La réunion a commencé par une présentation de Fabrice Prigent sur les dernières actualités en matière de sécurité.

http://www.ossir.org/resist/supports/cr/20040830/Resist-aout-2004.pdf

La prochaine réunion de ReSIST est prévue le 25 octobre 2004.

# Police, droit et informatique

Présentation du Capitaine Yves Le Hir, SRPJ de Toulouse, intervenant à titre personnel.

Supports fournis par le Capitaine Le Hir :

http://www.ossir.org/resist/supports/cr/20040830/Resist-droit-loi.pdf
http://www.ossir.org/resist/supports/cr/20040830/Droit_informatique.pdf

La présentation a débuté par un rappel de lois pénales applicables directement aux délits ou crimes informatiques :

- *loi Godfrain*[1], pour les atteintes au fonctionnement,
- *loi Informatique et Libertés*[2], pour tout ce qui concerne les fichiers nominatifs. Il a été souligné qu'un « fichier nominatif » est un fichier dont le contenu permet d'identifier un individu. De ce fait, des listes d'adresses électroniques ou des pages Web (si elles sont sujettes à des traitements automatisés) peuvent être considérées comme des fichiers nominatifs, du ressort donc de la CNIL. Dans le cadre de cette loi, le détenteur du fichier a une obligation de moyens quant à la protection de ces données.
- *Code de la Propriété Intellectuelle*, pour les questions de contrefaçon de marques ou de produits. Il prévoit tous les cas, dont directement les logiciels.
- *Code Monétaire et Financier*, pour ce qui concerne les moyens électroniques de règlement.

Certaines lois pénales sont indirectement applicables, lorsque l'outil informatique n'est que le vecteur d'un délit :

- loi de 1881 sur la presse (les textes ont été amendés afin de prendre en compte des supports autres que le papier journal), pour ce qui concerne la diffamation, l'incitation à la haine, l'apologie de crimes, etc.
- les lois et règlements concernant le secret de la correspondance,
- la mise en péril de mineurs, y compris leur exposition à des contenus à caractère pornographique,

1 La loi Godfrain est maintenant intégrée au Code Pénal, articles 323-1 et suivants.
2 La loi Informatique et Libertés est intégrée au Code Pénal, articles 226-16 et suivants.

- la contrefaçon de marques. Il est à noter que l'usurpation d'identité est une simple contravention; elle devient délit si elle expose le propriétaire (innocent) de l'identité usurpée à des poursuites pénales[3].

La loi Perben–2 a apporté quelques modifications supplémentaires, concernant entre autres la diffusion d'informations relatives à la fabrication d'engins explosifs, qui devient un délit.

*Question* : que doit/peut alors faire une société désireuse de limiter/contrôler la navigation de ses collaborateurs, notamment si elle constate l'accès à des sites illégaux ?

*Réponse* : la question couvre deux parties disjointes :

- L'existence d'un site à caractère illégal doit être portée à la connaissance de la justice et/ou de la police. Il n'y a là aucune notion de contrôle ou de surveillance des collaborateurs, on traite uniquement de l'illégalité du site en question.
- Pour les collaborateurs, il est nécessaire de disposer d'une charte de bonne conduite décrivant de manière claire les moyens automatiques de traitement d'information qui sont mis en place (par exemple traitement des journaux d'accès, listes blanches ou noires, résultats produits, etc.). Cette charte peut être opposable à un collaborateur.

## Que faire lorsque l'on est victime ?

1. Décider si l'on porte plainte ou non. En cas de dépôt de plainte, il est important de « bien déposer plainte » (voir plus loin).
2. Déposer plainte auprès d'une autorité compétente :
    - Auprès d'un commissariat ou d'une brigade de gendarmerie; procédure rapide, mais d'efficacité toute relative. Il n'est pas nécessaire que ce soit le commissariat ou la brigade du lieu du délit; le dossier sera transmis par la suite.
    - Par lettre–plainte auprès du Procureur de la République; il s'agit d'une lettre de forme libre, dans laquelle le plaignant doit exposer les faits, joindre des copies des pièces et des preuves qu'il a pu réunir, etc.
    - Porter plainte avec constitution de partie civile auprès du Doyen des Juges d'Instruction; cette procédure, lourde et longue, se fait par l'intermédiaire d'un avocat.
    - Après un premier contact (qui peut être téléphonique), déposer plainte auprès d'un service enquêteur spécialisé, les ESCI (Enquêteur Spécialisé en Criminalité Informatique) du SRPJ, ou les N–Tech en brigade de gendarmerie. Il existe aussi le BEFTI et l'OCLCTIC, basés sur Paris.
3. Les cadres juridiques de l'instruction de la plainte sont :

3 C'est à dire si l'identité usurpée est utilisée pour commettre un délit.

A) le flagrant délit, mais cela suppose que la procédure soit lancée « à la constatation d'un crime ou délit flagrant » (art. 53 du Code de Procédure Pénale), ou dans un temps très proche[4] de la commission de celui–ci. Les investigateurs disposent alors de moyens cœrcitifs importants.

B) l'enquête en mode préliminaire. Les investigateurs disposent de pouvoirs de réquisition, mais de moins de moyens cœrcitifs que pour le flagrant délit.

C) l'enquête en exécution de commission rogatoire, sous la direction d'un juge d'instruction. Il s'agit du cadre d'enquête le plus lourd et le plus long.

## Comment bien déposer plainte ?

Un « bon dépôt de plainte » peut faire une très grande différence sur le déroulement et éventuellement sur l'issue de l'enquête. Il s'agit donc d'un point qu'il ne faut pas négliger.

Quel que soit le cadre juridique de l'enquête, celle–ci peut être longue, de l'ordre de plusieurs mois, surtout si l'incident « sort des frontières ». Le plaignant doit garder à l'esprit la problématique de conservation des traces.

Celles qui le concernent (relatives à l'incident donnant lieu à plainte) doivent absolument être conservées, dans leur totalité. Le matériel ne doit pas être réutilisé, il doit être déconnecté du système informatique afin d'éviter les risques de destruction accidentèle de traces.

Une action rapide peut être déterminante car les journaux d'activité (FAI, sites Web, cyber–cafés) ont une durée de vie limitée. Si tous les gros FAI français conservent leurs journaux en moyenne durant un an, il n'y a aucune obligation effective en cela, et les sociétés implantées hors de France peuvent avoir des durée de conservation nettement plus brèves.

Enfin, s'il y a eu dépôt de plainte, il ne faut surtout pas contacter ou informer l'auteur de l'incident. Cela reviendrait à lui laisser toute lattitude pour détruire les traces qu'il pourrait avoir laissé, où qu'elles soient.

Question : quelle est la durée « optimale » de conservation des journaux de bord ?

Réponse : la CNIL dit « pas plus d'un an ». Les enquêteurs, quant à eux, disent « pas moins d'un an ». Il n'existe pas de règle, mais une durée longue est préférable. Outre la conservation des journaux, il faut s'assurer qu'ils ne peuvent pas être modifiés une fois archivés, et assurer les collaborateurs qu'ils

4 Il n'y a pas de précision de délai dans les textes. Ce sont les usages dans chaque Tribunal qui fixent ce « temps proche ». Le délai varie de 48 heures à une semaine, suivant les parquets. Le Code de Procédure précise par contre que l'enquête ne saurait excéder 8 jours, sauf cas particulier; au-delà, il y a basculement en enquête préliminaire (B) ou ouverture d'une information judiciaire (C).

ne seront utilisés que dans des cadres bien délimités

Question : imaginons que je relève un problème sur un site Web, et qu'il soit par exemple possible de consulter les données relatives aux clients du site (dans le style « affaire Tati »). Que dois–je faire ?

Réponse : il y a deux cas.

- Soit « je » suis client de l'entreprise en question, auquel cas j'ai toute légitimité à porter le dossier devant la CNIL (la protection de mes données personnelles n'est pas assurée) et à informer ladite entreprise du problème.
- Soit « je » ne suis pas client, et alors il n'y a aucune légitimité à « creuser le problème », ce qui pourrait tomber sous le coup de la loi Godfrain. Il reste pertinent d'informer la société qu'elle a ce genre de problème.

Question : Et s'ils ne font rien ?

Réponse : Plutôt que de creuser l'incident et le mettre sur la place publique, il est conseillé de passer par un CERT ou toute autre association officielle, qui aura plus de poids afin de faire bouger l'entreprise en question.

# Génération d'expressions rationnelles

Présentation de Denis Ducamp, HSC Toulouse.

http://www.ossir.org/resist/supports/cr/20040830/slct.pdf

Les différents outils dont nous nous servons écrivent souvent des informations dans des journaux de bord, que ce soit via syslog() ou par des outils spécifiques. L'administrateur réseau et le service sécurité doivent traiter ces données (sinon, il est inutile de les générer), et en extraire les éléments significatifs (qui peuvent différer selon les points de vue).

Après une remise en perspective de la notion de journalisation, nous avons abordé la question de l'extraction des informations « pertinentes » dans le volume des journaux de bord. Deux approches sont possibles :

- Une approche exhaustive et systématique, à base de listes blanches (événements autorisés, dont on ignore la présence dans les journaux) ou noires (événements dont l'occurrence dans un journal provoque une alarme), et
- Une approche expérimentale de mise en place progressive de filtres permettant, à partir d'un existant, de classifier les informations et de produire des alertes adaptées.

L'approche expérimentale revient à analyser les journaux dont on dispose et à en extraire les chaînes de caractères qui nous intéressent (soit pour les ignorer, soit au contraire pour avertir l'exploitant). Cette approche est efficace, mais laborieuse : un système actif peut produire plusieurs dizaines de méga–octets de journal de bord par jour.

L'outil présenté, `slct` (Simple Logfile Clustering Tool), accessible à l'URL http://kodu.neti.ee/~risto/slct, permet d'accélerer et de simplifier cette phase préliminaire d'analyse des journaux. Le principe est simple : l'outil examine un fichier et tente d'en extraire des expressions rationnelles qui décrivent plus d'un certain nombre de lignes.

Il ne reste à l'exploitant qu'à adapter ces expressions rationnelles selon les outils qui vont les traiter (grep, egrep, pcregrep n'utilisent pas les mêmes syntaxes), à les généraliser ou à les spécialiser, selon les besoins.

On peut définir trois classifications des chaînes à rechercher dans les journaux :

- les messages à ignorer, qui correspondent à des messages normaux de l'outil ou du système,
- les messages à remonter à l'exploitant, qui correspondent à des incidents ou des événements significatifs, et
- les messages restants, « non identifiées », qui vont permettre d'augmenter les listes précédentes.

L'ordre d'application des expressions régulières, pour nettoyer les journaux, peut être :

1. retirer du journal les chaînes à ignorer, rechercher dans ce reliquat les chaînes à remonter à l'exploitant et les lui envoyer, ou
2. rechercher les chaînes à remonter et les envoyer à l'exploitant, les retirer du journal ainsi que les chaînes à ignorer.

Dans le premier cas, si les expressions rationnelles décrivant les chaînes à ignorer sont trop permissives ou trop générales (cas où, du fait de l'expansion de méta–caractères, l'intersection avec la liste des expressions rationnelles à remonter n'est pas vide) le risque existe d'ignorer des événements importants. On préfèrera donc le second cas.

Dans les deux cas, le reliquat après ces extractions correspond à des chaînes inconnues, et doit donc *a priori* être remonté à l'exploitant pour qu'il puisse investiguer, adapter les listes à ignorer ou à remonter, etc.

Dans tous les cas, le fichier sur lequel on travaille est une copie du fichier archivé. La version archivée est la version complète telle que produite par les outils ou le système, et non pas la version nettoyée après application de diverses expressions rationnelles.