Atelier chiffrement des données

25/06/2013

Protection des ordinateurs portables

Circulaires CNRS du 16 janvier 2011 et du 21 décembre 2012

- Un constat
  - De nombreux ordinateurs régulièrement volés ou perdus
  - Des informations susceptibles d'être exploitées :
    - Données scientifiques
    - Données à caractères personnels
    - Identifiants
    - Informations privées de l'utilisateur
    - …

→ échanges par messagerie traités ultérieurement

Protection des ordinateurs portables et fixes

- L'orientation choisie : le chiffrement
  - Chiffrer tous les ordinateurs portables du CNRS en accord avec la demande du ministère de la Recherche
  - Solution la mieux adaptée à la diversité et à l'envergure de l'environnement informatique du CNRS
    - «*Généralement, il n'y a pas à entrer de mot de passe supplémentaire*»

Protection de base applicable à tous les ordinateurs portables

- Nouveaux Portables :
  - Windows et Linux : solution matérielle disques chiffrants

    → Commander les PC avec l'option «disques chiffrants» via le marché Dell et pour le marché HP.
  - Mac : solution logicielle native Filevault
  - Clefs USB : autochiffrantes recommandées par le CNRS (ex : Corsair)
- Parc existant
  - Windows 7, Vista, XP: solution logicielle Truecrypt (qualifié ANSSI, gratuit)
  - Windows 8 : solution logicielle bit-locker
  - Linux : solution logicielle native dm-crypt
  - Mac : solution logicielle native Filevault
  - Clefs USB : container TrueCrypt

Protection des données sensibles

- Données sensibles «ordinaires»
  - Rajout d'une deuxième couche de chiffrement

    → Conteneur TrueCrypt (qualifié ANSII, certification de sécurité de premier niveau (CSPN))

- Données «classifiées de défense»
  - Règles propres à définir avec le fonctionnaire de défense

Avertissement

- Mesure de chiffrement ne dispense pas :
  - Vigilance contre le vol
    → Protection des locaux, « ordinateurs attachés »,...
  - Fuite de données
    → option de conservation des disques en cas d'échange
  - Sauvegarde régulière des données
- Rappel sur
  - Restriction ou interdiction d'usage du chiffrement dans certains pays
    → recommandation d'usage d'une machine dédiée contenant un minimum d'informations réinstallé avant le départ et après le retour (voir Passeport de conseils aux voyageurs)
- Responsabilité du directeur d'unité
  - S'assurer que les mesures de protection des données sont bien mises en place

Des informations ...

https://aresu.dsi.cnrs.fr/spip.php?rubrique99

François Morris

Plan de l'atelier

- Introduction
- Mise en pratique du chiffrement
  - Chiffrement matériel (Paulo Mora de Freitas)
  - Chiffrement Windows Truecrypt (Paulo Mora de Freitas)
  - Chiffrement Windows Bitlocker (Paulo Mora de Freitas)
  - Chiffrement MacOS Filevault (Paulo Mora de Freitas)
  - Chiffrement Linux Dm-crypt (Jacques Beigbeder)
  - Chiffrement de conteneurs (Ludovic Billard)
- Table ronde impact du chiffrement (Pierre Vincens)
- Conclusion