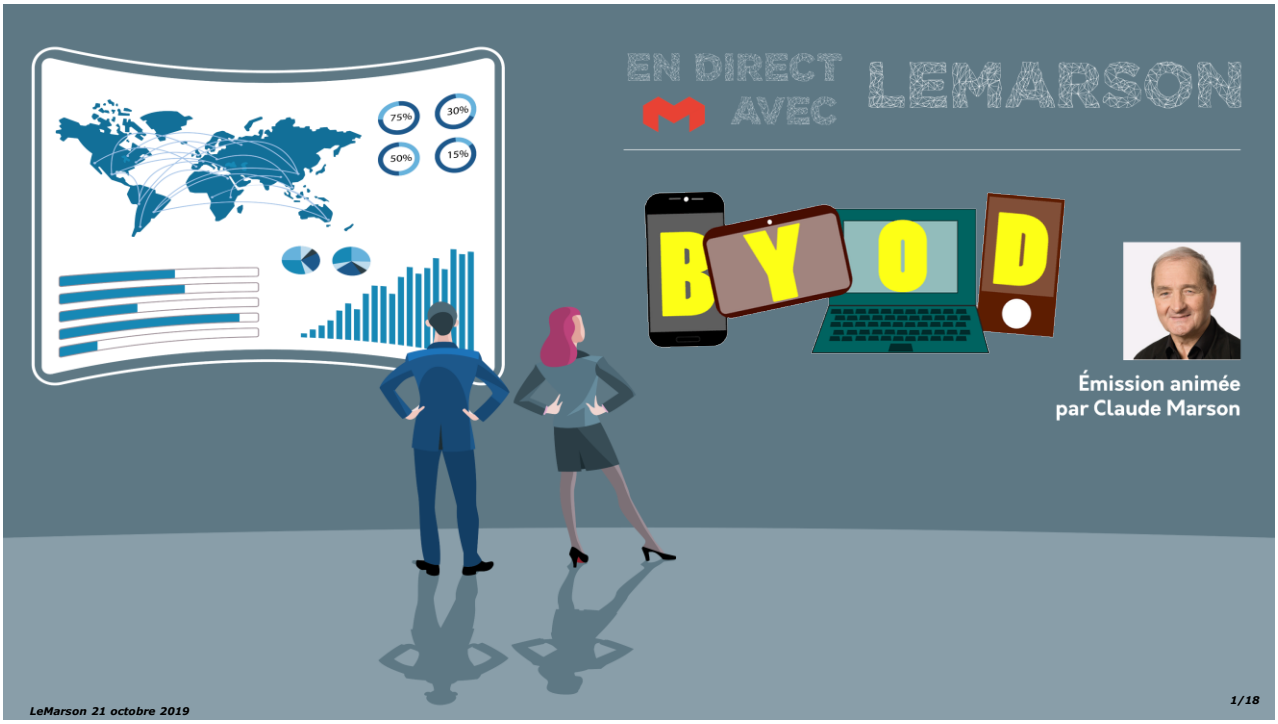
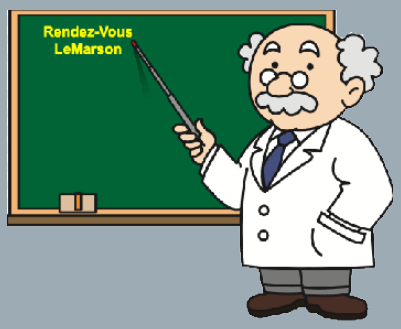


Le sommaire aujourd'hui

- Le BYOD et la méthode Coué
- Le sentiment général
- Les avantages du BYOD
- Les inconvénients du BYOD
- BYOD et l'impossible administration
- Les problèmes spécifiques de sécurité
- L'intégration forte des mobiles : l'indispensable annuaire LDAP
- Si on ne peut pas faire autrement
- Compartimentage d'usage
- Le chiffrement des données confidentielles
- Mise en œuvre d'un VPN
- Une seule architecture de développement
- Les 12 règles de base du BYOD : si vous y tenez vraiment…
- De notre point de vue



Le BYOD et la méthode Coué

- **Pratique qui consiste à utiliser ses équipements personnels dans un contexte professionnel.**
- Etude Forrester de 2013 : 70 % des usagers se servaient de leur mobile dans leur entreprise
- Sous la pression des fournisseurs et marketers (Forrester, Gartner…), les responsables TI se sont cru obligés de répondre à cette évolution
- Selon Forrester (2013), 66 % des employés utilisaient leurs appareils et applications personnels pour pallier aux lacunes de leur entreprise et 81 % ignoraient les interdits pour échanger avec leurs clients et collaborateurs. Un phénomène observé à tous les niveaux de responsabilités, et pas seulement chez les salariés de la génération Y…
- Méthode Coué, qui consiste à se persuader d'un fait, sentiment ou attitude, même si elle est contraire à la logique
- Le Gartner a procédé en juin 2014 à une étude portant sur 4.300 entreprises importantes, qui donne un certain nombre de chiffres concernant le BYOD.

Le sentiment général

IT Manager
Grosses désillusions
Le mobile n'entre pas dans le cadre de la stratégie mobile de l'entreprise
La sécurité et la confidentialité des données n'est plus garantie
L'exposition au piratage est plus grande

Ressources Humaines
Les employés sont satisfaits
L'ambiance est plus sereine
Meilleur sentiment de participation et d'intégration dans l'enetreprise

Directeur financier
Moins de pertes et de vols
Moins de dysfonctionnements (comme c'est bizarre…)

L'introduction du BYOD véhicule de grands espoirs à la fois de cdertaines directions opérationnelles et des utilisateurs.
Seuls les DSI sont plus circonspects quant à la finalité des opérations.

Directions opérationnelles
Se sentent mieux écoutées
Meilleure continuité de service
Plus grande confiance vis-à-vis du TI

Utilisateurs de LEUR mobile
MON smartphone
MA tablette

Les avantages du BYOD

- Les usagers veulent de la flexibilité et refusent d'être contraints par des règles d'usage des mobiles
- Durées d'apprentissage des nouveaux outils et applications moins important : on reste dans un cadre connu
- Meilleure productivité sur ce que l'on faisait : on gagne du temps
- On travaille plus, plusieurs journées rapportées sur une année
- Réduction des coûts "matériels" : estimation à 350 $/an/employé
- Correspond à l'usage des mobiles en déplacement et en télétravail (ce n'est pas la peine de rester chez soi pour travailler si c'est pour être encore plus contraint qu'au bureau !!!)
- Réduction de l'empreinte écologique… pas vraiment convaincus
- On est généralement plus à jour techniquement, alors qu'en entreprise, il faut passer par une phase de validation qui peut être longue : un décalage de plusieurs années par rapport aux modèles les plus récents, est chose courante
- Fait bénéficier l'entreprise de la "virtuosité" des dernières générations, rompues aux nouvelles pratiques
- Bon pour l'image de marque de l'entreprise : plus ouverte et résiliente, à l'écoute de ses employés

Les inconvénients du BYOD

- Une certaine inégalité liée aux différences d'équipements : syndrome de l'uniforme, faut-il que tout le monde ait le même ou au contraire, chacun peut-il improviser, ce qui aura un impact sur la productivité, la différence peut être un avantage
- La crainte que les usagers soient distraits par les applications, contenus personnels et réseaux sociaux (l'étude IBSG de Cisco en 2012 semble prouver le contraire)
- Coûts et difficultés de mise en place et de maintenance élevés, nécessité de disposer de compétences plus "universelles" dans l'entreprise
- Impossibilité de disposer d'un MDM adéquat, toujours en retard
- Problèmes potentiels juridiques, techniques et administratifs
- Répercussions "évidentes" sur la vie privée des utilisateurs : syndrome du mobile qui envahit tout, frontière entre vie privée et professionnelle plus floue…malgré les bonnes résolutions
- Les utilisateurs peuvent être amenés à participer aux frais
- De nombreux usagers n'apprécient pas que leurs données personnelles : photos, commentaires dans les réseaux sociaux, musiques, soient accessibles (hors virtualisation). Ils préfèrent les mettre dans un Cloud personnel… hors d'atteinte.
- Impossibilité de garantir l'accès au patrimoine applicatif de l'entreprise.
- Et surtout graves dangers liés au manque de sécurité : il est impossible de gérer un parc que l'on ne connaît pas.

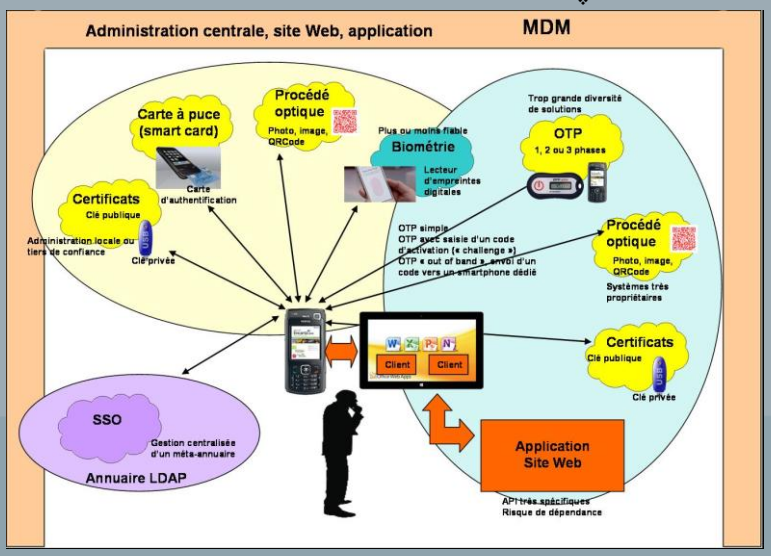
BYOD et l'impossible administration

- Dans une entreprise, avec des milliers de mobiles, il est impossible de laisser les usagers accéder aux applications sensibles avec leur équipement personnel
- Le mobile DOIT entrer dans un moule global, celui d'un MDM (Mobile Device Management)
- Le MDM est un prérequis indispensable à tout déploiement de tablettes et smartphones
- Dans l'absolu, un MDM vis-à-vis des mobiles…
- MDM reste compliqué à mettre en place et ce n'est pas un succès planétaire

Les problèmes spécifiques de sécurité

- Enquête de CheckPoint : sur 700 professionnels interrogés dans le monde (Amérique du Nord, Australie, Europe), 95 % se sentient menacés par des problèmes de sécurité et 42 % estiment que le BYOD a entraîné plus de 250 000 $ de frais liés à l'absence de sécurité
- Etude Kensington
- Il se perd 5 000 laptops, smartphones et tablettes tous les mois dans les aérogares au niveau mondial, qui ne sont pas réclamés et s'entassent dans les hangars
- De nombreux employés ne respectent pas les contraintes de sécurité et accèdent avec leur mobile à des applications sensibles, dans des lieux où ils ne devraient pas le faire
- Les nouvelles contraintes règlementaires, type RGPD peuvent entraîner des frais supplémentaires, voire être difficiles ou impossibles à implémenter
- La nécessité de contrôler les données manipulées et le contexte dans lequel elles le sont, peut induire des contrôles mal perçus et nuire au droit à la vie privée

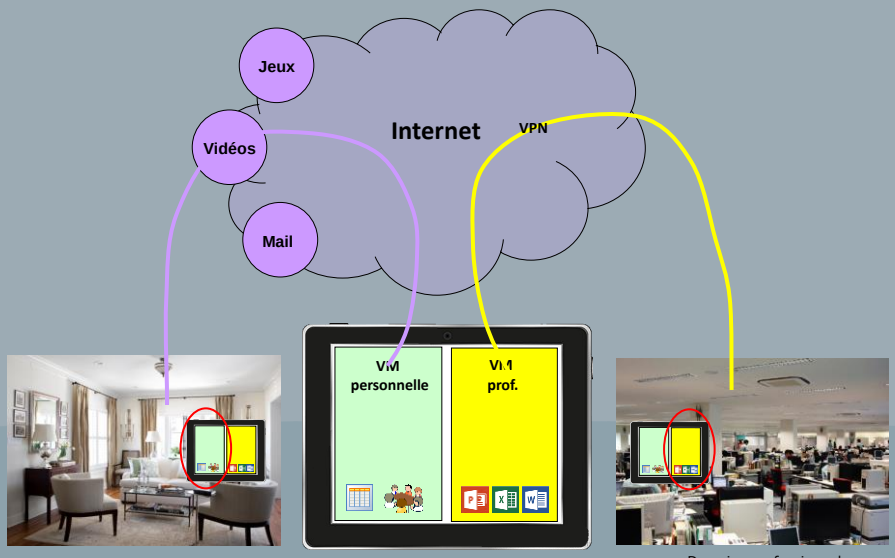
L'authentification forte des mobiles : indispensable LDAP



Si on ne peut pas faire autrement…

- Virtualisation des contenus pour isoler les machines virtuelles entre elles, professionnelle et personnelle, de manière à limiter le risque de pertes et de pollution des données, l'inquiétude principale des administrateurs d'aujourd'hui
- Applications webisées : transformer le mobile en terminal HTML5, sur lequel rien n'est installé (API), hormis l'indispensable pour faire tourner l'application HTML
- Passer par un VPN pour se connecter aux ressources de l'entreprise
- SSO doublé d'une politique intelligente des données d'identification
- Sécurisation des flux, via des antivirus et pare-feux
- Chiffrement des données confidentielles : il faut pouvoir le faire sur le mobile
- Mise en place d'une organisation, d'un service support, de procédures d'alertes et d'un véritable outil de gestion de la flotte de mobiles
- Politique de mots de passe renforcés ou disparition
- Procédures à suivre en cas de pertes ou de vols

Compartimentage d'usage des mobiles



Domaine personnel

L'espace tablette est divisé en deux machines virtuelles

Domaine professionnel

Le chiffrement des données confidentielles

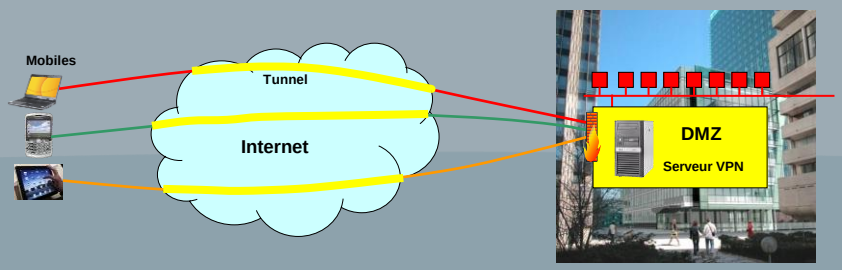
- Le mobile pose un double problème
  - L'identification de son propriétaire
  - La confidentialité des données stockées localement
- Le chiffrement permet de traiter différents aspects
  - La confidentialité : il ne faut pas que les données puissent être lues par un tiers
  - L'intégrité : il ne faut pas qu'un tiers puisse les modifier
  - L'authentification : il faut s'assurer que celui qui se connecte avec son mobile est bien celui qu'il prétend être
- Les types de chiffrement
- Pour chiffrer un contenu de smartphone, tablette ou netbook
- Pour authentifier le « propriétaire » des données, on peut passer par un système de signature électronique : empreinte chiffrée par la clé privée du signataire

PGP peut être utilisé sur Android et iOS pour sécuriser les accès et contenus

Le certificat stocké dans un mobile est fourni par un tiers ou une PKI (liée au MDM) locale et comporte une bi-clé privée et publique et des données qui seront vérifiées par le demandeur : connexion à une application Web (certificat du site), identité d'un partenaire

Mise en œuvre d'un VPN

- Un VPN : Virtual Private Network (RPV : Réseau Privé Virtuel) est un tunnel établi dans un réseau public, généralement Internet, pour assurer la pérennité des connexions en provenance des mobiles des utilisateurs.
  - On dit qu'il s'agit d'un tunnel car les trames émises par les mobiles sont encapsulées dans de l'IP Internet et restituées dans la forme adéquate à l'arrivée.
  - Connexion point à point.
- Il assure trois grandes fonctions



Les huit formes de développement mobile…

Mais n'en privilégier qu'une seule

Dans le cadre d'un BYOD renforcé et de développement d'applications spécifiques, il ne faut rien laisser sur le mobile et fonctionner uniquement en mode HTML 5
Attention à ne pas dépendre localement d'une API JavaScript

Les 12 règles de base du BYOD …si vous y tenez vraiment

- Elaborer un cadre "légal" d'usage BYOD
- Sensibiliser les utilisateurs sur les risques qu'ils prennent
- Connecter l'ensemble des mobiles à l'infrastructure réseau
- Le processus de déclaration et d'insertion sera simple
- La configuration se fera en temps réel
- De nombreuses fonctions seront accessibles en self service

EN DIRECT AVEC LEMARSON

Les 12 règles de base du BYOD …si vous y tenez vraiment

- Un soin particulier sera apporté à la protection des données d'identification des utilisateurs
- Statuer sur les applications à interdire : scanning IP, mutualisation de données, DropBox…
- En cas de départ d'un employé, les données entreprise seront protégées, alors que les mails personnels, applications, photos et autres informations personnelles resteront inaccessibles
- Mécanismes de protection adaptés aux contextes
- Etre à même de gérer les volumes de données en transit dans et hors réseau d'entreprise
- Faire du ROI un argument en faveur du BYOD

De notre point de vue

- Il y a des signes clairs de retournements de tendances et l'usage des terminaux en mode BYOD a fortement diminué ces dernières années
- Enquête CompTIA
- Ce n'est la mort du BYOD, mais une forte diminution d'usage
- Deux néologismes pour le remplacer :
  - CYOD ("Choose Your Own Device" : les employés choisissent leur terminal dans un vaste gamme proposée par l'entreprise, mais il faut explicitement les autoriser à l'utiliser dans un cadre personnel
  - COPE ("Corporate Owned, Personnally Enabled") : les employés sont explicitement autorisés à utiliser leur terminal d'entrise à des fins personnelles, mais ils sont responsables des installations et du support courant de l'appareil
- Il ne faut pas confondre domicile et entreprise
- La montée des attaques implique de mieux se protéger : il faut commencer par les mobiles et appliquer une politique draconienne de suivi et de contrôle : ce n'est pas suffisant mais nécessaire

Flexibilité, peu de contraintes	7	Contre l'uniformité	3
Apprentissage court	3	After hours	9
Meilleure productivité	8	Maintenance élevée	9
Périmètre de travail élevé	8	Impossibilité MDM	9
Coûts matériels réduits	7	Problèmes juridiques	8
Philosophie télétravail	2	Vie privée	9
Empreinte écolo	1	Participation aux frais	9
A jour techniquement	1	Partage inadéquat données	9
Virtuosité usagers	3	Garantie d'accès	9
Image de marque	2	Sécurité	10
	42		84

Dix critères pour et contre, pondérés de 1 à 10.
Les inconvénients du BYOD sont évalués au double des avantages.
Les pondérations sont contestables.

Nos prochains rendez-vous

EN DIRECT AVEC LEMARSON

Mercredi 13 novembre 2019 : **Actualités**
Mercredi 18 novembre 2019 : **Transformation digitale, restons sérieux…**
Vendredi 29 novembre 2019 : **Les nouveaux concepts du datacenter : SaaS, FaaS, serveurs désagrégés…**
Vendredi 6 décembre 2019 : **Actualités**
Vendredi 13 décembre 2019 : **Programmation fonctionnelle, de nouvelles pratiques à acquérir**

Je vous remercie de votre attention et à bientôt