Chiffrement des Données

Pierre-Yves Bonnetain-Nesterenko – Expert près la Cour d'Appel de Toulouse
Daniel Mouly – Expert près la Cour d'Appel de Bordeaux
CNEJITA – JFC du 18 juin 2019

Quelques rappels sur le chiffrement

- Ne protège que des données « inertes » : les données sont **toujours** consommées en clair
- Chaîne de chiffrement ne doit pas être brisée (comme chaîne du froid) :
  - données chiffrées ➔ sauvegardes chiffrées
- Algorithmes modernes robustes, sans portes dérobées
- **ATTENTION : le chiffrement est efficace, si vous perdez vos clés, vous perdez vos données**

Protéger des données par du chiffrement

- Principales méthodes envisageables :
  1. Chiffrement ponctuel de fichier
  2. Chiffrement de partition ou de disque
  3. Création d'une zone chiffrée dans un système de fichiers non chiffré
  4. Chiffrement en vue d'échanges sécurisés avec des tiers
- Comment choisir ?
  - Toujours s'interroger sur la motivation du chiffrement (analyse de risques) et le modèle de menaces (pourquoi, contre quoi, contre qui)

Chiffrement ponctuel

- Souvent une option offerte par une application, exemple Adobe Acrobat ou 7-Zip ou des suites de sécurité
- Avantages :
  - Relativement facile à mettre en œuvre (notamment chiffrement interne appli)
  - Généralement portable
  - Sauvegardes « nativement chiffrées »
- Inconvénients
  - Versions en clair du fichier peuvent subsister
  - Si sauvegarde quand version non chiffrée, finit dans les sauvegardes
  - Ne jamais suspendre session/arrêter ordinateur si version en clair existe (cf modèle de menaces)
  - Clé souvent faible (simple mot de passe)

Chiffrement de partition ou de disque

- Tout l'espace de stockage (support) est chiffré
- Option active de base sur machines récentes avec Windows 10 Pro (BitLocker) ou MacOS (FileVault)
- Activable à la demande sur ces mêmes systèmes
- Avantages
  - Pas d'accès aux données de la partition sans la clé
  - Peut-être transparent au logon pour le disque système Windows
  - Une fois la partition "ouverte", tout ce qui y est posé sera chiffré automatiquement
- Inconvénients
  - Pas de sauvegarde "offline"
  - Gestion des clés de récupération

Création d'une zone chiffrée dans un système de fichiers non chiffré

- Concept d'espace coffre-fort
  - Offert par la plupart des suites logicielles de sécurité
  - Plus petite granularité que le cas précédent
- Produit libre
  - VeraCrypt, héritier de TrueCrypt

Chiffrement en vue d'échanges sécurisés avec des tiers

- Problématique de gestion des clés
  - Préférer un système de chiffrement à clés asymétriques, aussi appelé chiffrement à clés publiques ou PKI
- Choisir (pour tous les tiers) un outil basé sur la norme OpenPGP, par exemple GnuPG
- Créer sa paire de clés
  - Stocker sa clé privée si possible sur une carte à puce, dans tous les cas
  - Diffuser sa clé publique auprès des tiers, récupérer la leur pour la mettre dans votre trousseau
- Vous êtes prêts !