Bring Your Own Device

11/06/2013

Vincent Toubiana

Expert à la Commission Nationale de l'Informatique et des Libertés

Définition

- **Traduit en « Apportez Votre Equipement personnel de Communication »**
  - A priori la définition exclue le télétravail
  - Définition du périmètre de l'entreprise

- **Une décision juridique rend la ligne floue:**
  - « Une clé USB, dès lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, est présumée utilisée à des fins professionnelles ».

Définition

Qu’est ce qui fait parti du BYOD?

- Connecter son smartphone sur le réseau de l’entreprise?
- Passer un coup de fil depuis son téléphone personnel?
- Utiliser son ordinateur depuis son domicile pour consulter ses mails professionnels?

Définition

- **On parle de BYOD si il y a une interconnexion :**
  - entre un terminal de l'employé et de l'employeur,
  - réalisée à des fins professionnelles.

- **Si cette interconnexion a lieu depuis le domicile de l'employé on parlera à la fois de BYOD et de télétravail.**

Déploiement courant

- **Un usage du BYOD qui est plus réactif qu'anticipé et proprement encadré par les entreprises.**

- **Le BYOD est souvent assimilé à une généralisation du télétravail**
  - Utilisation d'un terminal à l'extérieur de l'entreprise afin d'accéder à des ressources professionnelles.

- **Exemples de BYOD**
  - Consultation de la messagerie sur smartphone.
  - Accès au webmail depuis un PC.
  - Travaille à domicile sur un document professionnel transporté par un moyen quelconque (clé USB, email personnel, …).
  - Utilisation d'un ordinateur personnel lors d'un déplacement professionel.
  - Une employée apporte son propre ordinateur sur son lieu de travail et s'en sert pour un usage professionnel.

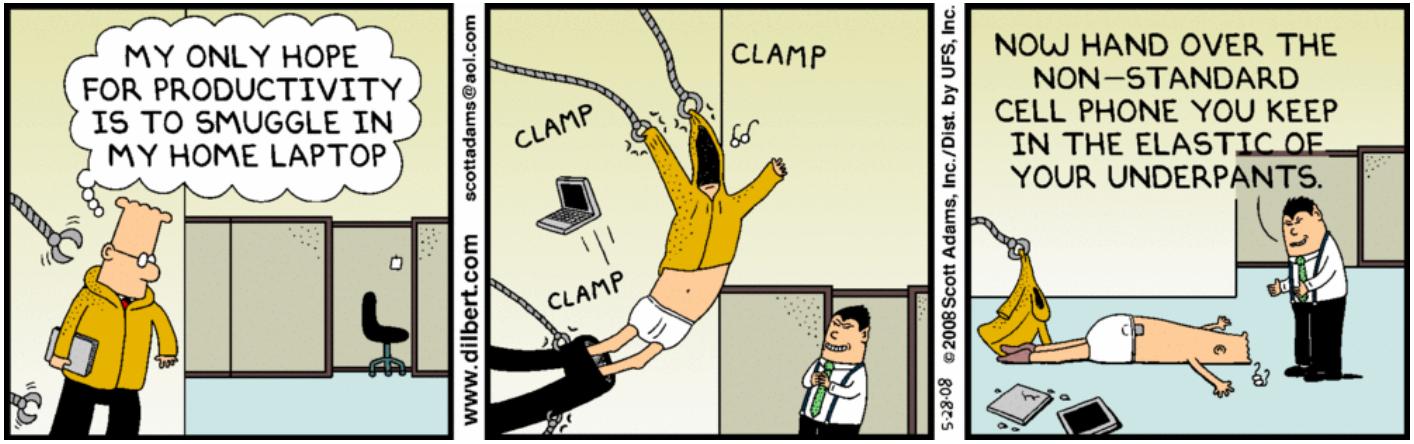
Sécurité et Vie Privée

- **Deux types de menaces à considérer :**

  - Sécurité des données personnelles: les données personnelles traitées par l'entreprise pourraient être compromises.

  - Données privée: les données privées des employés peuvent être divulguées à leur employeur via l'utilisation de leurs terminaux.

Dilbert's Time:
Sécurité des données personnelles



Risques pour l'entreprise

- **Sécuriser un parc informatique dont elle n'a plus l'entière maitrise :**
  - Amoindrissement de la politique de contrôle d'accès au réseau de l'entreprise,
  - Le terminal compromis d'un employé expose tout le réseau de l'entreprise (virus, chevaux de Troie),
  - Risque lié directement à l'utilisation de logiciel par un employé,
  - Possibilité qu'un employé s'approprie des données de l'entreprise.

Affaiblissement du contrôle d'accès aux ressources de l'entreprise

- **Risque: Les smartphones deviennent un point d'accès facilité aux ressources d'une entreprise**

- **Les web mails professionnels sont une forme de BYOD**

- **Nouveau marcher pour les applications de virtualisation**
  - Environnement virtuel dédié,
  - Code spécial pour accéder à l'environnement professionnel,
  - Possibilité d'effacement sans que les données de l'employé ne soient pas affectées,
  - L'employé ne doit pas jailbreaker (ou rooter) son téléphone.

Compromission d'un post de l'employé & Vol de donnée

Risque: Un employé apporte un terminal infecté

- Firewall inefficace: le virus se trouvera déjà à l'intérieur.
- Le terminal infecté tente de collecter les données de l'entreprise pour les repartager une fois connecté depuis le domicile de l'employé.

Comment adresser cette menace?

- Isoler les terminaux des utilisateurs sur un VLAN
- Agents de vérification en complément

Qui est responsable des logiciels installés

- **Qui est responsable pour l'utilisation illégitime de logiciel?**

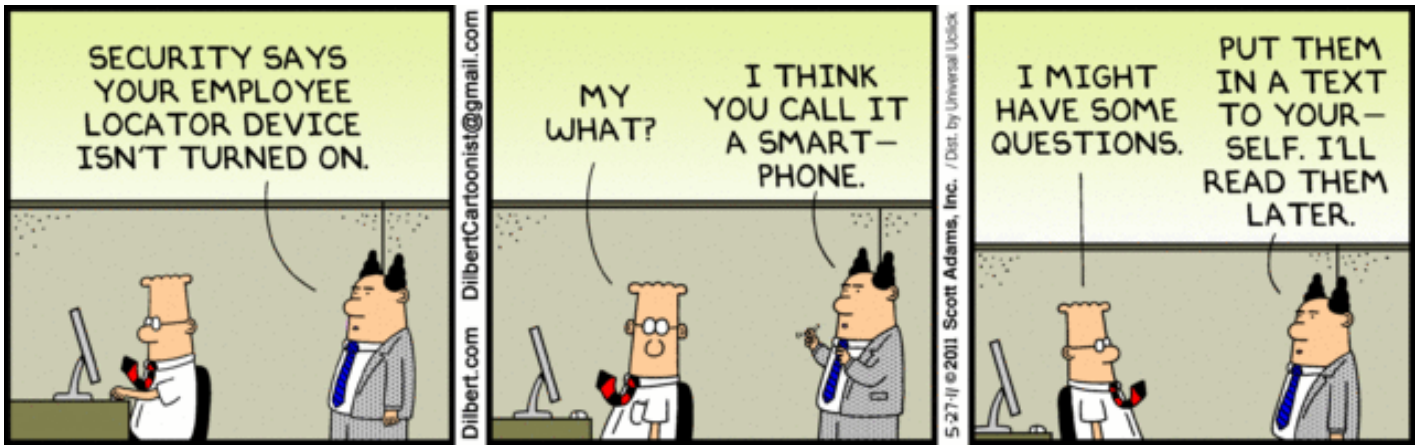
- **Peut on blacklister des applications sur les terminaux ne nous appartenant pas?**

- **Recommandation:**
  - **utilisation d'une session spécifique pour l'utilisation professionnelle**

Protéger les données personnelles et privées lors de voyage

- **Risque: Le terminal d'un employé est fouillé aux frontières**
- **Solution actuelle:**
  - **Effacer toutes les données sensibles du terminal**
  - **Chiffrer les données avec une passphrase inconnue de l'employé**
- **Comment sécuriser les données sur le portable de l'employé?**
  - **L'employer peut il ne pas connaitre le mot de passe d'accès à son terminal?**
  - **Comment effacées les données sur un smartphone?**
    - **Difficile de supprimer définitivement les données**
    - **Utiliser des cartes mémoires externes**

Dilbert's Time: Données privée



Définir le périmètre de l'environnement professionnel

- **Arrêt du 12 février 2013:**
  - **Une clé USB connectée à un ordinateur est considérée à usage professionnel**

- **En terme de BYOD, cela signifie-t-il que tout équipement apporté dans l'entreprise est à usage professionnel?**
  - **Peut on considérer que mon Smartphone est à usage professionnel dés lors que je me connecte au réseau wifi de l'entreprise?**

Définir le périmètre de l'environnement professionnel

- **Une clé USB a une seule finalité:**
  - **Le transport de fichiers**
  - **Tombe dans le périmètre professionnel dés lors qu'elle ne peut servir qu'à transporter un fichier de l'entreprise (si elle est connectée à un ordinateur de l'entreprise)**

- **Un ordinateur qui dispose de plusieurs fonctionnalités différentes ne serait pas nécessairement sujet aux mêmes règles.**

- **Recommandation**
  - **Considérer que sur l'équipement de l'employé tout est personnel à moins que ca ne soit explicitement marqué comme professionnel.**