AIEA

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Capitolo di Milano

Sicurezza e compliance delle App

Fabio Pacchiarotti (EY)

Roma 23/04/2015

Agenda

- Presentazione relatore
- Contesto di riferimento
- Sicurezza delle App
- Aspetti di compliance
- Conclusioni
- Bibliografia & sitografia
- Q&A

Presentazione relatore

Fabio Pacchiarotti

Esperienze nella consulenza aziendale per il governo dei sistemi informativi, la sicurezza delle informazioni e la gestione dei rischi IT.

Manager in EY dal 2014, attivo nei seguenti ambiti:

- Gestione della sicurezza delle informazioni
- Conformità alle normative vigenti
- Sicurezza IT
- Technology Innovation

Certificazioni:

- CISSP
- ISO/IEC 27001 Lead Auditor

Agenda

- Presentazione relatore
- Contesto di riferimento
- Sicurezza delle App
- Aspetti di compliance
- Bibliografia & sitografia
- Q&A

Introduzione

I dispositivi mobili stanno sostituendo i personal computer come piattaforma primaria di accesso alle informazioni

Worldwide Smartphone Sales to End Users by Operating System in 2014 (Thousands of Units)

Operating System	2014 Units	2014 Market Share (%)	2013 Units	2013 Market Share (%)
Android	1,004,675	80.7	761,288	78.5
iOS	191,426	15.4	150,786	15.5
Windows	35,133	2.8	30,714	3.2
BlackBerry	7,911	0.6	18,606	1.9
Other OS	5,745	0.5	8,327	0.9
Total	**1,244,890**	**100.0**	**969,721**	**100.0**

Source: Gartner (March 2015)

Diffusione delle App per dispositivi mobili

- La diffusione di App è aumentata conseguentemente, sia in ambito aziendale che in ambito consumer
  - Passaggio all'utilizzo di poche App (posta elettronica, calendario) allo sviluppo di App legate a specifici processi di business
  - Sviluppo di App per gestire i rapporti con la clientela

- La modalità di fruizione è sempre più promiscua

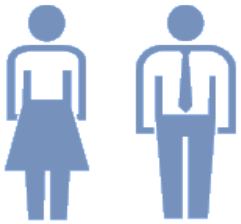
COBO	***COPE***	***BYOD***
Corporate Owned Business Only	*Corporate Owned Personally Enabled*	*Bring Your Own Device*
Utilizzo del dispositivo orientato esclusivamente alle App lavorative	L'azienda abilita il dispositivo all'utilizzo di App personali, salvaguardando l'utilizzo di quelle aziendali	L'azienda permette ai propri dipendenti l'installazione di App aziendali sui dispositivi personali

Nuovi paradigmi di interazione con l'utente

Lo sviluppo di App per terminali mobili permette di definire nuovi paradigmi di interazione con l'utente secondo un approccio **people-centered** e permette di:

- Portare le informazioni fino alle persone, indipendentemente da dove si trovano, nel preciso momento in cui si manifesta l'esigenza di accesso

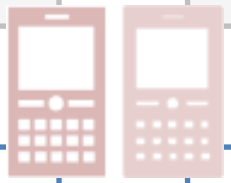
- Riconoscere il singolo utente, focalizzarsi sulle sue esigenze e le sue abitudini, fornendogli assistenza in modo contestuale e personalizzato



Ambiti di applicazione

App per utenti interni
Sviluppate per l'utilizzo del personale aziendale

- Efficientamento dei processi attraverso l'automazione e la dematerializzazione
- Estensione dell'accesso ai sistemi informativi al personale in mobilità (forza vendite, manutenzione)
- Dati e informazioni sempre disponibili con modalità «always-on»
- Sfruttamento delle funzionalità dei dispositivi mobili (geolocalizzazione, video) per l'ottimizzazione delle attività del personale e la gestione di informazioni complesse



App per utenti esterni
Sviluppate per l'utilizzo da parte dei clienti

- Interazione mirata e personalizzata con il singolo cliente
- Utilizzo di canali di comunicazionie diversificati (video, chat)
- Nuove modalità di avertising (differenziata per segmento di appartenenza, o mirata one-to-one)
- Analisi comportamentali relativamente all'utilizzo dell'App e ai servizi forniti
- Sefl Caring integrato direttamente con le piattaforme di CRM
- Acquisto di beni o servizi

Mobile Cloud Computing

Utilizzo di piattaforme di back-end per la gestione di specifiche funzionalità applicative e per lo storage delle informazioni

Supporto di specifiche funzioni di business attraverso l'accesso in tempo reale a dati aziendali

Accesso alle informazioni sempre disponibile per i clienti

Gestione dell'interazione con il customer care attraverso i social network

Gestione di nuovi canali di marketing, comunicazione promozionale e piani di loyalty

Nuove sfide per le aziende

L'aumento dei servizi per i quali viene richiesto lo sviluppo di App, unito al crescente numero degli utenti, presenta nuove sfide per le aziende:

- **Gestione del ciclo di vita delle App**, ancora più breve di quello di un software tradizionale (per esigenze di marketing, evoluzione dei dispositivi mobili, cambiamenti dei requisiti di business, ecc.)
- **Gestione del processo di governo delle App**, dalla progettazione iniziale fino all'installazione sui device dei dipendenti o alla pubblicazione sugli store
- Gestione delle **misure tecniche di sicurezza e degli aspetti di compliance** in base ai dati trattati
- Monitoraggio della diffusione di **App aziendali contraffatte**
- Analisi dei **feedback degli utenti**

E' fondamentale definire una strategia per la gestione delle App

Principali criticità

- Attenzione rivolta solo alle aspettative del business (funzionalità applicative, user experience)
- Assenza di **policy e procedure** per la gestione delle ciclo di vita delle App
  - Requisiti per lo **sviluppo di codice sicuro**
  - Requisiti per l'**infrastruttura ICT** (rete, servizi di gestione IT, applicazioni, gestione delle identità)
  - Requisiti per **il trattamento di dati personali** in conformità con le normative vigenti
- Ruoli e responsabilità per il **governo del ciclo di vita delle App** non individuati

Agenda

- Presentazione relatore
- Contesto di riferimento
- Sicurezza delle App
- Aspetti di compliance
- Conclusioni
- Bibliografia & sitografia
- Q&A

Principali rischi

App per utenti interni

- Perdita di informazioni dovute a:
  - Presenza di malware sul terminale
  - Controllo accessi non sufficientemente robusto
- Sfruttamento di vulnerabilità tramite:
  - Accessi non autorizzati
  - Reverse Engineering

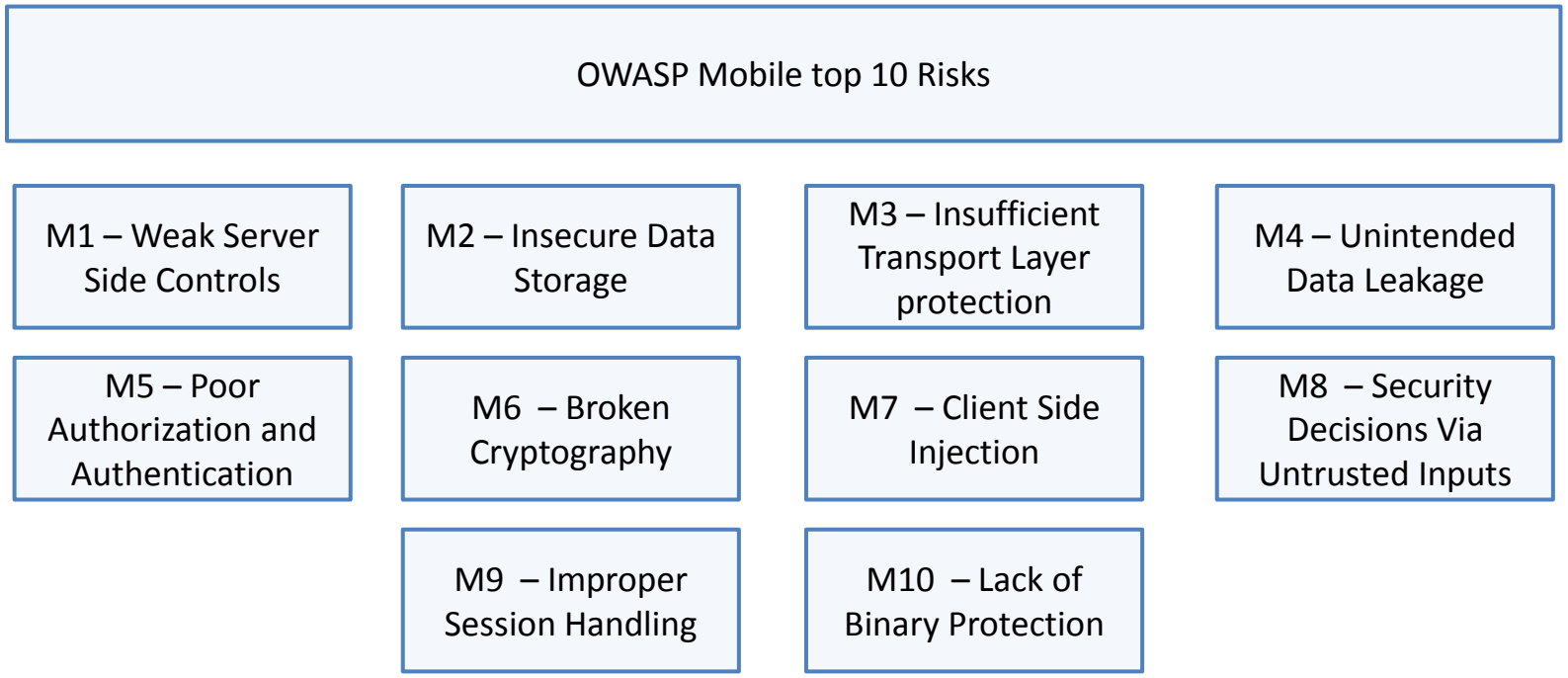
App per utenti esterni

- Compromissione del comportamento di fabbrica del dispositivo
- Presenza di malware sul terminale
- Presenza di App contraffatte che accedono senza autorizzazione ad informazioni presenti sul dispositivo:
  - Lista dei contatti
  - Elenco chiamate
  - Email
  - Dati di localizzazione

Il terminale sul quale viene eseguita l'App è un device untrusted

OWASP Top 10 Mobile Risks

- The «Open Web Application Security Project» (OWASP) è una iniziativa internazionale volta alla diffusione della cultura della sicurezza delle applicazioni web
- Si focalizza sulle aree di rischio invece che sulle specifiche vulnerabilità
- Oltre alla pubblicazione dei Top10 Mobile Risks ha dedicato un intero progetto alla sicurezza applicativa mobile



OWASP – M1

M1 - Weak Server Side Controls

- I server di back-end ai quali accedono le App non implementano adeguate misure di sicurezza per prevenire che utenti non autorizzati accedano ai dati

Impatti

- Perdita della confidenzialità e dell'integrità dei dati

Azioni di mitigazione

- Validazione dei dati
- Considerare il terminale come un dispositivo untrusted
- Hardening delle architetture esistenti

OWASP – M2

M2 - Insecure Data Storage

- Dati critici memorizzati localmente dall'App in maniera non sicura (salvati in cache, log, file XML, ecc.) ipotizzando che l'utente o altre App malevole non accedano al file system
- Assegnazione di permessi errati di lettura o scrittura ai file che contengono dati critici (username, token di authenticazione, password, ecc.)

Impatti

- Perdita della confidenzialità dei dati
- Violazione delle credenziali di accesso
- Accesso ai dati personali

Azioni di mitigazione

- Individuare in fase di progettazione tutti i dati ritenuti critici
- Salvare localmente sul dispositivo solo i dati strettamente necessari e per il tempo minore possibile
- Non usare le aree pubbliche (SD Card) per la memorizzazione di dati critici
- Utilizzare le API messe a disposizione dal sistema operativo per la cifratura dei file
- Non assegnare ai file contenenti informazioni critiche permessi di lettura o scrittura da parte di altre applicazioni

OWASP – M3

M3 - Insufficient Transport Layer protection

- Assenza totale di crittografia per la trasmissione dei dati alle piattaforme di back-end
- Utilizzo di SSL/TLS solamente durante la fase di autenticazione
- Utilizzo di algoritmi crittografici deboli
- Utilizzo di protocolli di comunicazione deboli
- Utilizzo di protocolli forti, ma vengono ignorati i warning di sicurezza o gli errori di validazione dei certificati

Impatti

- Perdita della confidenzialità e dell'integrità dei dati
- Furto d'identità
- Attacchi di tipo man-in-the-middle

Azioni di mitigazione

- Tutti i dati critici trasmessi o ricevuti dall'App devono essere cifrati, indipendentemente dal canale di comunicazione (Wi-Fi, rete telefonica, NFC)
- Implementare correttamente le connessioni cifrate attraverso certificati validi, firmati da CA valide e con chiavi di cifratura robuste
- Non ignorare i warning e le eccezioni di sicurezza

OWASP – M4

M4 - Unintended Data Leakage

- Memorizzazione non intenzionale di dati critici in aree di memoria del terminale facilmente accessibili da altre App (directory temporanee, cache web, log) a causa di errori di programmazione o dall'utilizzo di software di terze parti integrato durante lo sviluppo delle App

Impatti

- Violazione della privacy
- Dati critici conservati in aree non sicure per tempo indeterminato

Azioni di mitigazione

- Evitare di salvare nei crash log informazioni critiche, come le credenziali di accesso
- Utilizzare librerie di terze parti fidate e testate, che non contengono malware o backdoor
- Controllare le aree di memoria accessibili a tutte le App per verificare la presenza di informazioni critiche
- Testare l'applicazione su piattaforme differenti

OWASP – M5

M5 - Poor Authorization and Authentication

- Le credenziali dell'utente sono un caso particolare di dato critico e se non gestite correttamente possono essere utilizzate per l'accesso non autorizzato
- Utilizzo dei parametri immutabili del dispositivo (IMEI, IMSI, UUID) per l'autenticazione dell'App

Impatti

- Acceso non autorizzato
- Privilege esclation

Azioni di mitigazione

- Evitare di usare come unica forma di autenticazione dati collegati all'identità del dispositivo, in quanto potrebbero essere facilmente recuperati
- Evitare di cablare password o altri segreti precondivisi nei sorgenti dell'App
- Evitare di salvare password nella cache o nei log
- Evitare di validare le credenziali dell'utente sul terminale mobile, eseguendola sempre sui server di back-end
- Richiedere all'utente la creazione di password la cui robustezza è legata alla criticità dei dati trattati

OWASP – M6

M6 - Broken Cryptography

- Utilizzo errato di librerie di sicurezza
- Implementazione di algoritmi di crittografia personali

Impatti

- Perdita della confidenzialità e dell'integrità dei dati
- Privilege esclation
- Cambio della logica di business

Azioni di mitigazione

- Gestire le chiavi di cifratura secondo quanto indicato dall'algoritmo utilizzato, evitando di conservarle insieme ai dati criptati
- Sfruttare le API per la cifratura messe a disposizione dalla piattaforma Android o iOS
- Evitare di creare nuovi algoritmi di crittografia, sfruttare quelli ampiamente testati

OWASP – M7

M7 - Client Side Injection

- Esecuzione di codice malevolo sul terminale mobile attraverso l'App (XSS, HTML, SQL injection)
- Utilizzo da parte delle App di librerie dei browser

Impatti

- Privilege esclation
- Compromissione del terminale

Azioni di mitigazione

- Validazione dei dati per tutte le sorgenti di dati ricevuti dall'App

OWASP – M8

M8 - Security Decisions Via Untrusted Inputs

- Utilizzo da parte degli sviluppatori di campi nascosti o funzionalità nascoste per bypassare i controlli e le richieste di autorizzazioni all'utente per l'accesso alle informazioni personali

Impatti

- Privilege esclation
- Accesso ai dati

Azioni di mitigazione

- Esplicitare la richiesta di permesso all'utente
- Verificare che ci sia il permesso dell'utente prima di eseguire azioni che implicano l'utilizzo di informazioni personali

OWASP – M9

M9 - Improper Session Handling

- Mantenimento di sessioni molto lunghe da parte delle App per motivi di usabilità tramite cookie HTTP, token OAuth e servizi di autenticazione utilizzando come token di sessione l'identificativo del dispositivo
- Token di sessione condiviso in modo non intenzionale con terze parti

Impatti

- Privilege esclation
- Accesso non autorizzato

Azioni di mitigazione

- Prevedere un limite massimo ragionevole per le sessioni
- Generare i token di sessione in maniera casuale in modo che non siano prevedibili

OWASP – M10

M10 - Lack of Binary Protection

- Possibilità di eseguire da parte di un utente malevolo l'analisi e il reverse engineering del codice dell'App, per modificarlo ed inserire delle funzionalità nascoste

Impatti

- Esposizione delle proprietà intellettuali

Azioni di mitigazione

- Seguire tecniche di codifica sicura per i componenti di sicurezza presenti all'interno dell'App
- Prevenire l'analisi e il reverse engineering dell'App utilizzando tecniche di analisi statica o dinamica
- Rilevare in fase di esecuzione che il codice è stato aggiunto o modificato

Sviluppo sicuro di App - Considerazioni

- **Validare sempre i dati** lato server e sull'App (sia per i flussi inviati che per quelli ricevuti) al fine di evitare la compromissione del dispositivo
- Evitare di utilizzare lo **storage condiviso** dei dispositivi per il salvataggio di credenziali, token di autenticazione, chiavi di cifratura
- Non utilizzare **memorie rimovibili** per salvare, anche in maniera temporanea o cifrata, dati critici
- Utilizzare tecniche di **trasmissione crittografata**, indipendentemente dal canale di comunicazione utilizzato
- Prevedere un **limite massimo ragionevole per le sessioni**, generando token di sessione in maniera casuale e non prevedibili
- Prevedere meccanismi per impedire l'utilizzo di applicazioni che trattano dati critici su **dispositivi manomessi** sui quali sia possibile ottenere i massimi privilegi

Agenda

- Presentazione relatore
- Contesto di riferimento
- Sicurezza delle App
- Aspetti di compliance
- Conclusioni
- Bibliografia & sitografia
- Q&A

Aspetti legali

L'App è un prodotto software installato sul dispositivo dell'utente per l'erogazione di un servizio

EULA

Accordo di licenza con l'utente finale (End-User License Agreement) in grado da indirizzare:

- limitazioni d'uso
- limitazione di garanzia
- limitazione di responsabilità
- eventuali restrizioni

Termini e condizioni contrattuali

Se il servizio è soggetto a specifici termini e condizioni contrattuali, devono essere indicati esplicitamente:

- Modalità di erogazione e fruizione del servizio
- Responsabilità dell'utilizzo dell'App e dei servizi da essa erogati
- Altri aspetti legali relativi ai vincoli di proprietà intellettuale (es. divieto di decodificare, decompilare, disassemblare l'App o effettuare operazioni di reverse engineering)

Tutti i principali Store permettono di pubblicare tali informazioni in modo che siano accessibili anche prima del download

Trattamento dei dati personali

Se l'App tratta **dati personali** si applicano tutte le prescrizioni del Codice Privacy riferibili ai trattamenti tramite strumenti elettronici

Informativa privacy

Contiene le informazioni relative al trattamento dei dati personali riferiti all'utente dell'App in conformità all'art. 13 del D.Lgs 196/03

Relativamente al trattamento dei dati personali forniti deve indicare:

- Le finalità e le modalità del trattamento
- Il titolare del trattamento e il responsabile (qualora designato)
- I dati necessari all'erogazione del servizio e quelli facoltativi, senza i quali il servizio sarà ugualmente erogato
- I soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati
- Quali dati personali sono trattati dall'App localmente sul dispositivo o sulle piattaforme di back end
- La durata della conservazione
- I diritti del cliente in conformità all'art. 7 del D.Lgs 196/03
- Il diritto di revocare il consenso qualora acquisito

Deve essere mostrata prima che l'App inizi a raccogliere dati personali (alla prima attivazione)

Consenso al trattamento dei dati personali

Nel caso in cui l'App esegua il trattamento dei dati personali per **finalità ulteriori** opzionali rispetto a quelle previste per l'erogazione del servizio, tali finalità devono essere dichiarate nell'informativa e deve essere **acquisito un consenso** per ciascuna di esse

Consenso libero specifico ed informato

Esempi di trattamenti per i quali deve essere previsto un consenso esplicito:

- Profilazione individuale degli interessi dell'utente basata sul modo di interagire con l'App al fine di identificare i suoi comportamenti e le sue abitudini
- Condivisione dei dati personali con terze parti per attività di analytics
- Utilizzo dei dati personali per finalità pubblicitaria e commerciale
- Gestione dei dati di localizzazione

Ogni App ha un proprio ciclo di vita e deve gestire in autonomia i consensi richiesti all'utente, attraverso un'interfaccia che gli consenta di esprimere i consensi e rivedere le proprie scelte

Se l'App tratta **dati sensibili** l'acquisizione del consenso deve avvenire in forma scritta o con modalità giuridicamente equivalente

Trattamento dei dati personali - Considerazioni

La corretta gestione dei trattamenti dei dati personali è in primis un **elemento di sicurezza** e di **compliance normativa**

Se correttamente impostati, i trattamenti possono costituire un **vantaggio competitivo**, nel **rispetto delle normative** vigenti e della **trasparenza nei confronti dei clienti**:

- Profilazione delle abitudini d'uso del servizio
- Correlazioni dei dati acquisiti da App differenti sviluppate dall'azienda
- Interazione e supporto continuativo personalizzato
- Gestione di campagne di avertising ad hoc e gelolocalizzate
- Gestione dei piani di loyalty

Termini e condizioni contrattuali

Informativa privacy

Consenso

Tutela del brand

- Le App sono una vetrina dell'azienda e devono essere tutelate per proteggere il proprio brand
- Un efficace ed efficiente programma di **protezione del marchio** online non può prescindere dall'adottare una metodologia di monitoraggio della sicurezza delle App

- Richiede competenze tecniche, giuridiche e strumenti a supporto delle attività
- Deve prevedere un **monitoraggio continuativo**:
  - **Monitoraggio di tutte le App** riconducibili all'azienda disponibili sugli store, sia ufficiali che sui canali distribuzione alternativi (dove si trovano App potenzialmente alterate)
  - **Analisi statica e dinamica** delle App, al fine di determinare la presenza di codice malevolo
  - **Analisi legale** al fine di individuare possibili usi non autorizzati del brand, violazioni degli obblighi contrattuali o delle disposizioni normative vigenti che prescinde dall'alterazione del codice sorgente
  - **Gestione delle azioni di mitigazione**, che possono prevedere la rimozione dell'App dallo Store o il perseguimento di vie legali nei confronti degli autori di App contraffate

Agenda

- Presentazione relatore
- Contesto di riferimento
- Sicurezza delle App
- Compliance alle normative per il trattamento dei dati personali
- Conclusioni
- Bibliografia & sitografia
- Q&A

Conclusioni

- Lo sviluppo di App è una opportunità per le aziende, in quanto permette di acquisire **grandi quantità di dati** generati dai terminali mobile e di offrire **servizi personalizzati**
- E' fondamentale definire una strategia aziendale per la **gestione delle App**, in modo da indirizzare non solo le esigenze e le aspettative del business, ma il **governo del ciclo di vita delle App**
- L'attenzione agli **aspetti di sicurezza** deve essere parte integrante del processo di progettazione e sviluppo delle App, in quanto il terminale sul quale viene eseguita l'App è un device untrusted
- Deve essere assicurato il **rispetto della conformità alle normative** esistenti ed alle policy aziendali in materia di trattamento dei dati personali, che se correttamente impostato può costituire un vantaggio competitivo
- Deve essere eseguito un monitoraggio continuativo della sicurezza delle App riconducibili all'azienda nell'ambito di un **programma di protezione del brand**

Bibiliografia e sitografia

00461/13/EN WP 202 – Article 29 Data Protection Working Party – Opinion 02/2013 on Apps on Smart Devices
GSMA Privacy Design Guidelines for Mobile Application Development
Garante per la protezione dei dati personali: Smartphone e tablet: scenari attuali e prospettive operative
Oracle Community for Security - Mobile e Privacy
Oracle Community for Security - MOBILE ENTERPRISE: sicurezza in movimento
http://www.gartner.com/newsroom/id/2996817
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

Q&A

Contatti

Fabio Pacchiarotti | Manager | Advisory Services
fabio.pacchiarotti@it.ey.com

Ernst & Young Financial-Business Advisors
www.ey.com

Grazie…