Programmes malveillants

**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 d’assurer que l’information et les autres actifs associés sont protégés contre les logiciels malveillants.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Programmes malveillants » s’applique à l’ensemble du personnel ayant accès à l’information et aux autres actifs de l’organisation.

**1.3 Glossaire**

RSI – responsable sécurité de l’information

**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**

Installation de logiciels

Changements

Protection contre les logiciels malveillants

Gestion des vulnérabilités

Continuité d’activité

Sauvegarde

Plan de continuité d’activité

Séparation des environnements

Sensibilisation et formation

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

A.8.7 Programmes malveillants

La protection contre les programmes malveillants doit être appliquée et soutenue par une sensibilisation appropriée du personnel.

**5. Déroulement**

La protection contre les logiciels malveillants est basée sur :

* un logiciel de détection et de réparation
* une sensibilisation à la sécurité de l’information
* un accès approprié au système
* des contrôles de gestion des modifications

L'utilisation d'un logiciel de détection et de réparation à lui seul n'est généralement pas suffisante. Pour cela les éléments suivants sont pris en compte :

* appliquer des règles et des mesures qui empêchent ou détectent l'utilisation de logiciels non autorisés, cf. les procédures Installation de logiciels et Changements
* appliquer des mesures qui empêchent ou détectent l'utilisation de sites Web malveillants connus ou suspectés, cf. le fichier Protection contre les logiciels malveillants
* réduire les vulnérabilités pouvant être exploitées par des logiciels malveillants, cf. la procédure Gestion des vulnérabilités
* effectuer une validation automatisée régulière des logiciels et du contenu des données des systèmes (processus commerciaux critiques)
* enquêter sur la présence de fichiers non approuvés ou de modifications non autorisées
* établir des mesures de protection contre les risques liés à l'obtention et l’utilisation de fichiers et de logiciels avec origine des réseaux externes
* installer et mettre régulièrement à jour un logiciel de détection et de réparation de logiciels malveillants pour analyser les ordinateurs et les supports de stockage
* effectuer des analyses régulières qui incluent avant utilisation :
  + scruter toute donnée venant des réseaux ou d’un support de stockage
  + analyser à la recherche de logiciels malveillants les pièces jointes et les téléchargements des e-mails et des messageries instantanées
  + effectuer cette analyse à différents endroits (serveurs de messagerie, ordinateurs de bureau) et lors de l'entrée sur le réseau de l'organisation
  + analyse des pages Web accédées à la recherche de logiciels malveillants
* déterminer l'emplacement et la configuration des outils de détection et de réparation en fonction des résultats de l'évaluation des risques et en tenant compte :
  + des principes de défense en profondeur là où ils seraient les plus efficaces (passerelle réseau, messagerie électronique, transfert de fichiers) ainsi que dans les terminaux et les serveurs utilisateur
  + des techniques évasives des attaquants (fichiers cryptés) pour diffuser des logiciels malveillants ou l'utilisation de protocoles de cryptage pour transmettre des logiciels malveillants
  + de se protéger contre l'introduction de logiciels malveillants lors des procédures de maintenance et d'urgence, ce qui peut contourner les contrôles normaux contre les logiciels malveillants
* mettre en œuvre un processus pour autoriser la désactivation temporaire ou permanente de certaines mesures contre les logiciels malveillants, y compris les autorités d'approbation des exceptions, la justification documentée et la date de révision. Cela peut être nécessaire lorsque la protection contre les logiciels malveillants perturbe les opérations normales
* préparer des plans de continuité d’activité appropriés pour la reprise après des attaques de logiciels malveillants, y compris toutes les sauvegardes de données et de logiciels nécessaires selon les procédures Continuité d’activité et Sauvegarde et le Plan de continuité d’activité
* séparer les environnements où des conséquences catastrophiques peuvent survenir selon la procédure Séparation des environnements
* définir les activités et les responsabilités pour assurer la protection contre les logiciels malveillants, y compris la formation à leur utilisation, le signalement et la récupération des attaques de logiciels malveillants
* sensibiliser et former tous les utilisateurs sur la manière d'identifier et potentiellement d'atténuer la réception, l'envoi ou l'installation de courriels, de fichiers ou de programmes infectés par des logiciels malveillants selon la procédure Sensibilisation et formation
* appliquer la collecte régulière d’information sur les nouveaux logiciels malveillants (inscription à des listes de diffusion, consultation de sites Web pertinents)
* vérifier que l’information relative aux logiciels malveillants (bulletins d'avertissement) provient de sources qualifiées et dignes de confiance (sites Internet fiables, fournisseurs de logiciels de détection de logiciels malveillants) et qu'elle est exacte et informative

Il n'est pas toujours possible d'installer un logiciel qui protège contre les logiciels malveillants sur certains systèmes. Dans ce cas d’infection par des logiciels malveillants une ré imagerie complète du logiciel du système d'exploitation est nécessaire pour revenir à un état sécurisé.