



Architect of an Open World™

Réflexions sur le B.Y.O.D (smartphones, tablettes, ...)

Bruno OLLIVIER,
Sécurité Groupe

11/06/2013

LIBERATE IT

Sommaire

- L'intrusion des (nouveaux) terminaux dans nos S.I
- Motivations personnelles au BYOD
- Motivations de l'entreprise à aller vers le BYOD
- Analyse comparative sur l'introduction du BYOD
- Préoccupations pratiques
- Nouveaux risques ou mesures & Paradoxes
- Autres supports de réflexion

Toute ressemblance avec la réalité serait tout à fait fortuite

L'intrusion des (nouveaux) terminaux dans nos S.I

- Premier accroc au principe de la « maîtrise totale »
Mise à disposition d'un Extranet (**Use YOD**)
 - Pour tous et en particulier personnel en clientèle
 - Pour des applications web pas / peu / pas trop sensibles ...
 - *Pression pour applications à risque*
 - Panel de terminaux « sans limite », ergonomie + ou - bonne
- Terminal *externe* hors de nos murs (VPN IpSec)
 - Arrangement pour travail à la maison (développement..)
 - Accès en mode terminal de OK (CD bootable) à moins bien
 - Accès crise (H1N1 => VPN filtré + bureau à distance)
- Terminal *externe* au bureau (réseau interne)
 - Stagiaire avec PC ou MAC, Externes (infogérant, ...)
 - MAC (tous modes) et la panoplie associée, tablettes (VIP ...)
 - Autres intrus ? (bornes WiFi)
- GSM personnel voire bi-SIM

Motivations personnelles au BYOD

Rationnelles (pratiques) ou subjectives (image...)

- Equipement en substitution du PC (Any Type of Device)
 - Démarre plus vite et/ou plus performant
 - Plus léger
 - Meilleure autonomie
 - Meilleure esthétique
 - Ergonomie
- Famille des tablettes et smartphones
 - Légèreté, encombrement et autonomie - TOUT en UN
 - Manipulations plus simple lors de voyages, présentations
 - Connectivité native (3G, WiFi)
 - Ergonomie (écran tactile)
- Ne pas s'encombrer avec de multiples terminaux (tél & PC perso., pro. + voire « kit » crise)

Motivations de l'entreprise à aller vers le BYOD




















- Financières
 - Activité ne nécessitant pas de PC (fabrication, en clientèle...)
 - Support disparaissant:
 - Casse, perte, vol
 - Entretien et utilisation du terminal
 - *Reste le support:*
 - *pour l'accès aux applications et le fonctionnement du S.I applicatif*
 - Abonnement Clé 3G, Blackberry, GSM
 - Usage abusif
 - Validation détention «luxueuse» (ex: pas de Blackberry pour tous)
- Productivité et Satisfaction de l'employé
 - Avec le BYOD, l'employé compense les conséquences d'une gestion de masse (quelques modèles pas adaptés à tout)
 - Nécessité culturelle de OD inversement proportionnelle à l'âge

Analyse comparative sur l'introduction du BYOD

Mesures classiques

- Mesures / stations
 - Durcissement (Windows, LINUX)
 - Patch de sécurité
 - Anti-malware, intrusion, pare-feu
 - Gestion accès utilisateur / admin.
 - Chiffrement local/partagé/mail
 - Navigation Web filtrée
 - Supports amovibles
 - Audit/inventaire station
 - SSO local
- Mesures / réseaux
 - NAC pour station
 - Identification à partir des @IP
 - IDS (recherche d'intrus/marque...)
 - Isolation des réseaux

BYOD (nouveaux outils =>)


















- Grande diversité 
 - Parfois natif  réaliste sinon? 
 - Automatisation native  ou = 
 - Besoin management centralisé 
 - Accès incertain >> container 
 - Portabilité de la solution 
 - Mixité perso / pro 
 - Nativement impossible  ou 
 - Irréaliste/variété >> container 
 - Mixité perso./pro. voire déport 
- Accès Interne ou Externe? 
 - Si OD intégré  sinon 
 - Si interne alors authentification 
 - N'a plus de sens 
 - Nouvel Accès « WLAN OD » 

Analyse différentielle sur l'introduction du BYOD

Mesures classiques

- Mesures / Serveurs
 - Durcissement (Windows, LINUX)
 - Patch de sécurité
 - Anti-malware, intrusion, pare-feu
 - Gestion accès utilisateur / admin.
 - Chiffrement partagé
- Mesures / Services
 - SSO Web
 - SSO Windows
 - Webmail
 - Possibilité de mode hors connexion
 - Extranet
 - Applications internes
 - Publiable en externe
 - Limitée à l'interne (au sens réseau de confiance)

BYOD sans nouveaux outils

- Serveur en + / passerelles 
 - Inchangé 
 - Inchangé 
 - Inchangé 
 - Inchangé 
 - Selon orientation avec OD 
- Adaptation de services 
 - Compatible à 99% 

 - Selon OS, centralisé? 
 - Compatible à 99% 

 - Si isolation / privé 
 - Selon moteur applicatif 
 - Habillage Web (SSO Web?) 
 - Rejoint l'extranet 
 - Accès VPN en plus? 

Préoccupations pratiques

- Réglementation:
 - Bonnes pratiques obligatoires encore praticables? (principes, règles, instructions deviennent inadaptées)

- Légalité:
 - Utilisation **professionnelle** de licence ou services grand public
 - Utilisation de licence « interne » sur terminal personnel
 - Extension usage copie licence sur poste personnel ?
 - Employeur tenu de fournir moyens de travail
 - Cas particulier: traitement du vol, casse (assurance?)
 - Avantage en nature?: URSAAF, impôt
 - Travail en dehors des heures de travail...

- Contractuel
 - Que dire à nos clients sur l'usage d' Any Type of Device?

Préoccupations pratiques

- **Fonctionnement:**
 - Réintégration des actifs en cas de départ
 - Contrat cadre d'achat pour les employés
 - Panne = perte productivité du fait de l'employé? secours?
 - Compétence BYOD variable selon employé => BYOD < 100%
 - Règles séparation données personnelles et d'entreprise
 - Le moyen de géolocalisation devient natif – usage?
 - Adaptation de la charte sécurité de l'information
 - Responsabilité le l'employé dans son périmètre personnel

Préoccupations pratiques

- Monde du S.I – évolution
 - Gestion du réseau interne
 - Gestion du parc d'équipement (PC, tablette...)
 - Gestion des accès (authentification forte simple et efficace)
 - Adaptation méthode de développement, intégration...
 - >> station/réseau/serveur devient ATD/passerelle/serveur
 - Centralisation du stockage (généralisation mode déconnecté)
 - Quid de la sécurité basée sur l'isolation réseau?
 - Les équipements Mobiles ne sont que radio....

Nouveaux risques ou mesures & Paradoxes

- Nouveaux risques technologiques:
 - Ajout de solution coffre-fort électronique/passerelle (risqueVM)
 - Accès non autorisé au coffre-fort électronique déverrouillé
 - Mixité téléphone/internet + webcam/microphone
- Risques/mesures prenant une nouvelle dimension
 - Relatifs aux lieux d'utilisation et de stockage du Device (fourni par entreprise ou non)
 - « Effacement (utopique?) informations locales » sur départ, vol...

A expérimenter ? ...

- Paradoxes
 - Plus il y a de mesures coercitives en place, plus l'introduction de l' ATD va nécessiter d'adaptations
 - Any Type of Device conduit vers une amélioration de la prise en compte technologique de la sécurité (protection rapprochée)

ATD \longrightarrow Cloud - tout miser sur les VM ???

Merci de votre attention

Autres supports de réflexion

- Télécom & Devices

Evolution des usages et des offres

Ou des offres et des usages?

- C'est quoi l'ère post PC ?
- Orientations possibles
- Une opportunité pour les offreurs (sources de risques?)
- Web-ographie (2012)

C'est quoi l'ère post PC ?

PC

Personnal Computer

>> = Individuel <<

- Affichage, Parole et son
- Pointage (... , écran tactile)
- Claviers réels / virtuels
- Webcam
- Capteurs spécialisés

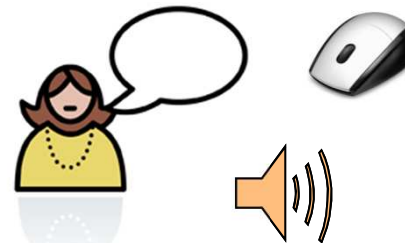
Nouveaux Terminaux

Traitements
Stockage

Interne et externe



Interfaces
Utilisateur



Amélioration continue sur l'ergonomie et la simplicité d'utilisation

Effet domino depuis le grand public vers le professionnel

1

Notre Système d'Information est-il adapté à ceux-ci? (IHM + accès)

Orientations possibles pour le Any Type of Device

- Le ATD en complément du poste de travail
 - Approche Extranet en continuité de l'existant
 - Poursuite extranet-isation web du S.I pour les services pertinents et acceptable dans ce mode
 - Pas de Stockage sur ATD sauf éventuellement via système applicatif intégrant ce service avec protection mode « coffre-fort électronique »
 - Avec stockage sur terminal
 - Approche Coffre-fort électronique en plus de l'existant
 - Extranet incluant une gestion sécurisée du stockage sur terminal
 - Probable préoccupation de ROI du **Total** Cost of Solution & Use
 - Une nouvelle forme de machine virtuelle apparaît...
 - . Lancement sous Navigateur Web
 - . Voire VM lancée par l'utilisateur sous l'OS
 - Approche Solution de gestion de parc hétérogène
 - = Démarche orientée réglementation et bonne pratique (maitrise)
 - EST-CE REALISTE ?

Orientations possibles pour l' Any Type of Device

- L' ATD comme poste de travail unique
 - Soit plus aucune donnée en local et extranet total
 - Requiert une connectivité permanente....
 - Soit un mode mixte - en central et avec données en local
 - Les solutions coffre-fort électronique (et PKI) via passerelle ou native ONT-ELLES DE L'AVENIR ?

- Choix du Any Type of Device
 - Equipement personnel:
 - Difficile de limiter marques et modèles
 - Probable que quelques caractéristiques minimales soient requises
 - Equipement fourni par l'entreprise
 - Fourniture de PC jusqu'à ce qu'il devienne un simple terminal Web
 - Puis fourniture terminal adapté au métier « instal. constructeur »

Une opportunité pour les offreurs ...

ZDNet IT Management	Comment faire cohabiter le BYOD et le parc applicatif de l'entreprise	07/06/2012 07:09
Cisco	Webinaire : Les enjeux du BYOD avec IDC et Cisco	05/06/2012 10:06
ZDNet IT Management	Débat - Du Bring au Buy your own device (BYOD), l'évolution de trop ?	17/05/2012 07:07
Login People	BYOD : Votre réseau est-il prêt pour l'accès mobile ?	10/05/2012 12:05
Good Technology	Watch a video on BYOD Security	18/04/2012 17:10
Les Actus de L'Informaticien	RIM & le BYOD, Apple poursuivi, Profit Warning Nokia, Panne Telehouse, Office Symbian...	12/04/2012 16:31
Good Technology	Reminder for our BYOD Mobile Security Webinar April 17	10/04/2012 16:29
Good Technology	Join Our BYOD Mobile Security Webinar	03/04/2012 16:29
Good Technology	Interactive quiz: Test your knowledge on secure BYOD.	20/03/2012 15:24
Good Technology Marketing	BYOD: Four Ways to Mitigate the Financial Risk of Mobile Devices.	22/02/2012 19:14
Wyse Technology	L'approche BYOD (Bring Your Own device – Apporter votre propre périphérique)	13/02/2012 12:08

Web-ographie

- <http://blog.markess.fr/2012/05/drh-collaborateurs-face-aux-reseaux-sociaux-applications-mobiles-collaboratives.html>
- http://www.pcworld.com/businesscenter/article/246760/pros_and_cons_of_bringing_your_own_device_to_work.html
- <http://nakedsecurity.sophos.com/2012/03/05/bring-your-own-practical-advice-for-handling-smartphones-in-the-workplace/>
- <http://www.techrepublic.com/blog/10things/10-myths-of-byod-in-the-enterprise/3049>
- <http://resources.infosecinstitute.com/tips-managing-byod-security/>
- <http://www.itrnews.com/articles/132941/phenomene-byod-va-amplifier.html>
- <http://www.zdnet.fr/blogs/green-si/byod-et-si-finalement-ce-n-etait-pas-le-probleme-de-la-dsi-39772390.htm>
- <http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2012-Byod-Synthese.pdf>
- <http://www.lemondeinformatique.fr/actualites/lire-le-clusif-se-penche-sur-le-phenomene-du-byod-49112.html>
- <http://www.lemondeinformatique.fr/les-dossiers/lire-securite-des-terminaux-mobiles-nouveau-casse-tete-pour-les-entreprises-508.html>
- http://www.gartner.com/technology/reprints.do?id=1-1AKF6MH&ct=120517&st=sb&mkt_tok=3RkMMJWWfF9wsRokuq3KZKXonjHpfsX56OQsXq%2BwIMI%2F0ER3fOvrPUfGjl4ATMJql%2FqLAzICFpZo2FFfFe%2BR
- <http://www.commentcamarche.net/faq/33899-byod-les-terminaux-mobiles-personnels-dans-l-entreprise>
- <http://www.journaldunet.com/solutions/dsi/bring-your-own-device-gerer-les-risques/bring-your-own-device-gerer-les-risques-techniques.shtml>



Architect of an Open World™

LIBERATE IT