Réunion OSSIR/SUR du 5/12/2000

I - Annonces diverses

- La prochaine AG aura lieu le matin de la prochaine réunion (10H, à confirmer) à l'ENS Cachan.
5 postes à pourvoir au CA (3 administrateurs dont le mandat a expiré,
1 démissionnaire, 1 non pourvu)
- profession de foi à envoyer à secretaire@ossir.org
- Produits dont on pourrait parler : Tripwire (qui vient de s'installer en France).

II - Echelon par Patrick Le Guyader (PLG Conseil)
---
1. Présentation
---
* Introduction
L'intervenant est un ex du Ministère de l'Intérieur. Il est resté à Kourou pendant 5 ans, de 1991 à 1996 et a vécu l'échec du vol 501 d'Ariane (le 4 juin 1996), puis est rentré à la fin de son contrat en Métropole fin 1996.
Il est actuellement consultant indépendant (www.atce.net).
On a beaucoup parlé d'Echelon mais il faut savoir que d'autres systèmes du même type existent ailleurs, comme par exemple le réseau SORM mis en place par l'ex-KGB (FSB). Récemment, les ISP russes ont été contraints d'accepter le raccordement de leur réseau au FSB.
En Angleterre, une loi récente oblige les providers à permettre l'accès à leurs réseaux au gouvernement UK.
En France, jusqu'au début des années 90, l'existence d'Echelon était pratiquement inconnue. Il aura fallu attendre la guerre du Golf pour que des satellites d'observation Héliosynchrones (Elios) soient lancés depuis Kourou.
* Info et desinformation
Sur Internet, dans les newsgroups et les forums de discussion, il y a énormément de désinformation ou d'informations complètement dépassées. Par exemple, après le crash de l'Airbus en Alsace, un certain nombre d'information erronées ont été diffusées par un concurrent.
* NSA
La NSA, National Security Agency, a été créée en 1952. Elle disposerait aujoud'hui d'un budget de 24 milliards de France et employerait plius de 40.000 personnes à l'écoute des télécommunications échangées dans le monde entier (téléphone, fax, GSM, e-mail etc.).
C'est le plus grand service de renseignement au monde.
Le projet Echelon a été initié dans un 1er temps par le pacte UKUSA (UK-USA) à la fin de la deuxième guerre mondiale, puis par la signature d'un accord secret entre les Etats-Unis, le Canada, Nouvelle Zélande, l'Australie et la Grande Bretagne.
Le réseau Echelon (projet 415) serait opérationnel depuis 1970.
Au départ, il y avait 9 stations d'écoute de part le monde. Aujourd'hui, il y en aurait une cinquantaine dans 20 pays sur les 5 continents.
95% des informations sont traitées par ordinateur. Les câbles sous-marins feraient l'objet d'une écoute intensive, comme les communications cellulaires.

La deuxième version du réseau existerait depuis 1979. Elle comprendrait 9 satellites VORTEX géostationnaires dont deux en charge de l'Europe.
D'ailleurs, les informations transmises en Europe sont traitées à la base de Menwith Hill, en UK. De plus, les satellites commerciaux de communication (comme INTELSAT) sont également écoutés.
Autre réseau : INTELINK. C'est un réseau de renseignement politique créé par le directeur de la CIA en 1994 et utilisé par 50.000 personnes. INTELINK peut être considéré comme l'intranet de la communauté du renseignement américain. Il existerait d'autres réseaux de ce type...
* Sécurité et manipulation : Crypto AG
Cette société suisse développait des logiciels de chiffrement qui contenaient des backdoors permettant de décrypter toutes les informations ainsi chiffrées. Elle travaillait pour des services de renseignement étrangers.
* Outils de recherche stratégique sur Internet
Des outils tels que TOPIC, SPIRIT, TAIGA permettent de faire de l'analyse sémantique (interrogation en langage naturel).
QWAM permet de fournir une interface unique permettant l'accès à plus de 350 bases de données (cf. http://www.quam.com).
* Chiffrement et outils de sécurité
Depuis la libéralisation de l'utilisation du chiffrement en France en mars 1999 (seuil relevé à 128 bits), beaucoup d'outils de chiffrements forts sont disponibles.
* Enquête du parlement européen sur Echelon
Le britanique Ducan Campbell, expert scientifique et investigateur, a révélé l'existence du réseau Echelon dès 1987. Le 5 mai 1999, à la demande du parlement européen, il a publié un document intitulé "Interception Capabilities 2000".
* La privatisation mondiale du renseignement
Aujourd'hui, des cadres sont formés à la guerre de l'information et on constate l'émergence de sociétés de renseignement privées (reconversion des hommes de l'ombre).
Aux USA, à l'université de la Défense nationale, on étudie les stratégies et les techniques de combat (guerre de l'information). En France, une école de guerre de l'information a été créée : DESS d'intelligence économique.
* Le role des gouvernements
Les américains, comme dans d'autres pays, forment leurs conseillers aux questions liées à l'Intelligence économique.
On peut dire qu'à côté des USA, l'Europe a une capacité de réaction mais un retard certain.
* Remarques et conclusions
L'économie est considérée aujourd'hui comme une composante de la Défense Nationale et Internet, comme une arme. L'info-guerre peut consister à déstabiliser une entreprise en diffusant de fausses informations dans des news groups, des forums, etc.
Pour relever le défi Américain sur ces nouveaux champs de bataille du renseignement la France et l'Europe sont-elles préparées ?
La réponse est négative compte tenu du retard pris (environs 20 ans) dans l'écoute satellitaire mais on peut espérer que le Vieux Continent, étant maintenant informé, sera à même de combler ce retard le plus tôt possible...

2 – Questions

Q: Beaucoup d'informations sont communiquées au conditionnel, qu'est-ce qui est vrai dans ce qu'on entend ?
R: Compte tenu de mon passé professionnel, je ne peux pas répondre précisément mais les médias se font suffisamment l'écho sur les sujets évoqués pour nous mettre en garde contre une utilisation contrôlée de tous les systèmes d'information...

Q: Il existe un film de la Télévision Néo-zélandaise qui montre les bases du pays où ils sont entrés : ils ont tout filmé. On voit de grandes salles machines avec des ordinateurs, et au niveau des bureaux, une salle de contrôle : une seule personne vient de temps en temps, aucun service de sécurité. La police a été prévenue de l'intrusion (probablement via une alarme discrète) mais le temps qu'elle arrive, ils ont filmé pendant 30-45 min. Il n'y a rien d'extraordinaire : juste grande salle machine avec machines classiques. Ce film passe dans certaines conférences.

Q: Points d'écoute chez ISP ?
R: En France, a priori pas grand chose.

Q: Que peut être intercepté ? Par téléphone fixe ? Par mail ?
R: Téléphone fixe à Paris par exemple, mais hors surveillance spécifique, a priori pas d'écoute.

Q: Utiliser du bon chiffrement : français ?
R: En France, certaines sociétés ne font pas les choses bien, donc ne pas choisir en fonction de critères géographiques. OpenPGP semble être la meilleure solution actuellement.

Q: Etape transitoire, pourquoi se limiter à 128 bits ? Une loi avait été annoncée ?!
R: NSP. La loi annoncée va bientôt sortir [NDLR: il s'agit de la LSI, Loi de la Société de l'Information. Elle devait être inscrite au calendrier parlementaire de l'année 2001, mais puisqu'il est déjà très chargé, il se peut qu'elle ne soit débatue au Parlement qu'au début de l'année suivante.]

3 – Références

Demande commune de plusieurs organisations afin que soit analysées les effets sur la vie privée des états-uniens 07/06/1999
http//www.cdt.org/security/echelon/echelon_signon.html

Système neuronal Berger-Liaw de reconnaissance de la parole plus rapide qu'une oreille humaine fine en environnement bruyant 30/09/1999
http//www.usc.edu/ext-relations/news_service/releases/stories/36013.html

Article dans Zdnews 29/06/2000
http//www.zdnet.co.uk/news/2000/25/ns-16248.html

Analyse de la FAS (Federation of American Scientists) 24/02/2000
http//www.fas.org/irp/program/process/echelon.htm

III - Le point sur la responsabilité juridique des administrateurs système

Olivier Perret, perret@pasteur.fr

1. Introduction

Cette intervention a été préparée à l'aide de l'ouvrage : "Droit de l'Internet" par Valérie Sédaillan (Netpresse) et le texte du jugement concernant l'ESPCI.
L'Internet n'est pas une zone de non droit, contrairement à ce qu'on a pu entendre parfois.
Le thème de la responsbailité juridique des administrateurs a déjà été abordée il y a quelques années à l'Ossir. Aux USA, on trouve des modèles de documents à faire signer à un employeur de façon à dégager la responsabilité d'un administrateur système. A priori, de tels documents n'existent pas en France.
Il y a beaucoup de chartes à destination des utilisateurs mais pas grand chose pour les administrateurs.
Concernant l'affaire de l'ESPCI, on en a beaucoup entendu parler dans la presse mais le jugement a été très mal relaté. Une des accusés est présente aujourd'hui : Françoise Virieux.

2. Intervention de F. Virieux

L'affaire a commencé en 1996 : une étudiante avait perdu tous ses fichiers : un des fichiers modifiés portait le nom d'un autre utilisateur du laboratoire, il avait pu modifier ce fichier car elle avait voulu restreindre les droits d'accès à un fichier mais s'était trompée, seuls cet utilisateur, T. et moi pouvions le modifier.
C'était lui : contacté, il dit que son compte a été piraté, Or, après enquête, il semblerait qu'il n'y ait eu aucun problème de ce type.
Deux mois plus tard, la même étudiante découvre que quelqu'un a envoyé un mail signé de son nom à une publication scientifique disant de ne pas publier un article qu'elle avait écrit alors qu'elle n'avait jamais fait une telle demande.
Elle accuse T. Il dément. Les soupçons se portent sur lui. En surveillant les fichiers de logs, j'ai vu qu'il recevait 50% des courriers reçus et envoyés par tout le laboratoire. Lui, recevait du mail de fournisseurs ISP et non pas d'adresses d'autres laboratoires (ENS, etc.).
Information du Directeur : il me dit de regarder s'il ne nuit à personne. Je le fais quelques jours puis j'abandonne. Mais plus tard, au court d'une opération de maintenance du serveur de messagerie, nous avons trouvé des propos diffamatoires et le Directeur m'a demandé de fermer le compte de T. qui n'est alors jamais revenu.
Quelques temps plus tard, convocation au commissariat pour destruction de données : cela ne semble pas grave.
Six mois après (en 1998), nouvelle convocation mais cette fois au SEFTI : je réponds que j'ai bien ouvert les mails de T.
Je suis mise en examen avec l'autre chercheur et du Directeur de laboratoire.
Le procès a eu lieu le 28 septembre 2000 et le verdict prononcé en novembre.
Condamnation : 10.000F solidairement + 5.000F chacun + amende de 10.000F pour moi et le Directeur, 5.000F pour l'autre car il aurait ouvert le mail par hasard suite à un problème.
Conclusions de la presse : mail = correspondance privée. Ok, mais c'était dans le cadre d'une utilisation professionnelle au labo. Aucune saisie n'avait été effectuée.
Le SEFTI n'avait pas compris la notion de répertoire personnel, par rapport à un ordinateur personnel. Impossible de s'exprimer au procès.

3. Conclusions

Il apparaît qu'il aurait fallu faire signer la charte par chacun : il existait une charte affichée dans le laboratoire et envoyée par mail à chacun mais le défendeur a affirmé ne pas en avoir eu connaissance.
Par ailleurs, on aurait dû employer les grands moyens dès le départ : porter plainte pour obtenir une perquisition et ne pas tenter de faire des investigations par nous-même.
D'après le code pénal, il existe deux articles concernant l'interception et le détournement de correspondances privées : les articles 432-9 et 226-15. Il semble que cela ne soit pas la même chose dans le public et dans le privé :- dans le public (fonctionnaire), que ce soit de bonne ou de mauvaise fois, c'est interdit (art. 432-9).- dans le privé, il faut prouver la mauvaise foi (art. 226-15).
Dans cette affaire, le Tribunal a estimé que les accusés étaient "investis d'une mission de service public", ce que ceux-ci ne comprenaient pas.
En conclusion, il aurait fallu informer les ingénieurs système de leurs droits et devoirs.
Cf. http://www.sage.com
Voir aussi le numéro de décembre d'Infosecu (http://www.cnrs.fr/Infosecu/Revue.html).
-- Eric Larcher (web@larcher.com, http://www.larcher.com)