JFC CNEJITA du 18 octobre 2016

Faille de sécurité
Ce qu'il ne faut pas faire

Daniel Mouly
Expert près la cour d’appel de Bordeaux

Bienvenue dans le monde des PME

- Cas réel :
  - PME de 30 personnes
  - 99 % d'ingénieurs
  - Grande majorité de (jeunes) développeurs
  - Autonomes dans la gestion de leur environnement
  - Pas de véritable responsable informatique
  - Encore moins de RSSI
  - Fournit des produits pour clients "sensibles"

La faille

- Genèse
  - Un des premiers ingénieurs recrutés devient gourmand
  - Il estime être l'auteur légitime des produits
  - Il est aussi le responsable informatique "de fait"
  - Il est "retourné" par un des actionnaires qui le convainc de quitter la PME et de tenter une nouvelle aventure

La faille (suite)

- Exécution
  - L'ingénieur en question démissionne
  - La PME espère le récupérer
  - Personne ne se préoccupe de ses droits d'accès
  - Il revient un weekend dans les locaux
  - Supprime tous les sources de "son" logiciel (mais en garde une copie pour lui…)
  - Il fait aussi le ménage sur le serveur de la PME

La faille (fin)

- Découverte
  - Le patron de la PME réalise qu'il a un souci
  - Il essaie de négocier et perd du temps
  - Il découvre finalement l'ampleur des dégâts
  - Il inventorie les erreurs :
    - Péremption des vidéos montrant l'intrusion du weekend
    - Réutilisation du laptop de l'ingénieur par un nouvel entrant (formatage et réinstallation de systèmes sur SSD)
    - Pas de sauvegardes, c'était l'ingénieur qui s'en occupait
    - La liste est encore longue

La réaction

- Houston, we have a problem
  - Produits installés dans des centrales nucléaires, plus de sources pour les maintenir
  - Intervention de la DGSI qui s'inquiète un peu
  - Appel désespéré à un expert informatique (votre serviteur) pour essayer de récolter quelques bribes de preuves
  - Dépôt de plainte (pénal)
  - Préparation d'une action en contrefaçon (sans les sources originaux…)