A propos des journaux de traces (fichiers de logs)

I - Introduction

Après réflexions collectives, il nous semble opportun de vous exposer un certain nombre d'éléments à propos de l'informatique, de son usage et des informations recueillies lors de son utilisation.

Notre routeur et tous nos serveurs informatiques prévus pour proposer des services réseaux (courrier électronique, serveur Web, accès distant, etc) produisent un certain nombre de journaux de traces (aussi dénommés fichiers de logs) dans lesquels sont consignées les traces de certaines activités des systèmes et de leur utilisation.

Pour une bonne gestion des ressources communes et pour des raisons de sécurité, la Direction de l'UHA, le RSSI et l'équipe informatique du réseau, sont amenés à examiner et explorer ces journaux.

Il est donc normal que chaque utilisateur soit bien conscient des informations qui sont stockées dans ces journaux, qui sont accessibles dans le cadre de notre travail (ce qui peut aller jusqu'à fournir ces informations à des services de police ou à la DST suite à un dépôt de plainte par exemple).

Aussi il est important de sensibiliser tous les utilisateurs à l'usage qui peut être fait du réseau et aux traces figurant dans les journaux qui découlent de cet usage.

II - Inventaire, par type d'usages, des traces qui sont conservées

- Dans tout ce qui suit :
  - nom signifie en fait le nom de login, autrement dit le nom utilisé dans l'adresse de messagerie (personne physique identifiée).
  - date signifie en fait "date et heure" précises (synchronisation NTP).
  - adresse réseau signifie l'adresse Internet (adresse IP).
- Il est donc conservé trace des :
  - connexions sous toute forme vers nos serveurs et notamment :

    -> on connaît

    - le nom de l'utilisateur sous lequel la connexion se fait,
    - l'adresse réseau de la machine depuis laquelle la connexion a été faite
    - les dates de début et de fin de connexion.
  - envoi/réception de messages électroniques, vers ou depuis nos machines
    -> on connaît
    - le nom et l'adresse courriel de l'émetteur et du destinataire,
    - la date de l'envoi/réception.
  - accès à un serveur WEB distant, depuis un navigateur utilisant notre système de proxy-cache Web

    -> on connaît

- l'adresse complète de la page consultée (URL),
- la date de la connexion,
- le nom de la machine individuelle depuis laquelle est faite la connexion, ou le nom du serveur collectif depuis lequel est faite la session initiée.
  En cas de machine individuelle, on connait donc a priori l'auteur de la connexion web, à savoir l'utilisateur référencé de la machine.

Toutes ces traces sont récupérées et conservées sur une machine à laquelle seule des techniciens habilités auront accès.
Elles sont conservées sur une durée de 12 mois.

Pour se prémunir d'intrusions et d'attaques de toutes sortes, à la fois depuis l'extérieur, mais aussi depuis l'intérieur , un système de filtrage est en place.

Sont gardées des traces de toutes les tentatives de connexion qui ont été refusées, ainsi que certaines connexions qui ont été autorisées

Elles sont conservées sur une durée de 12 mois.

III - Cadre d'usage de ces informations

- Pour en savoir plus : visiter le site de la CNIL http://www.cnil.fr/ .
  Fin 2004, suite notamment au vote par le Parlement français de la loi LCEN (Loi sur la Confiance dans l'Economie Numérique), le CNRS a traité de manière globale cette question et a réalisé une déclaration générique auprès de la CNIL.
  Voici les pointeurs pour connaître des détails; ils concernent le CNRS, mais l'Université en général, et l'UHA en particulier, se trouve dans une situation identique avec des obligations semblables. :
  - Site du Fonctionnaire de Défense du CNRS,
  - Article sur le sujet des traces dans la revue *Sécurité informatique*,
  - Politique de gestion des traces, définie par le CNRS et déclarée à la CNIL,
  - Décision parue au Bulletin Officiel du CNRS,
  - Charte du CNRS.

---

màj le 13/10/2006 robert.klein@uha.fr
