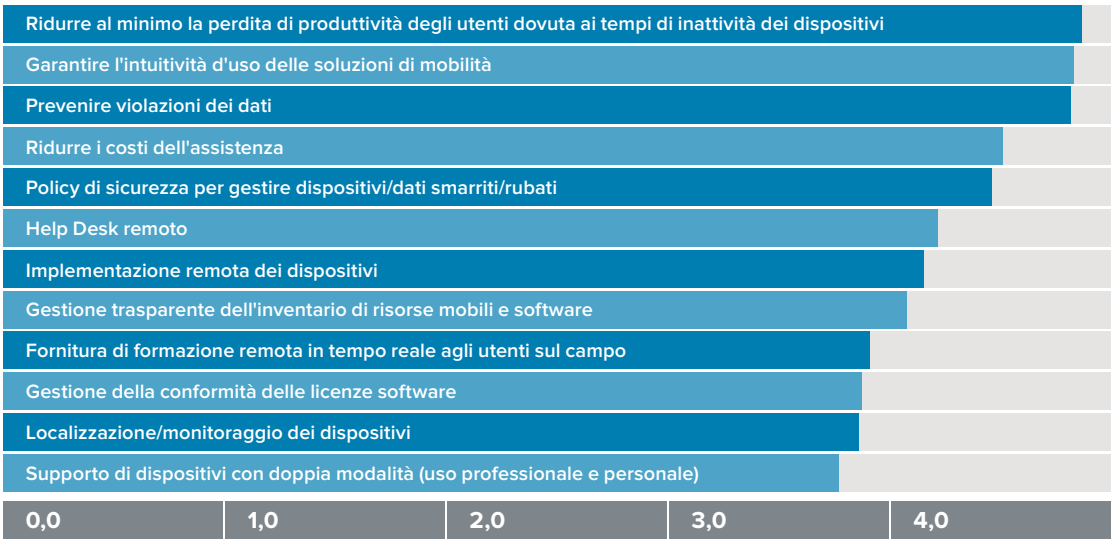
Questo cambiamento comporta il fatto di rendere sicuro il flusso di dati provenienti da un vasto numero di endpoint.

Identificare i rischi

Le caratteristiche di base dei dispositivi mobili implicano che essi siano esposti a un numero decisamente superiore di minacce alla sicurezza rispetto ai desktop. Il fattore di forma (piccole dimensioni e portabilità) li espone al rischio di furti. Se non gestiti correttamente, sistemi operativi e applicazioni multifunzione possono creare molteplici percorsi che i criminali informatici possono sfruttare. Inoltre, la comunicazione su connessioni che utilizzano reti Wi-Fi o di cellulari aperte e non protette riduce la protezione dei dati aziendali o dei clienti, il che richiede un'ulteriore attenzione nei confronti del controllo dell'accesso a reti non protette.

Secondo VDC, una società di analisti del settore, prevenire le violazioni dei dati costituisce uno dei tre timori principali quando si tratta di investire in mobilità aziendale. L'adozione di policy di sicurezza per la gestione di dispositivi e dati smarriti o rubati rientra a sua volta nelle cinque priorità, dopo la riduzione al minimo dei tempi di inattività, l'intuitività d'uso per gli utenti e la riduzione dei costi dell'assistenza. [1]

Valutate le seguenti problematiche legate alla mobilità in termini di importanza per la vostra azienda (1 = Estremamente irrilevante; 6 = Estremamente rilevante)



[1] *"Total Cost of Ownership Models - Enterprise and Government Mobility Applications", VDC Research, Josh Martin, David Krebs*

Tali rischi sono tutt'altro che semplicistici. Approfondite il discorso dei problemi di sicurezza generali e scoprirete minacce sia interne che esterne. La ricerca del VDC è corroborata da un'indagine di TechTarget SearchSecurity dedicata alle cinque problematiche principali inerenti alla sicurezza mobile aziendale.[1] Ciascuna delle problematiche principali individuate dai 487 partecipanti faceva riferimento a timori riguardanti i dati aziendali.

1. Perdita di dispositivi – per es. lasciare un tablet o uno smartphone aziendale in un taxi o ristorante
2. Sicurezza delle applicazioni – per es. dati messi a disposizione di sviluppatori di app mobili gratuite
3. Fuoriuscita di dati dai dispositivi – per es. il rischio che criminali informatici accedano ad applicazioni aziendali in funzione su dispositivi personali
4. Attacchi malware – per es. troian horse, strumenti di monitoraggio o applicazioni dannose
5. Furto di dispositivi – per es. esposizione dei dati dopo il furto di un dispositivo di fascia alta

In gioco ci sono la reputazione e gli introiti dell'azienda. Come riportato da un articolo apparso su CIO.com,[2] *"Maggiore è il numero di dipendenti e collaboratori esterni che utilizzano dispositivi mobili per accedere a sistemi, applicazioni e dati aziendali, più diventa importante proteggere tale accesso. Inoltre, è essenziale impedire a dispositivi mobili che dovrebbero stimolare la produttività e aumentare i profitti di aprire la strada a modi non autorizzati di accedere a informazioni e altre risorse; questo li trasforma invece in un pericolo e in una possibile perdita di entrate."*

Il problema persiste: quali misure specifiche può adottare la vostra organizzazione per affrontare la minaccia costante costituita da problemi di sicurezza mobile a livello aziendale?

[1] *Top 5 enterprise mobile security issues, Tech Target, 2012*

[2] *http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html*

Combattere le minacce

Visto che ci si affida sempre di più a tecnologie mobili, le imprese devono cercare di rispondere in modo più fluido ai problemi di sicurezza. Aggregando le analisi di Gartner, Forrester e Information Week, emergono solo alcune delle risposte principali che i team IT possono fornire per affrontare i rischi interni ed esterni.

Forrester sostiene inoltre il ricorso alle seguenti sette misure come essenziale per la gestione dei dispositivi mobili (MDM) e la sicurezza mobile:

- Applicazione di PIN (password "forti")
- Cancellazione selettiva (essenziale per un programma BYOD)
- Rilevazione di jailbreak/rooting
- Criptatura dei dati
- Reti VPN (Virtual Private Network)
- Protezione dalla fuoriuscita di dati (impedendo agli utenti autorizzati di provocare, inavvertitamente o intenzionalmente, fuoriuscite di dati)
- Limitazione dei dispositivi ActiveSync

Se l'azienda non è disposta a prendere sul serio la sicurezza mobile, le due serie di misure restano di fatto solo "liste di desiderata" dell'IT. La dirigenza svolge un ruolo chiave nel portare la sicurezza all'attenzione dei vertici aziendali e nel destinare risorse a combattere minacce sempre più sofisticate.

Per fare tutto questo in modo efficace, vale la pena di comprendere i requisiti normativi più diffusi e le best practice internazionali in materia di sicurezza. Un rapido esame di questi standard delinea le misure che ogni impresa dovrebbe includere nella propria policy per la sicurezza mobile:

- Protezione da smarrimenti e furti di dispositivi
- Protezione dei dati in movimento
- Protezione dei dati a riposo
- Gestione delle applicazioni mobili
- Conformità alle normative
- Controllo, gestione e monitoraggio dei dispositivi
- Protezione della privacy dei dati ad alto livello
- Riduzione al minimo dei costi amministrativi per mantenere sicure le piattaforme
- Robusti meccanismi di controllo dell'accesso/autenticazione
- Massimizzazione dell'utilizzo dell'infrastruttura IT legacy

L'impresa deve quindi andare avanti con una policy per la mobilità che includa queste misure di sicurezza nel proprio nucleo portante. Oltre agli scenari dei casi d'uso, la sicurezza dovrà esercitare la stessa influenza sulla scelta dei dispositivi e del sistema operativo.

FUNZIONALITÀ PER LA GESTIONE DELLA SICUREZZA[3]
Registrazione automatica e implementazione dei dispositivi
Password rafforzata
Cancellazione dei dispositivi, blocco remoto
Funzionalità di audit degli account utenti e dei dispositivi
Rilevamento di jailbreak
Funzionalità di protezione dei dati
Dispositivi di controllo delle applicazioni
NAC mobile
Antivirus, antispam, FW degli endpoint e IDS degli endpoint
Certificati basati sui dispositivi
Monitoraggio attivo delle protezioni di cui sopra
VPN aziendale
Gestione delle chiavi e gestione dei certificati

[3] Fonti: rapporto Information Week, novembre 2011; rapporto Forester, Answers to top mobile security questions, 2011; rapporto Gartner, MCM_MQ, aprile 2011.

Il costo di scelte di mobilità errate

Vista la proliferazione di rischi per la sicurezza, le imprese attratte da prezzi di ingresso bassi devono riesaminare l'utilizzo di dispositivi pronti per l'uso di classe consumer. La maggior parte dei sistemi operativi di classe consumer presenti in questi dispositivi non è dotata di tutte le funzionalità di sicurezza di cui necessitano le imprese. Alcuni studi indicano che il costo totale di esercizio (TCO) dell'utilizzo di dispositivi consumer per applicazioni di classe enterprise può essere superiore del 40-78% rispetto a dispositivi di classe enterprise progettati ad hoc.[3] La sicurezza costituisce un elemento importante di tale differenza.

"277 milioni di dispositivi mobili utilizzeranno qualche tipo di protezione entro il 2016."

I dispositivi consumer utilizzati in applicazioni aziendali costituiscono spesso un invito alle violazioni della sicurezza. In uno studio sul BYOD condotto da Decisive Analytics[4], quasi la metà (46,5%) delle aziende intervistate ha riferito una violazione di dati o della sicurezza dovuta all'accesso alla rete aziendale da parte di un dispositivo di proprietà di un dipendente. Per contrastare questa minaccia vengono fatti significativi investimenti. Tuttavia, non esiste alcuna garanzia che queste soluzioni alternative per la sicurezza continueranno a essere efficaci contro le minacce emergenti.

I dispositivi enterprise robusti progettati ad hoc, per contro, sono studiati e potenziati per soddisfare e semplificare la conformità con i principali obblighi normativi in materia di sicurezza. Il campo di applicazione della conformità in materia di sicurezza può essere molto ampio (per es. formazione degli utenti) oppure molto specifico (per es. la convalida dell'integrità degli algoritmi crittografici).

Nessun dispositivo o piattaforma di sistema operativo mobile può garantire la conformità in modo indipendente. Ma procurarsi dispositivi e piattaforme software da un produttore che si concentra sugli obblighi normativi aumenta le probabilità di conformità e riduce l'onere amministrativo della convalida. Questo, a sua volta, riduce il costo degli audit, può prevenire multe/sanzioni pecuniarie ed eliminare la necessità di segnalare violazioni di dati. Tutto questo si traduce in un miglioramento degli utili.

[3] "Total Cost of Ownership Models - Enterprise and Government Mobility Applications", Josh Martin e David Krebs, VDC Research; "A 3 Year Cost Comparison of Consumer-grade vs. Durable Smart Devices", Jack Gold, Gold Associates

[4] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Riflettori puntati sulla sicurezza del sistema operativo e delle applicazioni: Android

Le imprese che prendono in esame dispositivi di classe consumer possono scegliere fra diversi protagonisti del mercato: Google, Apple e Microsoft. La piattaforma Android di Google detiene la quota di mercato principale (81% del mercato globale nel 2015)[5]. La sua proposta di sicurezza intrinseca la rende inoltre interessante per le imprese che prendono in considerazione dispositivi di classe consumer. Soprattutto quando messa a confronto con piattaforme di sistemi operativi mobili alternativi. L'ambiente di prova delle applicazioni, il ricorso ad autorizzazioni per accedere alle risorse e la criptatura dei dati sono solo alcuni esempi delle potenti funzionalità di sicurezza di Android.

La maggior parte dei timori riguardanti la sicurezza di Android derivano dal potenziale malware all'interno di GooglePlay, l'app store della piattaforma. Apple controlla rigorosamente le applicazioni del proprio AppStore in quanto mantiene uno stretto controllo sul procedimento di iscrizione. Ciò nonostante, il rischio di sicurezza con GooglePlay è identico a quello di tutti gli app store pubblici. Ciascuno di essi è vulnerabile in termini di malware e di invasione della privacy (anche l'AppStore di Apple).

La prassi ottimale per eseguire i cosiddetti 'Corporate Liable Devices' consiste nel fornire il blocco della applicazioni e/o utilizzare un app store aziendale affidabile. Mobility Extensions (Mx) di Zebra offre un potenziamento della protezione. Semplificando la conformità ai requisiti di mobilità e agli obblighi normativi, le aziende possono usufruire di una sicurezza di classe enterprise su dispositivi di tipo consumer.

In combinazione con un app store aziendale, estensioni che includono il whitelisting, l'autenticazione tramite Active Directory/LDAP, la gestione delle chiavi e altre funzionalità fondamentali per la sicurezza aziendale assicureranno che i team IT possano rilasciare dispositivi consumer con la massima fiducia.

[5] http://www.idc.com/getdoc.jsp?containerId=prUS40664915

Quello che risulta chiaro è che la sicurezza mobile implica molto di più dell'assicurare l'integrità dell'azienda in caso di violazione di dati e dispositivi. Può supportare requisiti operativi specifici per la strategia mobile complessiva e ridurre il costo totale di esercizio delle implementazioni della mobilità a livello enterprise. Ma soprattutto, la sicurezza mobile continuerà ad evolversi e richiederà aggiornamenti e un riesame vigile continuo.

Mentre la mobilità aziendale ha fatto molta strada in pochissimi anni, la complessità dello scenario della sicurezza è cambiata (e continua a cambiare) radicalmente. Le problematiche sono complesse e le soluzioni ad ampio raggio. Esse dovranno essere esaminate singolarmente e unitamente alle priorità aziendali. Non ha senso adottare una policy di sicurezza rigorosa se questa poi limita le attività operative, vi rende poco competitivi e riduce la produttività dei dipendenti. D'altro canto, concentrarsi su tutti gli aspetti tranne la sicurezza vi lascia esposti al rischio di attacchi. Le policy di sicurezza mobile più robuste mitigheranno i rischi che vi trovate ad affrontare lasciandovi al contempo liberi di operare e innovare.

La chiave è bilanciare le priorità all'interno della policy in materia di sicurezza mobile, armonizzando i requisiti aziendali principali e le esigenze degli utenti finali con le policy di sicurezza secondarie che corrispondono ai diversi casi d'uso.

Un'utile lista di controllo

Vista la complessità e la quantità di considerazioni chiave, mettere a punto una policy per la sicurezza mobile dei dipendenti può apparire un compito arduo. Questa lista di controllo dovrebbe aiutarvi a fare in modo che qualsiasi scelta facciate abbia successo in tutta l'organizzazione, in particolare per quanto riguarda l'equilibrio fra esigenze degli utenti, dell'azienda e della sicurezza.

1. **Educate tutti:**
Assicuratevi che tutti siano consapevoli delle minacce alla sicurezza e create policy di utilizzo trasparenti che illustrino cosa ci si aspetta.

2. **Modificate periodicamente le password:**
La prassi ottimale consiste nell'aggiornare le password almeno ogni 30 giorni, e dovreste prendere in considerazione la possibilità di inserire l'obbligo di cambiare la password (con appositi criteri di robustezza) nelle vostre applicazioni.

3. **Ottenete la visibilità completa di tutti i vostri dispositivi:**
Utilizzate strumenti di gestione dei dispositivi mobili per localizzare immediatamente dispositivi smarriti o rubati e rendere inoffensivo il dispositivo o cancellare i dati. E utilizzate monitoraggio e avvisi per sapere dove si trova ogni dispositivo e come viene utilizzato.

4. **Create una whitelist:**
Assicuratevi che le persone accedano esclusivamente a una whitelist di siti web, approvati per l'uso con i vostri dispositivi.

5. **Proteggetevi dal malware:**
Creando una whitelist delle applicazioni interne e delle fonti di applicazioni sui vostri dispositivi, potete proteggervi da vettori di infezioni. Inoltre, controllare la capacità del dispositivo di effettuare il "sideloading" di applicazioni esterne – tramite una connessione esterna o una scheda di memoria – è un elemento fondamentale per tutelarvi dal malware e da altre applicazioni dannose.

6. **Aggiornate i dispositivi:**
Assicuratevi che i dispositivi eseguano sempre l'ultima versione dei programmi software, con aggiornamenti controllati e/o automatizzati.

7. **Suddividete i dati in appositi contenitori:**
Configurate i dispositivi in modo che i dati siano contenuti in aree criptate distinte, rendendo praticamente impossibile l'accesso ai dati da parte di aggressori.

8. **Adottate la criptatura completa:**
Dove le persone lavorano con dati altamente sensibili, potete criptare i dati archiviati sui dispositivi, nonché eventuali dati trasmessi su reti wireless.

9. **Utilizzate un app store aziendale:**
L'accesso ad app store pubblici andrà evitato e le applicazioni dovranno essere scaricate da un app store aziendale affidabile.

10. **Riesaminate continuamente la sicurezza:**
La sicurezza mobile non è un esercizio "mordi e fuggi": è fondamentale aggiornare costantemente strategie e best practice per gestire minacce che si evolvono continuamente

SCOPRITE PERCHÉ LA SICUREZZA È SOLO IL PUNTO DI PARTENZA QUANDO SI SCEGLIE UN NUOVO SISTEMA OPERATIVO MOBILE.

ESPLORATE LE ALTRE CONSIDERAZIONI CHIAVE CONSULTANDO LA PAGINA WWW.ZEBRA.COM/MOBILITYREVOLUTION

Sede centrale e Nord America
+1 800 423 0442
inquiry4@zebra.com

Sede Asia-Pacifico
+65 6858 0722
contact.apac@zebra.com

Sede EMEA
zebra.com/locations
mseurope@zebra.com

Sede America Latina
+1 847 955 2283
la.contactme@zebra.com