Appendice

Principali soluzioni per le diverse piattaforme

PRIVACY
On Cloud & Mobile

Principali soluzioni per le diverse piattaforme

Le indicazioni di seguito fornite non hanno la presunzione di essere un'analisi complessiva e dettagliata di tutte le soluzioni esistenti, ma hanno solo un valore indicativo, quale punto di partenza nell'identificazione più corretta per gli specifici ambiti operativi.

Principali soluzioni anti-malware

In relazione a quanto illustrato nelle misure minime di sicurezza, si evidenzia di seguito una breve sintesi delle soluzioni anti-malware esistenti.

Nome prodotto	Descrizione
AVG Mobile Security	Consiste in un software di sicurezza, designato principalmente per piattaforme Android, che consente di effettuare scansioni dell'intero dispositivo e rimuovere I virus individuati, di controllare la presenza di malware nel contenuto di siti web, email, SMS o di apps, di localizzare e bloccare il proprio dispositivo in caso di furto o smarrimento, di monitorare le prestazioni del dispositivo e individuare i settaggli o le applicazioni che ne rallentano il funzionamento e di filtrare chiamate e messaggi indesiderati. ***Fonte: www.avg.com***
Kaspersky Mobile Security	Consiste in una suite di sicurezza compatibile con la maggior parte delle piattaforme mobile, acquistabile tramite pc o dispositivo mobile dal sito del produttore. La protezione del dispositivo è garantita dascansioni antimalware real-time, aggiornamenti automatici riguardo le minacce più recenti, blocco delle connessioni potenzialmente dannose. Oltre alla protezione di base il software permette di archiviare files o cartelle criptate, di impostare numeri di telefono privati, di configurare un filtro Parental Control, di bloccare chiamate ed sms indesiderati e di localizzare tramite GPS il dispositivo smarrito o rubato. ***Fonte: www.kasperskystore.it***
ESET Mobile Security	Compatibile con le piattaforme Windows Mobile e Symbian, protegge in tempo reale i dispositivi effettuando scansioni all'accesso o su richiesta e bloccando i contenuti malevoli individuati. Offre inoltre funzionalità di firewall intelligente, antispam di SMS / Mms, cancellazione remota, blocco dei contenuti da remoto in caso di furto e controlli sulle funzioni vitali del dispositivo. ***Fonte: www.nod32.it***
BullGuard Mobile Security	Compatibile con quasi tutte le piattaforme mobile protegge il dispositivo da virus, spyware e frodi digitali. Presenta un'interfaccia basata sul web che offre accesso remoto al dispositivo perduto o rubato, e ne consente la localizzazione tramite GPS, il blocco e la cancellazione dei contenuti. Implementa inoltre funzionalità di controllo parentale, Firewall, spamfilter e backup. ***Fonte: www.bullguard.com***
McAfee Mobile Security	Disponibile sia per privati sia per imprese,è un sistema anti-malware che analizza e pulisce dispositivi mobili, impedendo la corruzione dei dati dovuta a virus, worms, Trojan, e altri codici malevoli. Le sue caratteristiche di protezione consentono di analizzare tutti i tipi di archivi, incluse e-mail, comunicazioni di testo, fotografie, e video. La tecnologia anti-malware protegge dati trasmessi tramite reti wireless, Bluetooth, Wi-Fi, e infrarossi. In caso di individuazione di minacce, vengono visualizzati allarmi istantanei e i file pericolosi sono rilevati e rimossi immediatamente; sono previsti aggiornamenti automatici per proteggere i dispositivi dalle ultime minacce. ***Fonte: www.mcafee.com***

Lookout Mobile Security	Progettato per piattaforme Android ed Apple, protegge i dispositivi dalle minacce legate a malware, spyware e permette di monitorare costantemente le applicazioni che accedono a dati privati e possono quindi comportare violazioni della privacy. In caso di furto sono previste funzionalità di localizzazione, blocco del dispositivo e cancellazione dei dati da remoto. ***Fonte: www.mylookout.com***
F-Secure Mobile Security	Garantisce protezione in tempo reale, prevedendo aggiornamenti automatici delle definizioni delle minacce, tramite scansione dei siti web, delle mail e dei messaggi e blocco del contenuto malevolo. Offre la possibilità di effettuare un back-up online dei propri dati e le funzionalità di localizzazione e blocco da remoto in caso di furto. ***Fonte: www.f-secure.com***
Norton Smartphone Security	Protegge la privacy e le informazioni personali su smartphone basati su Symbian e Windows. Ferma gli hackers ed impedisce ai criminali informatici di rubare informazioni o spiare l'utente quando è su una rete pubblica. Scopre e rimuove virus e altre minacce mobili prima che possano provocare problemi. Protegge da furto di informazioni private, spam di testo e multimediale, criminali informatici e minacce mobili. ***Fonte: www.symantec.com***
Trend Micro Mobile Security	Destinato a contesti sia aziendali sia privati, consente di disporre adeguate configurazioni del dispositivo e di aggiungere protezioni per ostacolare le minacce informatiche, quali malware, virus, worm e spyware, e ridurre il rischio di compromettere i dispositivi. Consente inoltre di implementare criteri definiti per l'accesso e la protezione dei dati tramite l'impiego di password, la crittografia dei dati e la rimozione remota dei dati dai dispositivi smarriti o rubati. ***Fonte: www.trendmicro.it***
Avast Mobile Security	Protegge i dati personali effettuando scan in tempo reale sui contenuti delle mail, dei messaggi e delle pagine internet visitate. Le definizioni dei virus sono aggiornate automaticamente. Sono disponibili funzionalità di filtro parentale e remote tracking, con la possibilità di inviare messaggi di alert via sms in caso di violazioni. In caso di furto o smarrimento è possibile bloccare il dispositivo da remoto e cancellarne il contenuto.
Dr. Web Mobile Security Suite	Consente uno scan real time delle pagine internet visitate e delle comunicazioni email, sms, mms, infrarossi e blutooth e la possibilità di effettuare scansioni su richiesta dell'intero dispositivo; i files individuati come sospetti vengono messi in quarantena e conseguentemente eliminati. Prevede la possibilità di creare white-list e black-list delle numerazioni da cui si vuole o meno ricevere chiamate o messaggi. In caso di furto è possibile il controllo da remoto del dispositivo. ***Fonte: www.drweb.com***

Principali soluzioni di wiping

In relazione a quanto illustrato in precedenza, si evidenzia di seguito una breve sintesi delle soluzioni di wiping esistenti per le principali piattaforme tecnologiche. Si evidenzia altresì che in aggiunta a quanto di seguito riportato ci sono comunque diverse Apps commerciali con funzionalità di remote wiping in linea con i requisiti Privacy installabili sulle diverse piattaforme (ad esempio WaveSecure (McAfee), Symantec Mobile Management, ecc).

Nome prodotto	Descrizione
iPhone	Apple permette nativamente il remote wiping, oltre ad altre funzionlità (come ad esempio la comparsa di messaggi del tipo "questo cell è stato smarrito dal Sig. Mario Rossi, prego contattarlo al num xxxx") in due modalità: - attraverso l'interfaccia web del servizio MobileME (in corso di migrazione verso il servizio free iCloud) su cui si è precedentemente registrati e dove, previa autenticazione, si può trovare la funzionalità di remote wiping sotto "Account -> Find My iPhone -> Remote Wipe". - attraverso l'installazione, ovviamente su un iPhone diverso dal proprio che è stato appena perso o rubato, di una App, da poco rilasciata dalla Apple su App Store, chiamata Find My iPhone che permette, previa autenticazione con il proprio account MobileMe, di localizzare il proprio iPhone, attivare il blocco ed effettuare wiping di tutti i dati. La App può essere installata solo su iOS 3.1.3 o più recente versione ed è free.
BlackBerry	Ogni dispositivo sotto il controllo BlackBerry Enterprise Server (BES) può essere "wipped" remotamente attraverso il comando Erase Data and Disable Handheld che può essere eseguito da un IT administrator. Questo commando permette, cambiando il valore del relativo parametro da "false2 a "true", di resettare il dispositivo alla configurazione di default cancellando la policy IT configurata, le applicazioni di terze parti e tutti i dati dell'utente. Utenti individuali con BIS e non con BES possono installare l'applicazione commerciale Roblock che permette, attraverso SMS o interfaccia WEB, il tracking del dispositivo, il recupero dei contatti, tacts, il blocco del dispositivo e il wipe remoto di tutto il dispositivo e delle media card. Questa App è disponibile per BlackBerry OS 4.2 e successive.
Android OS	Gli utenti con dispositivi basati su piattaforma Android possono installare l'applicazione commerciale SMobile Anti-Theft for Android che, una volta installata sul dispositivo, permette, previa autenticazione, di usufruire di una interfaccia web con, tra le altre, le seguenti funzionalità: - wiping del dispositivo - visualizzazione della localizzazione del dispositivo, via GPS, su google maps - lock del dispositivo - backup del dispositivo Un'altra applicazione, più orientata all'ambito enterprise, da poco compatibile anche con piattaforma Android, è "Absolute Software's Computrace Mobile" che, oltre a funzionalità di wiping avanzato, consente una completa gestione (Asset Management) del dispositivo.

Windows Mobile	Gli utenti dei dispositivi su piattaforma WindowsMobile possono usufruire del servizio Microsoft (free) "www.windowsphone.com- My Phone" che mette a disposizione previa autenticazione con il proprio Windows Live ID, le seguenti funzionalità: - lock del dispositivo - wipe del dispositivo e di eventuali card - comparsa di un opportuno messaggio sullo schermo - ring del dispotivo - localizzazione del dispositivo via GPS Per gli utenti enterprise gli amministratiri IT possono usufruire delle funzionalità di wipe remoto abilitando ActiveSync policy su Microsoft Exchange Server che peremtte anche di configurare un wipe locale dopo un deegtrminato numero di login falliti. Se si vuole dare agli amministratori IT ulteriori funzionlità per amministrare i dispositive mobile a disposizione degli utenti aziendali, si può installare applicazioni tipo "Absolute Software's Computrace Mobile" , con diverse altre funzionalità.
Symbian	Gli utenti con dispositivi basati su piattaforma Symbian possono installare l'applicazione commerciale Mobilewee OTA (disponibile anche per le atre piattaforme) che, una volta installata sul dispositivo, permette, previa autenticazione, di usufruire di una interfaccia web al sito www.mobiwee.com con, tra le altre, le seguenti funzionalità: - wiping del dispositivo - lock del dispositivo - backup del dispositivo

Principali soluzioni di encryption

In relazione a quanto illustrato in precedenza, si evidenzia di seguito una breve sintesi delle soluzioni di encryption esistenti per le principali piattaforme tecnologiche.

Nome prodotto	Descrizione
iPhone	I dispositivi mobile della Apple consentono nativamente un doppio livello di encryption. Tutti I dati presenti sul dispositivo vengono criptati mediante il sistema di encryption hardware accelerated AES-256. Pur trattandosi di un algoritmo robusto, il modo con cui esse è implementato (tutte le app in esecuzione sul dispositivo ricevono in chiaro i dati a seguito di una richiesta al SO) fa sì che il dispositivo possa risultare vulnerabile ad attacchi che prevedono l'accesso fisico al dispositivo (furto o smarrimento) pur non conoscendo la password utente (attacchi jailbreak). Un secondo livello di encryption, che non consente l'accesso ai dati se il dispositivo è bloccato con password, è disponibile di default solo per e-mail e allegati. In caso di presenza sul dispositivo di dati personali o sensibili oltre alle e-mail e allegati, si consiglia quindi di installare delle opportune Apps. Di seguito se ne riporta alcuni esempi. MEO, permette di cifrare, con algoritmo AES-256 o AES-512, molte tipologie di informazioni come testo, contatti, sms, photo ecc.. Per le diverse tipologie di informazioni è presente un form predefinito per il data input e il recupero della informazione stessa. A livello Enterprise si segnala la presenza sul mercato di diversi vendor (McAfee con Digital Trust, Symantec con Guardian Edge, ecc.) che offrono soluzioni che consentono l'attivazione di meccanismi di cifratura data-at-rest sicuri e configurabili, per qualsiasi tipo di informazione presente sul dispositivo, in linea con le politiche di sicurezza aziendali.
BlackBerry	I dispositivi Blackberry dispongono nativamente della funzionalità content-protection che, se abilitata, usa un algoritmo 256-bit AES per cifrare tutti i dati presenti su di esso. La lettura in chiaro delle informazioni sarà possibile solo inserendo la corretta password che permette di decifrare la chiave con cui sono cifrati i dati. La robustezza del meccanismo di autenticazione è la stessa sia che l'input dei dati avvenga con il dispositivo bloccato da password (si pensi alla ricezione di una mail e allegato) sia che il dato arrivi in input con dispositivo bloccato. Questo schema previene la possibilità, in caso di furto o smarrimento, di acquisire le informazioni in esso contenute (testo in input da tastiera o qualsiasi altra informazione come calendar, address book, mask, email e allegati e anche la cache del browser).
Android OS	I dispositivi basati su piattaforma Android (dalla versione 3 in poi) dispongono di un sistema di encryption hardware accelerated AES-256, ma al momento non ci sono informazioni dettagliate e consolidate sulla robustezza del metodo con cui è stato implementato. Le versioni di Android precedenti, invece, non hanno un sistema di encryption di default. Si consiglia l'uso di una applicazione che implenti un adeguato livello di encryption per eventuali dati personali e sensibili. Di seguito un esempio di applicazioni, una indicata per utilizzo personale e altre enterprise. Un esempio di applicazioni ad uso personale è Secret Safe che permette di cifrare molte tipologie di informazioni come testi, contatti, sms, photo ecc.. Tutte le informazione sono cifrate da una stessa master password. A livello Enterprise si segnala la presenza sul mercato di diversi vendor (McAfee con Digital Trust, Symantec con Guardian Edge, ecc.) che offrono soluzioni che consentono l'attivazione di meccanismi di cifratura data-at-rest sicuri e configurabili, per qualsiasi tipo di informazione presente sul dispositivo, in linea con le politiche di sicurezza aziendali.

Windows Mobile	I dispositivi su piattaforma WindowsMobile, dalla versione 6, mettono a disposizione delle API native per la crittografia mediante algoritmo 128 AES, ma tali funzionalità possono risultare poco robuste per alcuni tipologie di attacchi di tipo jailbreak. Anche in questo caso quindi è consigliabile l'uso di applicazioni con funzionalità di encryption più robuste. Ci sono diverse applicazioni, indicate per uso sia aziendale sia personale, che possono essere utili a tale scopo. Solo come esempio viene indicata l'applicazione Secubox che, mediante l'algoritmo 256 AES, crea una serie di aree nella memoria del dispositivo e di eventuali memory card. A livello Enterprise, si segnala la presenza sul mercato di diversi vendor (McAfee con Digital Trust, Symantec con Guardian Edge, ecc.) che offrono soluzioni che consentono l'attivazione di meccanismi di cifratura data-at-rest sicuri e configurabili, per qualsiasi tipo di informazione presente sul dispositivo, in linea con le politiche di sicurezza aziendali.
Symbian	I dispositivi basati su piattaforma Symbian mettono a disposizione API per funzionalità di cifratura, ma non dispongono generalmente di funzionalità attive per la protezione dei dati. Si consiglia pertanto l'uso di una applicazione, che magari utilizzi le API nativamente disponibili, che fornisca funzionalità di cifratura per eventuali dati personali e sensibili. Di seguito un esempio di alcune applicazioni. Touch Crypto è un valido tool di cifratura che usa l'algoritmo 128 AES per proteggere ogni tipo di file confidenziale presente sul dispositivo. Se non si possiede la password è impossibile accedere ai file cifrati. L'indicizzazione dei file cifrati consente una gestione centralizzata per il recupero di tali file e garantisce buoni livelli di performance. A livello Enterprise si segnala la presenza sul mercato di diversi vendor (McAfee con Digital Trust, Symantec con Guardian Edge, ecc.) che offrono soluzioni che consentono l'attivazione di meccanismi di cifratura data-at-rest sicuri e configurabili, per qualsiasi tipo di informazione presente sul dispositivo, in linea con le politiche di sicurezza aziendali.