

Politique type de gestion des journaux informatiques

Version 2.5 juin 2008

Ce document a été réalisé dans le cadre du groupe de travail SDS-SUP, mandaté par la Conférence des Présidents d'Université (CPU), la direction générale de la recherche et de l'innovation (DGRI), la direction générale de l'enseignement supérieur (DGES) et le Haut fonctionnaire de défense et de sécurité (HFDS) du ministère en charge de l'enseignement supérieur et la recherche.

La mission du groupe travail SDS-SUP animé par le CRU (Comité réseau des universités) est de mener des réflexions et de constituer un référentiel documentaire dans le domaine de la sécurité des systèmes d'information, notamment concernant les meilleures pratiques.

A ce titre, la « Politique type de gestion des journaux informatiques » s'est inspiré du document de « Politique de gestion de traces » du CNRS. Il a été mis à jour et complété afin garantir la cohérence globale des référentiels et la conformité à la législation et aux réglementations en vigueur, notamment pour les points relevant de la loi « informatique et libertés ». Le partenariat CPU/CNIL a permis de mener un travail collaboratif entre le groupe de travail SDS-SUP et la CNIL.

NdR : on pourra ajouter ici la position officielle de la CNIL sur le document définitif, voire ses commentaires ou conditions d'utilisation.

Politique de gestion des journaux informatiques

à

1 Définitions

- on entend par « établissement » « (désignation du nom)..... » ;
- on entend par « utilisateur » les personnels, étudiants, stagiaires, personnes invitées et en règle générale toute personne utilisant les moyens du système d'information ;
- on entend par « entités » les composantes, services ou laboratoires...

2 Contexte

Le fonctionnement de l'établissement passe par l'utilisation de systèmes d'information et de moyens de communications qui s'appuient sur des réseaux télématiques connectés à l'échelle mondiale. Ces réseaux, qui apportent une souplesse inégalée, ont également une grande vulnérabilité intrinsèque, et leur utilisation engage la responsabilité personnelle des utilisateurs, ainsi que dans certaines situations celle de l'établissement qui met ces moyens à leur disposition en tant qu'outils de travail.

L'utilisation des nouvelles technologies de communication pose le problème de la protection d'une part de l'information sensible¹ gérée par les utilisateurs et d'autre part des systèmes d'information sous la responsabilité de l'établissement. Les mesures mises en œuvre doivent permettre à l'établissement de remplir ses missions tout en satisfaisant aux exigences qui sont imposées par ses engagements vis-à-vis de ses partenaires, des réglementations sur la protection des données sensibles et la protection du patrimoine scientifique, de la loi sur la protection des données à caractère personnel (respect des droits de l'individu) et la sécurité des systèmes d'information.

Une déontologie et un contrôle de l'utilisation sont donc nécessaires, de même qu'une information et une sensibilisation des utilisateurs. L'établissement a mis en place des dispositions et moyens pour assurer la sécurité et le contrôle de l'utilisation des moyens télématiques, et d'autre part a fixé les conditions d'utilisation de ces moyens, afin de garantir les droits individuels de chaque utilisateur.

3 Principes de base

Une maîtrise de la fiabilité et de la sécurité du fonctionnement des systèmes d'information et une garantie de la légalité des transactions opérées nécessitent un contrôle s'appuyant nécessairement

¹ Informations sensibles au sens où la confidentialité (contrat, données de recherche, information nominatives, ..), l'intégrité (informations de gestion,...) et la disponibilité nécessitent une protection particulière.

sur l'enregistrement systématique et temporaire d'un certain nombre d'informations caractérisant chaque transaction, appelées journaux informatiques (ou logues).

3.1 Finalités des traitements

Les traitements de ces journaux informatiques ont pour finalités :

- de contrôler le volume d'utilisation de la ressource, détecter des anomalies afin de mettre en place une qualité de service et faire évoluer les équipements en fonction des besoins (métrologie) ;
- de vérifier que les règles en matière de sécurité des systèmes d'information (SSI) sont correctement appliquées ;
- de détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ;
- de détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité de l'établissement ;
- de détecter les utilisations des moyens informatiques contraires aux chartes ou au règlement intérieur de l'établissement.
- d'être à même de fournir les éléments de preuves nécessaires pour mener les enquêtes en cas d'incident et de répondre à toute réquisition de l'autorité judiciaire présentée dans les formes légales.

Les finalités précitées imposent d'aller au-delà d'un enregistrement et d'une exploitation de données statistiques. Ils impliquent nécessairement l'enregistrement, la conservation temporaire et l'éventuelle exploitation de données à caractère personnel, dans la mesure où des éléments contenus dans les traces permettraient de remonter à l'utilisateur.

Ces journaux et leur traitement doivent respecter les droits de chacun et notamment être conformes à la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 dite loi "Informatique et libertés". Ils doivent avoir satisfait au principe d'information préalable et de transparence ainsi qu'au régime déclaratif en vigueur auprès de la CNIL.²

3.2 Durée de conservation

La durée de conservation des journaux informatiques est de 1 an maximum. L'établissement s'interdit de les exploiter au-delà de 3 mois sauf sur réquisition officielle ou sous une forme rendue anonyme. Deux conteneurs de données sont donc définis, le premier reçoit les fichiers de logues vieux de moins de trois mois et les fichiers anonymisés quand ils existent. Le second reçoit les journaux contenant des données à caractère nominatif de plus de trois mois

3.3 Qualités des données collectées

Les informations journalisées doivent être factuelles et contextuelles, c'est à dire qu'elles doivent permettre de connaître l'environnement de la collecte, le système hôte, les logiciels mis en œuvre etc. L'heure relevée est une information importante parce qu'elle est souvent le premier élément utilisé pour rapprocher des journaux de différents serveurs. Il est donc indispensable que les machines produisant des

² Voir la fiche pratique relative au contrôle de l'utilisation des moyens informatiques dans le *Guide pratique Informatique et Libertés* pour l'enseignement supérieur et la recherche (ce guide est disponible sur le site de la CNIL et celui de l'AMUE)

logues soient synchronisées sur un serveur de temps,

D'éventuelles interruptions de la journalisation doivent être repérables par les destinataires de ces données.

3.4 Sécurité et intégrité des données

La politique de sécurité du système d'information (PSSI) fixe les règles de sécurité appliquées à ces fichiers. Ces règles assurent l'intégrité des données en les protégeant en particulier contre un effacement ou des modifications malveillantes. Au besoin, une base d'empreintes numériques ou des jetons d'horodatage permettent de surveiller l'intégrité des fichiers de journaux.

Les règles de sécurité limitent l'accès aux fichiers de logues de moins de trois mois aux seuls administrateurs destinataires de ces données tel qu'ils sont définis au paragraphe 4.2.1 avec authentification préalable. Les accès sont ponctuels et motivés par les tâches de ces personnes. Le conteneur de données consacré aux logues de plus de trois mois est en accès limité au RSSI et aux personnes désignées par le RSSI pour la mise en œuvre du droit d'accès aux intéressés et l'accès sur requête judiciaire.

La politique de sauvegarde de l'ensemble des données de l'établissement identifie les journaux contenant des données à caractère personnel dans le but de garantir leur suppression au delà d'une année.

Dans le cas d'une exploitation des journaux informatiques anonymisés, une copie anonymisée des logs est effectuée. L'anonymisation est réalisée dans le respect des règles de l'art, elle est irréversible. On se référera en particulier à l'expertise³ publiée par la CNIL dans ce domaine.

4 Les intervenants

4.1 Les utilisateurs

Tous les utilisateurs, tel qu'ils sont définis en introduction de ce document, sont tenus de respecter la politique de sécurité et les chartes en vigueur dans l'établissement.

4.2 La chaîne fonctionnelle SSI

En dehors des acteurs de la chaîne fonctionnelle rappelée ci-dessous, personne n'a de droit d'accès aux journaux informatiques comportant des données à caractère personnel, y compris la chaîne hiérarchique. **Ils sont tenus au devoir de réserve ou de discrétion professionnelle, voire au secret professionnel.**

4.2.1 Les administrateurs systèmes et réseau

Ils sont chargés de la mise en œuvre et de la surveillance générale des systèmes et du réseau et veillent au respect des règles de sécurité des systèmes d'information. À ce titre, ils gèrent les traces dans le respect des obligations générales de leur fonction (politique de sécurité, chartes).

³ <http://www.cnil.fr/index.php?id=1536>

Ils rapportent, à leur supérieur dans la chaîne fonctionnelle SSI, toute anomalie de fonctionnement ou tout incident pouvant laisser supposer une intrusion ou une tentative d'intrusion sur les systèmes ou le réseau.

Ils acceptent d'exécuter des traitements ou de fournir des informations pouvant inclure des données à caractère personnel uniquement à la demande de la chaîne fonctionnelle de sécurité.

4.2.2 Les autres acteurs de la chaîne fonctionnelle SSI :

- les correspondants de sécurité des systèmes d'information,
- le responsable de la sécurité des systèmes d'information (RSSI),
- l'autorité qualifiée de sécurité des systèmes d'information (AQSSI),
- le fonctionnaire de sécurité de défense (FSD).

Ils sont également tenus au devoir de discrétion professionnelle, et dans certains cas de secret professionnel en fonction de leur mission.

5 Les informations enregistrées

5.1 Informations journalisées par les serveurs (hors messagerie et Web) et postes de travail

Pour chaque tentative de connexion, d'ouverture de session de travail ou de demande d'augmentation de ses droits, tout ou partie des informations suivantes peuvent être enregistrées automatiquement par les mécanismes de journalisation du service :

- l'identité de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative (succès ou échec) ;
- les commandes passées.

Le choix d'une politique de centralisation des journaux informatiques des postes de travail peut être fait.

5.2 Services de messagerie, de messagerie instantanée, de forum et de listes de diffusion

Les serveurs hébergeant ces services mis en œuvre au sein de l'établissement enregistrent pour chaque message émis ou reçu tout ou partie des informations suivantes :

- l'adresse de l'expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur ;
- l'adresse des destinataires ;
- la date et l'heure de la tentative ;
- les différentes machines traversées par le message ;
- le traitement « accepté ou rejeté » du message ;
- La taille du message ;

- Certaines en-têtes du message, tel que l'identifiant numérique de message ;
- Le résultat du traitement des courriers non sollicités (spam) ;
- Le résultat du traitement antiviral ;
- Les opérations de validation ou de rejet par les modérateurs quand cela s'applique.

Les éléments de contenu des messages ne sont pas journalisés, néanmoins, les applications peuvent inclure des archives qui ne relèvent pas des journaux informatiques (chrono départ et réception).

5.3 Serveurs Web

On distingue les serveurs web exploités au sein de l'établissement et ceux situés en dehors de l'établissement

5.3.1 Serveurs Web de l'établissement

Pour chaque connexion les serveurs Web enregistrent tout ou partie des informations suivantes en fonction des exigences de qualité de service et de sécurité de l'application web :

- les noms ou adresses IP source et destination ;
- les différentes données d'authentification dans le cas d'un accès authentifié (intranet par exemple) ;
- l'URL de la page consultée et les informations fournies par le client ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;
- les différents paramètres passés.

5.3.2 Serveurs Web hors établissement

Lors que les utilisateurs sont des membres de l'établissement, pour chaque accès web via le réseau interne vers des serveurs externes peuvent être enregistrées tout ou partie des informations suivantes :

- les noms ou adresses IP source et destination et les différentes données d'authentification ;
- l'URL de la page consultée ;
- le type de la requête ;
- la date et l'heure de la tentative ;
- le volume de données transférées ;

L'article L.34-1 du code des postes et des communications électroniques précise que les opérateurs de communications électroniques sont tenus à une obligation de conservation des données de connexion mais que celles-ci "ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ". Cette interdiction s'applique donc en particulier à l'URL des pages consultées dans le cas où l'établissement offre des accès internet à des personnes extérieures à l'établissement. En effet, il est alors possible d'assimiler le service réseau de l'établissement à celui d'un opérateur de communications électroniques.

5.4 La téléphonie sur IP

L'usage de la téléphonie sur IP peut engendrer des enjeux spécifiques dans le domaine de la sécurité ou dans celui du contrôle du bon fonctionnement des réseaux, mais bien entendu, les principes relatifs à la loi « Informatique et Libertés » s'appliquent à la téléphonie sur IP comme aux autres systèmes de téléphonie.

Lorsque des relevés justificatifs des numéros de téléphone appelés sont établis, les quatre derniers chiffres de ces numéros sont occultés. Cependant, l'établissement peut éditer des relevés contenant l'intégralité des numéros appelés dans le cas où il demande aux personnels le remboursement du coût des communications personnelles ou dans celui où il a été constaté une utilisation manifestement anormale.

Le régime déclaratif de ces journaux fait l'objet de la norme simplifiée n° 47⁴ relative à l'utilisation de services de téléphonie fixe ou mobile sur les lieux de travail. En outre, la fiche pratique n°11 du guide « informatique et libertés » pour l'enseignement supérieur et la recherche⁵ intitulée « Utilisation du téléphone sur le lieu de travail » détaille ce cas.

5.5 Les équipements réseau

On appelle « équipements réseau » les routeurs, pare-feu, commutateurs, bornes d'accès, équipement de métrologie et d'administration de réseau, etc. Pour chaque paquet qui traverse l'équipement tout ou partie des informations suivantes peuvent être collectées :

- les noms ou adresses IP source et destination ;
- les numéros de port source et destination ainsi que le protocole ;
- la date et l'heure de la tentative ;
- la façon dont le paquet a été traité par l'équipement ;
- le nombre de paquets et le nombre d'octets transférés ;
- les données d'authentification ;
- les messages d'alerte.

5.6 Les applications spécifiques

On entend par « applications spécifiques », toute application autre que celles mentionnées ci-dessus qui nécessite pour des raisons de comptabilité, de gestion, de sécurité ou de développement, l'enregistrement de certains paramètres de connexion et d'utilisation.

Parmi ces applications nous pouvons citer les exemples suivants :

- accès aux bases de données ;
- accès à l'ENT (espace numérique de travail) ;
- service d'authentification (SSO) ;

Comme dans le cas des serveurs web internes, des journaux génériques sont susceptibles d'être constitués et tout ou partie des informations suivantes peuvent être collectées :

- l'identité de l'émetteur de la requête ;
- la date et l'heure de la tentative ;
- le résultat de la tentative ;
- les volumes de données transférées ;

⁴ <http://www.cnil.fr/index.php?id=1777>

⁵ http://www.cnil.fr/fileadmin/documents/approfondir/dossier/education/Guide_InfoLib_Web.pdf

- les commandes passées ;

Le traitement des logues décrit ici ne couvre pas l'ensemble des données conservées par ces applications qui de par leur nature peuvent historiser certaines transactions. Il est rappelé que si ces données visant à assurer la traçabilité des opérations ont un caractère personnel, elles sont alors soumises aux obligations de la loi Informatique et Libertés (déclaration auprès de la CNIL sauf en cas de désignation d'un Correspondant Informatique et Libertés (CIL), information préalable, etc).⁶

6 Finalités des traitements effectués et leurs destinataires

Les traitements effectués doivent permettre d'obtenir des journaux qui répondent aux principes de base énoncés précédemment, tout en restant conformes aux obligations légales sur la protection des données à caractère personnel et de la vie privée.

6.1 Résultats statistiques

Ceux-ci sont effectués automatiquement et permettent de contrôler les volumes d'utilisation des moyens mis à la disposition des utilisateurs en temps qu'outil de travail. Lors de l'exploitation de ces résultats on s'attachera à distinguer les résultats anonymes de ceux qui peuvent être rapprochés de l'identité d'une personne. Parmi tous ces traitements on trouvera :

- des traitements statistiques en anonyme, en volume transféré et en nombre de connexions ;
- des classements des services les plus utilisés en volume de données et en nombre de connexions ;

Les résultats « anonymes » peuvent être conservés au-delà des délais mentionnés au paragraphe 3 et être diffusés sur des sites Internet accessibles à tous. Par contre, les administrateurs systèmes et réseau limitent l'accès aux résultats contenant des données à caractère personnel à eux-mêmes et éventuellement à la chaîne fonctionnelle SSI. La durée de conservation de ces statistiques non anonymisées ne peut excéder celle des journaux utilisés pour produire ces statistiques.

6.2 Résultats d'analyse

La politique de sécurité, applicable à chaque ressource informatique qui génère des traces, définit des règles d'analyse systématique de ces traces afin de pouvoir détecter, dans les meilleurs délais, les incidents relatifs à la sécurité des systèmes d'information.

En cas d'incident, des analyses peuvent être faites par les administrateurs systèmes et réseau sur les traces disponibles. Les résultats ne peuvent être transmis qu'à la chaîne fonctionnelle SSI et au CERT-Renater ou CERTA pour les incidents de sécurité.

Dans ce cas, l'accès aux trafics et aux traces est limité aux exploitants des systèmes en charge d'analyser l'incident et au RSSI. L'extraction de l'information et son utilisation sont strictement limitées à l'analyse de l'incident. Si l'incident n'est pas avéré les résultats sont non transmis et

⁶ Le Correspondant Informatique et Libertés a été introduit en 2004 avec la réforme de la loi informatique et libertés. Sa désignation permet d'être exonéré de l'obligation de déclaration préalable des traitements ordinaires et courants. Seuls les traitements identifiés comme sensibles dans la loi demeurent soumis à autorisations et continuent à faire l'objet de formalités. Il a un rôle de conseil et suivi dans la légalité de déploiement des projets informatiques et, plus largement, de la gestion de données à caractère personnel.

immédiatement détruits.

6.3 Détection des usages abusifs

On entend ici par « usages abusifs » les usages du réseau qui sont contraires aux lois, règlement intérieur ou chartes d'usage des moyens informatiques. Sont aussi visés les usages qui compromettent les services du réseau de l'établissement (consommation excessive de bande passante, introduction de faille dans la sécurité du réseau, etc).

Les logues peuvent être exploités pour mettre en évidence ces abus. Par exemple, des classements des machines ayant consommé le plus de réseau en volume transféré et en nombre de connexions permettent souvent de détecter l'utilisation indésirable de protocoles de peer to peer ou la présence de serveurs pirates. Se référer à la fiche pratique « Contrôle de l'utilisation des moyens informatiques » du *guide pratique « Informatique et Libertés » pour l'enseignement supérieur et la recherche*.

Quand ils sont mis en œuvre, ces traitements le sont de façon systématique (ils sont appliqués à toutes les machines du réseau de l'établissement ou d'une partie donnée du réseau) et ne ciblent aucune personne ou catégorie de personnes.

6.4 Des journaux bruts

Ceux-ci permettent de replacer une action particulière dans son contexte, à des fins d'enquête. Dès l'apparition d'un incident, les journaux bruts pourront être requis par la chaîne fonctionnelle.

Les administrateurs systèmes et réseau sont chargés de l'application de la requête, et ils sont, pour cette activité, soumis au secret professionnel.

Les journaux bruts sont remis, à sa requête à l'autorité judiciaire afin de lui permettre de poursuivre une enquête.

6.5 Droit d'accès individuel

Chaque agent peut demander à consulter les traces qui le concernent. Les demandes doivent être faites par écrit auprès du directeur de l'entité d'hébergement.

La recherche est faite par l'administrateur, sur demande de sa hiérarchie, et les résultats sont transmis directement à l'utilisateur demandeur, sous la forme d'un «courrier personnel».

7 Informations des utilisateurs sur la politique de gestion des journaux informatiques

L'établissement doit informer ses utilisateurs de la gestion qui est faite des traces qui les concernent. Cela sera fait par la diffusion systématique de ce document qui sera référencé dans la charte informatique de l'établissement. Ce document sera rendu accessible à tout utilisateur par le réseau. Il pourra être mis en valeur dans l'intranet de l'établissement ou par voie d'affichage. Une attention particulière sera portée à la publicité de ce document lors de la mise à disposition de nouveaux services concernés par les journaux informatiques ainsi qu'auprès des nouveaux utilisateurs des moyens informatiques de l'établissement.⁷

⁷ Se reporter au guide pratique de la CNIL à l'attention des employeurs, sections "cybersurveillance sur le

Une information et une consultation préalable des instances représentatives des personnels doit être prévue.

Document de travail