Mathrice, 25 mars 2013, Caen

Protection des ordinateurs Portables...

...Reloaded

Bernard Perrot - CNRS - UMR6205
<bernard.perrot@univ-brest.fr>

… reloaded…

- Sujet à l'étude depuis de nombreuses années au CNRS (égide FSD, expérimentation IN2P3, …)
- Note du DGDR « Not11Y159DSI » du 16 janvier 2011 qui fait obligation de chiffrer les portables et équiper les nouveaux de disques auto-chiffrants
  - Suite à cette note, une présentation ici à Mathrice (Dijon) le 16 mars 2011 (s'y reporter…)
- Mais constat sans doute de la faible prise en compte de cette directive (nombreux vols de portables non protégés)
- Nouvelle note du DGDR « Not15YDSI-RSSIC » du 21 décembre 2012 qui rappelle la précédente, avec exigence de résultats !
  - Le dispositif technique est globalement le même, sans restreindre explicitement aux portables (mais aussi fixes « sensibles »)

Accompagnement DSI

- Rappel : c'est désormais la DSI qui a en charge la sécurité informatique, ce n'est plus le service du FSD.
- Notes, notices et FAQ sur le site de l'ARESU :
  - http://aresu.dsi.cnrs.fr/spip.php?rubrique99
  - FAQ mises à jour régulièrement, notices nouvelles…
- Un tableau de bord sur « Core » pour les CSSI des unités pour faire état de l'inventaire et avancement de l'opération :
- https://extra.core-cloud.net/collaborations/RSSI-CNRS/SitePages/Accueil.aspx
  - rubrique : « Enquête chiffrement »
- Les RSSI de régions sont les intermédiaires nécessaires/obligés, la DSI ne communique/traite pas/plus directement avec les ASR de labos…

Quoi chiffrer ?

- Au minimum :
  - tous les portables, qu'ils contiennent des données professionnelles confidentielles ou pas !
    Un portable contient <u>toujours</u> des données confidentielles, y compris (surtout !) personnelles !
  - les fixes :
    - administratifs
    - contenants des données professionnelles sensibles
    - présentant un attrait particulier pour un vol opportuniste
- Au mieux :
  - Tous les ordinateurs de l'unité (ce devrait être la politique pour toutes les machines neuves)

Comment chiffrer ?

- Si possibilité de disque auto-chiffrant, choisir cette option, c'est la plus performante et rapide à mettre en œuvre.
  - Difficulté potentielle : peu de choix (actuellement, seulement un DD 320 go), et pas de certitude que cette possibilité perdure (parce que plus disponible chez les fournisseurs, parce que plus au marché MATINFO3, …)
- Sinon …
- PC Windows 7 pro : *Truecrypt* (tout le disque, pas un container)
- PC Windows 8 pro : *Truecrypt* ou *BitLocker*
- PC HP : *HP Protect Tools* (i.e. *McAfee Endpoint Encryption*) ? (pas testé)

Comment chiffrer ?

- PC Linux : *dm-crypt* (natif dans Linux)
- MacOSX > 10.6 : *Filevault-2*. Natif, chiffre tous le disque, similaire à Truecrypt)
- MacOSX <= 10.6 : *FileVault-1*. Natif, pas trop le choix, pas très satisfaisant, chiffre seulement l'arborescence de l'utilisateur dans un container (idem Truecrypt en mode container).
- Double-boot Windows/Linux :
  - avec disque FDE : possible, voir document mise en œuvre
  - avec disque standard : utiliser Truecrypt pour Windows, et dm-crypt pour Linux
  - Mon avis : le double-boot est une technique obsolète, à abandonner au profit d'un système natif, et d'un second (ou plus) virtualisé sous le contrôle du natif.

Le futur ?

- Indisponibilité future des DD auto-chiffrants ?
  - Actuellement, plus que des 320 Go, et la politique de Seagate ne semble pas se diriger vers la pérennité des disques FDE...
- Boot UEFI ?
  - Les solutions logicielles ne supportent pas actuellement les boot UEFI (sauf McAfee Endpoint Encryption?)
  - Pas d'évolution de TrueCrypt depuis un an...
- Repli préférentiel (obligé) vers les solutions des éditeurs de système (Bitlocker, Filevault, ...) ?

Et les performances ?

- Si disque auto-chiffrant, aucun impact, performances natives !
- Si chiffrement logiciel :
  - Impact négligeable en comparaison de ceux des nombreuses tâches d'arrière plan courantes, anti-virus en particulier.
  - Bien moindre que la différence entre un DD 5400 rpm et 7200 rpm à laquelle vos usagers (ou vous) n'ont jamais fait attention...
- Si un utilisateur dit être notablement ralenti par le chiffrement :
  - Sa machine est très très ancienne, vous devriez la changer ;
  - Son anti-virus s'est « dégradé » dans le temps (classique) : réinstaller ou changer l'antivirus ;
  - Des botnet tournent en tâchent de fond : nettoyer la machine ;
  - Désinstaller eMule... ;
  - Effet « blouse blanche », c'est psychosomatique.

Ma conclusion...

- Il faut s'y mettre... c'est notre métier après tout...
- Se dire qu'il faut que le chiffrement des machines à la livraison doit être aussi reflexe qu'y installer un antivirus ou une suite bureautique !
- Pour vos utilisateurs pas convaincus, ne pas demander s'il y a des choses confidentielles sur la machine (ils disent en général que non), mais d'évaluer leur stress en supposant que leur machine est volée et que tout sont contenu peut être utilisé par un tiers malfaisant.
- Rappel : le chiffrement de surface ne protège que les ordinateurs arrêtés, utiliser du chiffrement de fichiers en sus si nécessaire.

Notes

Des questions ?