Journalisation

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

**6. Exigences de la norme ISO 27001 : 2022**

**7. Politique journalisation**

**7.1 Journaux**

**7.2 Protection des journaux**

**7.3 Analyse des journaux**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

La politique journalisation a pour objet de décrire les méthodes utilisées pour conserver et protéger les enregistrements des activités, événements et incidents de l’information dans notre organisation.

**2. Finalité**

La politique journalisation a pour finalité d’enregistrer des événements, de générer des preuves, d’assurer l'intégrité de l’information de journalisation, d’empêcher tout accès non autorisé, d’identifier les événements de sécurité de l’information pouvant conduire à un incident de sécurité de l’information et de soutenir les enquêtes.

**3. Domaine d’application**

La politique journalisation s’applique à tous les départements et actifs de notre organisation qui enregistrent des événements.

**4. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de la politique journalisation. Il est garant de son application. Il a l’appui du directeur et de tous les responsables de département concernés.

**5. Documents**

Journaux des événements

Synchronisation

Collecte de preuves

Protection de la vie privée

Incidents

Activités de surveillance

**6. Exigences de la norme ISO 27001 : 2022**

A.8.15 Journalisation

Des journaux qui enregistrent les activités, les exceptions, les pannes et autres événements pertinents doivent être générés, conservés, protégés et analysés.

**7. Politique journalisation**

**7.1 Journaux**

La politique journalisation pour la protection et la gestion des données détermine :

* l'objectif pour lequel les journaux sont créés
* quelles données sont collectées et enregistrées
* les exigences spécifiques aux journaux

Les journaux d'événements, cf. le fichier Journaux des événements, incluent pour chaque événement, selon le cas :

* les identifiants utilisateur
* les activités du système
* les dates, heures et détails des événements pertinents (connexion, déconnexion)
* l’identité de l'appareil, l’identifiant du système et son emplacement
* les adresses et protocoles de réseau

Les événements suivants sont pris en compte pour la journalisation :

* les tentatives d'accès au système réussies et rejetées
* les tentatives d'accès réussies et rejetées aux données et autres ressources
* les modifications de la configuration du système
* l’utilisation des privilèges
* l'utilisation de programmes et d'applications utilitaires
* les fichiers consultés et le type d'accès, y compris la suppression des fichiers de données importants
* les alarmes déclenchées par le système de contrôle d'accès
* l’activation et la désactivation des systèmes de sécurité, tels que les systèmes antivirus et les systèmes de détection d'intrusion
* la création, la modification ou la suppression d'identité
* les transactions exécutées par les utilisateurs dans les applications

Tous les systèmes ont des sources de temps synchronisées afin de permettre la corrélation des journaux entre les systèmes pour l'analyse, l'alerte et l'investigation d'un incident, cf. le fichier Synchronisation.

**7.2 Protection des journaux**

Les utilisateurs, y compris ceux disposant de droits d'accès privilégiés, ne sont pas autorisés à supprimer ou à désactiver les journaux de leurs propres activités. Ils peuvent potentiellement manipuler les journaux sur les installations de traitement de l'information sous leur contrôle direct. Il est nécessaire de protéger et de passer en revue les journaux pour maintenir la responsabilité des utilisateurs privilégiés.

Des contrôles protègent contre les modifications non autorisées de l’information des journaux et des problèmes de fonctionnement de l'installation de journalisation, notamment :

* la modification des types de messages enregistrés
* les fichiers journaux en cours de modification ou de suppression
* le défaut d'enregistrement d'événements ou l’écrasement d'événements enregistrés passés si le support de stockage contenant un fichier journal est plein

Pour la protection des journaux, les techniques suivantes sont utilisées :

* hachage cryptographique
* enregistrement dans un fichier en ajout uniquement et en lecture seule
* enregistrement dans un fichier de transparence publique

Certains journaux d'audit peuvent être archivés en raison d'exigences en matière de conservation des données ou d'exigences de collecte et de conservation de preuves selon la procédure Collecte de preuves.

Lorsque l'organisation envoie des journaux système ou d'application à un fournisseur (pour faciliter le dépannage d'erreurs), les journaux sont rendus anonymes (sans noms d'utilisateur, adresses de protocole Internet, d'hôte).

Les journaux d'événements peuvent contenir des données sensibles et des informations personnellement identifiables. Des mesures appropriées de protection de la vie privée sont prises selon la procédure Protection de la vie privée.

**7.3 Analyse des journaux**

L'analyse des journaux permet l'analyse et l'interprétation des événements de sécurité de l'information. De cette manière nous pouvons identifier les activités inhabituelles ou les comportements anormaux.

L'analyse des événements est effectuée en tenant compte des éléments suivants :

* les compétences nécessaires pour les experts réalisant l'analyse
* la procédure d'analyse du journal
* les attributs requis de chaque événement lié à la sécurité
* les exceptions identifiées grâce à l'utilisation de règles prédéterminées comme :
  + information de sécurité et gestion des événements (SIEM)
  + règles de pare-feu
  + système de détection d'intrusion (IDS)
  + signatures de logiciels malveillants
* les modèles de comportement connus et trafic réseau standard par rapport à une activité et un comportement anormaux
* les résultats de l'analyse des tendances ou des modèles
* les renseignements sur les menaces disponibles

L'analyse des journaux est soutenue par des activités de surveillance spécifiques pour aider à identifier et à analyser les comportements anormaux, notamment :

* examiner les tentatives réussies et infructueuses d'accès aux ressources protégées (serveurs de système de noms de domaine (DNS), portails Web)
* vérifier les journaux DNS pour identifier les connexions réseau sortantes vers des serveurs malveillants (serveurs de commande et de contrôle des « *botnets »)*
* examiner les rapports d'utilisation des fournisseurs de services (factures, rapports de service) pour détecter une activité inhabituelle dans les systèmes et les réseaux (en examinant les modèles d'activité)
* inclure les journaux d'événements de surveillance physique afin d’assurer une détection plus précise et une analyse des incidents
* corréler les journaux pour permettre une analyse efficace et précise. Les incidents de sécurité de l'information suspectés et réels sont identifiés (infection par un logiciel malveillant, détection de pare-feu) et faire l'objet d'une enquête plus approfondie selon la procédure Incidents

Les journaux système contiennent souvent un grand volume de données, dont la plupart sont étrangères à la surveillance de la sécurité de l’information. L’utilisation de programmes utilitaires ou d'outils d'audit appropriés pour effectuer l'interrogation des fichiers est possible.

La journalisation des événements constitue la base des systèmes de surveillance automatisés qui sont capables de générer des rapports consolidés et des alertes sur la sécurité du système selon la procédure Activités de surveillance.

L’outil SIEM (ou équivalent) peut être utilisé pour stocker, corréler, normaliser et analyser les informations des journaux, et pour générer des alertes. Les configurations à prendre en compte incluent l'identification et la sélection des sources de journaux appropriées, le réglage et le test des règles et le développement de cas d'utilisation.

Les fichiers de transparence publics pour l'enregistrement des journaux sont utilisés, par exemple, dans les systèmes de transparence des certificats. De tels fichiers peuvent fournir un mécanisme de détection supplémentaire utile pour se prémunir contre la falsification des journaux.

Dans les environnements du service en nuage, les responsabilités de gestion des journaux peuvent être partagées entre le client et le fournisseur.