Club de la sécurité de l'information français

CLUSIF

La judiciarisation d'une attaque cyber

Comment travailler avec un service de police en cas de cyber attaque ?

Sylvie SANCHIS
Commissaire de Police, Chef de la BEFTI

RETEX côté Police

- L'absence d'anticipation
  - Réduction du périmètre d'action ou dépassement du domaine de compétence des intervenants
  - Blocage des relations clients-prestataires

Les bonnes pratiques…

- Anticiper la crise
  - Définir les missions
  - Prévoir les absences
  - Connaître les contrats
  - Identifier des prestataires ponctuels

…conditionnent la plainte utile

- Préserver les traces
  Idéalement en numérique, sinon captures d'écran
  - Des serveurs et des sites internet compromis
  - Des fichiers chiffrés
  - Des journaux d'activité (logs)
  - Des éléments de communication avec les auteurs
  - Des paiements éventuellement effectués

La problématique des logs

- Vérifier les paramétrages des enregistrements
  - Nature et étendues des données enregistrées
  - Durée d'enregistrement et de conservation

- S'assurer de la disponibilité directe et rapide des journaux pour la victime (dispositions contractuelles)

Intérêt de la plainte

- Pour la victime
  - Comprendre les raisons et/ou le contexte de l'attaque
  - Identifier les modes opératoires
  - Identifier les auteurs
  - Récupérer les données métiers et limiter leur diffusion
  - Anticiper une nouvelle attaque

Intérêt de la plainte

- Pour les pouvoirs publics
  - Identifier et évaluer les menaces cybercriminelles
  - Lutter contre le chiffre noir
  - Attribuer des moyens adéquats

Modalité de la plainte

- Quand ?
- Où ? Commissariat ou service de Police Judiciaire
- Par qui ? Dirigeant ou mandataire
- Avec qui ? Technicien
- Avec quoi ?
  - Délégation de pouvoir, extrait Kbis
  - Premiers éléments
  - Évaluation du préjudice et des dommages

Orientation de la plainte

- Choix du service enquêteur par le Procureur de la République ou le juge d'instruction
- Si saisine BEFTI, contact régulier avec la victime
- Garantie de discrétion

Les investigations

- Contacts ANSSI, Inter-CERT, universitaires, chercheurs…
- Coopération en Europe et à l'étranger