Se préparer à la réponse judiciaire contre les attaques informatiques

Forum CERT-IST

Paris, 03 juin 2010

Lieutenant-colonel Éric FREYSSINET, DGGN/SDPJ

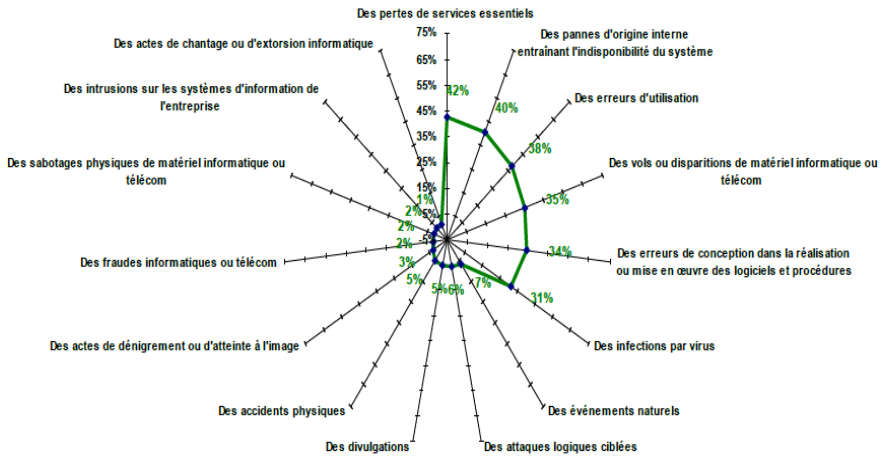
Plan

- Pourquoi il faut agir juridiquement
- Pourquoi on peut agir juridiquement
- Comment s'y préparer
- Comment agir

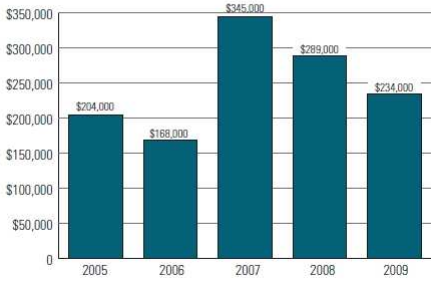
Pourquoi il faut agir

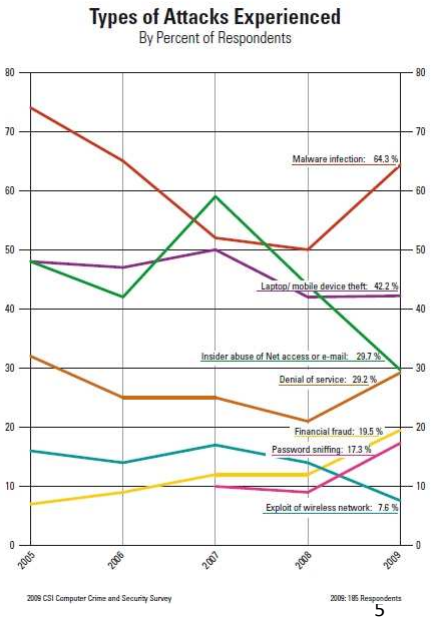
- Le nombre réel d'attaques informatiques
  - Beaucoup plus important que les chiffres publics
  - L'exemple des autres pays nous montre une autre réalité
- Si l'on veut durablement limiter le risque, il faut identifier et interpeller les auteurs. On ne peut pas les interpeller si:
  - On ne connaît pas leurs actes
  - On ne collecte pas de preuves
- Il va falloir transformer l'essai de l'obligation de notification d'incidents de sécurité

Étude CLUSIF 2008



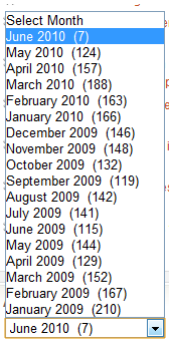
Étude CSI 2009





- US, 443 réponses
- http://gocsi.com/

Databreaches.net



Notification des incidents de sécurité

- Paquet « Télécom » voté en novembre 2009
  - Obligation qui concernera tous les opérateurs de communications électroniques
  - A transposer avant 25 mai 2011
- Proposition de loi Détraigne/Escoffier
  - Débattue au Sénat le 23 mars
  - Proposent d'appliquer d'emblée cette obligation à tous les responsables de traitements de données à caractère personnel
  - Mais, il n'y a pas que les traitements de données personnelles qui ont de la valeur. A suivre donc.

Proposition de loi Détraigne/Escoffier

- Texte voté par le Sénat et transmis à l'assemblée nationale qui modifie l'article 34 de la loi Informatique et libertés :
  - En cas de « violation du traitement de données à caractère personnel », le responsable de traitement :
    - Avertit le Correspondant Informatique & Libertés (CIL) ou à défaut la CNIL
    - Prend immédiatement les mesures nécessaires pour rétablir la protection de l'intégrité et de la confidentialité des données
  - Le CIL en informe la CNIL
  - Si la violation a affecté des données à caractère personnel d'une ou plusieurs personnes physiques, le responsable de traitement :
    - Informe ces personnes
  - Un inventaire des atteintes aux traitements de donnés à caractère personnel est tenu à jour par le CIL

Pourquoi on peut agir

- Parce que les partenaires judiciaires sont prêts
  - Sur le plan juridique
  - Sur le plan technique et des compétences
- Parce que cela n'implique pas forcément de révéler ses défauts
  - Ou parce que le temps judiciaire laisse le temps de les corriger

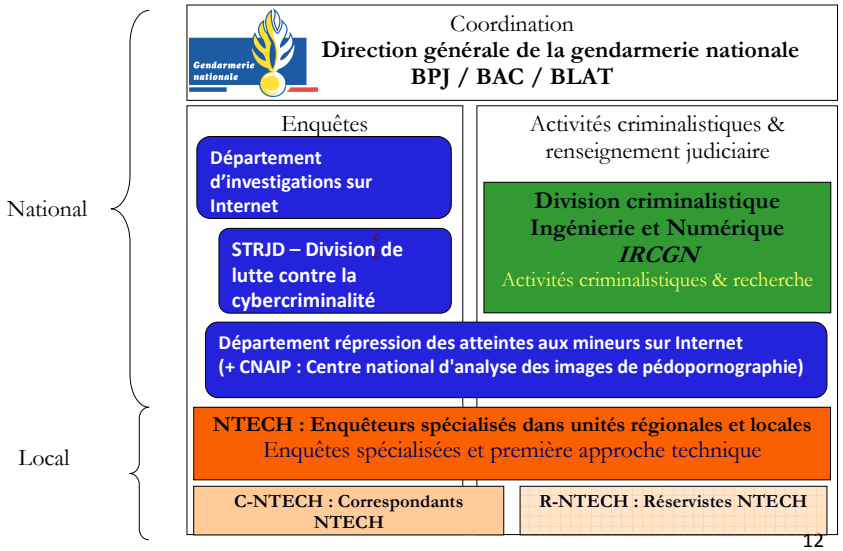
Les instruments juridiques

- Vous les connaissez
  - Convention du Conseil de l'Europe sur la cybercriminalité (2001)
  - Décision-cadre de l'UE relative aux attaques visant les systèmes d'information (2005)
  - Loi Godfrain (1988) en France et code de procédure pénale adapté
    - Maximum de cinq ans de prison, 75.000€ d'amende
    - Peines complémentaires

Les compétences sont là

- Vous connaissez les acteurs:
  - Police
    - DCPJ/OCLCTIC, PP/BEFTI, DCRI, ICC (ESCI)
  - Gendarmerie
    - IRCGN, STRJD, NTECH, C-NTECH
  - Justice
- Chacun, dans ses zones ou territoires de compétences s'est formé, adapté, est prêt à répondre
- Les compétences se développent évidemment aussi à l'étranger, et des partenariats sont en place

Résumé dispositif gendarmerie

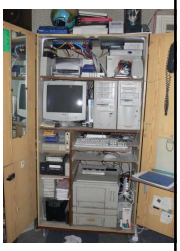


Les compétences sont là

- Vous connaissez les acteurs:
  - Police
    - DCPJ/OCLCTIC, PP/BEFTI, DCRI, ICC (ESCI)
  - Gendarmerie
    - IRCGN, STRJD, NTECH, C-NTECH
  - Justice
- Chacun, dans ses zones ou territoires de compétences s'est formé, adapté, est prêt à répondre
- Les compétences se développent évidemment aussi à l'étranger, et des partenariats sont en place

Les affaires sont traitées

- Beaucoup d'affaires se traitent dans la discrétion
- Parfois de « petites » affaires ont un impact important
  - UTOPI 62 (06/2006), HACKERs 21 (05/2008),…
- Des compétences pour couvrir tout le spectre des besoins:
  - Interventions dans les entreprises, chez les opérateurs, chez les hébergeurs
  - Perquisitions chez particuliers ou entreprises



Tous réclament une coopération intelligente

RSA: FBI Director Calls For Action Against Cyber Threat

By Stefanie Hoffman, ChannelWeb
2:33 PM EST ven.. mars. 05, 2010

Discuss This

FBI Director FBI Robert Mueller called on the U.S security community to minimize disclosure, coll governments and pursue investigations farther appears to be a losing arms race with cyber cri

"We are playing the cyber equivalent of cat and r thousands of IT professionals in a keynote durir Thursday. "We must make the cost of doing bus willing to bear,"

As part of his call to arms, Mueller pledged mini with protective orders and increased privacy for data breaches, in order to avoid loss of reputati momentum of federal and state data breach dis

"Notifying the authorities may harm your compet the disruption into your business," he said. "Tog the breadth and scope of this attack. For every ir are hundreds that will never make the headlines not the rule."

L'enquête judiciaire et la gestion des incidents de sécurité

- Détecter l'activité criminelle
- Recevoir les plaintes
  - Collecter les preuves, évaluer les dommages, rétablir le fonctionnement
    - Identifier et interpeller les suspects
      - Poursuivre (et obtenir réparation)

Nécessite: des personnels formés dans l'industrie et les services d'enquête ; en mesure de coopérer

Comment s'y préparer

- Évidemment, sécuriser ses systèmes d'information et être en mesure de détecter les attaques
- Collecter des traces de façon préventive
- Évaluer l'ampleur des atteintes
  - Pour savoir quoi partager de façon informelle
  - Pour déterminer quand déposer plainte
- Former ses personnels
- Connaître les acteurs locaux / nationaux

Quels critères pour un dépôt de plainte ?

- Création d'une grille d'évaluation adaptée aux risques :
  - Atteinte notable à des données personnelles
  - Atteinte à des données confidentielles
  - Préjudice financier / temps pour rétablir
  - Échanges avec les professionnels (mesurer ensemble la complexité de l'attaque, faire des rapprochements)
  - Échanges avec les services d'enquêtes

A	*
B	* * *
C	* *

Comment agir

- Préserver les preuves
  - Disponibles et extensives
  - Admissibles (leur qualité est documentée, leur contenu éventuellement signé)
- Prévenir les autorités
  - Coordonner avec elles la reprise d'activité
  - Ainsi que la procédure de mise à disposition des preuves
  - Mesurer le préjudice
- Préparer la communication
  - A coordonner avec les autorités
  - Prévenir les victimes tierces
  - Souligner positivement la préparation et la réaction

Préserver les preuves

- En droit français, la preuve est libre
- Mais plus on est capable de la valoriser, plus elle sera probante
  - Process de collecte documentés et propres
  - Signatures électroniques
- Privilégier des formats ouverts
- Mettre à disposition des spécialistes capables d'expliquer le fonctionnement des systèmes

Prévenir les autorités

- Ne pas chercher à régler le problème soi-même ...
- Des interlocuteurs qu'il faut connaître par avance
- Les intervenants locaux peuvent toujours se faire assister de spécialistes si nécessaire
- Prévoir des locaux pour les accueillir
- Désigner un point de contact technique (et éventuellement un point de contact juridique)
- Prévoir une procédure d'échanges au fil de l'eau, notamment par voie électronique
- La discrétion vaut aussi pour les victimes

Communication

- Essentielle :
  - Pour tirer le meilleur de la gestion de l'incident
  - Pour prévenir une communication négative
  - Pour se préparer au procès pénal qui est public
  - Pour expliquer les mesures correctrices apportées et rassurer les clients
  - Pourquoi ne pas communiquer sur la qualité de sa préparation à gérer ces incidents ?

www.gendarmerie.interieur.gouv.fr

Conclusion

- Partenariat
- Impliquer les services d'enquête
- Collecter des preuves
- Se préparer et planifier !

Eric Freyssinet, lieutenant-colonel
Direction générale de la gendarmerie nationale
Sous-direction de la police judiciaire
35 rue Saint Didier
F-75775 PARIS Cedex 16
Tél: +33 1 56 28 66 27
Mél: eric.freyssinet@gendarmerie.interieur.gouv.fr
http://blog.crimenumerique.fr/