Politique de gestion des traces informatiques

Sommaire

1. Préambule

Tout système d'information comporte la mise en œuvre de **journaux informatiques, qui consistent à tracer au cours du temps certaines actions données sur les équipements informatiques**.

De tels journaux s'avèrent nécessaires pour maîtriser la fiabilité et la sécurité des systèmes d'information. En particulier, ils sont utiles pour optimiser le déploiement des ressources (par exemple pour améliorer la répartition géographique des bornes Wi-Fi), ou encore pour analyser un problème (par exemple comprendre pourquoi tel courriel a été bloqué sur le serveur de messagerie).

Par ailleurs, l'université a l'obligation légale de conserver certaines traces de connexions pendant 12 mois, car celles-ci peuvent faire l'objet d'une réquisition judiciaire.

Le présent document décrit la politique de gestion des traces informatiques mise en œuvre à l'université Jean Moulin – Lyon 3.

2. Définitions

Journal informatique : fichier chronologique sur un équipement informatique, traçant certaines actions données au cours du temps.

Système d'information : ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications pouvant être mis à disposition par l'université.

Utilisateur : toute personne ayant accès aux ressources des systèmes d'information de l'université.

Administrateur système et réseau : agent ayant en charge l'administration informatique de serveurs et/ou d'équipements réseau.

Responsable de la Sécurité des Systèmes d'Information (RSSI) : personne en charge de la sécurité des systèmes d'information. Tout établissement d'enseignement supérieur doit désigner un RSSI titulaire et un RSSI suppléant, dont les contacts sont connus par le Ministère.

3. Principes

Certains journaux informatiques comportent des données permettant d'identifier, directement ou indirectement, des personnes : login de l'utilisateur, adresse IP[1], etc. La mise en œuvre de tels journaux constitue un traitement de données à caractère personnel, soumis au respect de la loi « Informatique et Libertés ». Les grands principes de la protection des données personnelles s'appliquent donc :

- la finalité doit être déterminée et légitime ;
- les données collectées sont pertinentes au regard de la finalité ;
- la durée de conservation est limitée, et proportionnelle à la finalité ;
- des mesures de sécurité empêchent que les données ne soient modifiées ou divulguées à des tiers non autorisés ;
- les personnes sont informées de l'existence du traitement et peuvent exercer leurs droits d'accès, de rectification et d'opposition.

[1] Adresse IP : adresse permettant d'identifier un ordinateur, par exemple 192.168.0.1.

Toute précision relative à la mise en œuvre des journaux dans le respect de la loi « Informatique et Libertés » peut être obtenue auprès du correspondant Informatique et Libertés de l'université (cil@univ-lyon3.fr).

Par ailleurs, il existe d'autres journaux ne permettant pas d'identifier des personnes : les données sont en ce cas anonymes. De tels journaux peuvent être conservés pendant une durée plus longue.

4. Finalités

La mise en œuvre de journaux informatiques vise plusieurs finalités distinctes :

- l'établissement de statistiques et d'indicateurs pour optimiser et faire évoluer les systèmes d'information ;
- la détection et l'analyse d'anomalies ou d'incidents de sécurité ;
- la détection des abus (usages contraires à la réglementation, au règlement intérieur ou pouvant engager la responsabilité de l'établissement) ;
- la mise à disposition des journaux sur réquisition judiciaire.

4.1. Evolution et optimisation des systèmes d'information

La mise en œuvre et le suivi d'indicateurs sont nécessaires pour prévoir l'évolution et l'optimisation des systèmes d'information.

Exemple : les journaux de connexion Wi-Fi permettent de générer des statistiques pour améliorer la répartition géographique des bornes Wi-Fi selon le nombre d'utilisateurs.

4.2. Détection et analyse des anomalies ou incidents de sécurité

En cas de comportement anormal, de dysfonctionnement remonté par un utilisateur, ou d'incident de sécurité, les administrateurs système et réseau et le RSSI s'appuient sur les journaux informatiques pour analyser les événements déroulés.

Exemple : un utilisateur ne parvient pas à accéder à une ressource donnée de l'ENT ; les administrateurs système et réseau analyseront les journaux du serveur concerné pour identifier la nature du problème.

Exemple : un utilisateur signale n'avoir pas reçu un courriel que son correspondant assure avoir pourtant envoyé ; les administrateurs système et réseau analyseront les journaux du serveur de messagerie pour comprendre ce qui s'est passé.

Exemple : un incident de sécurité, tel qu'un déni de service, se produit sur un serveur web ; les journaux seront utilisés pour analyser l'incident.

4.3. Détection des abus

L'université doit pouvoir s'assurer que l'usage des systèmes d'information n'est pas contraire à la réglementation ni au règlement intérieur, et ne compromet pas la fourniture des services réseau de l'établissement.

Exemple : les journaux peuvent permettre de détecter un nombre de connexions réseau très important, qui pourrait signaler la présence d'un logiciel malveillant sur un poste de l'université.

Exemple : les journaux peuvent mettre en évidence la saturation d'un équipement réseau, due à l'introduction non autorisée d'un matériel réseau.

Exemple : un envoi massif de courriels peut révéler qu'un compte de messagerie de l'université est utilisé par un intrus qui aurait découvert les identifiants du compte.

4.4. Mise à disposition des journaux sur réquisition judiciaire

L'autorité judiciaire peut présenter une réquisition visant la mise à disposition de certains journaux informatiques, dans le cas d'une enquête. Dans ce cas, le RSSI et le service des affaires juridiques s'assurent que la mise à disposition est réalisée conformément à la réglementation.

5. Destinataires des données

L'accès aux journaux informatiques comprenant des données personnelles est strictement réservé aux personnes habilitées, dans le cadre de leurs missions.

Ainsi :

- Les administrateurs système et réseau accèdent aux journaux informatiques de manière ponctuelle et motivée par les tâches dont ils sont chargés.
- Le RSSI consulte les journaux en cas d'incident de sécurité ou dans le cadre de la détection des abus.
- En cas d'incident de sécurité, le RSSI peut transmettre au CERTA[2] et au CERT-Renater[3] des extraits de journaux à des fins d'analyse.
- Dans le cas d'une utilisation manifestement abusive de la téléphonie, le supérieur hiérarchique peut demander à établir, de façon contradictoire avec l'agent concerné, un relevé justificatif complet des numéros de téléphone appelés.
- Les administrations de la justice, de la police et de la gendarmerie peuvent obtenir certains extraits de journaux, si elles justifient d'un droit à communication, en tant que « tiers autorisés » conformément à la loi « Informatique et Libertés ».

Par ailleurs, il convient de rappeller que toute personne peut demander à accéder aux données personnelles la concernant, conformément à la loi « Informatique et Libertés ».

Les journaux informatiques font l'objet de **mesures de sécurité** afin :

- de garantir que l'accès n'est possible qu'aux seules personnes autorisées, tel que précisé ci-dessus ;
- de les protéger de toute modification ou effacement malveillant.

6. Données traitées

Les données conservées dans les journaux informatiques peuvent varier selon le type de serveur ou d'équipement concerné. Le détail est fourni en annexe.

7. Durée de conservation des données

La durée de conservation des journaux informatiques est de 12 mois au maximum.

[2] CERTA : Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques
[3] CERT-Renater : structure organisant notamment l'aide en cas d'incident de sécurité pour les établissements de l'enseignement supérieur et de la recherche

Annexe : catégories de données enregistrées

Cette annexe décrit les catégories de données enregistrées dans les journaux informatiques, selon le type d'équipement concerné.

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 des droits d'un utilisateur, tout ou partie des informations suivantes peut être enregistré automatiquement par les mécanismes de journalisation du service :

- Identifiant de l'émetteur de la requête ;
- Date et heure de la tentative ;
- Résultat de la tentative (succès ou échec) ;
- Commandes passées.

Serveurs de messagerie

Les serveurs hébergeant la messagerie électronique et les listes de diffusion enregistrent, pour chaque message émis ou reçu, tout ou partie des informations suivantes :

- Adresse mail de l'expéditeur et éventuellement des éléments identifiant celui qui s'est connecté au serveur ;
- Adresse mail des destinataires ;
- Date et heure de la tentative ;
- Machines traversées par le message ;
- Traitement « accepté ou rejeté » du message ;
- Taille du message ;
- Certains en-têtes du message, tel que l'identifiant numérique du message ;
- Résultat du traitement antiviral ;
- Résultat du traitement de filtrage anti-spam ;
- Opérations de validation ou de rejet des messages par les modérateurs lorsque cela s'applique.

Les éléments de contenu des messages ne sont pas journalisés.

Serveurs web

Pour chaque connexion, les serveurs Web enregistrent tout ou partie des informations suivantes :

- Noms ou adresses IP source et destination ;
- Données d'authentification dans le cas d'un accès authentifié (intranet par exemple) ;
- URL de la page consultée et informations fournies par le navigateur ;
- Type de la requête ;
- Paramètres passés avec la requête ;
- Date et heure de la tentative ;
- Volume de données transférées.

Equipements réseau

On désigne par « équipements réseau » les routeurs, pare-feux, commutateurs, bornes d'accès Wi-Fi, équipements d'administration du réseau, etc. Pour chaque paquet qui traverse l'équipement, tout ou partie des informations suivantes peut être collecté :

- Noms ou adresses IP source et destination ;
- Protocole, ainsi que les numéros de ports source et destination ;
- Date et heure de la tentative ;

- Nature du traitement du paquet par l'équipement ;
- Nombre de paquets et d'octets transférés ;
- Messages d'alerte.

Téléphonie

Les équipements téléphoniques enregistrent les informations suivantes :

- Numéro appelant ;
- Numéro appelé ;
- Date et heure de l'appel ;
- Durée de la communication.

La gestion de la téléphonie suit les recommandations de la CNIL et fait l'objet d'une déclaration spécifique dans le registre des traitements de données à caractère personnel de l'Université.

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 à l'ENT ;
- Accès aux bases de données ;
- Services d'authentification (CAS, eduroam…).

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

- Identité de l'émetteur de la requête ;
- Date et heure de la tentative ;
- Résultat de la tentative ;
- Volume de données transférées ;
- Commandes passées.

Les traitements des journaux informatiques décrits ici ne couvrent pas l'ensemble des données conservées par les applications qui, de par leur nature, peuvent historiser certaines transactions. Il est rappelé que si ces données visant à assurer la traçabilité des opérations permettent d'identifier, directement ou indirectement, des personnes, alors elles sont soumises au respect de la loi « Informatique et Libertés » et font l'objet d'un enregistrement par le correspondant Informatique et Libertés dans le registre des traitements de données à caractère personnel de l'Université.