Ligne directrice sécurité de l'information et vie privée

Gestion des logs

(BLD LOG)

TABLE DES MATIÈRES

1. Introduction

Le présent document fait intégralement partie de la méthodologie de sécurité de l'information et protection de la vie privée au sein de la sécurité sociale. Ce document est destiné aux responsables et aux sous-traitants de l'information, au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de sécurité sociale (IPSS).

Les systèmes d'information et l'infrastructure ICT génèrent des logs pour de nombreuses activités, parfois à titre de statut, parfois à titre de résultat d'une activité d'un utilisateur ou gestionnaire, mais également des informations suite à des circonstances imprévues ou des erreurs.

Un log décrit se qui se passe dans les systèmes. Actuellement, les descriptions des systèmes sont parfois tellement détaillées qu'elles permettent de savoir pourquoi un événement s'est produit. Le logging permet à l'organisation de réaliser le suivi des transactions et de les contrôler. Beaucoup de systèmes informatiques utilisent le logging pour enregistrer des informations sur les erreurs qui se sont produites ou sur d'autres événements qui méritent l'attention de l'utilisateur ou du gestionnaire. Un log peut être formulé sous forme de fichiers de textes mais également sous forme de tableaux en base de données. L'objectif du logging est de recueillir et d'évaluer des données système et des avertissements en provenance p.ex. d'applications, de l'infrastructure réseau, de serveurs et ordinateurs.

La gestion des logs est souvent considérée comme un poste de frais. Toutefois, une solution adéquate de gestion de logs est comparable à un contrat d'assurance : c'est indispensable et vous devez payez pour l'avoir, mais vous ne l'utiliserez qu'en cas d'incident. Une gestion adéquate des logs est de plus en plus nécessaire pour pouvoir répondre aux exigences légales et réglementaires, par exemple pour l'exécution d'un audit de protection de la vie privée sur un système d'information. Plus l'importance augmente, plus les exigences imposées à la gestion des logs augmentent[1].

Les processus sont de plus en plus souvent automatisés et les autorisations sont également de plus en plus souvent numériques. En automatisant la gestion des logs, une organisation peut réaliser des économies d'échelle, mais il existe des risques. En cas de log entièrement numérique, des données peuvent se perdre et l'organisation ne peut plus s'appuyer sur des autorisations ou documents papier. Une organisation qui automatise la gestion des logs devra investir dans la sécurité des données et une procédure de sauvegarde/reprise. Une autre point d'attention lors de l'automatisation de la gestion de logs est la mise en place d'une séparation de fonctions au sein des systèmes automatisés. Lorsque la séparation de fonctions n'est pas correctement réalisée dans le logiciel, par exemple lorsqu'il est fait usage de comptes utilisateurs génériques (anonymes), une modification ne pourra pas être mise en rapport avec une personne individuelle et la valeur de la gestion des logs restera limitée.

Le présent document décrit les directives pour une gestion des logs.

[1] Voir à cet égard la politique en matière de classification de données.

2. Gestion des logs

Toute organisation souscrit les directives suivantes de sécurité de l'information et protection de la vie privée pour toutes les informations et systèmes d'information qui relèvent de la responsabilité de l'organisation.

1. L'organisation est tenue d'établir une procédure formelle de gestion de logs, de la valider, de la communiquer et de la maintenir.
2. Toutes les transactions, activités de contrôle, activités des utilisateurs, exceptions et événements/incidents de sécurité de l'information et protection de la vie privée doivent être établis de manière structurée dans des fichiers de logs distincts, de sorte que toute action puisse être mise en rapport avec les documents source et que toutes les actions réalisées puissent être contrôlées.
3. La gestion des logs doit être prise en compte dès la conception lors du développement et dès la définition des critères d'achat d'applications ou systèmes afin de réaliser la « security/privacy by design ».
4. Tout accès à des données de sensibilité confidentielle ou supérieure, doit faire l'objet d'un logging, conformément à la législation et à la réglementation applicables.
5. Les horloges de tous les systèmes informatiques de l'organisation doivent être synchronisées avec une horloge précise déterminée de sorte à permettre une analyse fiable des fichiers de logging sur différents systèmes d'information.
6. Les outils nécessaires doivent être disponibles ou développés pour permettre aux données autorisées d'être exploitées et analysées par les personnes autorisées. Grâce aux outils, il devrait être possible de consulter les logs rapidement, clairement et facilement.
7. L'utilisation du système fait l'objet d'un logging automatique autant que possible et lorsque ce n'est pas possible les gestionnaires de système ont recours à un log manuel.
8. Les fichiers de logging doivent être protégés contre tout accès par des personnes non habilitées, contre les modifications et suppressions.
9. Les fichiers de logging doivent être conservés durant une période déterminée, à des fins d'analyse et de contrôle futurs et conformément à la législation et à la réglementation. En particulier, les privacy logs doivent être conservés pendant au moins 10 ans.
10. La qualité du privacy log doit fournir une réponse appropriée pour justifier (basée ou non sur une autorisation préalable). Le log doit contenir une indication pour chaque enregistrement de traitement de qui a traité quelles données personnelles à quelles fins et avec quel résultat (OK, NOK).
11. La consultation des fichiers de logging fait toujours l'objet d'une procédure organisée au sein de l'organisation, avec un historique des demandes qui ont été approuvées/exécutées ou rejetées.
12. Le résultat de la gestion des logs doit régulièrement être analysé, rapporté et évalué.

Annexe A: Gestion documentaire

Gestion des versions

Date	Auteur	Version	Description de la modification	Date approbation	Date entrée en vigueur
2004	JM Gossiaux	1.0	Première version	26/03/2004	01/04/2004
2004	JM Gossiaux	2.0	Deuxième version	15/09/2004	01/10/2004
2005	JM Gossiaux	3.0	Troisième version	16/02/2005	01/03/2005
2005	JM Gossiaux	4.0	Quatrième version	03/11/2005	15/11/2005
2005	JM Gossiaux	5.0	Cinquième version	10/11/2005	01/12/2005
2006	JM Gossiaux	6.0	Sixième version	01/06/2006	01/07/2006
2017	M. Vael	V2017	Intégration EU GDPR	07/03/2017	07/03/2017
2018	Groupe de travail policy	V2018	Ajustements des temps de rétention, type des logs et composition des privacy logs	06/02/2018	01/01/2019

Erreurs et omissions

Si à la lecture du présent document, vous constatez des erreurs ou des problèmes, vous êtes invité, en tant que lecteur, à transmettre une brève description de l'erreur ou du problème et de sa localisation dans le document ainsi que vos données de contact au conseiller en sécurité de l'information (CISO) / délégué à la protection des données (DPO) de l'organisation.

Définitions

Pour garantir la cohérence en ce qui concerne la terminologie et les notions utilisées à travers les divers documents de politique, toutes les définitions relatives à la sécurité de l'information et à la protection de la vie privée sont regroupées dans un document spécifique : "Définitions sécurité de l'information et protection de la vie privée".

Annexe B: Références

Ci-dessous figurent les documents qui ont servi de source d'inspiration pour le présent document:

- ISO, "ISO/IEC 27001:2013 Information Security Management System Requirements", septembre 2013, 23 p.
- ISO, "ISO/IEC 27002:2013 Code of Practice for Information Security Management", septembre 2013, 80 p.
- ISACA, "COBIT 5 for Information Security", mai 2012, 220 p.
- SANS, "Information Logging Standard", juin 2014, 4 p.
- NIST, "Guide to computer security log management", septembre 2006, 72 p.

Ci-dessous figurent les références aux sites web qui ont servi de source d'inspiration pour le présent document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
- http://www.isaca.org/cobit
- http://cee.mitre.org/

Annexe C: Directives pour une gestion des logs sûre

Ci-après figurent les directives pour l'organisation d'une gestion des logs adéquate.

Responsabilités en matière de gestion des logs

La responsabilité pour l'organisation de la sécurité de l'information et de la protection de la vie privée incombe toujours à l'institution propriétaire de l'application traitant l'information (le responsable du traitement). Pour le propriétaire de l'application, cette responsabilité implique la nécessité de veiller à la mise en place d'une procédure organisée en matière de gestion des logs à des fins de sécurité de l'information et de protection de la vie privée.

Lorsqu'il s'agit d'une application à responsabilité partagée (le responsable du traitement conjoint), chaque organisation partenaire est co-responsable pour la mise en œuvre de la gestion de logs.

Si des missions de traitement d'informations sont confiées à un tiers (sous-traitants), l'organisation peut fixer les responsabilités et obligations en matière de gestion de logs dans un Service Level Agreement (SLA) ou un contrat, mais les tiers sont toujours tenus de prévoir les mesures organisationnelles, procédurales et technologiques adéquates conformément à la législation et réglementation en vigueur.

Organisation de la gestion des logs

L'organisation de la gestion des logs doit garantir une traçabilité des données à caractère personnel utilisées : applications utilisées, actions réalisées et informations utilisées. Elle doit garantir le rapport entre l'utilisateur et l'événement.

L'organisation de la gestion des logs comprend également l'exécution de toutes les tâches garantissant une gestion pérenne de tous les fichiers de logging durant le cycle de vie du log.

Une attention particulière est accordée aux aspects suivants :

1. la collecte sécurisée,
2. la conservation et l'archivage dans un format utilisable et sur des supports utilisables limitant tout risque de falsification,
3. la procédure d'alarme en cas de détection de faits majeurs, tels que l'impossibilité de tracer les fichiers de logging,
4. le contrôle de l'intégrité des mécanismes mis en place,
5. les procédures de gestion.

Qualité de la gestion des logs

Dans le cadre de la gestion des privacy logs, une réponse doit au moins pouvoir être fournie aux six questions suivantes :

1. Quelle activité a eu lieu ? (Quoi) (Opération)
2. A quelle moment l'activité a-t-elle eu lieu ? (Quand) (Date/heure)
3. Qui a réalisé l'activité ? (Quelle organisation) (Qui)
4. Sur quel système l'activité a-t-elle eu lieu ? (Comment) (ID de l'application)
5. Sur quel objet l'activité a-t-elle été effectuée ? (De qui) (La personne impliquée dans le traitement)
6. Quel est le résultat/statut de l'activité? (Réussie/échouée)

Les informations suivantes sont hautement souhaitables avec les privacy logs :

7. Pourquoi ? (Détail de l'activité/la finalité)
8. La date de fin de vie du log (Temps de rétention)
9. Quelle transaction sur la base d'un numéro unique ? (Quoi) (ID de transaction)

Obligations en matière de logs

a. Une organisation doit mettre en place une procédure formelle de gestion de logs, la valider, la communiquer et la maintenir :

1. un système de logging opérationnel,
2. le contrôle du respect de la procédure et du contenu des fichiers de logging,
3. la gestion, la conservation, l'archivage des fichiers de logging de sécurité de l'information et de protection de la vie privée et leur suppression à l'issue de leur durée de conservation,
4. la décision d'inclure les données de logging dans le plan de continuité de l'organisation,
5. l'accès contrôlé aux données de logging,
6. en tant que propriétaire de l'application, l'organisation doit prévoir et gérer les fichiers de logging de sécurité de l'information et de protection de la vie privée. Par exemple au niveau du moniteur transactionnel, du système d'exploitation, du système de gestion des autorisations, de la gestion et de la mise à jour des banques de données.
7. l'organisation doit réaliser des contrôles périodiques afin de s'assurer du respect des mesures qui la concernent.
8. tout utilisateur d'une application de la sécurité sociale ou d'une application ayant recours au réseau de la sécurité sociale doit être informé de l'existence de la gestion des logs et des objectifs de la gestion de logs.

b. L'utilisateur de la sécurité sociale est tenu de respecter les instructions et procédures applicables dans la sécurité sociale ou au sein d'autres réseaux.

c. Pour les applications présentes sur le portail de la sécurité sociale ou de la Plate-forme eHealth, le service de base de gestion des loggings est utilisé.

Toute demande d'utilisation d'une procédure alternative à la gestion des logs doit être dûment motivée et justifiée auprès de l'organisation propriétaire de l'application.

Automatisation de la gestion de logs

Dans le cadre de l'automatisation de la gestion de logs, il est souvent question de SIM (security information management), SEM (security event management) en SIEM (Security Information and Event Management) en ce qui concerne les fichiers de logging à caractère sécuritaire.
Sur le plan technique, il existe une série de bonnes pratiques, par exemple quant aux protocoles à utiliser, la façon d'envoyer et de recevoir des fichiers de logging, etc. Les processus en matière de gestion de logs ne sont pas simples : il ne s'agit pas d'envoyer simplement tous les fichiers de logging des serveurs vers la solution centrale de gestion de logs et de les faire analyser. Bon nombre de sources de données ne sont pas pertinentes. C'est pourquoi il convient d'examiner d'abord les sources de données disponibles et de déterminer les sources de données pertinentes. Ce qui n'est pas pertinent n'est pas centralisé.
Parmi les sources de données pertinentes, des exemples sont rédigés décrivant de manière formelle les événements susceptibles d'activer une action supplémentaire. Les besoins de l'organisation sont essentiels en ce qui concerne l'automatisation de la gestion de logs.

Définitions et temps de rétention

• Logs techniques / d'infrastructure :
Logs créés pour l'analyse technique et la récupération technique des actifs TIC. Temps de rétention souhaitable 6 mois sauf si d'autres dispositions légales prévoient une période de stockage plus longue.
• Logs d'entreprise :
Logs créés pour analyser et restaurer les systèmes transactionnels commerciaux. Temps de rétention souhaitable 2 ans sauf si d'autres dispositions légales prévoient une période de stockage plus longue.
• Logs de sécurité :
Logs créés dans le but de détecter et / ou d'analyser les événements et les incidents de sécurité. Temps de rétention souhaitable 5 ans sauf si d'autres dispositions légales prévoient une période de stockage plus longue.
• Les privacy Logs :
Logs créés pour répondre aux règles de confidentialité et y répondre. Temps de rétention voir chap. gestion des logs.

Annexe D: Lien avec la norme ISO 27002:2013

Nous vous renvoyons ici aux principales clauses de la norme ISO 27002:2013 en rapport avec le sujet du présent document.

Norme ISO 27002:2013	
Politique de sécurité	
Organisation de la sécurité de l'information	
Sécurité des ressources humaines	
Gestion des actifs	
Protection de l'accès	
Cryptographie	
Sécurité physique et environnementale	
Protection des processus	
Sécurité de la communication	
Maintenance et développement de systèmes d'information	**Oui**
Relations avec les fournisseurs	
Gestion des incidents de sécurité	**Oui**
Aspects de la sécurité de l'information dans la gestion de la continuité	
Respect	**Oui**

***** FIN DU DOCUMENT *****