CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Consumérisation de l'IT et sécurité des SI

Pascal Sauliere
Technology & Security Architect, CISSP, CCSK
Microsoft France

Sommaire

Vision et défis du DSI

Approche

- Sécurité du terminal
- Protection infrastructure et applications

Perspectives

Vision DSI

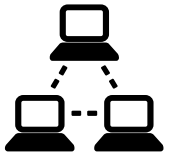
- 64% DSI voient d'un mauvais œil l'intégration d'appareils mobiles personnels au sein de leur entreprise
- Mais 49% considèrent que cela est nécessaire au futur de leur entreprise pour répondre au besoin de réactivité demandé par leurs clients
- 41% considèrent les employés responsables du contenu se trouvant sur les équipements personnels utilisés à des fins professionnelles
- 28% des entreprises françaises n'ont pas de politique dédiée pour gérer l'utilisation des mobiles personnels pour accéder aux informations de l'entreprise

Etude Eude Coleman Parkes portant sur 300 DSI France, Allemagne et Royaume Uni (décembre 2011)

Les challenges selon les DSI

68% pour l'adaptation des applications existantes à de nouveaux systèmes d'exploitation

65% sur les coûts de développement de nouvelles infrastructures



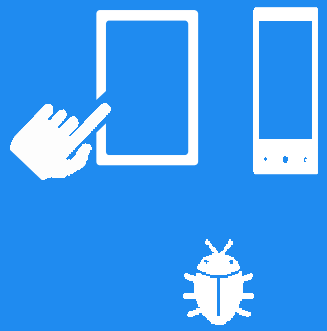
66% sur les coûts associés au développement de nouvelles applications d'entreprise

59% sur les risques de perte de données (par perte ou vol du terminal ou par attaques logiques)

Etude IDC (demande IBM) (13/07/2011)

Les deux piliers de l'approche

Sécurité du terminal



Jailbreak, rooting
Multiplication des OS
Mélange des données privées et entreprise
Sécurité des applications du marketplace
Gestion sous responsabilité utilisateur
Hors contrôle administration entreprise

Protection infrastructure et applications

Connexion au SI (interne et accès distant)
Niveau de confiance du terminal
Identification des données sensibles
Protection des données sensibles
Protection contre les fuites d'information
Publication messagerie/collaboratif
Publication des applications

Sécurité du terminal : contrôle EAS

Exchange ActiveSync (EAS)

Protocole pour le management des terminaux mobiles

Spécifications publiques, 44 politiques définies

Gestion du mot de passe

Chiffrement du terminal, S/MIME, synchronisation

Autorisation Bluetooth, Infrarouge, carte de stockage, caméra, bureau à distance…

Implémenté sur IOS, Android, Windows Phone, WebOS… sauf BlackBerry

Constat

Toutes les politiques ne sont pas implémentées

Pauvre vs configuration poste Windows (GPO)

Nécessité d'un outil d'administration multi-OS (Mobile Device Management)

Sécurité du terminal

Sécurité du terminal	Solution
Jailbreak, rooting	Mobile Device Management, choix OS
Multiplication des OS	Mobile Device Management, choix OS
Mélange données privées et entreprise	Chiffrement mails, documents, solution Silo
Sécurité applications du marketplace	Marketplace privé, isolation silo
Gestion sous responsabilité utilisateur	Politique sécurité, isolation silo
Hors contrôle admin entreprise	EAS, Mobile Device Management

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Protection infrastructure & applications

Protection infrastructure et applications	Exemple de solution
Connexion au SI depuis l'interne	Contrôle accès réseau 802.1x
Détermination des données sensibles	Classification
Protection des données sensibles	Isolation de serveur IPSec
Protection contre fuites d'information	Gestion Droits Numériques (RMS)
Publication Messagerie/Collaboratif	ActiveSync, Passerelle (UAG)
Publication Applications	Remote Desktop Service-VDI

Perspectives

Windows 8 et Windows Server 2012

Windows To Go : Windows 8 Entreprise sur une clé USB

- BitLocker avec mot de passe
- DirectAccess, SCCM, UE-V, App-V 5.0

Hyper-V Client : Environnement d'entreprise dans machine virtuelle

- Windows 7 ou Windows 8
- DirectAccess, SCCM, UE-V, App-V 5.0

Accès aux applications et contrôle du périphérique

- Windows RT (ARM) : Company Apps, ActiveSync, chiffrement
- Scénarios VDI, Portail UAG
- SCCM 2012, Portail applicatif Windows Intune