Journée de Formation Technique du 18 Octobre 2016

Conservation de la preuve

Dominique VAN EGROO
dve@fintoo.fr
Tél : 06 27 14 39 91

Sommaire

- Pourquoi conserver la preuve ?
- Quels risques ?
- Principaux cas
- Les preuves à disposition
- A faire vs à éviter

Pourquoi conserver la preuve ?

- **Permettre une investigation**
- **Identifier la source d'une attaque / fraude**
- **Disposer d'éléments pour servir de base à une procédure Pénal, civile, prud'homale**
  - **Prouver des faits et convaincre le juge**
  - **Attention le régime de la preuve est différent**
    - **Procédure pénale : liberté de la preuve**
    - **Procédure prud'homale : la preuve doit être licite (information du salarié)**

Quels risques

- **Preuve incomplète**
  - **Tous les éléments n'ont pas été conservés / obtenus**
- **Preuve discutable**
  - **Intégrité de la preuve**
- **Disparition / Altération de la preuve**
  - **Actes volontaires vs négligences**

Principaux cas

- Vol / Extraction d'informations
- Fraudes
  - De la fraude aux notes de frais à la fraude à la téléphonie
- Intrusions internes / Externes
  - Usurpation d'identité
  - Vol / Extraction de données
  - Suppression / altération de données…
- Piratage de sites Internet

Les principales preuves à disposition

- Contenu des disques durs
- Contenu de la mémoire
- Copie des machines virtuelles
- Traces d'audit (fichiers de logs)
  - Applications, serveurs Web, OS
  - Systèmes proxy, pare-feu, IDS
- Traffic réseau
- Contenu de la messagerie
- Contenu des bases de données

Attention à la date et à heure des systèmes

A faire vs à éviter

- Adapter la collecte de preuves selon le contexte
- Faire intervenir un huissier avec un expert dès le départ pour l'appréhension de la preuve voire la recherche de la preuve
  - Pas d'intervention directe du client sur les systèmes vs Indépendance
    - Cas de fraudes, incidents internes
  - Huissier séquestre d'une copie
- Solliciter sans tarder des tiers / prestataires la conservation des traces
- Collecte de preuves sécurisée : Empreintes, supports non réinscriptibles

A faire vs à éviter

- Fraudes
  - Conservation des traces applicatives
  - Prise de copie de la messagerie
  - Prendre copie des disques
- Attaque réseau / intrusion
  - Déconnecter les systèmes du réseau
  - Envisager selon le cas le déclenchement du PRA
  - Prendre copie de la mémoire et des disques vs VM
  - Prendre copie des fichiers de logs
- Vol / Extractions d'informations
  - Prise de copie de la messagerie
  - Prendre copie des disques
  - Prendre copie des fichiers de logs

Merci de votre attention

Dominique VAN EGROO
dve@fintoo.fr
Tél : 06 27 14 39 91