Comité Réseau des Universités

Politique de gestions des journaux informatiques dans les établissements d'enseignement supérieur

serge.aumont@cru.fr

Comité Réseau des Universités

Statut du document

- Document de travail
- Inspiré de la déclaration à la CNIL des logs faite par le CNRS
- Pour le moment uniquement une proposition
- Très forte demande des établissements due à l'insécurité juridique

Comité Réseau des Universités

Un document issu de techniciens de la sécurité

- Les logs sont au cœur de la problématique de SSI
- Les universités sont
  - Employeurs
  - Hébergeur de contenus ou éditeur
  - Fournisseur d'accès internet
  - …

Comité Réseau des Universités

Les finalités

- Monitoring applications et réseau
- Surveillance de la SSI
- Détection des défaillances et intrusions
- Détection des abus contraires aux lois, aux chartes et au règlement intérieur
- Indices et éléments de preuve pour des enquêtes

Comité Réseau des Universités

Durée de conservation

- 3 mois : finalités internes
- 1 an : sur réquisition des autorités « présentées dans les formes légales »

- 2 conténaires pour 2 politiques d'accès
- Pas de spécification de l'implémentation des « conténaires »

Comité Réseau des Universités

Les intervenants

- Administrateurs
- La chaîne fonctionnelle SSI
  - Correspondant sécurité
  - RSSI
  - AQSSI
  - Fonctionnaire de défense

Comité Réseau des Universités

Les données journalisées

- Messagerie, forum, listes de diffusion
- Serveurs web internes à l'établissement
- Serveurs web externes
- Les équipements réseaux
- Les applications spécifiques

http://www.cru.fr

Première réunion annuelle du réseau des Correspondants Informatique et Libertés
mercredi 5 décembre 2007

Comité Réseau des Universités

La messagerie

- Machine d'origine et de destination
- Le « sender », les destinataires
- Tailles, Message-Id
- Données d'authentification (SMTP/AUTH)
- Filtrage anti-virus anti-spam
- Listes de diffusion : décisions des modérateurs

http://www.cru.fr

Première réunion annuelle du réseau des Correspondants Informatique et Libertés
mercredi 5 décembre 2007

Comité Réseau des Universités

Serveurs web internes

- Journalisation des accès
- Machine d'origine
- URL
- Données d'identification
- Données échangées

http://www.cru.fr

Première réunion annuelle du réseau des Correspondants Informatique et Libertés
mercredi 5 décembre 2007

Comité Réseau des Universités

Serveurs web externes

2 cas :

- Les personnels (et les étudiants ?)
- Les personnes de passage

- Article L34-1 du code des télécommunications : pas de journalisation du contenu des communications
- La mort des proxy http ?

http://www.cru.fr

Première réunion annuelle du réseau des Correspondants Informatique et Libertés
mercredi 5 décembre 2007

Comité Réseau des Universités

Équipements réseaux

Il faut pouvoir répondre à la question « A qui était attribuée cette adresse IP à cette date ? ».

- les noms ou adresses IP source et destination ;
- les numéros de port source et destination ainsi que le protocole ;
- la date et l'heure ;
- les données d'authentification ;

Comité Réseau des Universités

- L'organisation transversale des logs plus que jamais indispensable
- Ce document est une aide pour élaborer votre politique de gestion des journaux informatiques
- Les logs existent depuis toujours
- Principal gain Informatique et Libertés : assurer la transparence