Federal Information Security Policy Guideline

Guide pour le logging et le monitoring

21/11/2019

FISPDOC04 V1.2

Remarque importante : Le présent document est un guide qui résulte d'une collaboration entre des experts en sécurité de l'information des différents services fédéraux (SPF, OIP, IPSS). Les mesures présentées sont considérées comme des mesures minimales applicables raisonnablement de manière commune à tous les services fédéraux. Elles se basent sur des normes internationales et des bonnes pratiques en matière de sécurité de l'information ainsi que sur les expériences des participants au groupe de travail FISP.

Si des mesures plus strictes sont requises pour un service fédéral pour des raisons réglementaires ou autres raisons formelles et impérieuses, on peut supposer que ces mesures sont prioritaires sur les mesures prévues dans le présent guide.

Groupe de travail

.be

Table des matières

Contenu du présent document

Orientation du document

Le présent document fait partie intégrante de la méthodologie pour la sécurité de l'information au sein de l'Administration fédérale (projet FISP).

Chaque organisation fédérale doit disposer d'une politique et de processus en matière de sauvegarde des évènements (logging).

Objectif de sécurité du document

Cette politique a été rédigée pour proposer des mesures de sécurité de l'information relatives à la sauvegarde des évènements (logging), de manière à concrétiser la politique de sécurité.

Champ d'application

Cette stratégie ne constitue pas une description complète de processus pour la sauvegarde des évènements (logging) et ne contient pas de descriptions de produits, mais contient suffisamment d'informations pour poser des choix (stratégiques) opportuns et créer une conscientisation concernant la sauvegarde des évènements (logging).

Confidentialité du document

Distribution publique

Clause de non-responsabilité

Il s'agit d'une politique basée sur les pratiques internationales en matière de sauvegarde des évènements (logging). Si vous souhaitez appliquer cette directive à votre organisation, vous devez d'abord procéder à une évaluation et vérifier si d'autres restrictions, règles ou pratiques légales s'appliquent à votre organisation. Adaptez la politique de sécurité en fonction de votre organisation !

Durant le Conseil des ministres du 3 mai 2019, un avant-projet de loi a été soumis, portant révision de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Si cette loi est adoptée, la politique FISP sera mise à jour étant donné que la politique actuelle ne tient pas compte des évolutions légales futures.

Responsabilités

Le présent document est destiné au conseiller en sécurité de l'information (CISO) et au délégué à la protection des données (DPO) de l'institution publique de l'administration fédérale, aux responsables du traitement de l'information (y compris les sous-traitants des systèmes d'informations), à l'officier de sécurité et aux autres intervenants dans des domaines connexes (ex. le gestionnaire de documents).

Propriétaire

Le groupe de travail FISP est propriétaire du présent document.

Introduction

Les systèmes d'information et l'infrastructure ICT génèrent des loggings 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.

Cette stratégie propose des mesures de sécurité de l'information concernant la sauvegarde des évènements (logging) pour les organisations fédérales. Le document contient l'information nécessaire pour poser des choix (stratégiques) appropriés et créer une prise de conscience. Les mesures proposées sont liées à la classification de l'information proposée au niveau de la politique de sécurité de l'information fédérale.

Un avis est également formulé à l'égard des mesures à prendre pour la gestion des loggings. De plus, des indications sont également données sur la rétention et la sécurité des enregistrements d'audit, la manière de gérer les erreurs dans les enregistrements d'audit ainsi que le suivi, l'analyse et le rapport d'audit.

Il ne s'agit toutefois pas d'une description complète des processus de sauvegarde des évènements (logging) et de surveillance ni d'une description de produit. Une description détaillée concernant le principe de sauvegarde des évènements (logging) et de surveillance se trouve dans le document FISP « Logging & Surveillance - Explication ».

Logging

La sauvegarde des évènements (logging) en tant que mesure de sécurité

Le journal d'audit et les pistes d'audit constituent une mesure de sécurité importante en tant que telle. Cela fonctionne de manière préventive, le suivi des informations des loggings d'audit permet de détecter les premiers signaux d'une cyber-attaque. Ensuite, les démarches nécessaires peuvent être entreprises pour faire cesser cette attaque et/ou prévenir d'autres conséquences.

Cela fonctionne également de manière réactive dans la mesure où l'analyse des loggings et la corrélation avec d'autres sources d'information permettent de savoir ce qui s'est précisément passé. A titre réactif, la sauvegarde des évènements (logging) peut apporter un soutien dans le processus de gestion des risques. Elle peut être utilisée à titre de soutien au processus de gestion des problèmes. On peut l'utiliser pour tirer des leçons d'incidents et cela peut faire office de preuve - preuve juridique. Enfin, c'est également pratique pour une utilisation statistique.

L'objectif de la sauvegarde des évènements (logging)

Il peut exister différentes raisons (conformité, statistiques et raisons opérationnelles) pour lesquelles une organisation peut décider de créer un journal :

- Détection de comportements suspects (abus interne, accès non autorisé, hacking,...) et de cyber-attaques.
- Support pour analyse légale et corrélation
- Charge de preuve (collecte de matériel de preuve, détection de fraude...)
- Conformité à la réglementation en vigueur
- Processus d'appui (rapport...)
- Support IT maintenance et opérations
- Débogage, tests
- Surveillance de la performance des applications et systèmes
- …

La source de la sauvegarde des évènements (logging)

Toutefois, l'important n'est pas seulement l'objectif de la sauvegarde des évènements (logging), mais également la source des événements du journal. Les sources d'un journal peuvent être très diverses :

- Applications (informations sur le compte d'utilisateur, actions opérationnelles, manipulation de données, utilisation d'information)
- Réseau (routeurs, switches, AP,...)
- Logiciel et dispositifs de sécurité (IDS.IPS, Firewalls, antimalware software, Remote access (VPN), Web proxies, authentication services, vulnerability management software, network quarantine servers, …)
- Serveurs et bases de données
- Middleware (ESB, …)
- Systèmes d'exploitation (fixes/mobiles), événements système, enregistrements d'audit
- Périphérique : MFP,...
- Centre de données et bâtiment (badges, CVC, surveillance,...)
- Environnements virtuels : (serveurs virtuels, réseaux, hyperviseurs, …)
- Applications LAN

- …

Il est crucial de savoir pourquoi le journal a été créé et quelle est la source de l'événement du journal. Cela permet de déterminer aussi dans une certaine mesure le type de mesures de sécurité qu'il faut prendre. Ainsi, les mesures de sécurité pour la sauvegarde des évènements (logging) concernant le support et la maintenance IT différeront de celles portant sur la détection d'un comportement suspect. Un événement du journal découlant d'applications ou d'un logiciel de sécurité diffère quant aux mesures de sécurité. Par conséquent, les mesures de sécurité doivent correspondre au motif de la sauvegarde des évènements (logging) et à la source de l'événement.

Les fichiers loggings

Certaines informations sont protégées par le journal. Les fichiers loggings doivent être protégés contre les accès non autorisés. Le journal lui-même doit se voir attribuer la même catégorie d'information que la catégorie de l'information qu'il protège. Vu que cette information est reprise dans les logging, les mesures correspondantes doivent donc être aussi appliquées à l'information du journal. Cela vaut surtout pour les logging des applications et, dans une moindre mesure, pour les logging système, car ces derniers ne contiennent généralement pas d'information applicative.
Les fichiers loggings peuvent contenir les fichiers suivants : ID, activités système, dates, durées, détails sur les événements, utilisation de privilèges, adresses réseau,...
Les fichiers loggings peuvent aussi protéger des informations personnelles et sensibles. Pour ces logging de protection de la vie privée, il faut prendre les mesures adéquates à l'égard de la vie privée.

Les mesures suivantes devraient être appliquées afin de garantir la confidentialité, l'intégrité et la disponibilité des informations du journal tout au long du cycle de vie de ces informations :

Confidentialité :

- Contrôle de l'accès physique ou logique ;
- Cryptage des informations du journal.

Intégrité :

- Garantir l'accès en « lecture seule » aux informations du journal ;
- Appliquer une séparation des fonctions ;
- Enregistrer les informations du journal de manière centrale ;
- Horodatage et signature électronique.

Disponibilité :

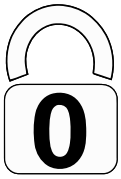
- Enregistrer les informations du journal de manière centrale ;
- Sauvegarder les fichiers loggings ;
- Inclure la sauvegarde des évènements (logging) dans les DRP (disaster recovery plan).

Classification de l'information - Logging

Mesures générales

Le logging et la sécurité des fichiers logging devraient être organisées en conformité avec la classification de l'information de cette politique globale de sécurité de l'information (FISP). Les mesures proposées sont des mesures superposées. Cela implique que les mesures de la classe d'information inférieure peuvent rester applicables aux classes supérieures, à l'exception de mesures techniques incompatibles. De plus, la complexité et la force des mesures évoluent avec la classe.

Catégorie	

	• Utilisation de comptes privilégiés.
	• Logging des applications : les mesures cryptographiques concernant les informations des loggings sont au même niveau que l'application d'où sont tirées ces informations.
	• Logging des événements :
	  ○ Mettre en place une politique de journal pour tous les systèmes et applications,
	  ○ Mettre en place une sauvegarde des évènements (logging) en soutien du processus des incidents :
	  ▪ type d'événement,
	  ▪ où et quand l'événement a eu lieu,
	  ▪ cause et conséquence de l'événement,
	  ▪ comptes liés à l'événement.
	• Surveillance des événements d'effacement du journal
	• Enregistrement local des informations du journal
	• Protéger les enregistrements d'audit pour garantir l'intégrité.
	• Horodatage des enregistrements d'audit par l'application d'une synchronisation des horloges.
	• Limiter l'accès aux enregistrements d'audit à la seule fonction de consultation (« lecture seule »).

	• Protéger l'enregistrement d'audit pour garantir non seulement l'intégrité, mais aussi la confidentialité grâce à la protection physique et au contrôle d'accès logique. • Mettre en place une piste d'audit pour le traitement de l'information et l'utilisation d'outils système. • L'horodatage des enregistrements d'audit par l'application d'une synchronisation des horloges avec une horloge externe approuvée. • Analyse périodique des enregistrements d'audit. • Utiliser des outils d'analyse et de rapport • Évaluer chaque année la fonction d'audit. • Le logging doit aussi être journalisée : ○ l'ouverture d'un nouveau fichier journal, le déplacement, la modification du nom ou la suppression d'un fichier journal, la consultation, la suppression ou la modification du contenu d'un fichier journal doivent être journalisés afin de détecter un accès non autorisé. • Enregistrement central des informations du journal. • Limiter la période de rétention de l'information locale du journal au cache (jusqu'à la vérification de l'enregistrement central).

	• Générer et suivre des alarmes lorsque la capacité de stockage des fichiers logging atteint 80%. • Conservation/archivage à long terme des informations du journal conformément à la loi et la réglementation.
	• Aucune mesure supplémentaire n'est identifiée pour l'information de catégorie 2.
	• Protéger l'enregistrement d'audit pour garantir non seulement l'intégrité, mais aussi la confidentialité grâce à des mesures cryptographiques. • Intégrer le logging avec des capacités de scannage et de surveillance. • Appliquer des horodatages en combinaison avec la signature électronique. • Appliquer des corrélations d'événements • Gestion centrale des fichiers logging • Générer et suivre des alarmes en temps réel en cas de problèmes avec la fonction d'audit. • Appliquer le principe des 4 yeux pour toute modification à la fonctionnalité d'audit.
	• Aucune mesure supplémentaire n'est identifiée pour l'information de catégorie 4. • Pour cette catégorie, il faut tenir compte d'autres exigences de sécurité sur la base de la loi du 11/12/1998.

Gestion des loggings

Les mesures présentées dans le présent chapitre sont des mesures minimales pour la gestion des loggings. Toute organisation fédérale 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 fédérale.

Mesures générales pour les loggings

- Une organisation doit mettre en place une procédure formelle de gestion des loggings, la valider, la communiquer et la maintenir :
    - un système de journal opérationnel ;
    - le contrôle du respect de la procédure et du contenu des fichiers logging ;
    - la gestion, la conservation, l'archivage des fichiers logging de sécurité de l'information et de protection de la vie privée et leur suppression à l'issue de leur durée de conservation ;
    - la décision d'inclure les données des loggingss dans le plan de continuité de l'organisation,
    - l'accès contrôlé aux données des loggings ;
    - en tant que propriétaire de l'application, l'organisation doit prévoir et gérer les fichiers loggings 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.
    - L'organisation doit réaliser des contrôles périodiques afin de s'assurer du respect des mesures qui la concernent ;
    - les rôles et responsabilités concernant la gestion des loggings doivent être clairs au sein de l'organisation. Là où c'est possible, il faudrait éviter que les administrateurs système aient la possibilité de désactiver ou supprimer leurs propres loggings concernant leurs propres activités.
- L'organisation devrait fixer les transactions, les activités de contrôle, les activités des utilisateurs, les exceptions et les événements/incidents ayant trait à la sécurité de l'information et la protection de la vie privée dans des fichiers loggings distincts, de sorte que chaque acte puisse être corrélé aux documents sources ou que les traitements effectués puissent être contrôlés.
- La gestion des loggings 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 ».
- Tout accès à des données de sensibilité confidentielle ou supérieure, doit faire l'objet d'une sauvegarde des évènements (logging), conformément à la législation et à la réglementation applicables.
- Les horloges internes 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 loggings sur différents systèmes d'information.
- Les outils nécessaires doivent être disponibles ou développés pour permettre aux données des loggings d'être exploitées et analysées par les personnes autorisées. Grâce aux outils, il devrait être possible de consulter les loggings rapidement, clairement et facilement.
- L'utilisation du système fait l'objet d'une sauvegarde des évènements (logging) automatique autant que possible et lorsque ce n'est pas possible les gestionnaires de système ont recours à un journal de bord manuel.
- Les fichiers loggings doivent être protégés contre tout accès par des personnes non habilitées, contre les modifications et suppressions.

- Les fichiers loggings 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.
- L'organisation de la gestion des loggings englobe également l'exécution de toutes les tâches garantissant une gestion durable de tous les fichiers loggings pendant le cycle de vie des loggings. Les aspects suivants font l'objet d'une attention particulière :
    - la collecte sécurisée,
    - la conservation et l'archivage dans un format utilisable et sur des supports utilisables limitant tout risque de falsification,
    - la procédure d'alarme en cas de détection de faits majeurs, tels que l'impossibilité de tracer les fichiers loggings,
    - le contrôle de l'intégrité des mécanismes mis en place,
    - les procédures de gestion.
- La consultation des fichiers loggings 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.
- Le résultat de la gestion des loggings devrait être analysé, rapporté et évalué régulièrement.

Mesures spécifiques supplémentaires pour les loggings de protection de la vie privée

- Les loggings de protection de la vie privée doivent être conservés pendant une période déterminée, en vue de vérifications et contrôles futurs et conformément à la législation et la réglementation.[1]
- La qualité des loggings de protection de la vie privée doit apporter une réponse appropriée pour justifier l'utilisation (basée ou non sur une autorisation ou une habilitation préalable). Pour chaque activité, le journal doit indiquer :
    - qui a traité des données à caractère personnel et pourquoi,
    - qui est concerné par ces données à caractère personnel,
    - à quelles fins les données à caractère personnel doivent être traitées,
    - avec quel résultat le traitement a-t-il été effectué (OK, NOK).

  Dans la gestion des loggings de protection de la vie privée, il faudrait répondre au moins aux six questions suivantes :
    - Quelle activité a eu lieu ? (Quoi) (opération)
    - A quel moment l'activité a-t-elle eu lieu ? (Quand) (Date/heure)
    - Qui a réalisé l'activité ? (Quelle organisation) (Qui)
    - Sur quel système l'activité a-t-elle eu lieu ? (Comment) (ID de l'application)
    - Sur quel objet l'activité a-t-elle été effectuée ? (De qui) (La personne impliquée dans le traitement)
    - Quel est le résultat/statut de l'activité ? (Réussie/échouée)

  Les informations suivantes sont hautement souhaitables dans les loggings de protection de la vie privée :

[1] Par ex. la BCSS établit que les fichiers journaux de protection de la vie privée doivent être conservés 10 ans.

- Pourquoi ? (Détail de l'activité / finalité)
- La date de fin de vie du journal (temps de rétention).
- Quelle transaction sur la base d'un numéro unique ? (Quoi) (ID de transaction)

Logging de bord manuels

Les loggings de bord manuels devraient faire l'objet d'une attention particulière parce que le risque de violation de la confidentialité, de l'intégrité et de la disponibilité est plus importante que pour les loggings automatisés :

- la procédure et le suivi manuels accroissent le risque d'erreurs, d'incohérences ou d'absences d'information ;
- l'accès physique au journal de bord doit être sécurisé ;
- la disponibilité du journal de bord doit être garantie, notamment par la réalisation de copies.

Les mesures d'atténuation visant à sécuriser les loggings de bord manuels sont notamment les suivantes :

- sécuriser l'accès physique au moyen d'une armoire ignifuge fermant à clé ;
- tenir à jour des copies du journal de bord ;
- numériser et enregistrer en tant que fichier PDF ;
- contrôle et principe des 4 yeux.

Rétention et sécurité des enregistrements d'audit

Les enregistrements d'audit doivent être stockés de manière sûre et ensuite conservés à des fins d'analyse. Cela comprend ce qui suit :

- Application d'un modèle de cycle de vie aux données des loggings, compte tenu de la disponibilité opérationnelle et de l'archivage des données des loggings.
- Seules les personnes autorisées peuvent avoir accès aux enregistrements d'audit et aux fichiers des loggings.
- Les paramètres du système d'audit ne peuvent être modifiés que par du personnel autorisé et moyennant application du principe des 4 yeux.
- Les enregistrements d'audit doivent être disponibles pour analyse et rapport lorsque nécessaire, notamment en cas d'enquête interne ou externe.
- Les enregistrements d'audit doivent être conservés suffisamment longtemps, conformément à la législation et la réglementation en vigueur.

Gestion du stockage

Comme décrit ci-dessus, les enregistrements d'audit doivent être conservés suffisamment longtemps. Cela signifie qu'une capacité de stockage suffisante - éventuellement hors ligne - doit être disponible et qu'il faut tenir compte de l'impact potentiel sur la performance du système/de l'application.

Le principe de la minimalisation des données doit aussi s'appliquer à la sauvegarde des événements (logging). « Don't log what you don't need ! »

Gestion des erreurs dans l'audit

Pour garantir que les informations de l'audit soient toujours disponibles, il est important de détecter et résoudre à temps les erreurs durant la sauvegarde des évènements (logging). C'est la raison pour laquelle la sauvegarde des évènements (logging) devrait être conçue de telle manière que le personnel autorisé soit toujours informé des problèmes. Il peut s'agir de problèmes portant sur la production et la gestion des informations des loggings.

Si la sauvegarde des évènements (logging) n'est plus possible, il n'est plus possible de démontrer qui a eu accès à un système ou une information, si des messages ont été envoyés ou reçus ou si des données ont été insérées et par qui. Cela implique des risques pour la sécurité de l'information.

Les organisations fédérales poseront les choix suivants :

- Laisser fonctionner le système ou l'application normalement et ne pas enregistrer de sauvegarde des évènements (logging), avec pour conséquence la perte des informations des loggings.
- Journaliser le système ou l'application de manière locale et ensuite synchroniser cette sauvegarde des évènements (logging). De nombreux systèmes/applications peuvent être journalisés de manière locale, de sorte que les informations des loggings sont temporairement en sécurité. Dès le moment où le mécanisme de sauvegarde des évènements (logging) central est de nouveau disponible, les enregistrements collectés sont envoyés. Il faut néanmoins veiller à ce que la sauvegarde des évènements (logging) locale n'utilise pas la totalité de la capacité de stockage disponible du système. Dès le moment où le stockage local arrive à son maximum, il faut à nouveau décider si on reste en production ou non.
- Mettre le système ou l'application hors production. Cela signifie que les processus opérationnels qui y sont liés ne sont plus disponibles en tant que tels et qu'il faut peut-être activer le processus de continuité de l'activité. La mise hors production signifie que les violations ne passeront pas inaperçues et que le journal d'audit ne présentera pas de hiatus, mais cela se fait au détriment du fonctionnement opérationnel.

Suivi, analyse et rapport d'audit

Les fichiers loggings doivent être régulièrement analysés pour :

- détecter les infractions aux directives,
- détecter et suivre les activités inhabituelles,
- tester l'effectivité des mesures de sécurité.

Des rapports d'audit doivent être réalisés périodiquement et mis à la disposition du management. Il faut éviter que le rapport se limite à des détails techniques.

Le rapport d'audit doit être intégré dans le processus de gestion des incidents et problèmes. Seul le personnel autorisé peut concevoir et réviser des rapports d'audit.

Lien avec d'autres mesures

Lien avec le PAM en tant que mesure

La mesure PAM ou Privileged Access Management décrit de quelle manière l'utilisation de droits privilégiés attribués aux gestionnaires système, développeurs,… doit être attribuée et suivie. Cet aspect est décrit dans le document « IAM + PAM ».

Lien avec les mesures cryptographiques

Les fichiers loggings contiennent toute une gamme d'informations et doivent donc à leur tour satisfaire au modèle de classification de l'information. En conséquence, il est envisageable que les informations des loggings se voient attribuer la catégorie d'information 3 ou plus, ou que les données à caractère personnel soient enregistrées dans les fichiers loggings, auquel cas les mesures cryptographiques décrites dans le document « politique cryptographique » sont d'application.

Gestion du document

Historique

Date	*Auteur*	*Version*	*Description des modifications*
13/06/2019	BOSA	V.0.1	First draft
18/06/2019	FISP workgroup	V. 1	Mise à jour basée sur commentaires
20/06/2019	FISP workgroup	V.1.1	Mise à jour basée sur les commentaires de la réunion du GT
21/11/2019	FISP workgroup	V.1.2	Distribution publique

Approbations

Date	*Approbateur(s)*	*Version*
21/11/2019	FISP workgroup	V.1.2

Sources

Ce document a été rédigé à l'aide des sources suivantes :

- Vo Classification de l'information – Mesures minimales – SIEM
- BCSS – BLD LOG
- CEI 27001/2

Lien avec une autre politique

Dépendance de documents internes

Réf.	*Titre*
FISPDOC01	*Guide pour la catégorisation des informations*

Positionnement de la politique par rapport à la norme ISO 27001

Section	***Objectifs et mesures de référence***	*En relation (X = Oui*
	Contexte de l'organisation	
	Leadership	
	Planification	
	Support	
	Opération	
	Évaluation du travail presté	
	Améliorations	

Positionnement de la politique par rapport à la norme ISO 27002

Section	**Objectifs et mesures de référence**	En Relation *(X = Oui)*	Objectifs/Mesures *(Détail)*
	Politique de sécurité de l'information		
	Organisation de la sécurité de l'information		
	Sécurité des ressources humaines		
	Asset management		
	Contrôle d'accès		
	Cryptographie		
	Sécurité physique et écologique		
	Sécurité opérationnelle	*X*	*12.4.*
	Sécurité de la communication		
	Acquisition, développement et maintenance des systèmes d'information		
	Relations avec les fournisseurs		
	Gestion des incidents de sécurité de l'information		
	Sécurité de l'information dans la gestion de la continuité des opérations		
	Conformité		