ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

L'adozione dei mobile device e gli impatti sul sistema aziendale di gestione della sicurezza dei dati

Rodolfo Mecozzi (E&Y)

Roma 16/04/2013

Agenda

- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

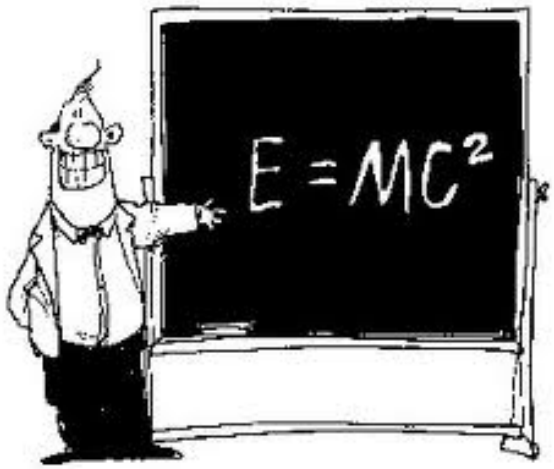
Agenda

- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

Presentazione relatore

Rodolfo Mecozzi

Esperienze nella consulenza aziendale per il governo dei sistemi informativi, la sicurezza delle informazioni, la gestione dei rischi IT ed il miglioramento delle performance dei processi IT.



Attualmente Senior Manager del gruppo IT Risk and Assurance di Ernst & Young e attivo nei seguenti ambiti:

- IT risk transformation
- IT assurance
- IT security
- Technology innovation

Agenda

- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

La diffusione dei device mobili

Entro il 2020, il 40% delle revenue ICT ed il 98% della sua crescita di industry sarà guidata dalle tecnologie che oggi rappresentano il 22% della spesa ICT, ovvero quelle della c.d. terza piattaforma: cloud, social, analytics e **mobile.**

Fonte: IDC Predictions 2013: Competing on the 3rd Platform

La diffusione dei device mobili

Mobile Devices

Più di 7B di Smartphone nel 2014

Entro il 2014, il numero dei dispositivi mobili presenti in tutto il mondo supererà la popolazione mondiale con un tasso di penetrazione del 96% a livello globale, entro la fine dell'anno

- International Telecommunication Union

Mobile Web Traffic

119% Crescita nel Traffico mobile

Il traffico dati su mobile effettuato tramite smartphone crescerà di 50 volte tra il 2011 ed il 2016, con un tasso di crescita annuale a pari al 119%

- Pew Research Center

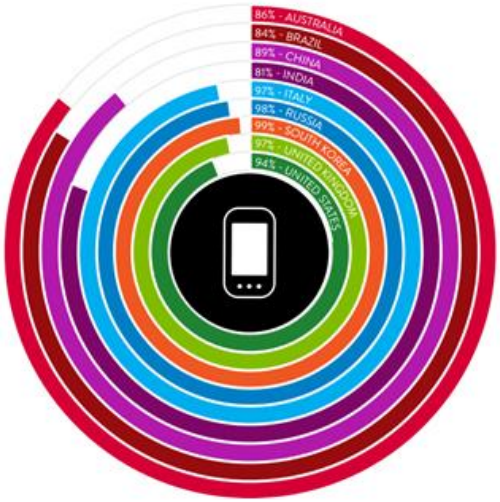
Mobile App Projects

4:1 Rapporto App Mobile/PC

Entro il 2015, i progetti di sviluppo di App mobile raggiungeranno un numero pari a quattro volte rispetto ai progetti software per PC

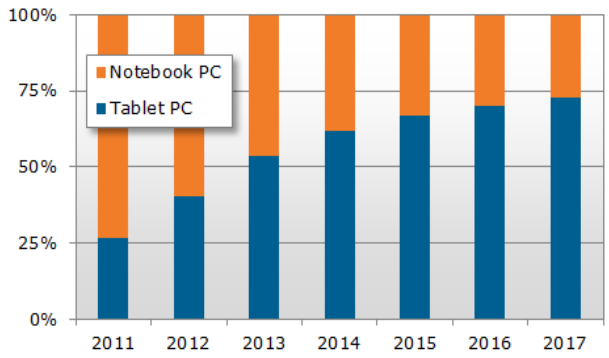
- Gartner

La diffusione dei device mobili



Nielsen

L'indagine Nielsen presentata al Mobile World Congress 2013 (The Mobile Consumer – A Global snapshot) mostra le altissime percentuali di penetrazione world-wide dei mobile device.
In Italia, il 97% degli italiani tra i 16 ed i 64 anni utilizza un device mobile.
La ricerca conferma il trend in costante aumento nell'utilizzo degli smartphone sia nella nostra vita quotidiana sia sul lavoro.



Npd DisplaySearch

Secondo le rilevazioni di DisplaySearch, i tablet supereranno quota 240 milioni di unità nel 2013 raggiungendo una sostanziale parità rispetto ai computer mobili venduti a livello mondiale, con una domanda prevista in costante crescita per i prossimi anni.

La diffusione dei device mobili

The consumer driven Revolution

"The reuse of technology across the consumer and enterprise is the way forward. People will ask for what they buy with their own money at work"

Steve Ballmer

La diffusione dei device mobili

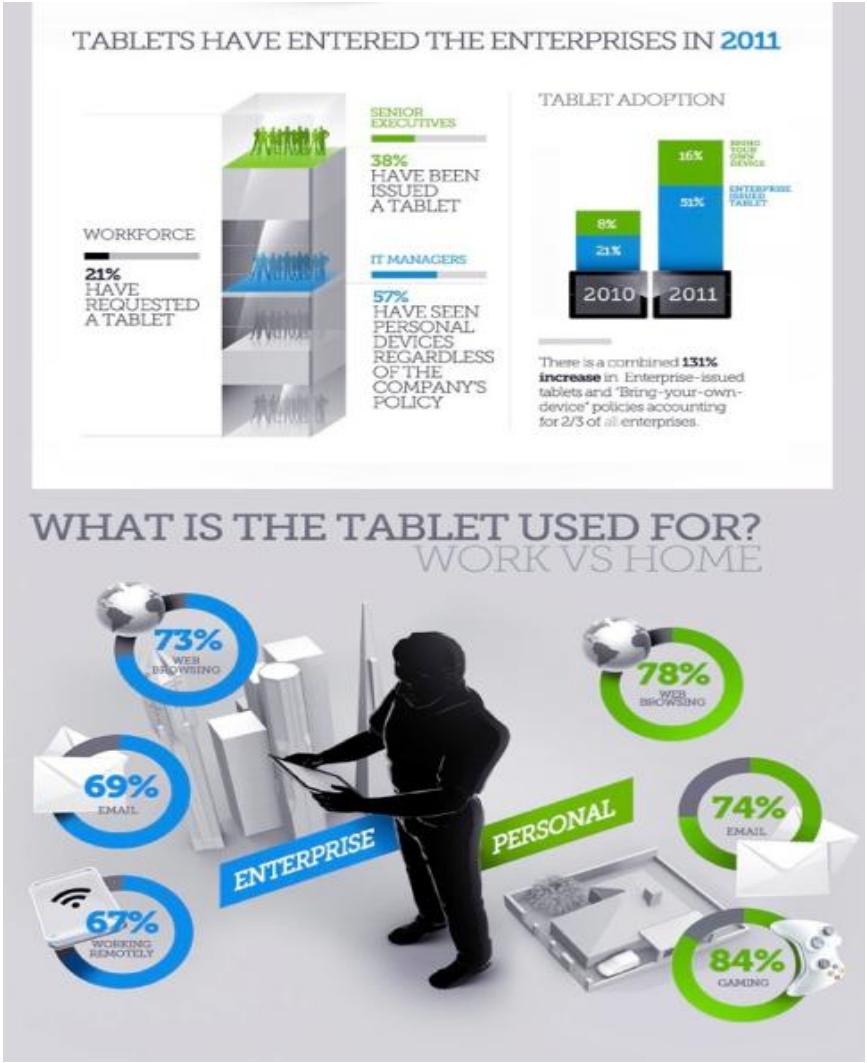
La diffusione di dispositivi mobili non ha precedenti. Apple ad esempio: nel solo Q1 del 2012, sono stati venduti 15 milioni di iPad (il numero totale di iPad venduti dopo due anni era di 67 milioni, lo stesso numero di Mac sarebbe stato venduto in 24 anni).

Alcune interessanti statistiche sui device mobili:

- nel 2012, più del 50% dei dispositivi è stato venduto senza una porta wired (Morgan Stanley Market Trends)
- entro il 2015 ci saranno 7,4 miliardi di dispositivi 802.11n nel mercato (ABIResearch)

Fonte: Vertic research, April 18, 2012

La diffusione dei device mobili



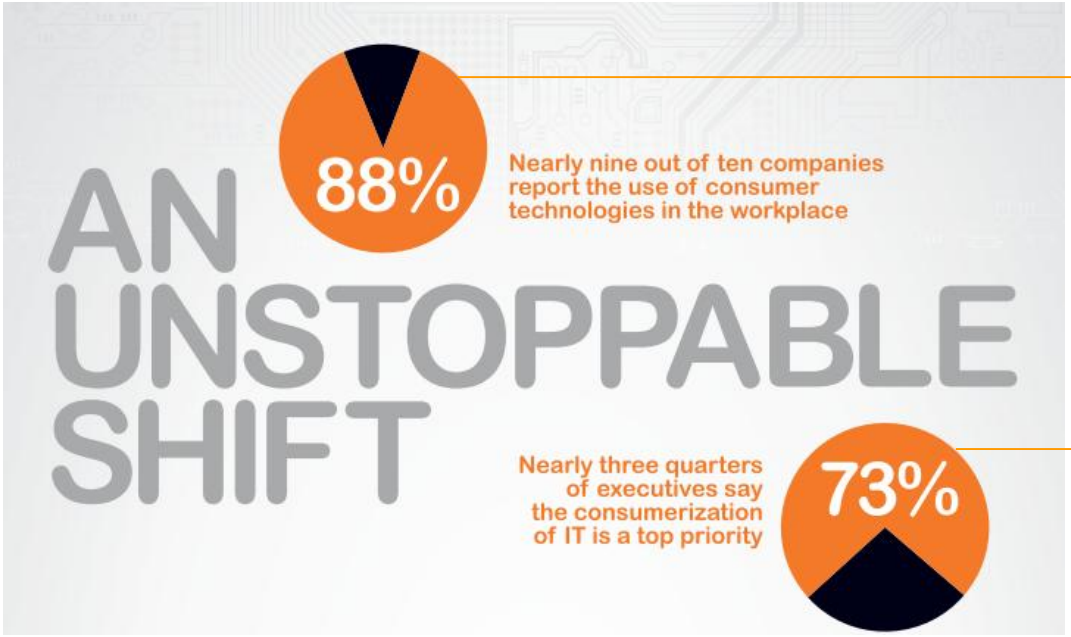
Secondo questa Infografica, la diffusione dei tablet in azienda giocherà un ruolo fondamentale nel business futuro.

- L'adozione dei tablet aziendali aumenterà del 50% ogni anno
- Le piattaforme iOS e Android saranno adattate per incontrare i bisogni delle aziende e i tablet Windows 8 sfonderanno nel mercato
- L'introduzione di tablet Quadcore, le tecnologie di quarta generazione 4G, il Cloud Computing e la continua adozione del HTML5 renderà i tablet ancora più integrati nell'ambiente di lavoro

Fonte: Vertic research, April 18, 2012

La diffusione dei device mobili

I dipendenti portano i propri smartphone e tablet al lavoro, usandoli anche per accedere alle applicazioni aziendali: **BYOD** ("bring your own device" cioè "porta il tuo device personale in azienda").



88% delle aziende **conferma l'utilizzo** da parte dei dipendenti di dispositivi personali

73% dei dirigenti afferma che la consumerizzazione IT è una **priorità attuale**

Fonte: ricerca commissionata da Avanade a Wakefield Research, Jan 2012 [600+ business and IT leaders in 17 countries]

La diffusione dei device mobili

Fonte: ricerca commissionata da Avanade a Wakefield Research, Jan 2012 [600+ business and IT leaders in 17 countries]

La ricerca ha evidenziato alcuni risultati che chiariscono alcuni concetti relativi alla consumerizzazione dell'IT

Le aziende si aprono al cambiamento che l'IT Consumerization impone

Le aziende investono in personale e risorse per agevolare l'IT Consumerization

L'uso delle tecnologie personali nel luogo di lavoro non costituisce uno strumento efficace di reclutamento o fidelizzazione

Le applicazioni aziendali, da CRM a ERP, iniziano a trovare spazio sui dispositivi personali

I dispositivi personali che entrano nel luogo di lavoro sono numerosi e diversi

Gran parte delle aziende ha già subito violazioni della sicurezza a causa dell'IT Consumerization

La diffusione dei device mobili

La consumerizzazione dell'IT è fenomeno in rapidissima ascesa.

Condizione necessaria all'evoluzione dei device mobili ed al loro utilizzo in ambito lavorativo è l'evoluzione della potenza elaborativa dei dispositivi stessi. Un esempio:

- CPU: TI ARM core 220 MHz
- RAM: 32 MB
- Internal Memory: 30 MB
- Display: 176x208 pixel, 262000 colours TFT
- GSM, GPRS, UMTS, Bluetooth v2.0
- Triband
- Fotocamera 2 MP

2005

Nokia N70

- CPU: Quad-core 1.4 GHz
- RAM: 1 GB
- Internal Memory: 8 GB ROM e microSD fino a 32 GB
- Display: 720 x 1280 pixel, 16M colours
- GSM, HSDPA, GPS, Wi-Fi 802.11 b/g/n, Bluetooth v3.0
- Quadband
- Fotocamera posteriore 8 MP con flash LED e anteriore 1.3 MP

2012

Huawei Ascend D quad

La diffusione dei device mobili

Due viste diverse dello stesso inarrestabile processo:

Vista dipendente:

- *Sempre più persone dispongono di device mobili personali e li portano con sé anche in ambito lavorativo.*
- *Alcuni top manager già utilizzano device mobili per scopi di business come "richiesta speciale".*
- *I mobile device portano innovazione e consentono di incrementare la flessibilità.*
- ***"Vorrei usare il mio device anche per lavoro"***

Vista azienda:

- *I mobile device sono stati progettati principalmente per il mercato consumer.*
- *Preoccupa la gestione dei device multipiattaforma, la sicurezza e la protezione dei dati.*
- *L'utilizzo di device personali impatta sulla compliance a requisiti normativi.*
- ***"Sono sufficientemente sicuri e affidabili per gestire informazioni aziendali?"***
- ***"Che impatto avranno queste soluzioni sui processi e che ritorno avrò dall'investimento?"***

La diffusione dei device mobili

Utenti/dipendenti appagati nella ***scelta del dispositivo*** *come nella vita privata così in ambito lavorativo*

Vista dipendente:

- *Sempre più persone dispongono di device mobili personali e li portano con sè anche in ambito lavorativo.*
- *Alcuni top manager già utilizzano device mobili per scopi di business come "richiesta speciale".*
- *I mobile device portano innovazione e consentono di incrementare la flessibilità.*
- ***"Vorrei usare il mio device anche per lavoro"***

Utenti/dipendenti più ***flessibili e produttivi*** *avendo a disposizione il proprio dispositivo*

Utenti/dipendenti più ***responsabili*** *nell'utilizzo del dispositivo*

Possibile ***riduzione dei costi*** *di hardware e connettività*

La diffusione dei device mobili

Azienda preoccupata della ***sicurezza di un dispositivo consumer*** *sulla protezione dei dati aziendali*

Vista azienda:

- *I mobile device sono stati progettati principalmente per il mercato consumer.*
- *Preoccupa la gestione dei device multipiattaforma, la sicurezza e la protezione dei dati.*
- *L'utilizzo di device personali impatta sulla compliance a requisiti normativi.*
- ***"Sono sufficientemente sicuri e affidabili per gestire informazioni aziendali?"***
- ***"Che impatto avranno queste soluzioni sui processi e che ritorno avrò dall'investimento?"***

Azienda preoccupata degli impatti sulla ***compliance normativa*** *(posso controllare le configurazioni? posso limitare le funzionalità? posso segregare i dati aziendali da quelli personali?)*

Cosa fare se l'utente/dipendente ***perde il proprio dispositivo****?*

*Ma la consumerizzazione comporta un'****effettiva riduzione dei costi****?*

La diffusione dei device mobili

Different work styles are changing today's technologies at work
WindowsVideos
(http://www.youtube.com/watch?v=kMZL2RE3-S0&feature=player_embedded)

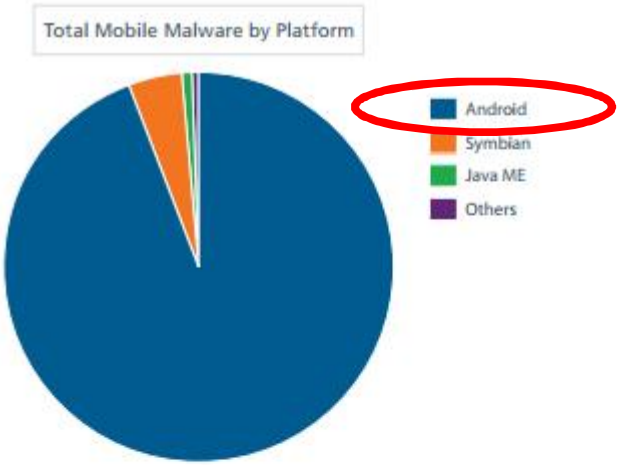
Agenda

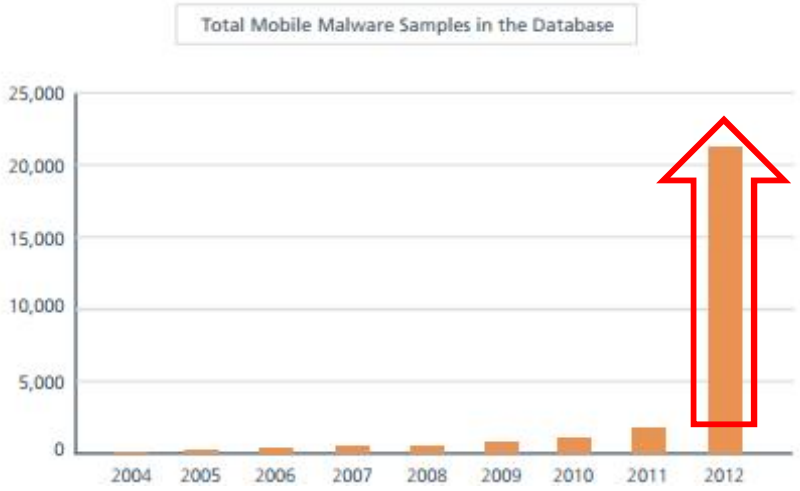
- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

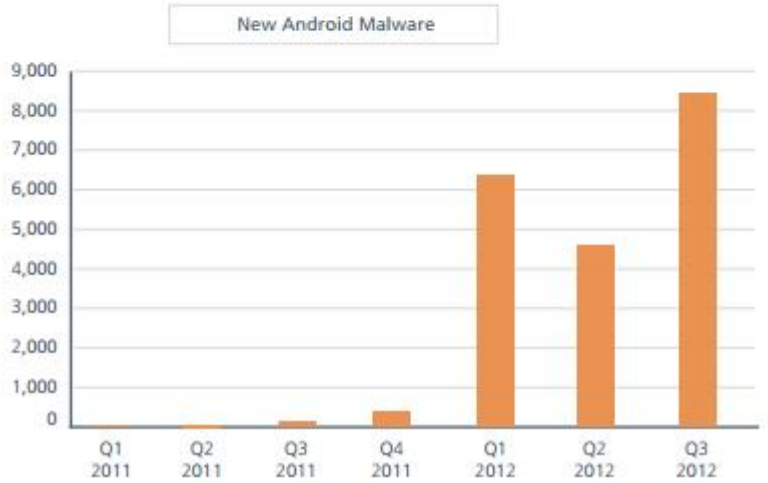
Minacce e vulnerabilità del mobile computing

Le analisi di McAfee dimostrano un marcato trend positivo nella rilevazione dei malware sul mobile in generale.

In particolare, Android dimostra essere la piattaforma mobile con i più rilevanti rischi di sicurezza.

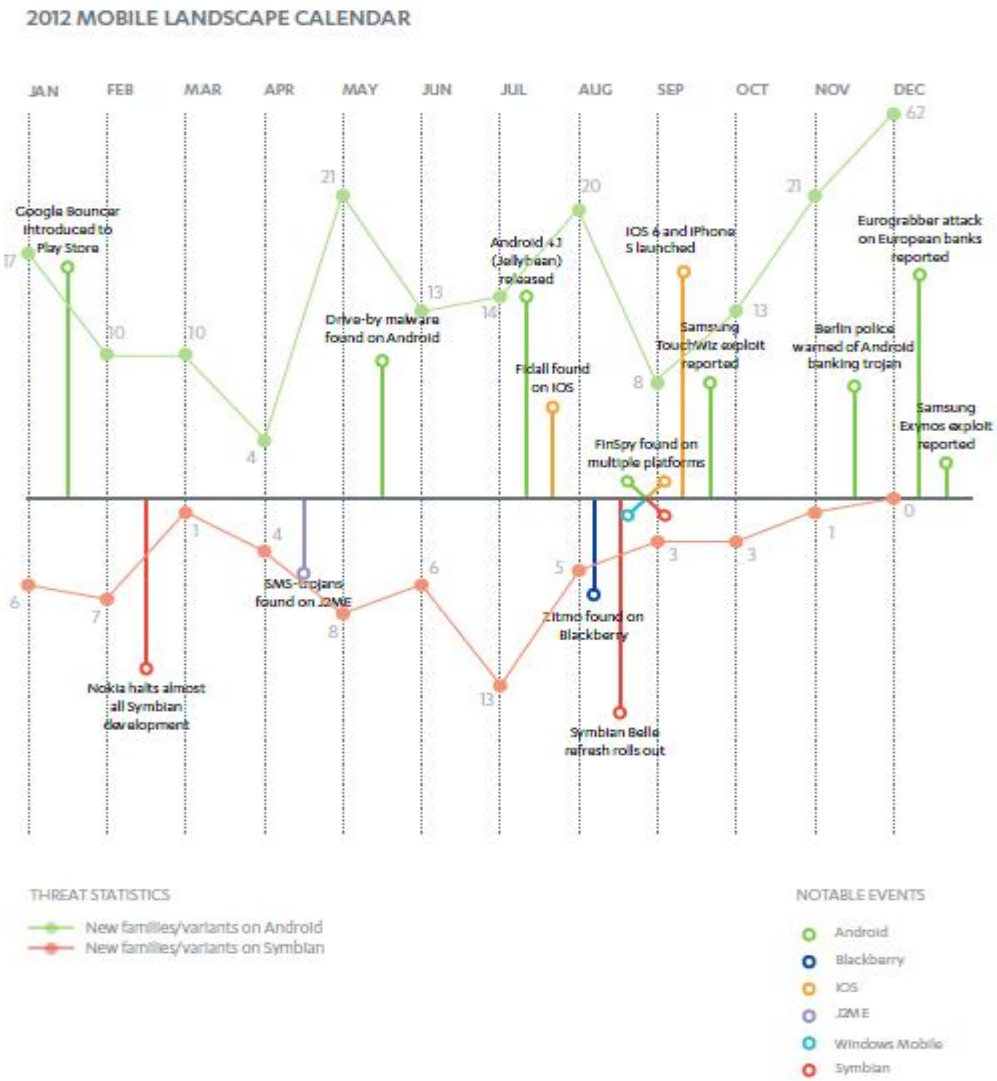




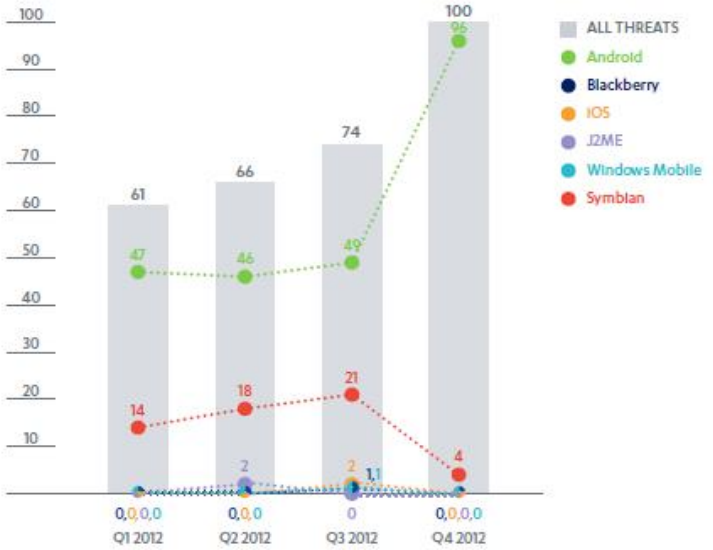


***Fonte**: McAfee Threats Report Third Quarter 2012*

Minacce e vulnerabilità del mobile computing



Anche le analisi di F-Secure confermano nel 2012 un trend delle minacce sul mobile che si è concentrato sulle piattaforme Android.

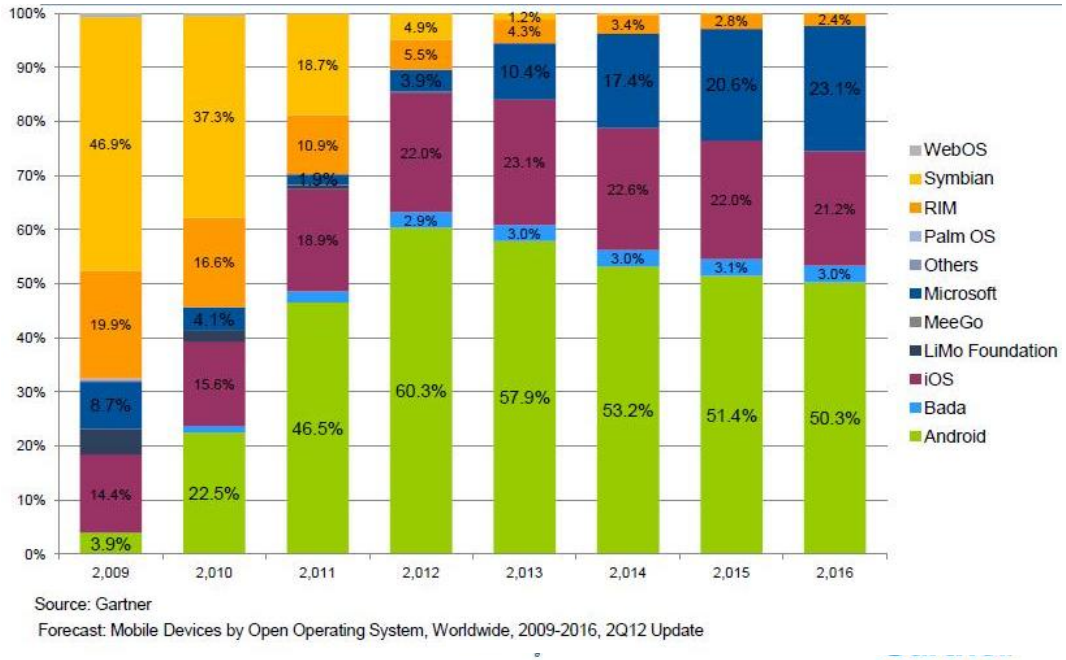


***Fonte**: F-Secure Mobile Threat Report Q4 2012*

Minacce e vulnerabilità del mobile computing

Il più diffuso sistema operativo per dispositivi mobili nel 2009 era Symbian ma nel giro di pochi anni si sono diffusi numerosi altri sistemi.

Secondo le previsioni di Gartner, nel 2016 Android si confermerà leader di mercato con una percentuale di device superiore al 50% di quelli esistenti.



Source: Gartner
Forecast: Mobile Devices by Open Operating System, Worldwide, 2009-2016, 2Q12 Update

Minacce e vulnerabilità del mobile computing

Tali analisi trovano nella matrice del Cybercrime Return on Investment (CROI) di Cisco una possibile spiegazione: uno degli ambiti del cybercrime più profittevoli risulta essere proprio quello dei mobile device.

The Cisco CROI Matrix predicts cybercrime techniques that will be "winners" and "losers" in 2012.

Minacce e vulnerabilità del mobile computing

Web and network based attacks	I siti web malevoli sfruttano il browser dell'utente attraverso logiche malevoli finalizzate all'installazione di malware o al furto di dati confidenziali dal dispositivo.
Malware	I malware per i dispositivi mobili non differiscono sostanzialmente da quelli per computer e possono essere categorizzzati nelle tradizionali categorie, ad esempio virus, worm e trojan horse
Social engineering attacks	Gli attacchi di social engineering come il phishing, sono finalizzati ad ingannare l'utente per il furto di informazioni sensibili o installazione di malware.
Resource and service availability abuse	Obiettivo di questo attacco sono le risorse di rete di un dispositivo. Lo spam email da dispositivo sotto attacco e attacchi di tipo DOS possono essere due minacce derivanti da questo attacco
Malicious data loss	La perdita di dati avviene quando un dipendente o un cracker preleva (involontariamente o meno) informazioni critiche da un dispositivo o network protetti.
Attack on device data integrity	In un attacco mirato all'integrità dei dati, il cracker tenta di accedere e corrompere i dati senza esserne autorizzato. Le finalità di questo attacco possono essere di solo disturbo all'operatività del proprietario dei dati o potenzialmente per un guadagno

Minacce e vulnerabilità del mobile computing

HolyColbert

Like the Comedy Central comedian, this Android attack dubbed HolyColbert, appears to have a sense of humor. Adding to the snarky sense of comedy is the tie-in date of May 21, 2011, the alleged "end of the world" perpetuated by some media sources. On this date, the malware began automatically replying to SMS messages sent to infected devices with the following text: "Cannot talk right now, the world is about to end." The malware then Trojaned a legitimate, if controversial, free application called the "Holy F***ing Bible," before randomly selecting one of several other similar anti-Christian messages and proceeding to text them to everyone on the victim's contact lists. Meanwhile, the malware also changed the devices' wallpaper, sent the user's e-mail and phone number to a remote website and contacted the command and control server every 33 minutes. The attack also subscribed users to a mailing list related to the Colbert Report. Officially known as the Android/smspacem.Altr, the attack targets mobile devices running Android 2.1 or greater.

(Image provided by Symantec)

Google moves to delete 'RuFraud' scam Android apps

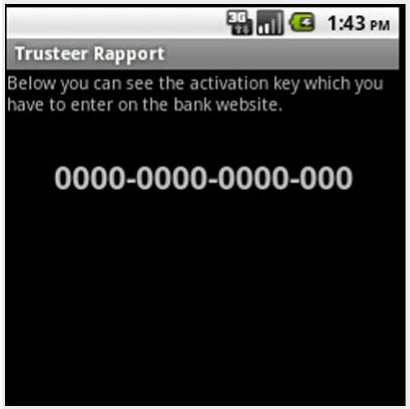
Google has removed 22 applications from its Android Market after they were discovered to contain fraudulent software.

Apps posing as popular third-party software such as Angry Birds tricked users into sending premium text messages.

Android Malware Quadruples Between 2011 And 2012

+ Comment Now + Follow Comments

Malware targeting Google's Android mobile platform has almost quadrupled between 2011 and 2012, according to Finnish security firm F-Secure.



Zitmo

The Android SMSSpy, or Zitmo, was found in a fake Android application appearing to be from Trusteer, a security firm which ironically does not have an Android security solution. Zitmo, an acronym for Zeus in the Mobile, has now been written to run on the Android system, expanding the platform past Windows Mobile, Symbian and Blackberry operating systems.

At its core, Zitmo operates as a man-in-the-middle attack by intercepting two-factor authentication that banks use to validate the identity of the account holder when entering login credentials, typically with a one-time password that is sent to a mobile device via SMS. During the attack, the malware essentially lifts SMS texts containing bank account passwords and other sensitive information sent to the user, which are then promptly funneled to a remote server. Even if a particular bank doesn't require two-factor authentication, Zitmo can forward and spy on all SMS messages, making it a valid threat.

(Image provided by Webroot)

Android.Lightdd and Android.Jsmshider

Android.Lightdd and Android.Jsmshider are two Android malware threats that open back doors on infected devices. The attacks are unique in that they borrow a staged downloader strategy from traditional PC malware in an attempt to complicate infection to the point where a user can't uninstall the malicious apps.

(Image provided by Symantec)

Nuovo malware per Android: invia messaggi a tutti i contatti! Attenzione

Tutti gli utenti Android che utilizzano una versione pirata, o applicazioni scaricate illegalmente, potrebbero essere colpiti da questo nuovo malware che cerca di umiliare gli utenti, inviando SMS a tutti i contatti in rubrica. Il malware si chiama Android.Walkinwat, ed è stato segnalato per primo da Symantec. Il malware potrebbe essere preso solamente attraverso mezzi

Minacce e vulnerabilità del mobile computing

Il malware **DroidDream** ha colpito alcune applicazioni presenti sul Google Android marketplace, trasformando le stesse App in "portatrici" del virus.
Il malware, una volta sul dispositivo, era in grado di eseguire codice come amministratore nel sistema operativo Android.
Nel peggiore dei casi il malware avrebbe potuto anche arrivare ad impossessarsi delle funzionalità che amministrano gli SMS (LINK), creando una sorta di invio continuo di messaggi con un relativo danno economico non indifferente per il proprietario dello smartphone.
Google, rimosse le App dal marketplace, ha eseguito una rimozione del virus da remoto.

Zitmo (Zeus-in-the-Mobile) e **SpitMo** (SpyEye-in-the-Mobile) sono software malevoli progettati appositamente per rubare i Mobile Transaction Authentication Number (mTAN). Sono multipiattaforma e sottraggono codici mTAN senza che l'utente se ne accorga, andando a pescare direttamente gli SMS, reindirizzandoli ai loro numeri di comando e controllo per approfittare dei dati che si possono trovare nel loro contenuto.

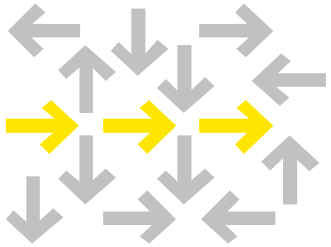
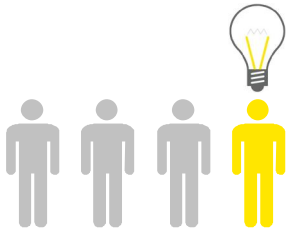
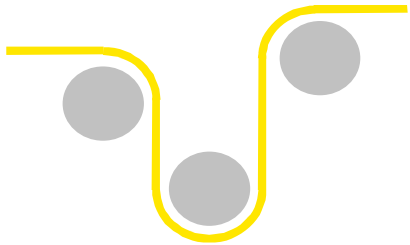
Presi da soli, ZitMo o SpitMo sono spyware ordinari, in grado di provvedere all'inoltro di messaggi SMS. Tuttavia, il loro utilizzo in coppia con i programmi ZeuS o SpyEye (Trojan che usa sistemi di keylogger e compilazione di form) consente di poter superare la linea di difesa rappresentata dall'utilizzo del codice segreto mTAN nell'effettuazione delle transazioni bancarie in quanto gli SMS possono essere usati dai cybercriminali per confermare le operazioni finanziarie eseguite tramite i conti bancari violati.

Agenda

- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

Gli ambiti di applicazione del mobile computing

I possibili modelli di applicazione della **disruptive technology** rappresentata dal mobile computing

Interno		Esterno
Migliorare produttività	**Abilitare dipendenti**	**Creare nuovi business**
Migliorare la produttività dei dipendenti esterndendo l'utilizzo delle applicazioni esistenti (es: mobile timesheet)	Abilitare i dipendenti tramite nuovi o evoluti processi interni di business (es: mobile field support, mobile CRM)	Individuare nuovi mercati, nuovi prodotti /servizi o nuove strategie di offerta (es: mobile commerce app)
		
Trasformare l'infrastruttura tecnologica tramite l'evoluzione della delivery	Fornire ai dipendenti i migliori tool al creare un nuovo impulso alla produttività	Sviluppare un nuovo servizio o proporre un servizio esistente con nuove modalità

Gli ambiti di applicazione del mobile computing

Gli ambiti di applicazione (interni ed esterni) dal punto di vista aziendale

"Interno" sui processi aziendali
(device usato dal personale aziendale)

- *Efficientamento dei processi interni attraverso l'automazione e la dematerializzazione*
- *"Prolungamento" dei sistemi informativi all'esterno sul territorio: (forza vendita, squadre operative / manutenzione)*
- *Dati e informazioni disponibili con modalità "always-on" e "anywhere"*
- *Sfruttamento delle feature di geolocalizzazione per servizi e informazioni a valore aggiunto*

"Esterno"
(device usato – anche – dai clienti)

- *Interazione con i clienti mirata, fino a livello "one-to-one"*
- *Canale di comunicazione di tipo "rich contents" (es. video)*
- *Nuovi canali di advertising*
- *Acquisizione di dati sui comportamentali dei clienti*
- *Self-caring del cliente direttamente integrato con CRM (modifica anagrafica, variazioni contratto, comunicazione consumi, apertura segnalazione guasti)*

Gli ambiti di applicazione del mobile computing

Ambito di applicazione interna

Processo di vendita

- Visite degli agenti più efficienti (anche tramite servizi di geolocalizzazione)
- Visite più focalizzate sugli aspetti maggiormente rilevanti (nuovi prodotti, nuova campagna pubblicitaria, nuove opportunità, promozioni o sconti)

- Possibilità per il cliente di monitorare la disponibilità dei prodotti
- Possibilità per il cliente e per il venditore di selezionare il miglior prodotto anche con simulazione on-line
- Possibilità per il cliente e per il venditore di selezionare offerte e scontistiche personalizzate in real-time

Gli ambiti di applicazione del mobile computing

Ambito di applicazione interna

Processo di vendita

Le Direzioni Commerciali che gestiscono forze vendita distribuite sul territorio possono giovarsi della flessibilità garantita da tablet e smartphone

Diminuzione del lavoro di back office ed aumento delle performance del personale chiave

Riduzione dei tempi operativi per la distribuzione delle informazioni e per la presa d'ordine

Miglioramento dell'efficacia nella presentazione dei prodotti (trasferimento dei cataloghi dalla carta al supporto elettronico)

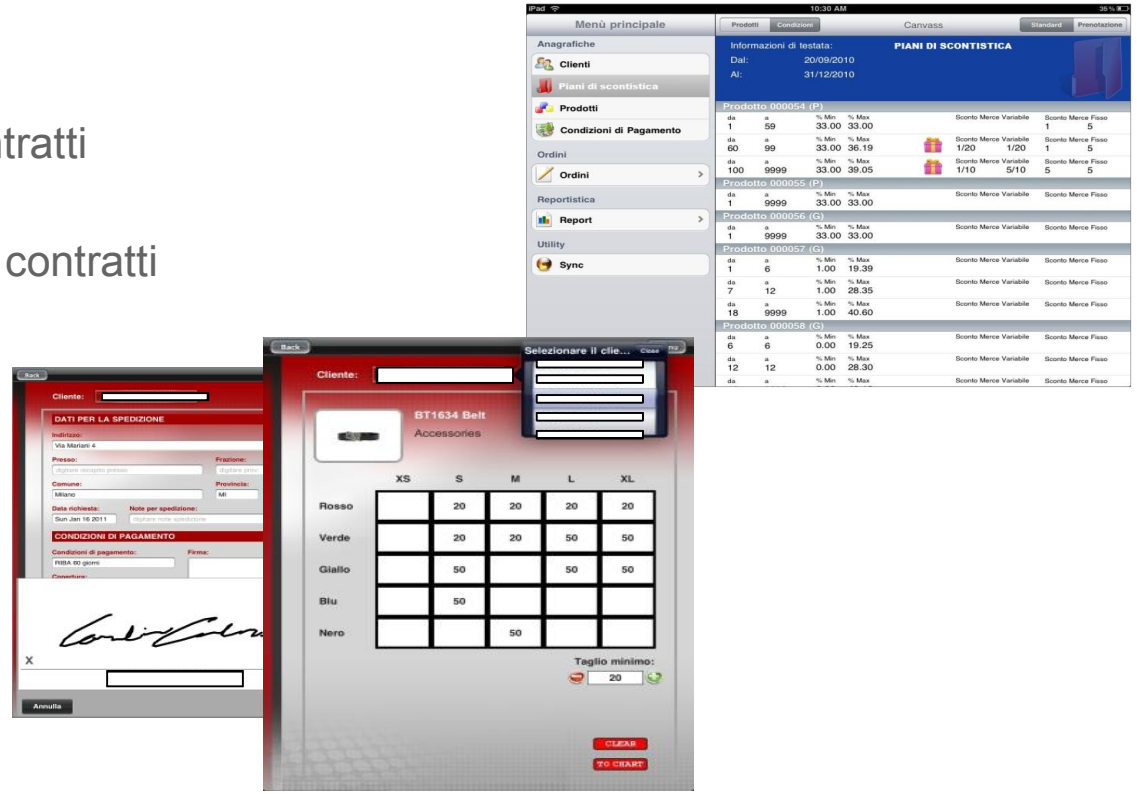
Miglioramento dei flussi informativi (comunicazioni bidirezionali, dati centralizzati e dispositivi on field always on)

Gli ambiti di applicazione del mobile computing

Ambito di applicazione interna

Order management

- Raccolta ordini in elettronico e integrazione con l'order management
- Firma elettronica dei contratti
- Archiviazione digitale dei contratti



Gli ambiti di applicazione del mobile computing

Ambito di applicazione interna

Comunicazione interna

- Forme di apprendimento anywhere - anytime (ubiquitous learning)
- Incentivazione di collaborazioni informali e responsabilizzazione nella costruzione sociale di conoscenza (attivazioni di network)

- L'adozione di una strategia di Unified Communications & Collaboration (UCC)
- Miglioramento dei flussi informativi grazie all'accesso alle informazioni everywhere anytime grazie all'utilizzo di connessioni wireless in mobilità
  - *Riduzione della "latenza" (tempi morti, assenza di risposta) a causa della comunicazione frammentata*
  - *Accesso alla documentazione online (mobile storage)*

Gli ambiti di applicazione del mobile computing

Ambito di applicazione esterna

Campagne pubblicitarie

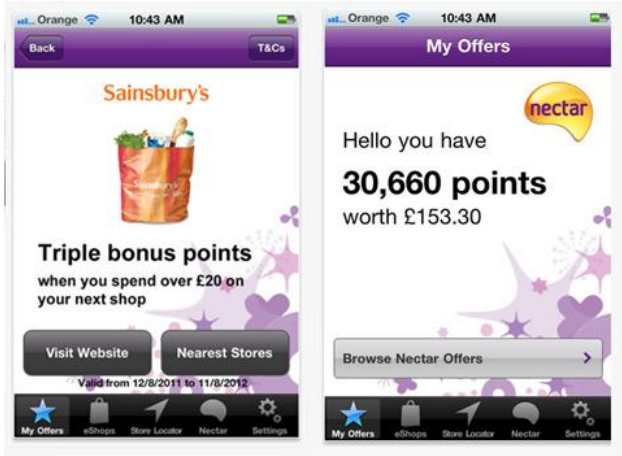
- Comunicazione mirata ai clienti, differenziata per segmento cliente (es. su base età), potenzialmente one-to-one
- Canale di comunicazione “always-on” (in logica push)
- Campagne mirate e targettizzate (potenzialmente one-to-one)
- Rich content communication (video di spiegazione, tool di simulazione, avatar per spiegazioni, etc.)

- *Miglior efficacia dell’advertising*
- *Immediatezza, certezza redemption campagne digitali e identificazione certa dei clienti che hanno aderito*
- *Maggiore efficacia per link diretto e immediato tra pubblicità e ritorno del cliente per aderire all’offerta*

Gli ambiti di applicazione del mobile computing

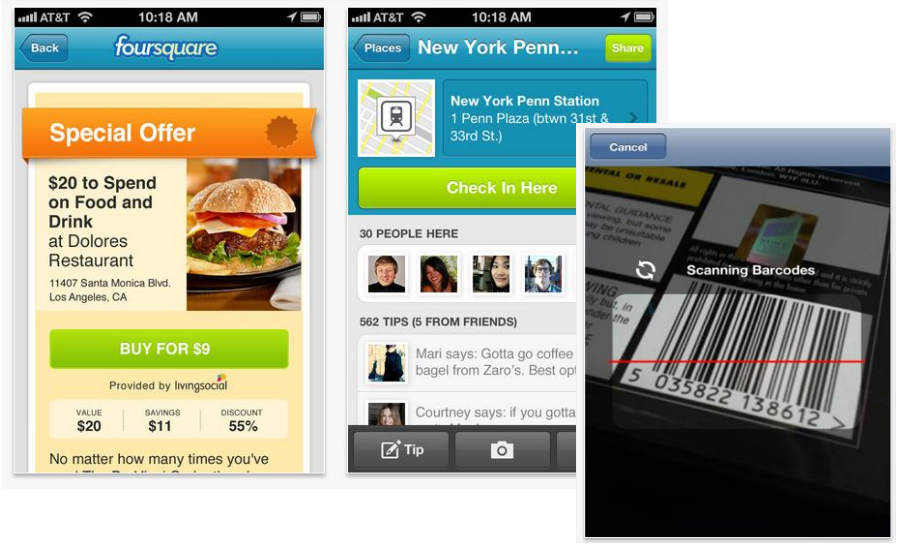
Ambito di applicazione esterna

Proximity marketing e Loyalty



- Segnalazione di servizi, prodotti e promozioni in una determinata area
- Buy/Visit stores and gain points
- QR Code scan per sbloccare contenuti in-app

- Online ed in-store client experience
- Loyalty building
- Offerte con target specifico (“remind me if there is an offer on that product)

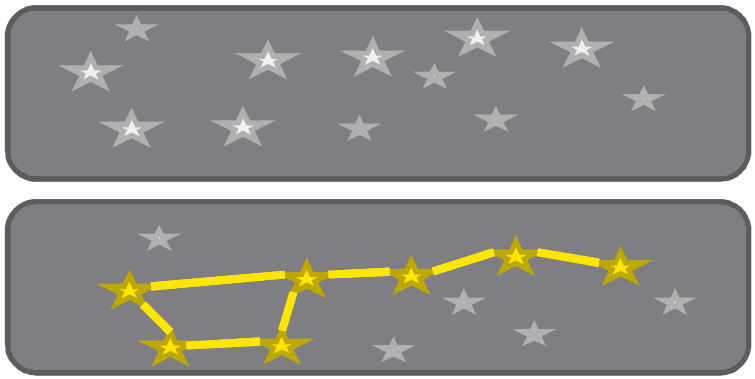


Gli ambiti di applicazione del mobile computing

Ambito di applicazione esterna

Realtà aumentata

- Diffusione di campagne di comunicazione che sfruttino applicazioni in augmented reality, per accrescere l'interattività dell'esperienza, aumentare la fidelizzazione del cliente o acquisire clienti nuovi



Gli ambiti di applicazione del mobile computing

Automotive

- (Vendite) Applicazione che permette alla forza vendita, passando di fianco ad ogni auto nei concessionari, di ricevere le informazioni necessarie sul modello in vendita
- (Customer Service) Applicazione utilizzata presso le officine per gestire l'anagrafica clienti al momento della consegna dell'auto da lasciare in riparazione.

- Applicazione che permette di visionare cataloghi, prodotti, e inserire ordini

Fashion and luxury

Real Estate

- Applicazione che permette di identificare le case in vendita nella zona limitrofa tramite geolocalizzazione, definire il percorso di visite ottimale da seguire, memorizzare fotografie delle abitazioni visitate e inviarle al cliente

- Applicazione che si interfaccia con sensori posti sull'impianto casalingo e permette di verificare l'andamento dei propri consumi di energia
- Applicazione per la field force che permette di ottimizzare le attività di stacco clienti

Energy

Pharma

- Applicazione che contiene cataloghi e schede prodotti.
- Adozione dei tablet per le forze vendita e gli informatori scientifici

- Applicazione per mostrare la gamma prodotti, fornire un supporto nel processo di scelta delle promozioni migliori e inserire ordini.

Telco

Agenda

- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

Come gestire la diffusione dei device mobili

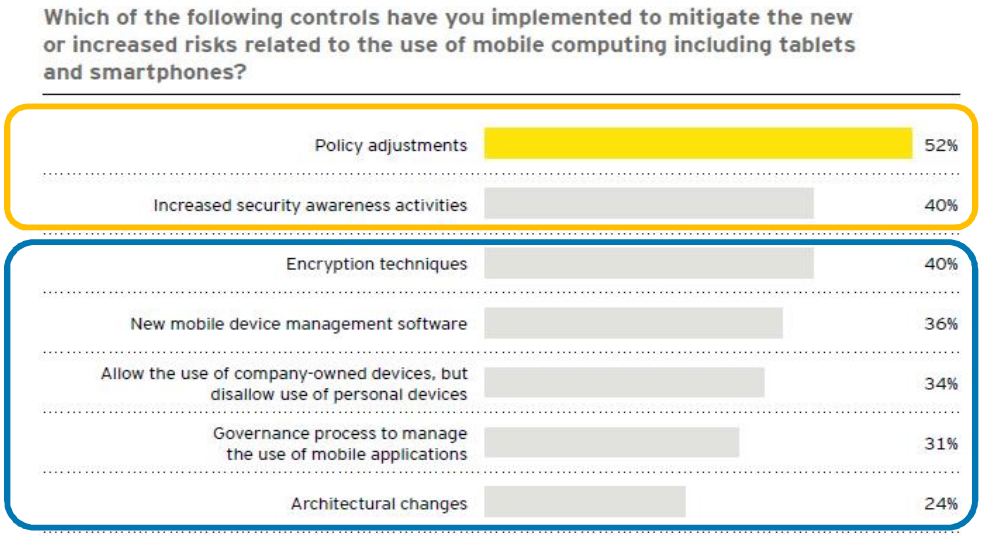
- Le soluzioni mobile rappresentano un'opportunità di innovarsi e la possibilità di **nuovi paradigmi** di servizio
- Offrono la prospettiva di processi più **flessibili** ed efficienti, una maggiore integrazione del personale, **risparmio** di costi per l'acquisto di hardware e connettività
- Migliore clima aziendale e **soddisfazione dei dipendenti**

- Coerenza e lungimiranza negli **investimenti** (adattamento della strategia, pianificazione e gestione del cambiamento, valutazioni ROI, etc.)
- Gestione dei device, **sicurezza** delle informazioni e **compliance** a normative

Necessario sviluppare una strategia mirata alla creazione e gestione di una vera e propria organizzazione mobile, minimizzando nel contempo i rischi legati alla sicurezza e all'impatto sull'infrastruttura aziendale.

Come gestire la diffusione dei device mobili

Come le aziende si stanno muovendo nella gestione del mobile computing?



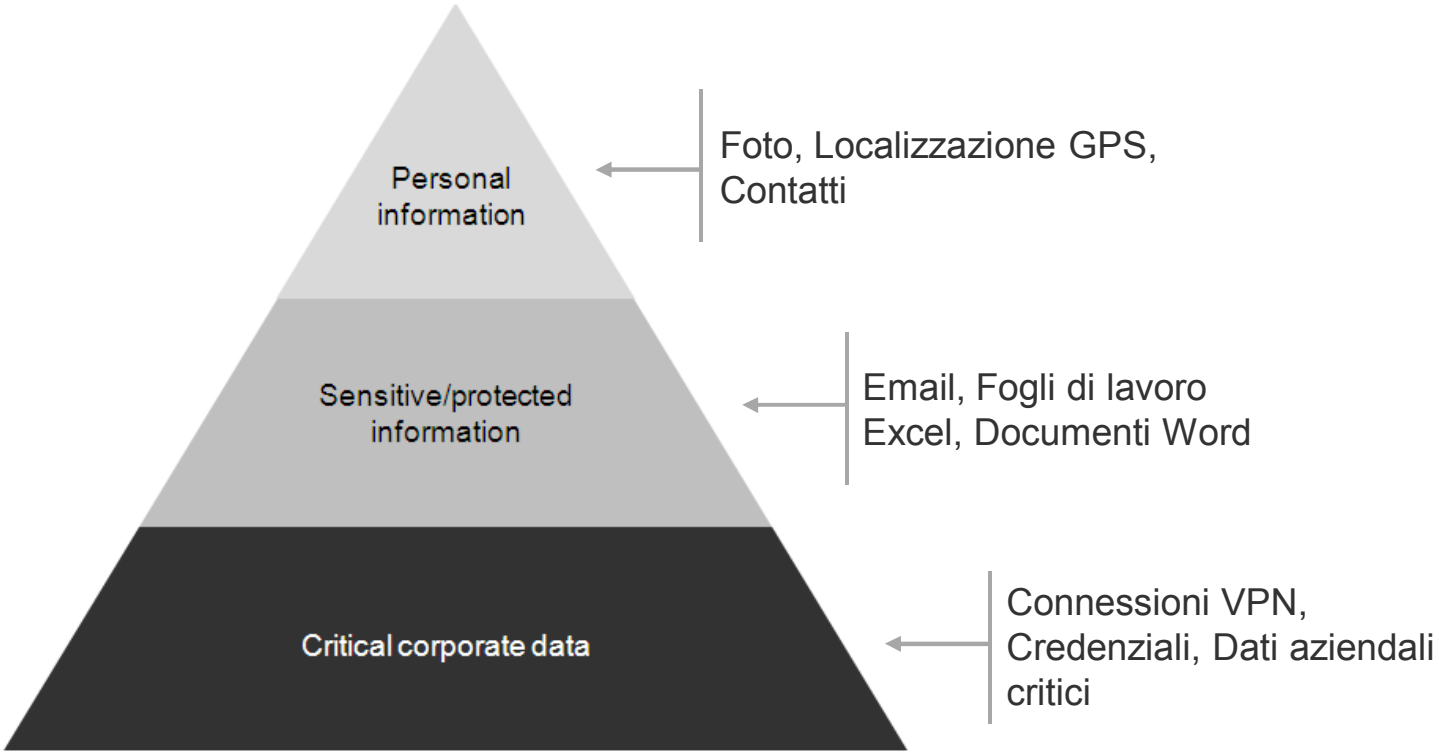
La maggior parte delle aziende intervistate ha iniziato ad affrontare la tematica dell'introduzione del Mobile Computing in azienda principalmente da un punto di vista organizzativo, aggiornando le policy ed effettuando attività di sensibilizzazione del personale

Altre soluzioni più tecnologiche relative alla cifratura, alle relative modifiche architetturali o all'adozione di soluzioni specifiche di Mobile Device Management sono adottate da un minore numero di società.

***Fonte**: Global Information Security Survey di Ernst & Young che raccoglie annualmente l'opinione dei responsabili IT e della Sicurezza Informatica di 52 diversi paesi*
Le prinicipali contromisure adottate dalle aziende che hanno implementato il paradigma del mobile computing

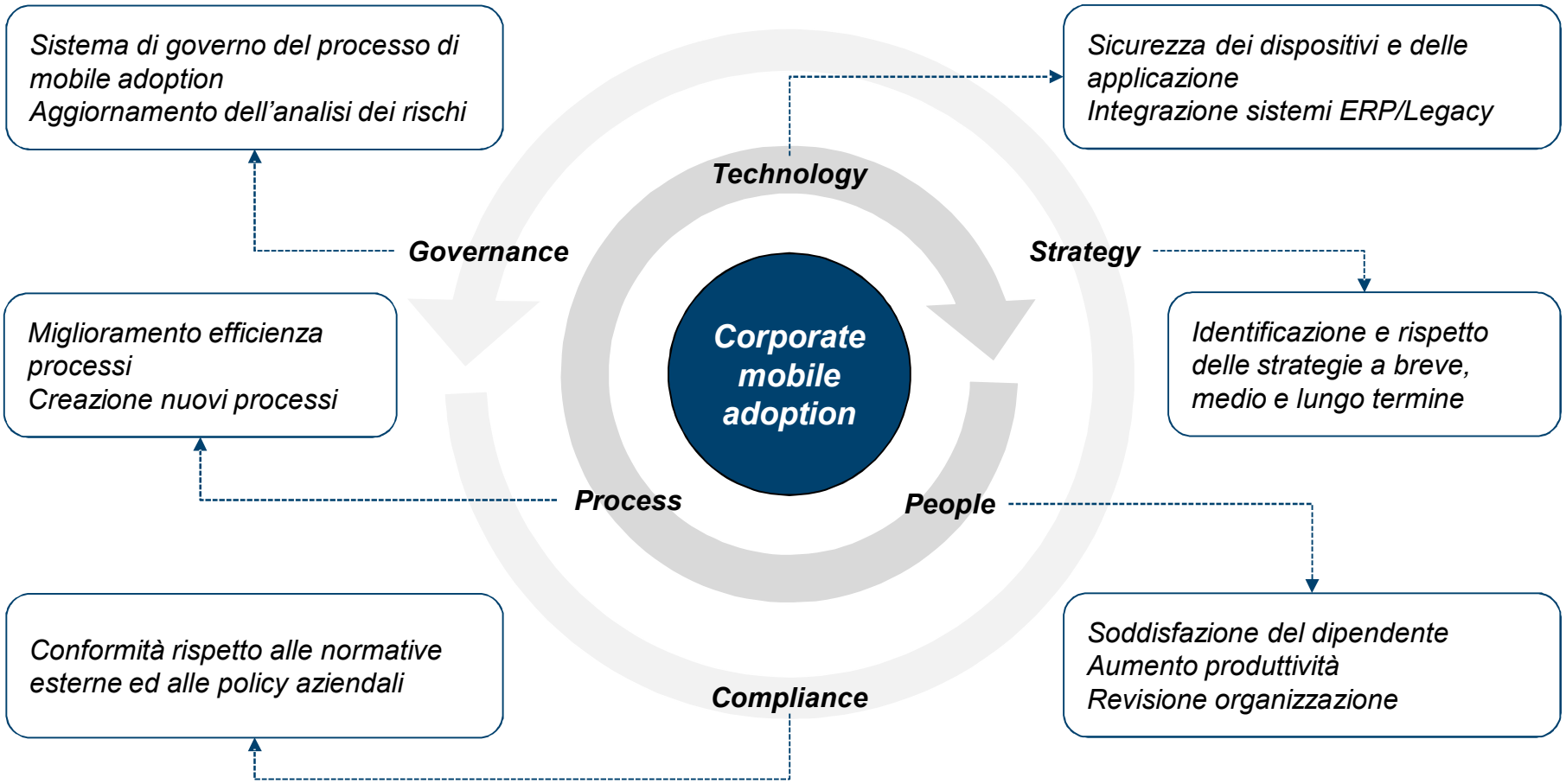
Come gestire la diffusione dei device mobili

Nel frattempo i mobile device stanno diventando una “miniera” di dati personali ed aziendali che potrebbero essere oggetto di attacco informatico…



Come gestire la diffusione dei device mobili

Le soluzioni che si vogliono realizzare devono considerare un approccio olistico che assicuri il rispetto degli obiettivi aziendali

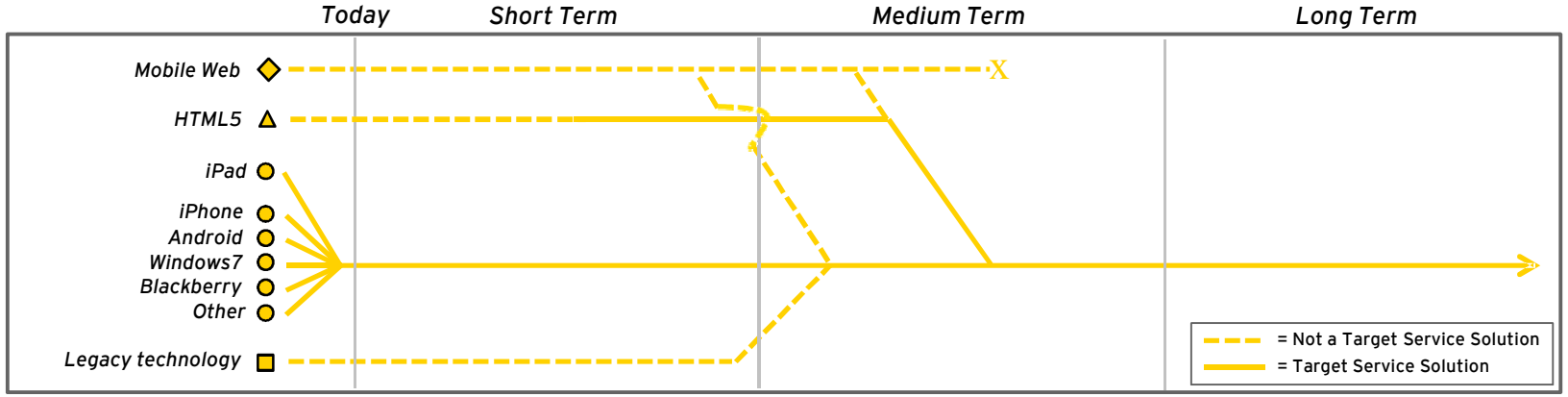


Come gestire la diffusione dei device mobili

La determinazione di una chiara **strategia** a supporto della mobile adoption aziendale si configura quale aspetto essenziale per la futura corretta implementazione di processi e tecnologie.

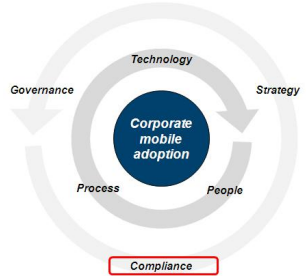
La strategia dovrà identificare un **business case sostenibile** al fine di valutare i potenziali benefici ottenibili da un progetto di mobile adoption e rendere
Esplicite le possibilità di raggiungimento degli obiettivi aziendali che possiamo riassumere nella sostenibilità del rapporto tra costi previsti (es: organizzativi e gestionali) e benefici attesi (es: soddisfazione e produttività dei dipendenti).

Un piano evolutivo delle tecnologie che si prevede di adottare/dismettere potrebbe facilitare le considerazioni a lungo termine da parte del management.



Come gestire la diffusione dei device mobili

L'adozione dei dispositivi mobili evoluti (smartphone e tablet) in ambito lavorativo comporta la necessità di assicurare il rispetto della **conformità** rispetto alle normative esterne ed alle policy aziendali.



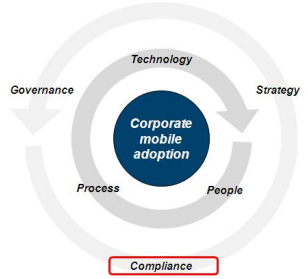
Con particolare riferimento al D.lgs.196/2003 (c.d. Codice Privacy), la Oracle Community for Security (**c4s.clusit.it**) ha realizzato uno studio finalizzato ad individuare gli adempimenti che le aziende italiane sono obbligate a rispettare, prima, durante e dopo l'esecuzione di trattamenti di dati personali dei clienti effettuati attraverso l'utilizzo dei dispositivi mobili.

Lo studio evidenzia come smartphone e tablet debbano essere introdotti in ambito aziendale solo a fronte di un'attenta **analisi dei rischi**, condotta anche in funzione dei tipi di trattamenti di dati che l'azienda abitualmente effettua.

Dallo studio emerge inoltre, come le criticità in termini di rischio possano essere correlate ad aspetti di **natura tecnologica** (come ad esempio l'eterogeneità delle caratteristiche tecnologiche dei dispositivi, la complessità del portafoglio aziendale degli asset, l'esistenza di vulnerabilità tecniche), ma anche ad elementi legati ad aspetti di **natura sociale** quali, ad esempio, comportamenti non idonei da parte delle personale aziendale.

Come gestire la diffusione dei device mobili

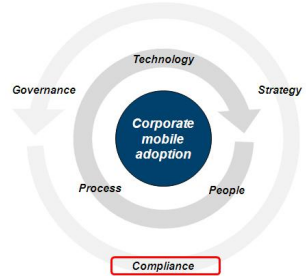
Le categorie di rischio individuate dal Gruppo di Lavoro specificatamente in relazione all'utilizzo dei device mobili in ambito lavorativo sono sotto riportate:



- **Rischi correlati ai comportamenti degli utilizzatori**, quali ad esempio
  - gestione impropria credenziali di accesso
  - gestione impropria dei servizi sul dispositivo
  - comunicazioni non sicure e disclosure di dati
- **Rischi correlati agli strumenti**, quali ad esempio derivanti da
  - virus informatici
  - attività di hacking e sniffing
  - danneggiamento dispositivi
- **Rischi correlati al contesto fisico-ambientale**, quali ad esempio
  - furto o smarrimento dei device mobili
  - indisponibilità delle infrastrutture centralizzate (ad esempio infrastruttura BES)
- **Rischi correlati a trattamenti non conformi a normative/policy aziendali**, quali ad esempio
  - acquisizione di dati di localizzazione senza opportuna informativa agli utenti
  - profilazione utente senza preventiva raccolta del consenso

Come gestire la diffusione dei device mobili

Lo studio sottolinea poi di porre particolare attenzione ad **alcune specifiche attività di trattamento**, relative a dati personali particolarmente critici, quali ad esempio, i trattamenti legati alla geolocalizzazione dei dispositivi che possono essere lecitamente realizzati solamente a fronte di un opportuno e preventivo adempimento degli aspetti legali di notificazione ed informativa/raccolta di consapevole consenso.



Ulteriori indicazioni evidenziate dal Gruppo di Lavoro sono relative alla necessità che hanno le aziende di rivedere le **misure di sicurezza prescritte dal Codice Privacy** e da specifici provvedimenti emessi dal Garante Privacy, in funzione del particolare contesto tecnologico caratterizzato dall'utilizzo dei dispositivi mobili in ambito lavorativo.

In particolare, le prescrizioni derivanti dal Codice Privacy e relative ad aspetti di sicurezza quali il controllo degli accessi logici, il salvataggio dei dati e l'adozione di soluzioni anti-malware, debbano essere opportunamente **analizzate alla luce delle caratteristiche dei dispositivi mobili** per poter essere completamente soddisfatte, mentre per quel che riguarda le prescrizioni derivanti da specifici provvedimenti emessi dal Garante Privacy, quali ad esempio quello relativo alla "**dismissione** RAEE" debbono essere previste idonee attività di cancellazione dei dati presenti in tutti gli elementi che caratterizzano tipicamente i dispositivi mobili (dalla memoria interna alla SD esterna).

Come gestire la diffusione dei device mobili

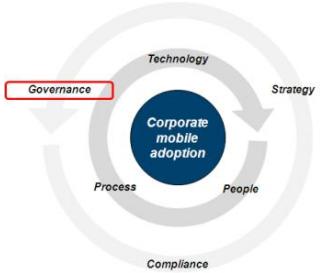
La realizzazione di un sistema di **governance del mobile** dovrà focalizzarsi sui seguenti aspetti (*):

- assicurare l'**allineamento strategico** tra le strategie tecnologiche mobili ed i piani strategici aziendali;
- monitoraggio dell'**erogazione operativa** dei servizi mobili in termini di produzione dei benefici attesi rispetto agli obiettivi strategici;
- individuazione delle **risorse** in termini di investimenti migliori, della protezione delle risorse ritenute maggiormente critiche;
- analisi dei **rischi** in termini di gestione delle minacce e delle vulnerabilità delle tecnologie mobili aggiornata nel tempo;
- misurazione della **performance** tramite un buon sistema di KPI che includano, in particolare, anche l'ambito della Internet Brand Reputation.

(*) *Sulla base delle aree dell'IT Governance definite dall'IT Governance Institute nello standard CobiT*

Come gestire la diffusione dei device mobili

Nell'ambito dell'identificazione e della gestione dei rischi e delle opportunità in ambito Mobile, ENISA (*) ha prodotto una serie di pubblicazioni al fine di identificare e razionalizzare una struttura comune di valutazione di rischio.



Risks	
R1	Data leakage
R2	Improper decommissioning
R3	Unintentional data disclosure
R4	Phishing
R5	Spyware
R6	Network spoofing attacks
R7	Surveillance
R8	Diallerware
R9	Financial malware
R10	Network congestion

Opportunities
Sandboxing and capabilities
Controlled software distribution
Remote application removal
Backup and recovery
Extra authentication options
Extra encryption options
Diversity

Usage scenarios
Consumer (C)
Employee (E)
High official (H)

Recommendations	
C	Automatic locking (it locks automatically after some minutes)
	Check reputation (for new apps or services)
	Scrutinize permission requests (for new apps or services)
	Reset and wipe (before disposing of or recycling their phone)
E	Decommissioning (memory wipe processes)
	App installation (app whitelist for sensitive corporate data sec)
	Confidentiality (memory encryption)
H	No local data (and non-caching app)
	Encryption software (additional call and SMS encryption sw)
	Periodic reload (smartphones may be periodically wiped)

(*) *L'ENISA è l'agenzia europea per la sicurezza delle reti e dell'informazione con lo scopo di garantire all'UE un elevato livello di sicurezza delle reti e dell'informazione*

Smartphones: Information security risks, opportunities and recommendations for users
December 2010

enisa European Network and Information Security Agency

ISACA Sistemi informativi: averne fiducia e trarne valore Rome Chapter

Come gestire la diffusione dei device mobili

Risks related to costs

RC1	Increased risk of loss of value when employees bring the organisation's brand into disrepute by uncontrolled use of consumerized services/devices
RC2	Increased variety and complexity of devices, systems and applications, all requiring management, will lead to increased costs
RC3	More use of mobile devices is likely to result in more lost devices and thus increased costs
RC4	Additional spending to ensure that security requirements do not act to either prevent appropriate consumerization or to encourage inappropriate use of consumer devices

Risks related to legal and regulatory issues

RLR1	Corporate governance and compliance control over employee-owned devices will be weaker
RLR2	Interoperation, usage models and change of security context between applications and systems will make enforcement of legal and regulatory compliance controls more difficult
RLR3	Lack of clear distinction between corporate and personal data on employee-owned devices will make e-discovery more difficult and may lead to litigation with employees

Risks related to data confidentiality/integrity/availability

RD1	Potential loss of corporate data as a result of unauthorized sharing of information on employee's devices and sharing of devices
RD2	Potential loss of corporate data as a result of access by unknown users and unmanaged devices to enterprise networks
RD3	Potential loss of corporate data as a result of difficulty of controlling security in application-rich mobile devices, especially if employee-owned
RD4	Increased risk of mobile devices being the target of attack for the acquisition of corporate data

Opportunities

O1	Potential financial opportunities
O2	Potential Human Resources benefits
O3	Potential Data Management opportunities
O4	Potential operational opportunities

	OPPORTUNITY				
RISK	O1	O2	O3	O4	COMMENT
RC1	X	(X)			
RC2	X				
RC3	X				
RC4	X				
RLR1	(X)		X	(X)	
RLR2	(X)		X	(X)	
RLR3		X	(X)		
RD1	(X)		X	X	
RD2	(X)	(X)	X	X	
RD3	(X)	(X)	X	X	
RD4	(X)	(X)	X	X	

Legend: X primarily counteraction of a risk; (X) secondary counteraction of risk

Consumerization of IT: Top Risks and Opportunities
Responding to the Evolving Threat Environment
[Deliverable – 2012-09-28]

enisa European Network and Information Security Agency

ISACA Sistemi informativi: averne fiducia e trarne valore Rome Chapter

Mobile device e sicurezza dei dati aziendali

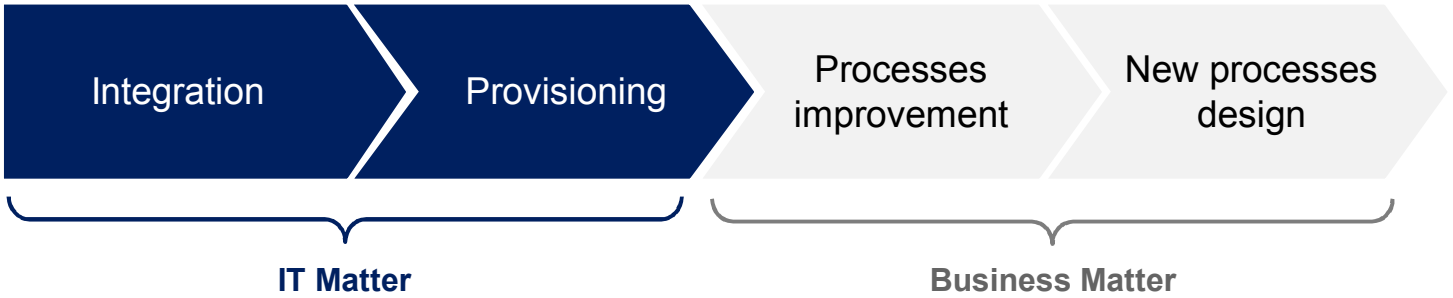
Come gestire la diffusione dei device mobili

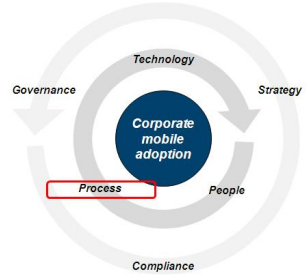
L'ambito degli **aspetti organizzativi e procedurali** ricopre un ruolo centrale in considerazione del concetto stesso di consumerizzazione.

- Sessioni di **formazione** verso gli utilizzatori dei dispositivi mobili evoluti e di chi ne gestisce l'infrastruttura correlata
- Integrazione dei **modelli organizzativi** preposti alla sicurezza dei dati e delle informazioni con eventuali ruoli dedicati al governo dei dispositivi e/o delle infrastrutture centralizzate correlate
- Adozione di **policy dedicate** all'utilizzo dei dispositivi e/o alla loro gestione (es: procedure di configurazione, comportamenti accettati aziendalmente)

Come gestire la diffusione dei device mobili

Solo una questione di sistemi informativi?





Nella realizzazione di un progetto per l'introduzione dei device mobili in azienda, devono essere individuati i **processi** che si vogliono supportare (processi core o servizi trasversali) ed analizzare tutti i possibili impatti.

Collaboration
- Gestione meeting a distanza con partecipazione interattiva e condivisione materiale multimediale
- Discussion forum & team working

Supply Chain
- Previsione della domanda per garantire la disponibilità prodotto al miglior prezzo tra store tradizionale e mobile

Esperienza di acquisto
- Modalità di acquisto, assistenza pre-vendita e post-vendita
- Estensione del programma di fidelizzazione

Order management
- Raccolta ordini in elettronico
- Firma digitale dei contratti
- Archiviazione elettronica dei contratti

Commercio On-Line
- Catalogo online dei prodotti
- Prezzo store tradizionale e online
- Tipo di promozioni, targeting su segmenti cliente specifici

Relazionale
- Segmentazione e profilazione clientela
- Gestione degli impatti delle piattaforme sociali

Come gestire la diffusione dei device mobili

Alcune misure tecniche di protezione…

Disable bluetooth connection
Disable wi-fi capabilities
Backup and Restore Management
Applicat Enabling PIN request
Patchin Automatic look-up
Filtering Enabling Protection Code
Istant m Network APP Black list
Secure Secure Multi-logon disabling
Disablin Secure SIM/IMEI authentication
Remote Secure Implement Infrareds management
Remote Reputati DB Strong No Memory Card
Remote Remote Different lo Filtering external wap-push (sms and web-link)
Restricti Strong a Data Encry Secure FOTA (firmware over the air) configuration
Restricti Sandbox GSM/UMT Configura Antivirus
Automa Firewall Data/Functi Centralize Antispam
Decomis Network Logging Warning j Antimalware
Impleme Endpoin SSL VPN A Explicity r Restrictive Profiling

… procediamo con ordine

Come gestire la diffusione dei device mobili

I **fattori critici nella scelta dell'infrastruttura** devono tenere in considerazione i meccanismi per la protezione dei dati sul dispositivo, la sicurezza dei sistemi centrali e le misure ai fini della compliance normativa.

Ove richiesto dalle specifiche esigenze di business, è necessario valutare la **presenza delle seguenti feature nei device** e nei sistemi di gestione dei dispositivi da adottare:

- *Presenza di una password di accesso "forte"*
- *Blocco dopo un periodo di inattività*
- *Separazione dei dati aziendali dai dati personali*
- *Remote Wipe (corporate content wipe o total wipe)*
- *Cifratura della memoria (interna ed esterna)*
- *Autenticazione tramite certificati*
- *Monitoraggio della manipolazioni dei dati sul dispositivo*
- *Firewall ed Antivirus*
- *VPN di accesso alle risorse aziendali*
- *Archiviazione e backup dei dati*

Come gestire la diffusione dei device mobili

Il mercato offre attualmente numerose soluzioni per il **Mobile Device Management**, in grado di consentire una interfaccia di accesso comune ai contenuti da parte di differenti device mobili.

Alcuni dei criteri che possono influenzare la **scelta della soluzione MDM** sono:

- *Dispositivi supportati (cellulari, smartphone, tablet)*
- *Piattaforme supportate (iOS, Android, Windows 7)*
- *Policy Enforcement*
- *Security e Compliance*
- *Separazione dei dati personali da quelli aziendali*
- *Gestione dell'inventory*
- *Rilascio di nuovo software e aggiornamenti*
- *Amministrazione e Reporting*
- *Gestione dei servizi di rete*

Come gestire la diffusione dei device mobili

Stesso discorso per il mercato delle soluzioni di **Mobile Application Management** per la gestione centralizzata di applicazioni interne, pubbliche ed acquistate, spesso integrate con i software di MDM.

Alcuni dei criteri che possono influenzare la **scelta della soluzione MAM** sono:

- *Creazione di un catalogo personalizzato delle App installabili*
- *Distribuzione in base alla profilazione o ai gruppi di appartenenza degli utenti*
- *Customizing della profilazione*
- *Integrazione con gli App store pubblici*
- *Limitazione delle applicazioni utilizzabili (su app già installate) tramite black list o white list*
- *Monitoring real-time dello stato del dispositivo (App inventory)*
- *Rilevazione istantanea delle installazioni non consentite*
- *Installazione delle applicazioni in modalità Push OTA (Over-The-Air)*
- *Politiche di versioning delle App*

Come gestire la diffusione dei device mobili

In definitiva:

Effettuare attività di Valutazione degli **Scenari di Business**, del **Ritorno sugli Investimenti** e sui Processi di Gestione degli Asset

Effettuare **Risk Assessment** nel caso di adozione di piattaforme mobili

Definire il **modello di Governance** e **Linee Guida** per l'uso dei dispositivi mobili e dei relativi software di sicurezza

Limitare il trasferimento di **dati critici** ai terminali mobili o considerare solo accesso RO

Utilizzare **software MDM/MAM** per gestire dati a diversa classificazione, implementare policy di sicurezza e stabilire controlli di monitoraggio

Effettuare **Vulnerability Assessment** e **Penetration Test** sui device mobili, le App e l'infrastruttura sottostante - focus sul data storage lato device

Predisposizione ed erogazione di **iniziative di formazione** focalizzate

Stabilire un **programma per il monitoraggio** e la valutazione delle nuove minacce

Come gestire la diffusione dei device mobili

How consumerization is changing the role of IT
WindowsVideos
(http://www.youtube.com/watch?v=3nNe8BbXDj8)

Agenda

- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

Case study

Contesto di riferimento

Come discusso, il continuo aumento di dispositivi mobile concessi in dotazione ai dipendenti delle aziende comporta una serie di problematiche legate alla loro gestione. Da questa considerazione, la necessità di definire:

- un **modello di gestione della security dei device**, che garantisca la confidenzialità e l'integrità dei dati aziendali in essi contenuti;

- un **modello di gestione delle applicazioni di interesse aziendale presenti sui dispositivi**, con particolare attenzione al deployment, all'aggiornamento e alla segregazione degli ambienti di lavoro.

È il caso di una realtà industriale significativa a livello nazionale con la necessità di definire un'architettura sicura ed efficiente per la gestione del parco-dispositivi già presente in azienda, in linea con le leading practices.

Case study

Obiettivi del progetto

L'azienda vuole:

- scegliere ed adottare una soluzione tecnologica che meglio soddisfi le proprie esigenze in tema di adozione del paradigma mobile;
- definire le linee guida sia per la configurazione e la gestione in sicurezza dei device (destinate al personale IT) sia per il corretto utilizzo dei dispositivi mobili (destinate ai utilizzatori finali).

Quali le attività necessarie?

- Ricercare, tra i principali prodotti sul mercato, una soluzione tecnologica che risponda alle esigenze; valutare e comparare le soluzioni individuate, sulla base dei requisiti tecnologici e di sicurezza
- Identificare le linee guida più appropriate per le policy di configurazione, gestione e utilizzo dei dispositivi mobili.

Case study

Attività svolte

Step 1: ***Definizione dei requisiti di business e valutazione impatti***

Step 2: ***Software Selection***

- Mobile Asset Inventory
- Identificazione dei requisiti funzionali
- Individuazione delle caratteristiche delle soluzioni tecnologiche disponibili
- Selezione dei player MDM/MAM sulla base delle esigenze aziendali
- Proof of Concept per le best fitting solution
- Scelta della piattaforma MDM/MAM tra il subset di soluzioni

Step 3: ***Redazione delle policy***

- Individuazione delle feature di sicurezza supportate dalle soluzioni
- Raccolta dei requisiti funzionali per l'utilizzo dei dispositivi mobili
- Definizione delle linee guida per la redazione delle procedure di configurazione destinate al personale IT e delle policy di utilizzo per gli utenti finali

Case study

Requisiti ed impatti

Al fine di collezionare i requisiti necessari all'individuazione di una soluzione per la gestione dei device mobili e valutarne preliminarmente gli impatti, è necessario individuare gli stakeholder della C-suite da coinvolgere:

- Chief Information Officer (inclusi Infrastructure/Application/ Telecommunication Mgr)
- Chief Technology Officer
- Chief Information Security Officer
- Chief Human Capital Officer
- Chief Legal Officer
- Chief Compliance Officer

Case study

Software selection

Si dovrebbero quindi organizzare meeting ad-hoc con i differenti stakeholder del progetto, durante i quali affrontare diverse tematiche, tra le quali:

- normative interne procedurali già in essere;
- numero e tipologia di device in dotazione ai dipendenti;
- soluzioni tecnologiche già utilizzate per gestire i device;
- procedure in essere per la configurazione iniziale dei device;
- procedure per il deployment delle applicazioni di interesse aziendale;
- valutazione degli impatti legali dell'adozione del paradigma mobile.

Case study

Software selection

La definizione dei requisiti funzionali deve essere condivisa con il gruppo di lavoro al fine di selezionare la piattaforma MDM/MAM.

Tra quelle riportate sul quadrante magico di Gartner, la **selezione delle soluzioni tecnologiche** dovrà tener conto del rispetto dei requisiti emersi in fase preliminare.

Source: Gartner (May 2012)

Le best fitting solution dovranno quindi essere **testate** in appositi laboratori, durante i quali verificare la corretta applicabilità delle impostazioni di sicurezza per le tipologie di device presenti in azienda.

Case study

Redazione delle Policy

L'esecuzione di un **Risk Assessment** è finalizzato ad identificare i **rischi** connessi all'utilizzo dei dispositivi mobile in azienda, ad esempio:

- utilizzo non autorizzato del dispositivo e accesso non autorizzato alla rete aziendale e ai dati di sistema
- connessione a reti Wi-Fi non aziendali
- malware e virus
- furto e smarrimento

Le possibili minacce dovranno quindi essere catalogate sulla base del loro **impatto** sui processi aziendali:

- sicurezza della trasmissione dati e della rete aziendale
- sicurezza dei dati sul dispositivo
- sicurezza fisica del device

Case study

Redazione delle Policy

Si rende quindi necessario individuare le **impostazioni di sicurezza** applicabili ai dispositivi mobili per ridurre l'impatto delle minacce rilevate.

Tali feature possono essere formalizzate in una **Mobile Security Baseline** che evidenzi il livello di impatto di ogni impostazione sui rischi corrispondenti.

Ad esempio, le **feature** rilevate possono essere suddivise nelle seguenti categorie :

- *Accesso al dispositivo* (es: password all'accesso, regole per la creazione della password, auto-lock per inattività)
- *Gestione remota del dispositivo* (es: monitoring dello stato del dispositivo, blocco e wipe da remoto)
- *Sicurezza dei dati* (es: cifratura dei dati, backup dei dati, antivirus)

Case study

Redazione delle Policy

Ad integrazione della Security Baseline, sarebbe consigliato individuare alcune funzionalità la cui disabilitazione potrebbe garantire un livello di sicurezza ulteriore.

Tale esercizio può essere formalizzato in un **Mobile User Profiling** al fine di associare i profili di utilizzo ipotizzati (es: dirigenti, funzioni tecniche, funzioni di supporto) con le funzionalità (es: disabilitazione della funzione di hard-reset, utilizzo del tethering, utilizzo connessioni NFC, esecuzione dei plug-in, esecuzione javascript, accesso App store interni e/o esterni).

La scelta delle funzionalità da abilitare tiene conto, oltre al ruolo dell'assegnatario, dell'utilizzo previsto per il dispositivo e della tipologia di device.

In tale fase, l'elaborazione dei profili di utilizzo deve coinvolgere le disposizioni della direzione risorse umane e organizzazione.

Agenda

- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

Bibliografia e sitografia

http://www.idc.com/research/Predictions13/downloadable/238044.pdf

http://www.nielsen.com/us/en/newswire/2013/how-the-mobile-consumer-connects-around-the-globe.html

http://www.displaysearch.com/cps/rde/xchg/displaysearch/hs.xsl/130107_tablet_pc_market_forecast_to_surpass_notebooks_in_2013.asp

http://www.vertic.com/blog/year_of_the_enterprise_tablet_infographic/

http://www.avanade.com/Documents/Resources/consumerization-of-it-executive-summary-italian.pdf

http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf

http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q4%202012.pdf

http://www.gartner.com/id=2056717

http://www.gartner.com/id=2019515

http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf

http://www.ey.com/IT/it/Issues/Managing-risk/Global-Information-Security-Survey-2012

http://c4s.clusit.it

http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users

http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COIT_Mitigation_Strategies_Final_Report

http://www.kaspersky.com/it/about/news/virus/2012/Virologia_della_telefonia_mobile_Parte_5

Agenda

- Presentazione relatore
- La diffusione dei device mobili
- Minacce e vulnerabilità del mobile computing
- Gli ambiti di applicazione del mobile computing
- Come gestire la diffusione dei device mobili
- Case study
- Bibliografia & sitografia
- Q&A

Q&A

Contatti

Rodolfo Mecozzi | Senior Manager | IT Risk & Assurance

Rodolfo.Mecozzi@it.ey.com

Ernst & Young Financial-Business Advisors Spa

www.ey.com

Grazie...

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter