30 novembre 2010

Smartphones et sécurité

Quel positionnement pour le RSSI ?

Gérôme BILLOIS
gerome.billois@solucom.fr

Chadi HANTOUCHE
chadi.hantouche@solucom.fr

solucom
management & IT consulting

Qui sommes-nous ?

- Cabinet indépendant de conseil en management et système d'information

  coté sur NYSE Euronext

- Dans le top 5 des cabinets de conseil SI

  selon une étude Pierre Audoin Consultants 2009

- Notre mission ?

  porter l'innovation au cœur des métiers,
  cibler et conduire les transformations créatrices de valeur,
  faire du SI un actif au service de la stratégie des entreprises

- ✓ 20 ans d'existence
- ✓ Près de 1 000 collaborateurs
- ✓ Notre cible : le top 200 des grandes entreprises et administrations
- ✓ Croissance annuelle moyenne sur 5 ans : 30 %

30 novembre 2010 - Propriété de Solucom, reproduction interdite

Six practices …

Stratégie & management
➔ Mobiliser l'entreprise sur ses clients et son développement

Transformation SI
➔ Aligner le SI sur la stratégie d'entreprise et les besoins métiers

Gouvernance SI
➔ Améliorer la performance économique et opérationnelle

Télécoms & innovation
➔ Apporter de la valeur grâce aux nouveaux services de communication

Architecture SI
➔ Rendre le SI performant par une approche orientée services

Sécurité & risk management
➔ Manager les risques et mettre le SI en conformité réglementaire

… au service des grands programmes de transformation

> Practice Sécurité & Risk Management
Une typologie de missions alignée sur l'ISO 27001

- Analyse / cartographie des risques
- Politique et gouvernance de la sécurité
- Mesure de maturité et stratégie ISO 27001
- Conformité *(CNIL, PCI-DSS, Solvency II)*

- Centres de compétence sécurité
  - Animation des filières sécurité
  - Insertion de la sécurité dans les projets
  - Sensibilisation et formation
  - Contrôle permanent

Plus de 150 consultants sécurité !

- Protection des données
  Nouveaux modèles d'ouverture du SI, architectures de sécurité, chiffrement, PKI et services de confiance
- Identity & access management
  Role management, provisioning, fédération, SSO, authentification forte, biométrie
- Plan de continuité d'activité
  Plan de continuité métier, plan de continuité informatique, tests et exercices

- Gestion opérationnelle de la sécurité
- Tableaux de bord sécurité
- Plan de contrôle permanent

- Audits de sécurité et tests d'intrusion

LSTI
Certifié NF ISO/CEI 27001:2005
SOLUCOM – Certificat LSTI/SMSI/11

Agenda

1. Le renouveau des smartphones
2. L'évolution des besoins de sécurité
3. Quelles plateformes aujourd'hui ?
4. Comment gérer de multiples plateformes ?
5. Quid de l'usage personnel en entreprise ?
6. Quelle position pour le RSSI ?

Le renouveau des smartphones
Évolution du téléphone mobile

Le mobile : de son invention en 1984… aux terminaux de demain

Voix & Sms

Multimédia

Internet mobile

Interaction avec l'environnement ?

Années 90

1991 Premier réseau GSM

Années 2000

2001 Premiers téléphones **couleur**

2003 Premiers téléphones 3G

2007 Sortie de **l'iPhone**

Depuis 2007

2009 Lancement d'Android

Le renouveau des smartphones
Smartphones et sécurité : un tournant récent

- Un marché actif depuis des années…

- … mais qui connaît un vrai renouveau avec l'arrivée en force des smartphones « nouvelle génération »

  - Prévision 2010 (IDC) : 270 millions d'unités vendues dans le monde, 55% de plus qu'en 2009

Comment intégrer les nouveaux smartphones dans le SI en toute sécurité ?

Le renouveau des smartphones
Des usages Entreprise en progression

Besoin « métier » historique

- **Suivi d'intervention et de maintenance**
- **Scan de code barre** pour la gestion d'inventaire
- **Signature de reçus** lors de la livraison de colis

Déploiement dans le domaine de la logistique, du transport, de l'énergie…

Besoin « bureautique » en renouveau

- **Usage téléphonie et messagerie**
- **Aujourd'hui Internet, multimédia**
- **Demain applications, y compris métier**

De nouvelles fonctionnalités qui arrivent en force !

Le renouveau des smartphones
Quels sont les acteurs du marché ?

- Des positions dominantes déterminées par les produits :
  RIM est encore majoritaire, l'iPhone bouscule le marché
- Des nouveaux venus à surveiller :
  Android et Windows Phone 7

Une réalité : le parc de smartphones de l'Entreprise devient multi-plateformes

Le renouveau des smartphones
Des attentes de plus en plus fortes

Applications standard

Messagerie
(Push) Mail/SMS

Internet
Web riche

Agenda
Réunions, Tâches

Contacts
Tél, mail, etc.

Bureautique
Word, Excel, PowerPoint

Téléphone

Exigences

Utilisateurs

Ergonomie

- Interface intuitive
- Mode de saisie efficace

Fonctionnalités

- Applications standard (et « Entreprise »)
- Applications personnelles téléchargeables (jeux…)
- Matériel innovant (multimédia, appareil photo, GPS…)

Performances

- Connectivité internet rapide (Edge, 3G, WiFi)
- Faibles latences à l'usage et autonomie élevée

Fiabilité

- Intégrité des données

DSI

Sécurité du SI

- Chiffrement des communications et contrôle de flux
- Authentification terminal et utilisateur sur le SI

Sécurité du terminal

- Authentification locale
- Chiffrement des données et protection de la configuration locale
- Solution de sécurité / Gestion des droits locaux

Gestion du parc de terminaux mobiles (MDM)

- Cycle de vie de l'appareil: Provisioning, Production, Maintien, Monitoring, Arrêt de service
- Inventaire, déploiement des configurations, administration distante

Le renouveau des smartphones
L'usage « personnel » des mobiles devient une préoccupation…

- Envie des utilisateurs d'avoir accès aux fonctions multimédia des terminaux
  - Musiques, vidéo, applications personnelles

- Demande de plus en plus forte des collaborateurs pour utiliser leurs périphériques personnels
  - Historiquement les PDA, mais de plus en plus les smartphones et les tablettes tactiles

- Des attitudes variées chez les grands comptes
  - Interdiction, tolérance, sensibilisation…
  - … et des pratiques « sauvages » très répandues

Mais dans tous les cas une forte demande des utilisateurs…

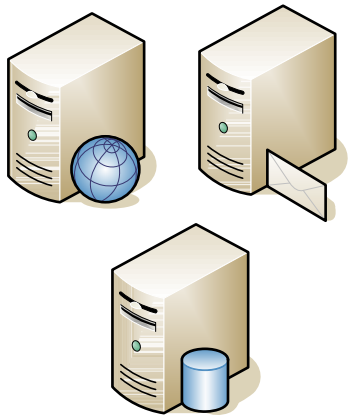
…que doit aujourd'hui gérer le RSSI !

Agenda

1. Le renouveau des smartphones
2. L'évolution des besoins de sécurité
3. Quelles plateformes aujourd'hui ?
4. Comment gérer de multiples plateformes ?
5. Quid de l'usage personnel en entreprise ?
6. Quelle position pour le RSSI ?

L'évolution des besoins de sécurité
Des risques à évaluer sur l'ensemble de la chaîne de liaison…

Terminaux
et données



Réseau opérateur
et/ou Internet

SI de
l'Entreprise

L'évolution des besoins de sécurité
…qui se concrétisent dans des scénarios bien réels

Type	Scénario de risque	Criticité
Vol ou perte du mobile	Récupération des **données personnelles du collaborateur**, ainsi que des **données de l'Entreprise** accessibles par le collaborateur	**Majeur**
	Utilisation du mobile pour **se connecter au SI** de l'Entreprise avec les droits courants	**Majeur**
	Utilisation du **compte de l'utilisateur** pour se connecter ultérieurement au SI de l'entreprise avec les droits courants	**Important**
Écoute des communications / accès réseau	Récupération des **données** transitant par les différents types de canaux utilisés par le smartphone (GSM mais aussi et surtout Wi-Fi / Bluetooth)	**Important**
	Modification des données transmises entre le terminal et le SI de l'entreprise	**Important**
	Connexion et **intrusion** sur le terminal puis potentiellement sur le SI de l'entreprise	**Majeur**
Piégeage du mobile	**Récupération** des données stockées sur le smartphone du collaborateur	**Important**
	Installation **d'applications ayant des fins malicieuses** (vol de données, fraude télécom, GPS tracking, micro/caméra, intrusion, etc.)	**Important**
	Interruption des fonctions essentielles du smartphone	**Faible**

L'évolution des besoins de sécurité
Des bonnes pratiques à décliner en fonction de votre contexte

Fonction de sécurité	Préconisation de mise en œuvre
Solution de gestion des **paramétrages sécurité**	**Obligatoire (pour une flotte de plus de 100 terminaux)** 
Solution de gestion des **mises à jour de sécurité**	**Obligatoire** 
Authentification locale (mot de passe terminal)	**Obligatoire** 
Authentification forte (SI interne)	**Fortement recommandé** 
Effacement à distance des données	**Obligatoire** 
Chiffrement du terminal	**Obligatoire** 
Chiffrement de **bout en bout** de l'ensemble des communications data	**Obligatoire sur flux Entreprise (si usage Wi-Fi)** 
Maîtrise de la **plateforme de distribution d'applications**	**Fortement recommandé** 
Isolation inter-applicative	**Fortement recommandé** 
Antivirus/pare-feu locaux au smartphone	**Faiblement recommandé** 

Agenda

1. Le renouveau des smartphones
2. L'évolution des besoins de sécurité
3. Quelles plateformes aujourd'hui ?
4. Comment gérer de multiples plateformes ?
5. Quid de l'usage personnel en entreprise ?
6. Quelle position pour le RSSI ?

Le renouveau des smartphones *BlackBerry*

BlackBerry → iOS → Android → Windows Phone

- La plateforme entreprise historique
  - Des parts de marché importantes
  - Un parc fortement installé en entreprise qui va aujourd'hui vers le grand public
- Deux atouts : efficacité et sécurité
  - Une ergonomie avancée pour la messagerie
  - Une sécurité pensée dès la conception sur toute la chaîne de liaison
- Mais une plateforme « attaquée »
  - Historiquement sur le volet de la sécurité, du fait de l'utilisation du « NOC »
  - Et aujourd'hui sur le front de l'ergonomie du terminal, du multimédia, des applications et de la navigation Internet qui impacte « l'image » du terminal

Le renouveau des smartphones
BlackBerry et sécurité

BlackBerry → iOS → Android → Windows Phone

- Des fondamentaux solides
  - Socle de gestion à distance performant et fonctionnellement très complet en standard
  - L'OS du terminal est solide et permet une isolation native des applications avec une gestion fine des droits
- Les faiblesses existantes sont gérables
  - Sur le terminal : installation d'applications « espion », suppression temporaire des politiques de sécurité…
  - Sur le poste utilisateur : faiblesse du chiffrement des sauvegardes…
  - Sur les serveurs : configuration du BES…
- Mais un virage vers d'autres usages qu'il faudra suivre attentivement
  - Webkit en tant que navigateur Web…
  - OS QNX pour la tablette PlayBook…
- Et toujours les interrogations sur l'usage du NOC…
  - Ravivées par une actualité récente cet été

Un choix qui reste pertinent pour les grandes organisations qui ne craignent pas l'externalisation d'une partie de la chaîne de liaison

Le renouveau des smartphones
iPhone

BlackBerry → **iOS** → Android → Windows Phone

- Un succès incontestable dans le grand public…
  - Ergonomie, multimédia, applications…
- …qui entraîne de fortes demandes en entreprise !
  - Un vecteur de productivité mais aussi d'image
  - En majorité pour les usages « PIM » mais de plus en plus pour des usages « Métiers »
- Un modèle maitrisé de bout en bout par Apple
  - Mise à disposition d'applications contrôlées
  - Matériels uniques

Le renouveau des smartphones
iPhone et sécurité

BlackBerry → iOS → Android → Windows Phone

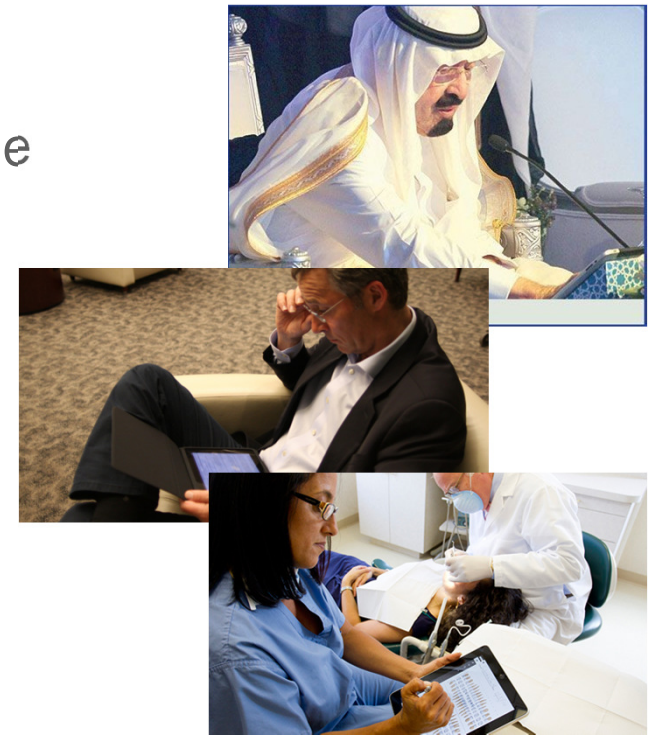
- Historiquement des faiblesses importantes mais des améliorations à chaque version de l'OS et du matériel
  - Par exemple puce matérielle de chiffrement à partir du 3GS
- L'arrivée de l'iOS 4.1/4.2 change la donne avec la gestion de flotte
  - Détection des applications installées, effacement sélectif, surchiffrement sélectif, déploiement d'applicatif…
  - *Attention un produit tiers est requis*
- Des difficultés dans la gestion sont toujours présentes
  - Utilisation d'iTunes
  - Mise à jour de l'OS forcément intégrale
- Et surtout des doutes persistent sur le « jailbreak »
  - En particulier la capacité à le détecter et à le bloquer
  - Sur les impacts vis-à-vis des nouvelles fonctionnalités de sécurité

Des améliorations récentes qui augmentent significativement les capacités de gestion et les fonctionnalités sécurité

Le renouveau des smartphones
iPad

BlackBerry → iOS → Android → Windows Phone

- Un périphérique dont l'usage se répand rapidement
  - Plus de 4 millions d'iPads vendus dans le monde
  - En plus haut lieu dans les entreprises
  - Mais également auprès des équipes internes dans de nombreux secteurs
    - Vente, médical, immobilier, journalisme…
- Une utilisation majoritairement en consultation/navigation
  - Dans une moindre mesure en création de contenu



Une demande naissante chez nos clients, en particulier pour les COMEX et pour certains usages métiers

Le renouveau des smartphones
iPad et sécurité

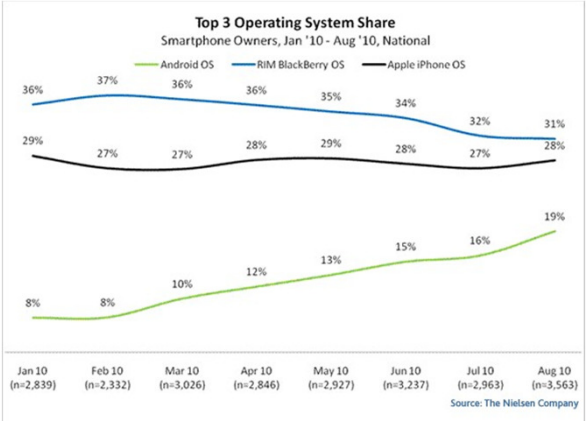
BlackBerry → iOS → Android → Windows Phone

- Une **situation très proche de l'iPhone**
  - Même OS, même système de gestion, quasiment même plateforme matérielle…
- Mais des **usages différents** qui peuvent renforcer certains risques
  - Stockage des documents
  - Création de documents
  - Accès aux Intranets
  - Application métiers…

En première approche, appliquer les mêmes mesures que sur l'iPhone.
Des mesures de sensibilisation additionnelles peuvent être envisagées.

Le renouveau des smartphones
Android

BlackBerry → iOS → **Android** → Windows Phone

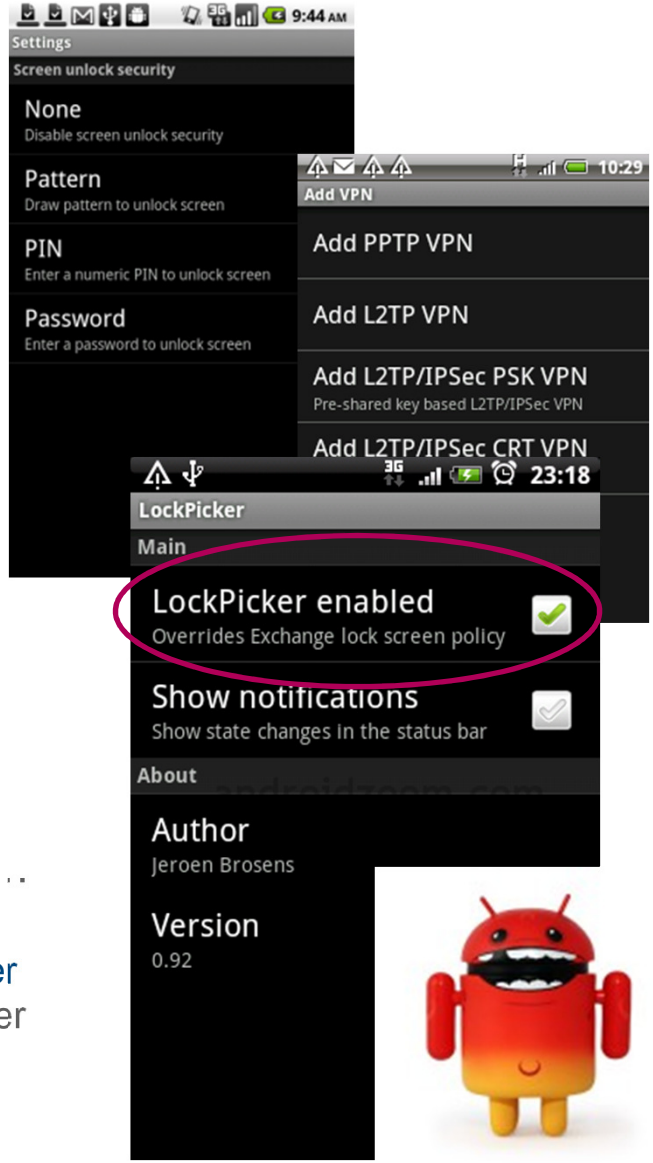


- Un OS grand public, en pleine croissance
  - Crée en 2007
  - 17,2% de parts de marché en 2010 (Gartner)
- Une force : l'ouverture de la plateforme…
  - Multiplication des terminaux permettant une large offre pour les utilisateurs
- …mais également un frein : la fragmentation du marché
  - Des difficultés pour les développeurs et une ergonomie parfois en retrait
- Une mise à disposition simple des applications
  - Pas de validation préalable mais capacité à les interdire ensuite
  - Des applications pouvant accéder largement à l'OS

Le renouveau des smartphones
Android et sécurité

BlackBerry → iOS → **Android** → Windows Phone

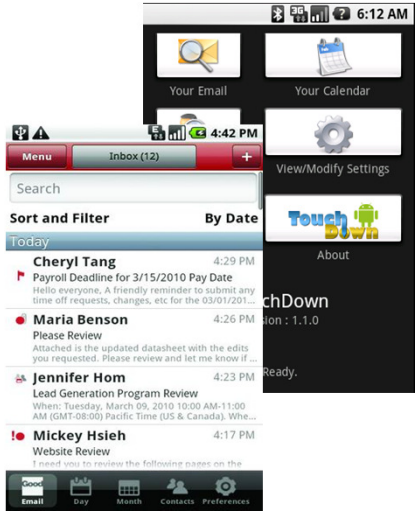
- Un OS jeune basé sur un noyau Linux
  - Un cœur développé par Google
  - Des adaptations par les constructeurs/opérateurs
- Des fonctionnalités sécurité implémentées nativement
  - Isolations des applications avec validation de l'accès aux données et fonctions sensibles à l'installation (mais souffrant de limitations dans la granularité de la protection)
  - Fourniture dans l'OS d'API de fonctions de sécurité (AES, SHA, HMAC)
- Des nouveautés récentes qui sont les bienvenues (été 2010)
  - Configuration par les politiques d'Exchange ActiveSync (mot de passe solide, effacement à distance…)
- Mais des fonctionnalités parfois facilement contournables…
  - Par exemple, l'application *Lockpicker* disponible dans le Market "An app that disables the Exchange lock screen as soon as the server has enforced its policy by using a background service and an observer on the system setting. This requires no polling, scripting, etc. and survives reboots/enforcements."



Le renouveau des smartphones
Android et sécurité

BlackBerry → iOS → Android → Windows Phone

- Des manques importants pour s'imposer comme une solution entreprise
  - Absence de chiffrement intégral/matériel
  - Absence de durcissement « fiable »
  - Absence de contrôle lors de l'installation d'application
  - Manque de plateforme de gestion de flotte
- Mais un écosystème sécurité en plein développement
  - Pour toutes les fonctions de sécurité
  - Et même pour compenser les limitations hardware



Un virage récent vers l'entreprise avec la dernière version de l'OS mais un système encore trop jeune pour une adoption large

Le renouveau des smartphones
Windows Phone 7

BlackBerry → iOS → Android → Windows Phone

- Une sortie très récente : 21 octobre

- Une plateforme avec un potentiel certain
  - Intégration forte dans l'écosystème Microsoft
  - De nombreux partenariat aussi bien constructeurs qu'opérateurs

- Mais un système encore très jeune
  - Absence de copier/coller, de multitâche, de tethering
  - Impossible de se connecter à des Wi-Fi dont le SSID est masqué
  - Pas de rétro-compatiblité avec les applications Windows Mobile

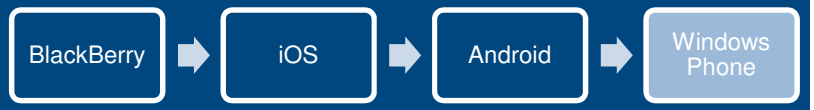
- Et surtout très orienté vers le grand public…
  - Xbox Live, Zune, Windows MarketPlace…

Le renouveau des smartphones
Windows Phone 7 et ergonomie

BlackBerry → iOS → Android → Windows Phone

- Une nouvelle approche dans le monde des smartphones…
  - Interface graphique « Metro » basée sur des « hubs » et des « tuiles »
- … mais aussi au niveau de l'éco-système
  - Ouvert vers les constructeurs mais « standardisé » au niveau matériel
  - Des applications validées mais de manière transparente
  - Se situant finalement entre Google et Apple

Le renouveau des smartphones
Windows Phone 7 et sécurité



- Un nouvel OS dont le fonctionnement est encore peu connu
  - Basé sur un cœur Windows CE
- Des fonctionnalités classiques implémentées
  - Utilisation des politiques d'Exchange ActiveSync (mot de passe et sa longueur, effacement à distance…)
  - Fourniture dans l'OS d'API de fonctions de sécurité (AES, SHA, HMAC)
  - Localisation à distance
- Des manques importants pour s'imposer comme une solution entreprise
  - Absence de chiffrement intégral
  - Manque de plateforme de gestion de flotte (n'est pas inclus dans SCCM)
  - Connectivité VPN uniquement avec Microsoft UAG
- Et un discours sécurité parfois surprenant pour justifier des manques fonctionnels !
  - "Information is further protected by not allowing access to data via PC tethering or support for removable SD cards"

Une situation assez similaire à celle de l'iPhone ou d'Android à leurs débuts, qui inspire la prudence dans un premier temps !

Dernière minute :
jailbreak
Windows Phone 7

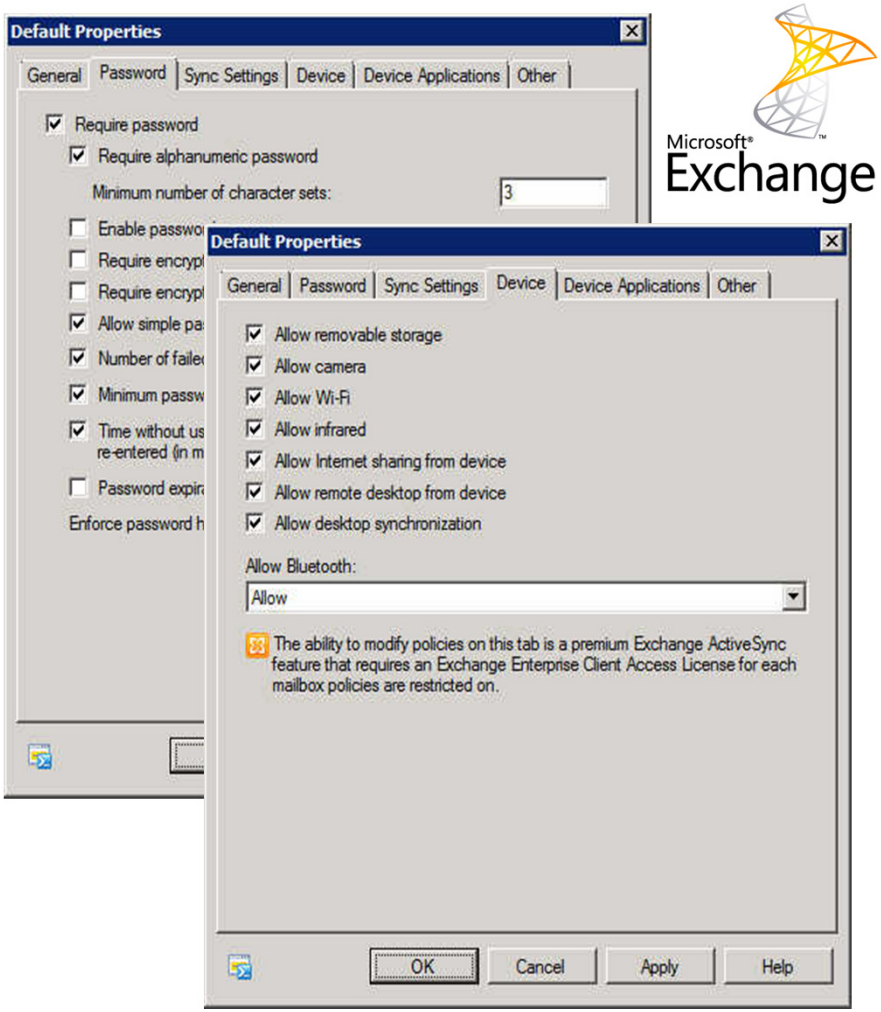
Agenda

1. Le renouveau des smartphones
2. L'évolution des besoins de sécurité
3. Quelles plateformes aujourd'hui ?
4. Comment gérer de multiples plateformes ?
5. Quid de l'usage personnel en entreprise ?
6. Quelle position pour le RSSI ?

Comment gérer de multiples plateformes ?
Comment l'entreprise peut-elle gérer la diversité des plateformes ?

Une première étape : Exchange ActiveSync

- Un majorités des terminaux le supportent nativement
- Un standard de fait pour la messagerie mais de plus en plus pour la gestion du parc
- Une solution intégrée, indépendante de la plateforme mobile…
- …mais qui en masque certaines finesses et des terminaux qui ne supportent pas l'ensemble des critères
- Hormis pour le BlackBerry de RIM, qui possède son système propre

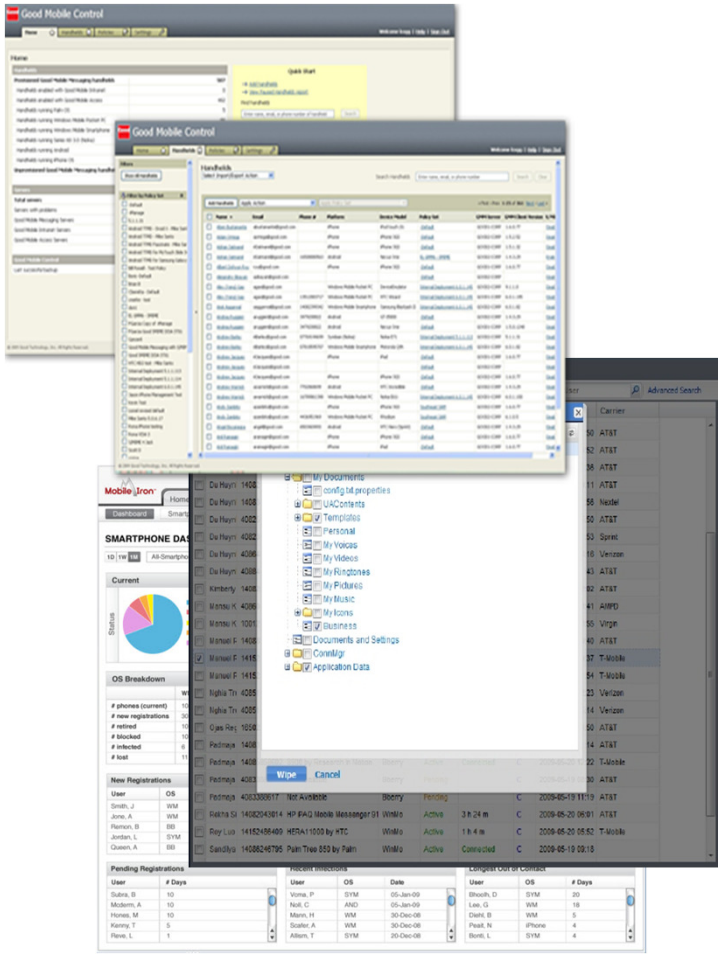


Microsoft® Exchange Server 2010

Comment gérer de multiples plateformes ?
Comment l'entreprise peut gérer la diversité des plateformes ?

Des solutions industrielles : les plateformes dédiées

- Permet un suivi complet du cycle de vie (déploiement, suivi des propriétaires…)
  - Apporte une finesse plus forte sur les critères de sécurité et peut profiter des spécificités des plateformes (effacement sélectif des données…)
  - Des possibilités d'interface avec les solutions RIM également
  - Reste cependant dépendent des capacités et de l'ouverture de la plateforme
  - Un marché en pleine explosion
  - Des acteurs historiques et des nouveaux entrants



TRUST DIGITAL™

McAfee® Proven Security™

IBELEM Expert Data Mobile

MobileIron™

SYBASE®

airwatch™

Comment gérer de multiples plateformes ?
Design type de solution « professionnelle » à la cible

- Déploiement de smartphones fournis par l'entreprise
  - Ouverture uniquement aux terminaux répondant aux critères de sécurité de l'organisation
  - Raccordés à la messagerie en utilisant Exchange ActiveSync
    - Y compris pour les systèmes de messagerie non Exchange (Lotus…)
  - Gérés par une plateforme de gestion multi-plateformes
  - Connectés au SI par l'intermédiaire d'un tunnel chiffré
    - Majoritairement authentification par certificat

Mais cela ne répond aujourd'hui qu'à une partie de la problématique du RSSI…

Agenda

1. Le renouveau des smartphones
2. L'évolution des besoins de sécurité
3. Quelles plateformes aujourd'hui ?
4. Comment gérer de multiples plateformes ?
5. Quid de l'usage personnel en entreprise ?
6. Quelle position pour le RSSI ?

Quid de l'usage personnel en entreprise ?
Usage des terminaux personnels : une demande en pleine explosion !

- Les smartphones sont aujourd'hui largement utilisés par l'ensemble de la population…

- … et plus uniquement par les jeunes cadres
  - 20% des téléphones vendus dans le monde sont des smartphones (Gartner Q2 2010)

Une demande et une opportunité pour la DSI: permettre l'usage de smartphones personnels pour accéder au SI de l'entreprise

Quid de l'usage personnel en entreprise ?
Des mouvements entamés à l'étranger… et en France !

"**JPMorgan** would not buy iPhones or Android phones for employees, as it now does with BlackBerrys. Rather, the bank would allow employees to use the devices to send and receive corporate e-mail if they make the purchase themselves"

JPMorgan

"**UBS** is testing the possibility of allowing employees to use an iPhone or other smartphone to connect to UBS's e-mail system without restricting the private use of the device"

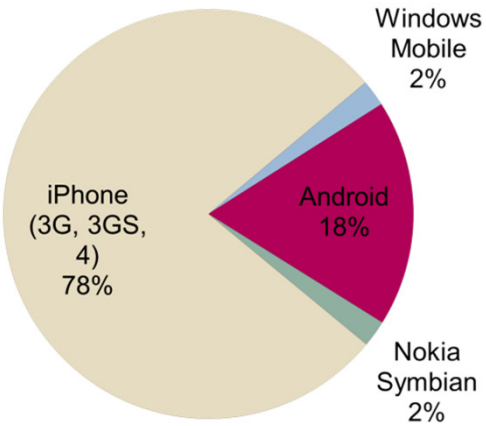
UBS

Mais aussi dans des grands comptes français…

…et dans certains cabinets de conseil en management et SI

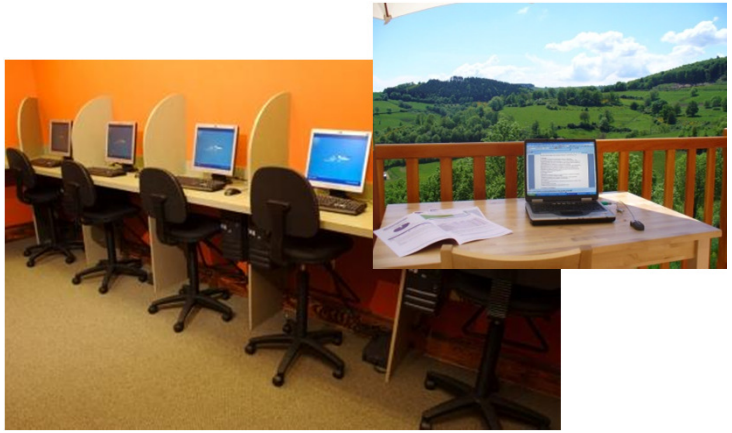
solucom
management & IT consulting

Répartition des smartphones pour 200 collaborateurs

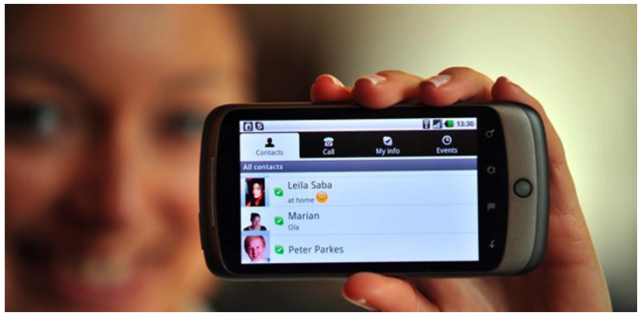


Quid de l'usage personnel en entreprise ?
Un parallèle avec des usages déjà existants

- Une logique proche des PC banalisés
  - Utilisation d'équipements personnels ou partagés (le fameux cybercafé)
  - A la maison, en voyage…



- Des critères cependant différents :
  - Le fonctionnement nécessite souvent un stockage sur le périphérique
  - L'authentification forte rend l'utilisation peu ergonomique
  - L'utilisation est plus fréquente
  - L'équipement est largement personnel



Comment couvrir ces risques sur des terminaux personnels ?

Quid de l'usage personnel en entreprise ?
Quelle latitude pour sécuriser un équipement personnel ?

- L'entreprise peut imposer des critères pour autoriser l'accès aux services
  - Code PIN, chiffrement, version minimale de l'OS…
- Mais trop rendront le service peu attractif
  - Code PIN trop complexe, limitation d'installation d'application…
- Voire même parfois être rédhibitoires !
  - Effacement à distance
  - Traçabilité des accès / géolocalisation
  - Redirection des accès Web

npr

by MARTIN KASTE

When Your Company Kills Your iPhone

November 22, 2010

A few weeks ago, Amanda Stanton's iPhone suddenly went black.

She had been talking on it and navigating with a GPS app during a work trip to Los Angeles. Then, without any warning or error message, the phone quit.

Everything was gone — all her contacts, photos and even the phone's ability to make calls.

It was only after she got home to Silicon Valley that she found out that her phone had been killed by her employer, a publishing company.

The wipe was done by mistake, and Stanton wouldn't have been surprised to see this kind of remote control on a company phone.

But this iPhone was hers.

Quid de l'usage personnel en entreprise ?
Une solution possible : les silos « entreprise »

- La mise en place de silos applicatifs « entreprise » permet d'isoler les données de l'entreprise dans des espaces spécifiques

- Et de mettre en œuvre un niveau avancé de sécurité uniquement sur l'usage professionnel
  - Chiffrement, authentification…
  - Vérification du terminal (version de l'OS, compromission…)
  - Blocage des applications si non-respect des règles

- En revanche, il existe des risques résiduels dus à une potentielle compromission de l'OS
  - Installation de keylogger/screenlogger
  - Capture des fichiers et bruteforce sur le chiffrement

L'usage personnel reste complètement libre,
les données professionnelles étant protégées par ailleurs

Quid de l'usage personnel en entreprise ?
Deux implémentations possibles pour le silo sécurisé

En utilisant les fonctionnalités des plateformes de gestion

- Identification d'espaces et d'applications « entreprise » pour appliquer des mesures de sécurité additionnelles
- Disponible sur peu de plateformes aujourd'hui (iPhone récemment) et encore limité fonctionnellement
- Solution moins facile à accepter pour l'utilisateur car l'administrateur pourra toujours avoir accès à l'ensemble du terminal

En déployant une application dédiée

- Une véritable isolation dans une application dédiée aux fonctions professionnelles
- Une indépendance plus forte par rapport à la plateforme mobile
- Des solutions plus faciles à appréhender et à accepter pour l'utilisateur
- Des premiers retours d'expérience concluants

Quid de l'usage personnel en entreprise ?
Une dimension juridique et RH à ne pas négliger

- Une inquiétude à lever : la propriété des données reste celle de l'entreprise

- D'un point de vue juridique, il n'existe pas encore de jurisprudence
  - Assurance du matériel : qui paie en cas de casse/vol lors d'une utilisation sur le lieu de travail pour un usage professionnel ?
  - Capacité de traçabilité : qui s'assure que les contraintes réglementaires sont bien respectées ?
  - Quelle responsabilité de l'employeur en cas d'action sur un matériel perso ?

- D'un point de vue RH, attention également à ne pas créer de discrimination
  - Le service ne doit pas être obligatoire ou même recommandé, il doit s'agir d'un confort additionnel pour les utilisateurs

Dans tous les cas, l'usage doit absolument être encadré par une charte spécifique !

Agenda

1. Le renouveau des smartphones
2. L'évolution des besoins de sécurité
3. Quelles plateformes aujourd'hui ?
4. Comment gérer de multiples plateformes ?
5. Quid de l'usage personnel en entreprise ?
6. Quelle position pour le RSSI ?

Quelle position pour le RSSI ?

- Tout d'abord réagir positivement aux demandes (ou anticiper !) en communiquant sur la prise en compte de ces nouveaux usages

- Définir sa cible sécurité minimum en fonction des usages par l'intermédiaire d'une analyse de risque

- Suivre les phases de mise en œuvre et prévoir un audit
  - Sur le pilote ou les premiers déploiements

- Rester en veille sur un domaine où l'actualité évolue très vite !

Quelle position pour le RSSI ?
Les principaux messages

- Les nouveaux usages ne pourront pas être stoppés
  - Usage personnel de smartphones professionnels (installation d'applications non-professionnelles)
  - Usage professionnel de smartphones personnels (consumérisation)
  - Le parc devient multiplateformes *de facto*
- Les réflexes historiques de sécurité « tout restreindre » ne conviennent plus
  - Les solutions jugées trop sécurisées sont rejetées par les utilisateurs
  - Les risques doivent être évalués différemment en fonction de la plateforme et des usages
- Des méthodes de sécurisation innovantes existent et se développent
  - Les nouvelles plateformes de gestion de flotte
  - Les silos applicatifs portant leur propre sécurité
- L'existence de solutions innovantes permet d'atteindre une cible sécurité
  - Pouvant être un « compromis » dans un premier temps
  - Qui sera amenée à se renforcer au fil des années

La sécurité se doit **d'autoriser ces nouveaux usages** et de **proposer des solutions réalistes** pour les accompagner

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

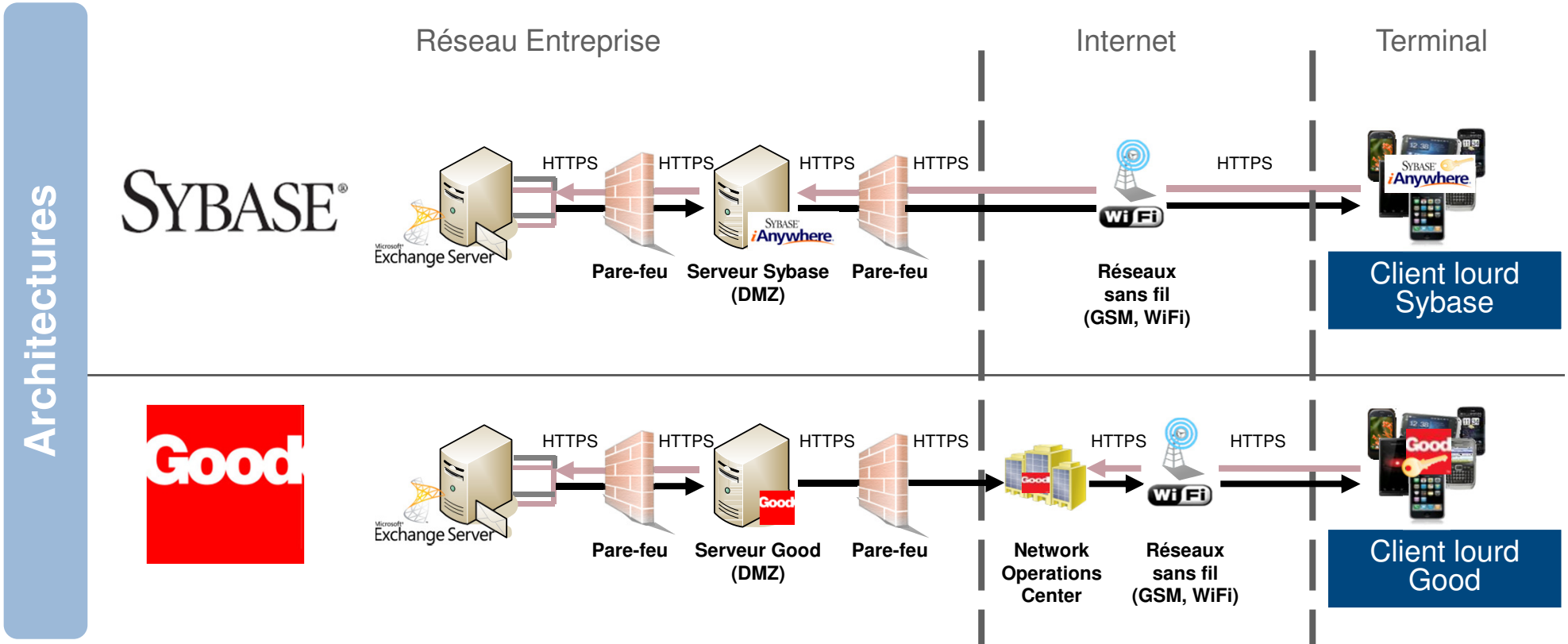
Contacts

Gérôme BILLOIS
Responsable de département
Tel : +33 (0)1 49 03 27 45
Mobile : +33 (0)6 10 99 00 60
Mail : gerome.billois@solucom.fr

Chadi HANTOUCHE
Consultant Sécurité
Tel : +33 (0)1 49 03 25 87
Mobile : +33 (0)6 22 41 22 05
Mail : chadi.hantouche@solucom.fr

Usage personnel
Les acteurs des applications dédiées

- Deux acteurs principaux du marché identifiés à l'heure actuelle : **Sybase** et **Good Technology**
- Deux principes d'architecture différents : **avec ou sans NOC**



30 novembre 2010 - Propriété de Solucom, reproduction interdite