Gestion des vulnérabilités

**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**

**5.1 Identification**

**5.2 Évaluation**

**5.3 Prise de mesures**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de prévenir l'exposition à des vulnérabilités techniques.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Gestion des vulnérabilités » 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**

Inventaire des actifs

Relations avec les fournisseurs

Accord fournisseur

Codage

Vulnérabilités techniques

Registre des vulnérabilités

Installation de logiciels

Incidents

Changements

Sécurité des réseaux

Sensibilisation et formation

Registre des incidents

Continuité d’activité

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

A.8.8 Gestion des vulnérabilités techniques

Des informations sur les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenues, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et des mesures appropriées doivent être prises.

**5. Déroulement**

**5.1 Identification**

Un Inventaire des actifs à jour est un prérequis pour gérer efficacement les vulnérabilités techniques. L’inventaire contient le fournisseur du logiciel, le nom du logiciel, les numéros de version, l'état actuel du déploiement et le responsable du logiciel.

Les éléments suivant sont pris en compte pour identifier les vulnérabilités techniques :

* définir et établir les rôles associés à la gestion des vulnérabilités techniques (surveillance, évaluation des risques, mise à jour, suivi des actifs et coordination requise)
* identifier les ressources d'information qui seront utilisées pour identifier les vulnérabilités techniques pertinentes et maintenir la sensibilisation à leur sujet
* tenir à jour la liste des ressources d'information en fonction des changements dans l'inventaire ou lorsque d'autres ressources nouvelles sont trouvées
* exiger des fournisseurs de système d'information (y compris leurs composants) qu'ils assurent le signalement, le traitement et la divulgation des vulnérabilités selon la procédure et la politique Relations avec les fournisseurs et le fichier Accord fournisseur
* utiliser des outils d'analyse des vulnérabilités adaptés aux technologies utilisées pour identifier les vulnérabilités
* vérifier si suite à l’analyse et l’identification la correction des vulnérabilités a réussi
* réaliser des tests d'intrusion ou évaluer les vulnérabilités de manière planifiée, documentée et reproductible par des personnes compétentes et autorisées pour aider à l'identification des vulnérabilités
* faire preuve de prudence car les tests d’intrusion peuvent entraîner une défaillance de la sécurité du système
* utiliser des bibliothèques tierces et du code source pour les vulnérabilités selon la procédure Codage

Des moyens sont développées pour :

* détecter l'existence de vulnérabilités dans les produits et services
* recevoir des rapports de vulnérabilité de sources internes ou externes

La politique Vulnérabilités techniques établit un point de contact public (forum) sur le signalement et la divulgation des vulnérabilités. Les vulnérabilités sont encouragées et enregistrées dans le fichier en ligne Registre des vulnérabilités.

**5.2 Évaluation**

Les éléments suivants sont pris en compte afin d’évaluer les vulnérabilités techniques identifiées :

* analyser et vérifier les rapports pour déterminer les activités d'intervention et de correction nécessaires
* identifier les risques associés et les actions à entreprendre pour toute vulnérabilité technique potentielle identifiée
* mettre à jour, si nécessaire les systèmes vulnérables ou l'application d'autres mesures

**5.3 Prise de mesures**

La procédure Installation de logiciels inclut les recommandations pour la gestion des mises à jour sans retard des logiciels.

Les éléments suivants sont pris en compte afin de résoudre les vulnérabilités techniques :

* prendre des actions appropriées et opportunes en réponse à l'identification de vulnérabilités techniques potentielles
* définir un calendrier pour réagir aux notifications de vulnérabilités techniques potentiellement pertinentes
* mener l'action selon les procédures Incidents et Changements en fonction de l'urgence de la vulnérabilité technique
* utiliser uniquement des mises à jour provenant de sources légitimes (ou dignes de confiance)
* tester et évaluer les mises à jour avant leur installation afin de s'assurer qu'elles sont efficaces et qu'elles n'entraînent pas d'effets secondaires indésirables
* traiter en priorité les systèmes à haut risque
* développer des mesures correctives (mises à jour ou correctifs)
* tester pour confirmer l’efficacité de la correction ou de l'atténuation
* fournir des mécanismes afin de vérifier l'authenticité de la correction
* si aucune mise à jour n'est disponible ou si la mise à jour ne peut pas être installée, considérer d'autres mesures, telles que :
  + appliquer toute solution de contournement suggérée par le fournisseur du logiciel ou d'autres sources pertinentes
  + désactiver les services ou les fonctionnalités liés à la vulnérabilité
  + adapter ou ajouter des contrôles d'accès (pare-feu) aux frontières du réseau, cf. la procédure Sécurité des réseaux
  + protéger les systèmes, appareils ou applications vulnérables contre les attaques grâce au déploiement de filtres de trafic appropriés (correctifs virtuels)
  + accroître la surveillance pour détecter les attaques réelles
* sensibiliser le personnel à la vulnérabilité, cf. la procédure Sensibilisation et formation

Pour les logiciels acquis, quand le fournisseur propose une application pour installer ces mises à jour automatiquement, la décision est prise au cas par cas afin de garder le contrôle sur le moment où la mise à jour est effectuée.

Les actions entreprises de gestion des vulnérabilités techniques sont enregistrées dans les fichiers Registre des vulnérabilités et Registre des incidents.

Pour un fournisseur de services en nuage, la gestion des vulnérabilités techniques est assurée par le fournisseur et fait partie de l’accord signé, cf. Accord fournisseur.

Quand la mise à jour ne résolve pas la vulnérabilité technique de manière adéquate et peut avoir des effets secondaires négatifs, un retard dans la mise à jour peut être envisagé et une évaluation des risques associés est réalisée selon la procédure Continuité d’activité.