BYOD Matériel personnel au travail et matériel professionnel à la maison : 12 points pour une bonne sécurité | Denis JACOPINI

Si l'on parle souvent des avantages et des désagréments du BYOD, la base reste après tout d'adopter la politique qui correspond aux besoins de l'entreprise. Cela permet ainsi de savoir si l'on applique un BYOD total ou un CYOD (Choose Your Own Device) voire un COPE (Corporate Owned, Personally Enabled).

Et pour arriver aux bonnes conclusions, il faut se poser les bonnes questions.

1. Le BYOD : mais pour qui ?
C’est en premier lieu une question fondamentale. Faut-il permettre le BYOD à l’intégralité des employés, ou juste certains métiers, uniquement les cadres voire seulement les principaux dirigeants ? Répondre à cette question est primordial avant de mettre en place une bonne politique de BYOD, car de cette réponse découleront bien des conséquences.

Il faut toutefois bien avoir en tête que si tout le monde n’est pas autorisé à pratiquer le BYOD, cela n’empêchera pas certains d’amener leurs appareils sans prévenir qui que ce soit, ce qui pourrait créer quelques complications par la suite. Intégrer une telle donnée est indispensable.

2. Quels appareils ?
Une fois le personnel concerné enfin déterminé, il convient de se poser une question équivalente sur les appareils. Faut-il tous les accepter ? Se limiter à une marque ou un système d’exploitation particulier ? Aujourd’hui, même si les Androphones et les iPhone captent la majeure partie du marché, cibler les appareils acceptés est aussi un élément majeur qui simplifiera la vie du DSI et du patron.

Par exemple, n’autoriser que des appareils sous iOS dont la dernière version a été installée impliquera une gestion moins complexe que de permettre tous les Androphones, vieux comme récents, qui ne fonctionneront même pas sous la même version d’Android et qui comptent des dizaines de marques différentes. Et la logique est similaire pour les tablettes tactiles.

3. Quelles applications ?
On connaît désormais qui pourra exploiter le BYOD et quels appareils seront concernés. Très bien. Reste désormais à régler la question tout aussi fondamentale des logiciels. Quelles applications seront acceptées ? Certaines bien spécifiques devront-elles être installées ? Seront-elles extérieures à l'entreprise ou programmées en interne spécifiquement pour les employés ? Est-il utile ou non de passer par une interface multi-OS et multi-écran à la Exo U ?

Là encore, afin de mettre en place une bonne politique de BYOD, toujours en fonction des besoins de l'entreprise, cibler les applications autorisées est primordial. Mais là encore, le risque que l'employé utilise d'autres applications est réel et doit être pris en compte. Plus on impose de limite et plus les mauvaises surprises sont multipliées. L'avantage de laisser une liberté totale est donc que les parades à cette liberté seront calculées.

4. Impliquer toutes les branches de l'entreprise
Une fois les trois premiers points enfin réglés, si l'on souhaite que la politique de BYOD se passe pour le mieux, il faut impliquer toutes les branches de l'entreprise. Que ce soit les ressources humaines, les juristes, évidemment le DSI, etc. Pourquoi ? Tout simplement, et c'est toujours la même chose, pour une question de besoin, mais aussi ici de précision.

Le responsable des RH apportera forcément un regard différent du DSI, qui lui-même ne pensera pas aux mêmes problématiques que le juriste. L'un insistera pour que les règlements quant au BYOD traient bien des différences entre les données privées et professionnelles. Un autre pensera à l'aspect technique, tandis que son voisin préviendra des différents risques de

plaintes.

5. Mettre en place une infrastructure réseau suffisante
Vous savez qui utilisera quoi et comment. Vous pouvez donc prévoir (à peu près) quel sera le trafic qui sera utilisé dans votre entreprise tous les jours. Et qui dit BYOD dit généralement une utilisation bien plus forte des réseaux mobiles, que ce soit en Wi-Fi ou en 3G/4G. Une augmentation qu'il faut donc prévoir si vous voulez éviter que vos employés commencent sérieusement à s'agacer des débits.

Sachant que certains employés peuvent avoir deux, trois voire quatre appareils en même temps connectés, il est capital de mettre en place l'infrastructure suffisante pour assurer un réseau de qualité. Augmenter ses débits fixes et obtenir des routeurs Wi-Fi puissants sera probablement indispensable. Il faudra de plus s'assurer que les forfaits mobiles des employés soient suffisamment volumineux.

6. Simplifiez, soyez clair et prévoyez
Lorsque vous allez commencer à mettre au point vos règles de politique de BYOD, il faut à la fois penser à la simplifier tout en prévoyant le futur. Faire simple, être direct et clair permet d'éviter les failles et les abus de ces dernières. Utiliser les mots justes et précis, c'est s'assurer que les règles seront bien appliquées.

Enfin, il faut absolument prévoir. Le marché évolue à grande vitesse et vos règles du jour ne seront peut-être pas viables dans trois ans ou peut-être même moins. Il faut donc là encore ne pas être trop spécifiques aux produits du moment et

généraliser afin d’englober les appareils et les applications du futur.

7. Lasécurité

C’est l’évidence même, on ne cesse d’en parler, c’est généralement la priorité numéro un des entreprises (BYOD ou non), la sécurité est un point majeur à régler. Elle dépendra évidemment des sujets 1, 2 et 3 évoqués dans notre précédent article, à savoir ceux rapportés aux utilisateurs de BYOD, aux appareils autorités et aux applications permises.

La sécurité pour le BYOD, ce sont des règles de bonnes conduites et des règles techniques. Que ce soit par rapport au cloud, à à l’accès aux données sensibles selon les réseaux utilisés, aux mises à jour des logiciels, aux mots de passe, aux protections, à la perte de l’appareil, etc. Tout doit être réglé au millimètre et prévoir toutes les catastrophes possibles est indispensable.

Et surtout, la sécurité implique un rapport de confiance entre l’employé et sa direction. La pire des situations seraient que l’employé se soit rendu compte qu’il a subi un vol de données et qu’il ne dise rien. La transparence et la rapidité sont ainsi indispensables pour assurer un maximum de sécurité.

8. La question des données personnelles

Outre le plan sécuritaire, celui du droit et du respect des données privées doit aussi être réglé. S’arranger pour séparer les données privées/personnelles des données professionnelles dans les appareils est ainsi plus que conseillé. L’entreprise doit le faire pour ses employés mais aussi pour elle-même, ne

serait-ce que pour éviter quelques désagréments et plaintes dans le futur.

9. Avoir la mainmise sur l’appareil

Certes, dans le cadre du BYOD, le PC portable, le smartphone ou la tablette appartient à l’employé. Néanmoins, comme pour les données personnelles, dès lors que le professionnel s’intègre dans l’appareil, l’entreprise a donc un droit de regard.

Il faut donc bien faire comprendre à l’employé que son appareil personnel peut être surveillé et que l’entreprise peut avoir accès à certaines données, y compris personnelles. Clarifier ce point dès le départ évite ainsi les mauvaises surprises.

10. Quelles solutions MDM ?

MDM, signifie Mobile Device Management, que l’on peut traduire en gestion des terminaux mobiles. Les solutions MDM sont indispensables pour toutes les entreprises (surtout les grandes) qui disposent d’une flotte importante d’appareils, qu’ils appartiennent ou non à l’employé par ailleurs.

Dans le cadre strict du BYOD, les solutions MDM ont souvent l’avantage d’être multiplateforme et sont l’une des armes pour sécuriser son réseau et ses données. Elles permettent en effet d’identifier les terminaux mobiles connectés, de les activer et les désactiver comme on le souhaite, d’installer des applications à distance, de les mettre à jour, de bloquer les appareils à distance ou des applications spécifiques, de géolocaliser les appareils, d’imposer des mots de passe ou

même le chiffrement des données, etc. En somme, un BYOD sans MDM paraît presque impensable.

11. En cas de casse ou de vol

Même si l'appareil n'appartient pas à l'entreprise, il faut néanmoins prévoir le cas où ce dernier casserait, tomberait en panne ou tout simplement serait volé. Les données présentes sur l'appareil ou disponibles à distance peuvent être sensibles et prévoir une telle éventualité est obligatoire quand on sait que les cas de casses et de vols sont nombreux.

Bien entendu, un système de blocage à distance est indispensable en cas de vol, tout comme le fait de chiffrer ses données. Pour la casse, moins il y a de données stockées directement dans l'appareil (sans copie en ligne), moins la situation sera catastrophique.

12. En cas de départ

Enfin, on n'y pense pas toujours, mais si l'employé vient avec son appareil, il repart évidemment avec en cas de départ, de fin de contrat ou de licenciement. C'est un point crucial à ne pas manquer dès le début de la politique de BYOD.

Il faut ainsi prévoir à l'avance le futur départ de l'employé et par conséquent le rapatriement de toutes les données qu'il détient, en sus de leur suppression sur son ou ses appareils. Dans le même esprit, il faudra donc l'empêcher d'avoir accès via ses appareils aux réseaux et serveurs de l'entreprise. Cela peut là encore éviter certains désagréments.

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
  - RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

DÉSIGNATION
N° DPO-15945

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé
et référencé

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041

84).
« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Source : http://www.zdnet.fr/actualites/12-points-a-traiter-pour-une-bonne-politique-de-byod-1-2-39804195.htm