Cybercriminalité : cyberattaques, phishing, vol de données

Comment réagir ?

Université des CIL – Janvier 2016

Plan

Propos introductifs : le CIL et la cybercriminalité

1. Les actions préventives du CIL

1.1 Identification des risques
1.1.1 Les cybermenaces : cyberattaques, phishing
1.1.2 Réalisation d'études d'impact

1.2 Identification des mesures à prendre
1.2.1 Mesures s'agissant des données
1.2.2 Formalisation des mesures

2. Les actions curatives du CIL

2.1 Le rôle du CIL dans le cadre du dépôt d'une plainte
2.1.1 Pourquoi déposer plainte ?
2.1.2 Collecte et transmission des éléments utiles

2.2 Le rôle du CIL dans le cadre de la notification d'une faille de sécurité
2.2.1 La généralisation de l'obligation de notification avec le Règlement européen
2.2.2 Le CIL, une personne relai pour l'autorité de contrôle, une personne ressource pour l'entreprise

Propos introductifs

Le CIL et la cybercriminalité

1 . Les actions préventives du CIL

- Identification des risques
- Identification des mesures à prendre

- **Identification des risques**

Les cybermenaces : cyberattaques et phishing

Les cyberattaques

- **Qu’est-ce qu’une cyberattaque?**

Une atteinte à un système de traitement automatisé de données à des fins malveillantes. Elle peut avoir pour objectif d’extraire des données, de les détruire, de les modifier ou d’altérer le fonctionnement normal du système ou de bloquer son fonctionnement.

- **Essai de typologie**
  - Cyberattaques à visée revendicatrice
  - Cyberattaques mercantiles
  - Cyberattaques aux fins d’espionnage

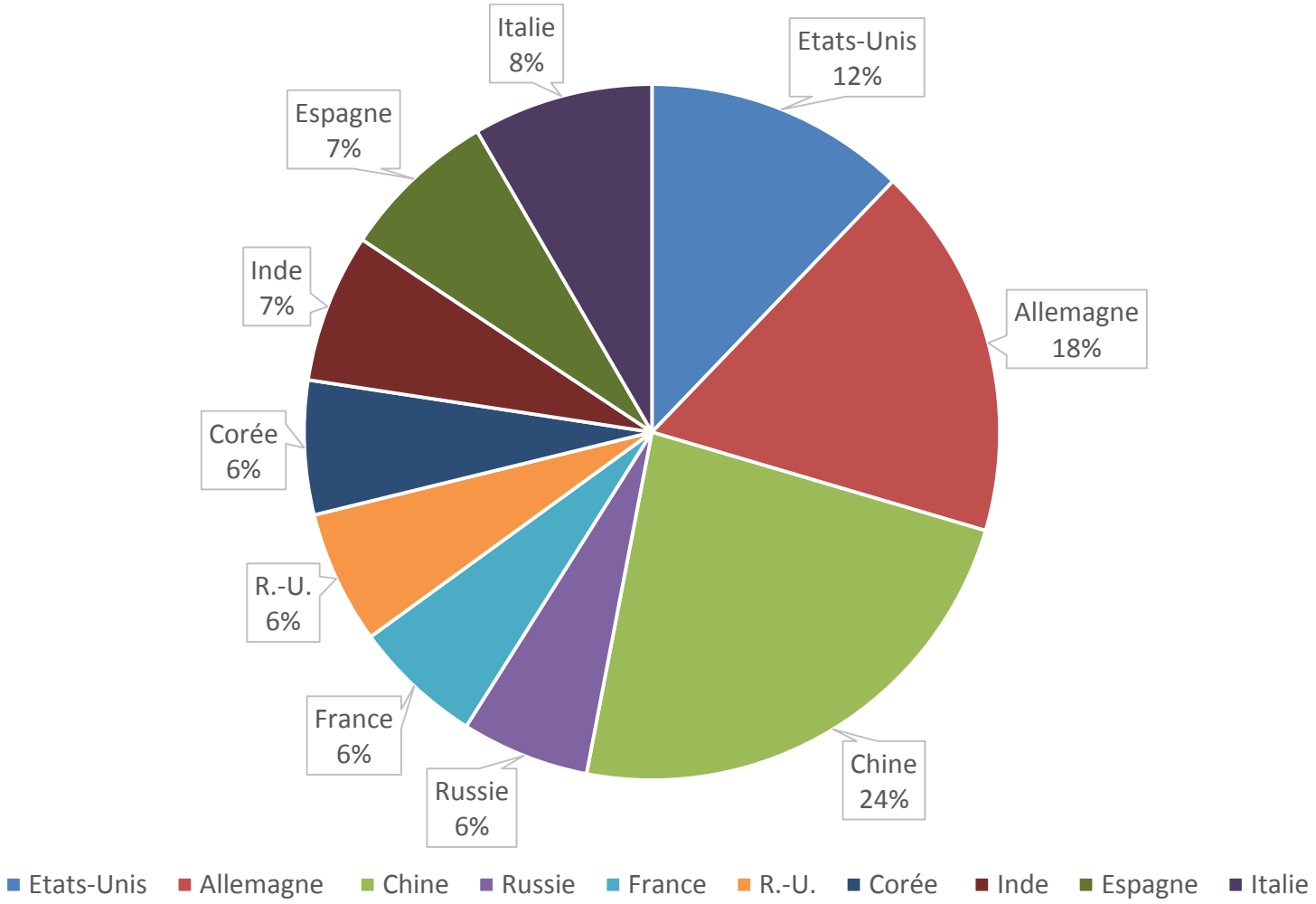
- **Etat des lieux des cyberattaques**

-En 2015 le nombre d'attaques DDOS a augmenté de 179,66% par rapport à l'année 2014. (Source: Akamai State of the Internet Security, 2015)

-Elles visent toutes les entreprises (sociétés du CAC 40 et PME, sociétés privées et organismes publics).

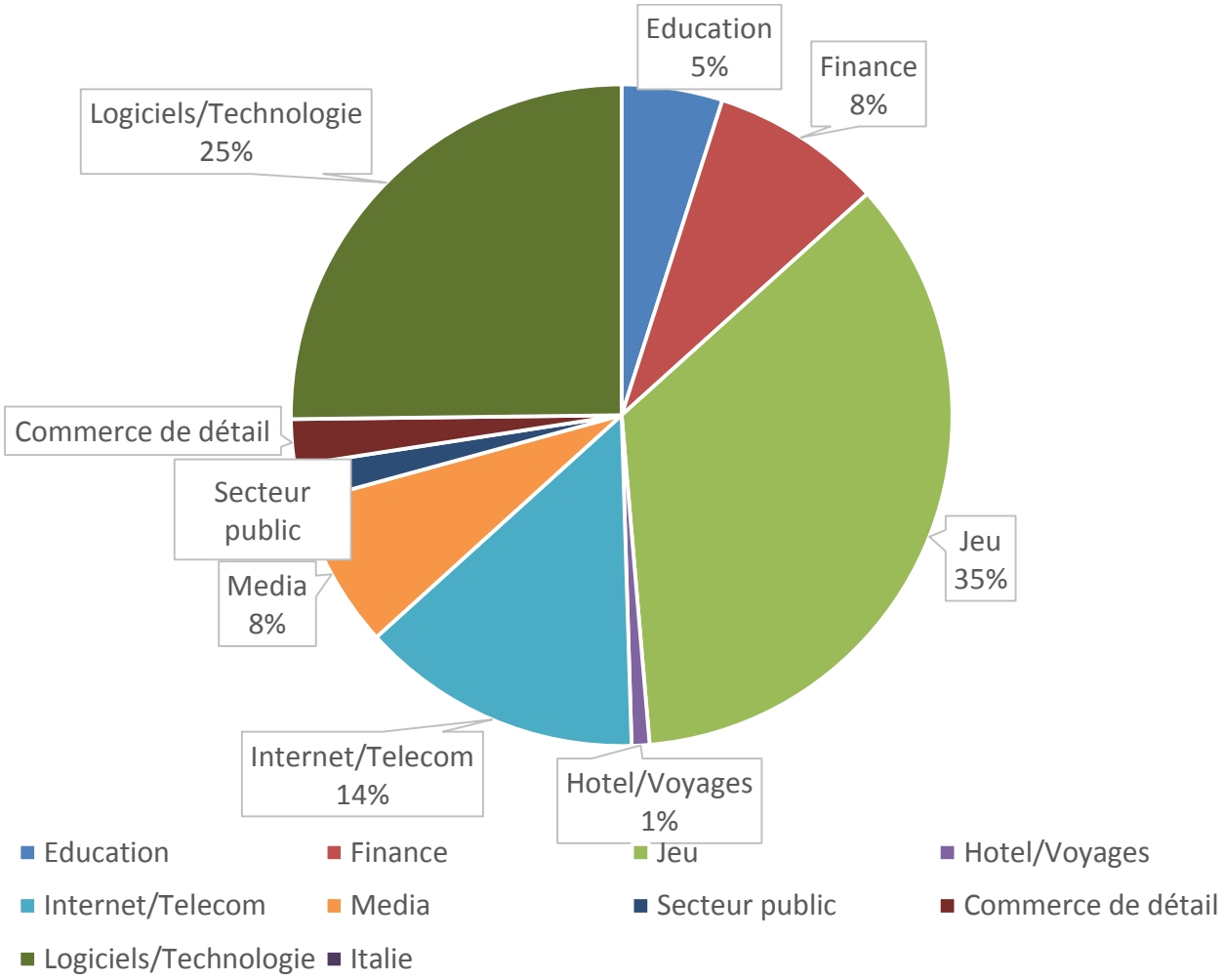
-Elles visent tous les secteurs d'activité.

Top 10 des pays à l'origine d'attaques DDOS au 1er trimestre 2015



Source: Akamai State of the Internet Security, 2015

Top 10 des secteurs d'activité les plus visés par des attaques DDOS au 1er trimestre 2015



Source: Akamai State of the Internet Security, 2015

- **Appréhension des cyberattaques par le droit pénal**

  - **L'accès ou le maintien frauduleux dans un système de traitement automatisé de données**

Art. 323-1 du Code pénal :

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

- **Le fait d’entraver ou de fausser le fonctionnement d’un système de traitement automatisé de données**

Art. 323-2 du Code pénal :

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

- **Le fait d'introduire frauduleusement des données d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données**

Art. 323-3 du Code pénal :

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

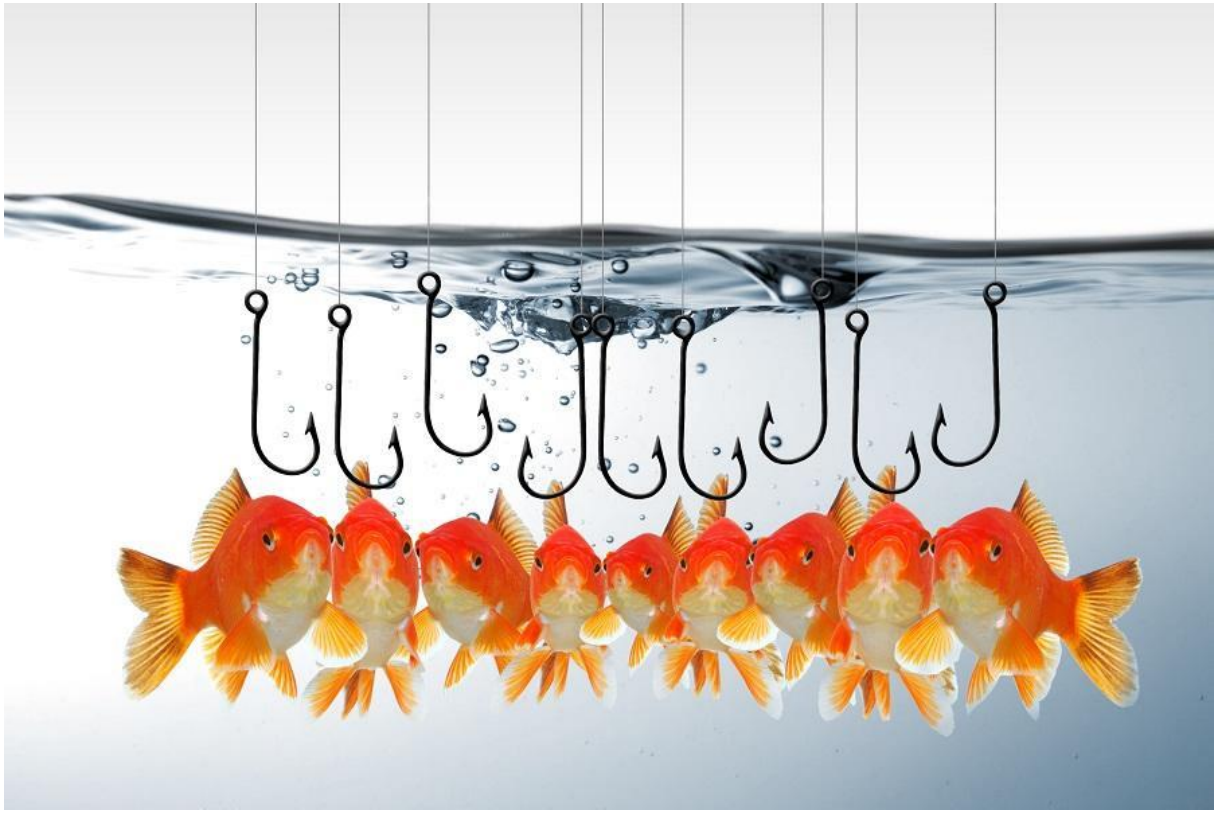
- **Appréhension des cyberattaques par la loi informatique et libertés**

Art. 34 LIL: « Le responsable de traitement doit prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès ».

Manquement sanctionné pénalement :

Art. 226-17 du Code pénal: « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est punie de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

Le phishing



- **Qu’est-ce que le phishing?**

L’hameçonnage ou le phishing est une méthode de tromperie utilisée pour obtenir des données à caractère personnel d’internautes au moyen de messages électroniques et de sites internet revêtant l’apparence de messages ou de sites émanant d’entreprises légitimes telles que des établissements financiers ou des administrations publiques.

- **Appréhension du phishing par le droit pénal**

➢ L'escroquerie ou la tentative d'escroquerie (art. 313-1 à 313-3 du Code pénal)

➢ L'usurpation d'identité (art. 226-4-1 du Code pénal)

➢ La contrefaçon (art. L. 716-9 du CPI)

➢ Faux et usage de faux (art. 441-1 du Code pénal)

Les cybermenaces, quelles conséquences pour la société ou l'organisation victime?

- conséquences financières,
- atteinte à l'image et à la réputation de la société.

1.1.2 Réalisation d’études d’impact

Le règlement européen prévoit la réalisation d'études d'impact (art. 33)

-L'autorité de contrôle doit établir et rendre publique une liste des traitements soumis à cette obligation.

-Le contenu de l'étude d'impact :

- une description systématique du traitement envisagé,
- une étude de la nécessité et de la proportionnalité du traitement,
- Une étude des risques pour les droits et libertés des personnes concernées,
- les mesures envisagées pour couvrir ces risques.

Cette étude d'impact peut s'appuyer sur des audits:

-audit de sécurité,
-audit de protection des données.

1.2 Identification des mesures à prendre

- Mesures s’agissant des données
- Formalisation des mesures

2. Les actions curatives du CIL

- Le rôle du CIL dans le cadre du dépôt d'une plainte

- Le rôle du CIL dans le cadre de la notification d'une faille de sécurité

➢ Le dépôt d’une plainte

- **Pourquoi déposer plainte?**

-un outil de communication interne,
-un outil de communication externe,
-le suivi de l’enquête.

- **Collecte et transmission des éléments en vue du dépôt d'une plainte**

-une chronologie des faits,

-un résumé des mesures prises/ des investigations internes (généralement effectuées par le DSI),

-communication des éléments qui peuvent être utiles aux services d'enquête : en-têtes techniques, liste d'adresses IP, etc.

-des éléments de contexte (analyse d'impact sur la vie privée des personnes concernées)

- **Le rôle du CIL dans le cadre de la notification d'une faille de sécurité**

- **La généralisation de l'obligation de notification avec le règlement européen**
  - Obligation de notification de violation de données à caractère personnel à la CNIL

    (art. 34 bis de la Loi informatique et libertés)
  - Obligation de déclaration d'un incident de sécurité à l'ANSSI

    (art. L. 1332-6-1 à L. 1332-6-6 du Code de la Défense)
  - Obligation plus étendue sous l'égide du règlement européen

Le règlement européen prévoit une <u>double obligation</u>:

-une obligation de notification à l'autorité de contrôle (article 31)

-une obligation de communication à la personne concernée (article 32)

2.2.2 Le CIL, une personne relai pour l'autorité de contrôle, une personne ressource pour l'entreprise

-C'est le point de contact entre la société et l'autorité de contrôle:

→ Analyse et documentation de la violation,

-C'est le point de contact entre les personnes concernées par la violation et la société:

→ Réponses aux réclamations et plaintes.

Conclusion

Nous vous remercions de votre attention

Avez-vous des questions?

Géraldine Péronne
peronne@vigo-avocats.com

Emmanuel Daoud
daoud@vigo-avocats.com