Matérialiser et documenter la preuve pour préserver les intérêts

JFC CNEJITA – 18 Octobre 2016

Pourquoi ?

- Lorsque un incident se produit -> conséquences +/- graves
- La nature de l'incident détermine si il y a lieu de le porter à la connaissance des autorités judiciaires et d'entreprendre une action en justice par voie de dépôt de plainte
- Au préalable, il faut essayer de déterminer si l'incident est intentionnel ou accidentel
- Rassurer la direction de l'organisation qui se pose bcp de questions

1. Une attaque informatique a eu lieu, quelles sont les démarches techniques envisageables ?

- Si suspicion d'attaque -> il est important que les constatations techniques soient effectuées dans les meilleurs délais
  - Contacter un service de judiciaire (mais…)

ou

  - Procéder soi même aux constatations

ou

  - Faire appel à un huissier

ou

  - Faire appel à un expert

2. Quelles mesures conservatoire ?

- Processus classic de gestion d'incident de sécurité:
  - Confiner
  - Isoler
  - Sauvegarder
  - Collecter les renseignements
  - Communiquer

2. Quelles mesures conservatoire ?

- Sauvegarder:
  - les journaux
  - les documents, courriels, fichiers
  - le traffic réseau supervisé
  - mémoires volatiles / non volatiles

2. Quelles mesures conservatoire ?

- Collecter les renseignements:
  - Internes:
    - Premières personnes ayant détecté l'incident
    - Personnes ayant assisté à l'incident
  - Externes:
    - Prestataires de services

3. Qu'est ce qui est utile ?

- Topologie / Architecture
- Historique de l'incident
- Observation
- Acquisition
- Documentation

4. Comment préserver la preuve numérique ?

- Gestion de l'incident -> modification de la scène de crime
- Obtenir de façon légale les "preuves"
- Effectuer une copie au plus près de la scène de crime (copie intégrale, dite "bit à bit")
- Sauvegarder l'ensemble des journaux
- Certifier les données fournies par un tiers

- Valider l'intégrité (original)

5. Vers qui se tourner pour déposer plainte ?

- Rappel: la plainte est l'étape préalable à une ouverture judiciaire
- La majorité des infractions à la cybercriminalité sont des délits: 3 ans pour déposer plainte
- Chez qui ?
  - service territorial de police ou de gendarmerie le plus proche de l'entreprise
  - parquet du ressort

6. Statuts de la personne habilité à déposer plainte ?

- Seule les mandataires sociaux ou une personne mandatée est habilitée à déposer plainte en qualité du représentant légal de l'entreprise

7. Quels éléments communiquer ?

- Document attestant de l'identité du plaignant
- Éléments intéressants l'enquête
  - Rapport d'expert

Questions ?

Coordonnées services dédiés

SDLC/OCLCTIC
Sous-Direction de Lutte contre la Cybercriminalité, Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de l Dépend de la Direction Centrale de la Police Judiciaire.
Compétence nationale, point de contact international
Tel : 01 47 44 97 55

http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-directio

BEFTI
Brigade d'enquêtes sur les Fraudes aux Technologies de l'Information.
Dépend de la Direction Régionale de la Police Judiciaire de la Préfecture de Police de Paris. Compétence sur Paris et la petite couronne.
Tel : 01 55 75 26 19
http://www.prefecturedepolice.interieur.gouv.fr/

DGSI
Direction Générale de la Sécurité Intérieure.
Compétence nationale. Enquête sur les crimes et délits pouvant porter atteinte à la sûreté de l'Etat. Tel : 01 77 92 50 00
http://www.interieur.gouv.fr/

Gendarmerie Nationale/C3N
Pôle judiciaire de la gendarmerie nationale.
Centre de lutte contre les criminalités numériques. Compétence nationale.
Tel : 01 78 47 36 52 http://www.gendarmerie.interieur.gouv.fr