BYOD VS RSSI

Le couple BYOD / RSSI est-il fait pour s'entendre ?

Conférence CLUSIS – Lausanne – 12 juin 2012

animé par Bruno KEROUANTON – RSSI Etat du Jura

© 2012 Bruno Kerouanton – GC Sécurité

CLUSIS

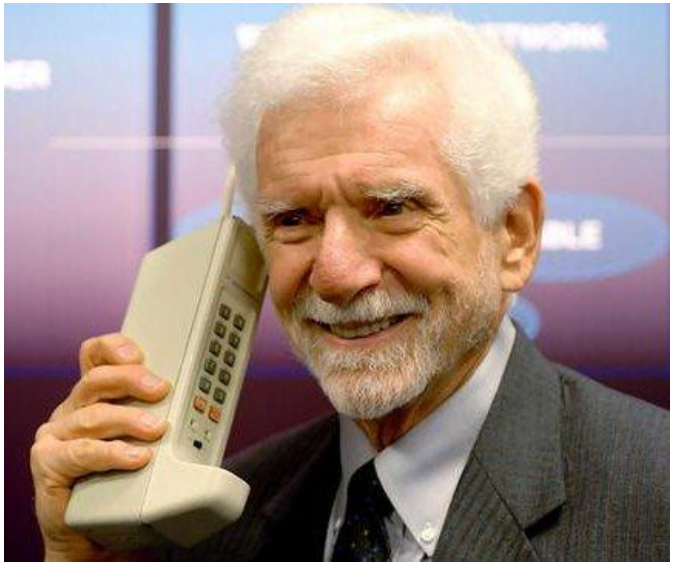
BYOD ?

Amenez vos propres équipements

Un concept anglo-saxon venu :

- De l'IT ?
- De la direction ?
- Des utilisateurs ?
- *Probablement pas du RSSI !*

(quoi que…)



© 2012 Bruno Kerouanton – GC Sécurité

Les 3 catégories de BYOD

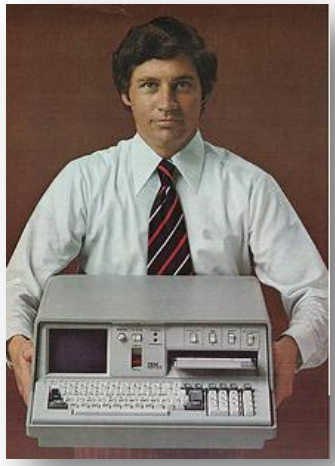
- Ordinateur (portable)

- Smartphone

- Tablette

© 2012 Bruno Kerouanton – GC Sécurité

BYOD



Une situation adaptée ?

– Oui pour les entreprises individuelles et PMI/PME *(Celles qui n'ont pas de RSSI…)*

– Partiellement pour les grosses organisations

(Celles qui ont un RSSI…)

© 2012 Bruno Kerouanton – GC Sécurité

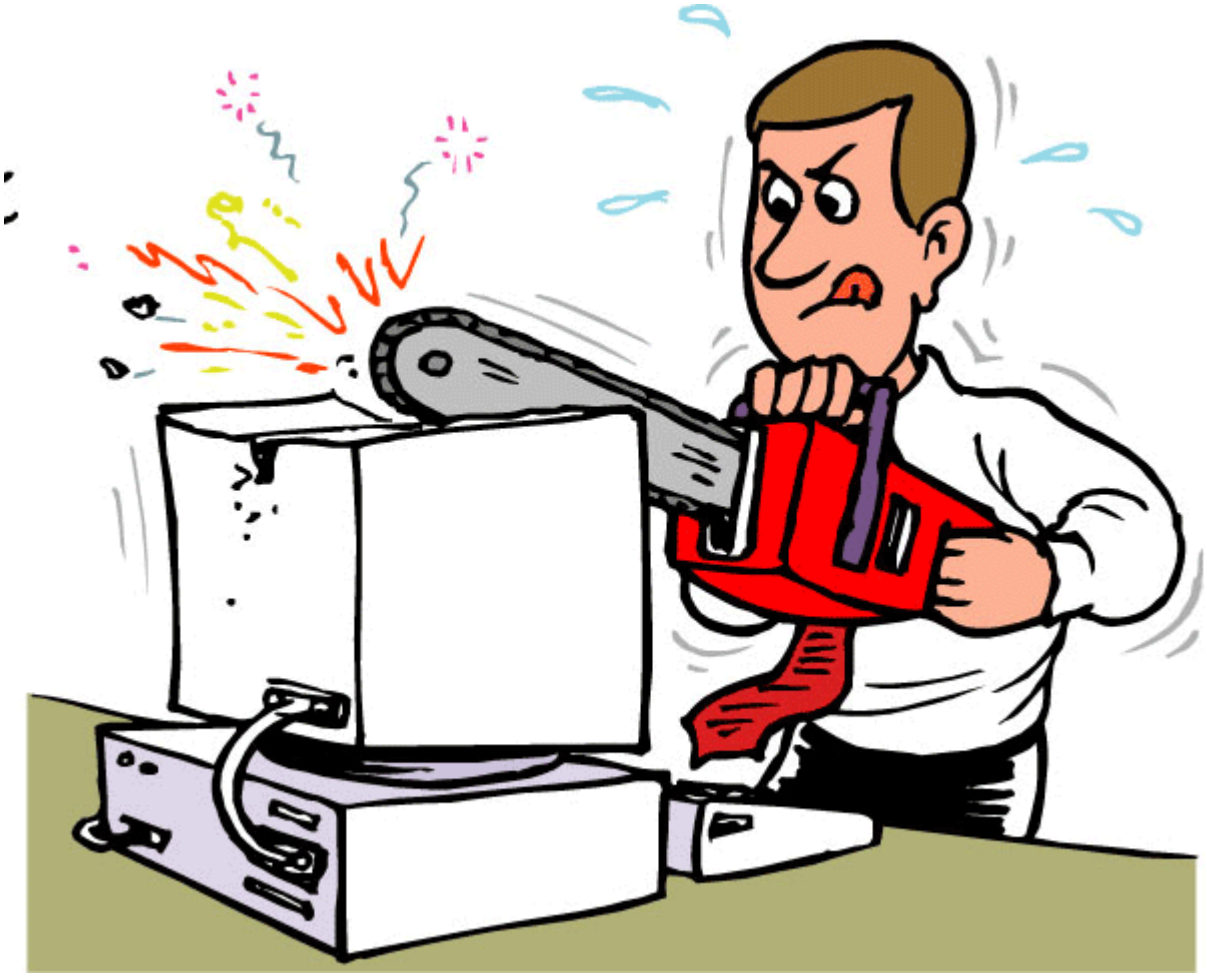
BYOD vs Télétravail

«Du bureau à la maison…
… A la maison au bureau»

- Reprend certaines bases
- **Enjeux… et problèmes similaires !**
- Quelles solutions adopter ?

© 2012 Bruno Kerouanton – GC Sécurité

Les risques



© 2012 Bruno Kerouanton – GC Sécurité

Responsabilités

- Vol/perte de l'appareil ➔ Qui assure ?
- Antivirus, pare-feu... ➔ Qui paie et configure ?
- Licences logicielles ➔ Qui est le «propriétaire» ?
- Mises à jour ➔ Qui s'en charge ?
- Support helpdesk ➔ Quelles sont les limites ?
- Utilisation familiale ➔ Qui définit les règles ?
- Utilisation «borderline» ➔ Comment agir sans risque ?
- Etc. etc. etc…

© 2012 Bruno Kerouanton – GC Sécurité

Un exemple : le p2p

- Un utilisateur apporte son PC portable au bureau.
- Logiciels de Peer-to-Peer installés, et lancés au démarrage.
- <u>Qui est responsable</u> :
  - en cas de téléchargements de fichiers illégaux ?
  - en cas de fuites de données ?

© 2012 Bruno Kerouanton – GC Sécurité

Un exemple : La famille

- L'ordinateur familial est utilisé au bureau

- Les enfants s'en servent également le soir pour jouer en ligne, télécharger et aller sur Facebook.

- Ils font fuir des documents professionnels par mégarde, voire par jeu…

- Ils récupèrent les licences des logiciels installés, et les partagent sur des réseaux peer-to-peer…

© 2012 Bruno Kerouanton – GC Sécurité

Un exemple : les forensics

- Un incident a eu lieu sur l'ordinateur personnel d'un employé
- Est-il légal d'investiguer sur celui-ci ?
- Quelles sont les conséquences ?

© 2012 Bruno Kerouanton – GC Sécurité

Un exemple : l'utilisation «borderline»

La jurisprudence…ne fait pas le moine !

Légalement, domaine flou

On ne peut reprocher à un employé d'apporter sur son ordinateur personnel du contenu pornographique…

Un vrai casse-tête pour l'employeur !

Le fait de consulter des sites pornographiques au travail peut-il justifier un licenciement pour faute grave ?

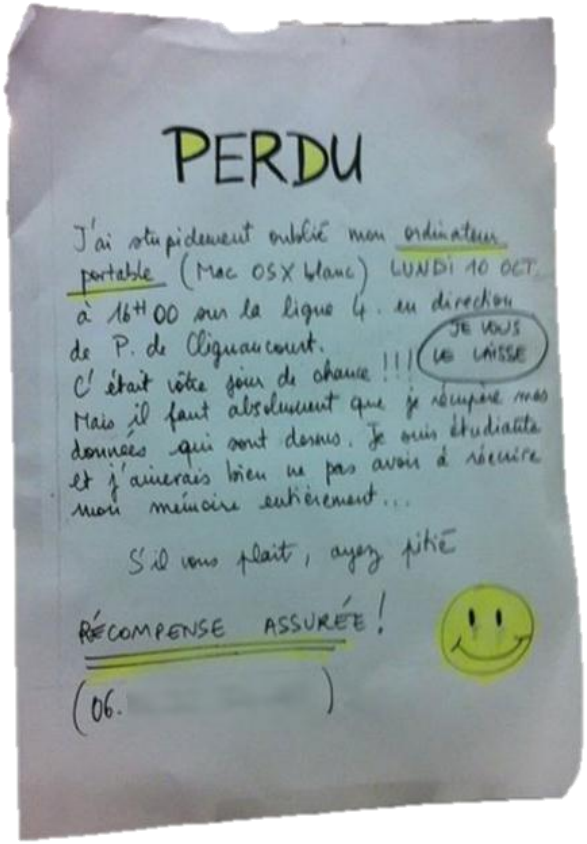
par SÉBASTIEN FANTI le 5 JUIN 2012 dans NEWS

La Cour de cassation française vient de rendre deux décisions intéressantes à plus d'un titre, décisions reproduite sur le site legalis.net.

Sans surprise, le fait de consulter de tels sites au moyen d'un ordinateur de l'entreprise pendant les heures de travail peut justifier un licenciement pour faute grave. Dans un cas, le licenciement pour faute grave a été considéré comme licite, l'employé ayant agi à réitérées reprises au vu de tout le monde. Le deuxième cas est révélateur du degré de responsabilité de l'employeur. La Cour de cassation a considéré, nonobstant le caractère objectivement plus grave des faits (une propagation de virus issue de la consultation avait endommagé le système informatique), que le licenciement pour faute grave n'était pas justifié. Le salarié avait signalé l'existence du virus et il existait dans cette entreprise une pratique ainsi décrite et qualifiée: « *constatant sans dénaturation que si le taux de téléchargements en provenance de son ordinateur était élevé, la pratique existait dans l'entreprise même en l'absence du salarié, elle (la cour d'appel dont la décision est querellée) a pu considérer que cette utilisation du matériel informatique professionnel en infraction au règlement intérieur à l'origine de la dégradation involontaire du système*

© 2012 Bruno Kerouanton – GC Sécurité

Un exemple : la perte



- Un utilisateur arrive le matin sans son ordinateur : Il ne le retrouve pas.
- Perte de productivité, le temps qu'on lui reconfigure un nouvel ordinateur.
- De plus, il se plaint que l'employeur a l'obligation de fournir les outils de travail.

© 2012 Bruno Kerouanton – GC Sécurité

Un exemple : la revente

L'employé veut un ordinateur plus récent,
il revend son ordinateur sur Ricardo.ch

Mais… il n'a pas effacé ses données…

Qui est responsable de la fuite d'infos confidentielles ?

© 2012 Bruno Kerouanton – GC Sécurité

Qu'en dit le RSSI ?

BYOD ? C'est inéluctable !

Le rôle du RSSI
est d'accompagner le changement,
pas de l'empêcher ;)

Soyons pragmatiques…

© 2012 Bruno Kerouanton – GC Sécurité

Des pistes

pour accompagner le changement :

- Des Mesures techniques

- Des Mesures organisationnelles

© 2012 Bruno Kerouanton – GC Sécurité

Informer

- L'employé doit être informé et sensibilisé face aux risques du BYOD

- L'employeur également doit l'être…

  Les Directions ne voient souvent que les avantages du BYOD

Ne pas interdire, mais rendre attentif

© 2012 Bruno Kerouanton – GC Sécurité

Responsabiliser

Le BYOD est un droit pour l'employé…

…il a donc des devoirs envers l'employeur

Acceptation et Signature d'une charte d'usage

Clarifier les limites du BYOD

© 2012 Bruno Kerouanton – GC Sécurité

Protéger

Utiliser des solutions techniques pour protéger les données

- Smartphone, Tablette :
  - Sandboxing, effacement à distance…
- PC Portable :
  - Logiciels antivirus et de sécurité gérés à distance
- **Dans tous les cas :**
  - Limiter la manipulation de données sur l'équipement
  - Utilisation de TS, VDI et autres via VPN

Attention aux conséquences légales des outils techniques

© 2012 Bruno Kerouanton – GC Sécurité

Suivre l'évolution

- Le BYOD est-il une mode ?
  - Non, mais cela va vite…

- Cycle d'évolution rapide
  - des usages
  - des technologies
  - de la législation

- des menaces
- des parades

Domaine à surveiller en permanence !

© 2012 Bruno Kerouanton – GC Sécurité

QUESTIONS ?

Merci pour votre attention

http://bruno.kerouanton.net

© 2012 Bruno Kerouanton – GC Sécurité