Activités de surveillance

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

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

**5. Déroulement**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de détecter des comportements anormaux et des incidents potentiels de sécurité de l’information.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Activités de surveillance » s’applique aux personnes responsables de la surveillance des réseaux, des systèmes et des applications.

**1.3 Glossaire**

RSI – responsable sécurité de l’information

CPU – *central processing unit* - unité centrale de traitement

DNS – *domain name system* - système de noms de domaines

**2. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de cette procédure. Il est garant de son application. Il a l’appui du directeur.

**3. Documents**

Surveillance

Journaux des événements

Gestion des vulnérabilités

Registre des incidents

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

A.8.16 Activités de surveillance

Les réseaux, systèmes et applications doivent être surveillés pour des comportements anormaux et des mesures appropriées doivent être prises pour évaluer les éventuels incidents de sécurité de l’information.

**5. Déroulement**

L'étendue et le niveau de surveillance sont déterminés conformément aux exigences de sécurité de l'entreprise et de l'information et en tenant compte des lois et réglementations applicables. Les enregistrements de surveillance sont conservés pendant des périodes de conservation définies dans le fichier Surveillance.

Le système de surveillance inclut les éléments suivants :

* le trafic sortant et entrant :
  + du réseau
  + du système et
  + des applications
* l’accès aux systèmes, serveurs, équipements de réseau, système de surveillance, applications critiques, etc.
* les fichiers de configuration système et réseau de niveau critique ou administrateur
* les journaux des outils de sécurité (antivirus, système de détection des intrusions, système de prévention des intrusions, filtres Web, pare-feu, prévention des fuites de données)
* les journaux d'événements relatifs à l'activité du système et du réseau, cf. Journaux des événements
* la vérification que le code en cours d'exécution soit autorisé à s'exécuter dans le système et qu'il n'a pas été altéré
* l’utilisation des ressources (CPU, disques durs, mémoire, bande passante) et leurs performances

L'établissement d'une ligne de base de comportement normal est nécessaire pour surveiller tout ce qui est anormal par rapport à cette ligne de base. Les éléments suivant sont pris en compte :

* l’examen de l'utilisation des systèmes en périodes normales et de pointe
* les heures d'accès habituelles, le lieu d'accès, la fréquence d'accès pour chaque utilisateur (ou groupe d'utilisateurs)

Le système de surveillance est configuré par rapport à la ligne de base afin d’identifier les comportements anormaux, tels que :

* arrêt imprévu d’un processus ou d'une application
* activité généralement associée à des logiciels malveillants ou au trafic provenant d'adresses IP ou de domaines de réseau malveillants connus
* caractéristiques d'attaque connues (déni de service)
* comportement inhabituel du système (journalisation des frappes, écarts dans l'utilisation des protocoles standard)
* goulots d'étranglement et surcharges (mise en file d'attente du réseau)
* accès non autorisé (réel ou suspecté)
* analyse non autorisée d'application, de système et de réseau
* tentatives réussies et infructueuses d'accès aux ressources protégées (serveurs DNS, portails Web, systèmes de fichiers)
* comportement inhabituel de l'utilisateur et du système (par rapport au comportement attendu)

Une surveillance continue via un outil de surveillance est utilisée. La surveillance est effectuée en temps réel ou à intervalles périodiques, en fonction des besoins et des capacités de l'organisation. Les outils de surveillance peuvent :

* gérer de grandes quantités de données
* s'adapter à un paysage de menaces en constante évolution
* permettre une notification en temps réel

Les outils sont également capables de reconnaître des signatures et des données spécifiques ou des modèles de comportement de réseau ou d'application.

Les logiciels de surveillance automatisés sont configurés pour générer des alertes (consoles de gestion, messages électroniques, systèmes de messagerie instantanée) en fonction de seuils prédéfinis. Le personnel est dédié à répondre aux alertes et est correctement formé pour interpréter avec précision les incidents potentiels.

Les événements anormaux sont communiqués aux parties concernées afin d'améliorer les activités suivantes :

* audit
* évaluation de la sécurité
* analyse et surveillance des vulnérabilités selon la procédure Gestion des vulnérabilités

Les indicateurs positifs du système de surveillance en temps opportun sont en place afin de minimiser l'effet des événements indésirables sur la sécurité de l'information, cf. le Registre des incidents.

La surveillance de la sécurité est améliorée selon les éléments suivants :

* tirer parti des systèmes de renseignements sur les menaces
* tirer parti des capacités d'apprentissage automatique et d'intelligence artificielle
* utiliser des listes de blocage
* entreprendre une série d'évaluations techniques de la sécurité (évaluations de vulnérabilité, tests d'intrusion, simulations de cyber-attaques, exercices de cyber-réponse) et utiliser les résultats de ces évaluations pour aider à déterminer la ligne de base (comportement acceptable)
* utiliser des systèmes de surveillance des performances pour aider à établir et à détecter un comportement anormal
* exploiter les journaux en combinaison avec les systèmes de surveillance

La surveillance des communications anormales aide à l'identification des « *botnets* » (ensemble d'appareils sous un contrôle malveillant).