Politiques relatives à la gestion des vulnérabilités et des correctifs

Modèle

# Utilisation de ce document

* Cette politique a été rédigée de manière à ce que le document puisse être utilisé pour les 3 différents niveaux d'assurance de **CyFun.** (**Basique**, **Important**, **Essentiel**)
* Les besoins requis pour atteindre un certain niveau d'assurance seront précisés en indiquant le texte proposé dans la couleur mentionnée ci-dessus.

Contenu

[Utilisation de ce document 2](#_Toc157679160)

[Autorité et révision 3](#_Toc157679161)

[Contrôle et révision des documents 3](#_Toc157679162)

[Gestion des versions 3](#_Toc157679163)

[Intro 4](#_Toc157679164)

[Gestion des vulnérabilités 4](#_Toc157679165)

[Évaluation des risques 4](#_Toc157679166)

[Recherche de vulnérabilités internes 4](#_Toc157679167)

[Recherche de vulnérabilités externes 4](#_Toc157679168)

[IDS/IPS 5](#_Toc157679169)

[Politique de divulgation coordonnée des vulnérabilités CVDP (Important, Essentiel) 5](#_Toc157679170)

[Gestion des correctifs 5](#_Toc157679171)

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents** |  |
| Auteur |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date d'approbation** | **Approuvé par** | **Description du changement** |
|  |  |  |  |

# Intro

Une vulnérabilité est une faille ou une faiblesse, une erreur de conception ou de mise en œuvre, un manque de mise à jour à la lumière des connaissances techniques existantes, qui peut compromettre la sécurité des technologies de l'information. Une vulnérabilité peut entraîner un événement inattendu ou indésirable et être exploitée par des tiers malveillants pour porter atteinte à l'intégrité, à l'authenticité, à la confidentialité ou à la disponibilité d'un système ou pour nuire à un système. Plus de 90 % des infections par des logiciels malveillants ou des cybercrimes commencent par l'exploitation d'une fuite connue. Les systèmes qui autorisent les connexions entrantes à l'internet, tels que les serveurs web et les serveurs de courrier électronique, font notamment l'objet de nombreuses attaques chaque jour.

Il est donc essentiel d'éliminer le plus grand nombre possible de vulnérabilités connues. Pour ce faire, nous avons besoin d'un bon système de gestion des correctifs et d'une surveillance des vulnérabilités.

Le présent document fait partie d'un ensemble de documents destinés à aider **[l'organisation]** à mettre en place une stratégie solide en matière de cybersécurité.

# Gestion des vulnérabilités

## Évaluation des risques

**L'[Organisation]** procède à une évaluation annuelle des risques qui détermine les risques sur la base des menaces, des vulnérabilités et des impacts sur les processus et les actifs de l'entreprise. Ces vulnérabilités font référence à une faiblesse dans le matériel, les logiciels ou les procédures de [l'organisation].

## Recherche de vulnérabilités internes

Les systèmes critiques et confidentiels doivent faire l'objet d'une analyse de vulnérabilité au moins une fois **par an**, par **trimestre** ou **en continu.** Les systèmes hautement critiques et hautement confidentiels doivent être analysés au moins une fois par mois.

Des outils d'analyse des vulnérabilités ou des \*tests de pénétration peuvent être utilisés pour étudier les vulnérabilités des systèmes. Ces outils contiennent une base de données de vulnérabilités connues et peuvent analyser un seul système ou même un réseau entier pour y trouver des vulnérabilités. Les outils d'analyse n'analysent que les vulnérabilités auxquelles ils ont accès. Par exemple, si des services sont bloqués par des pare-feu, ils ne peuvent pas en rendre compte.

Ces outils classent les faiblesses en différents niveaux de risque. Toutefois, il faut savoir que le risque le plus élevé est lorsque la vulnérabilité peut être exploitée à partir de l'internet. Si ce n'est pas le cas, le risque demeure car un système infecté peut l'utiliser pour propager des logiciels malveillants à d'autres machines du réseau, mais la probabilité est plus faible.

## Recherche de vulnérabilités externes

En plus de l'analyse interne, une analyse externe des vulnérabilités (pen test) devrait être effectuée **annuellement, trimestriellement** ou en **continu**. Les résultats de ce test externe devraient constituer la base d'un plan annuel, semestriel ou mensuel d'amélioration de la vulnérabilité et servir de mesure indépendante de la sécurité du système.

## IDS/IPS

Alors que les scanners de vulnérabilité sont utilisés pour détecter les risques potentiels, les systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) assurent une surveillance du réseau en temps réel pour vérifier si des actions malveillantes sont en cours. Les systèmes IDS peuvent envoyer une alerte dès qu'ils constatent un comportement suspect. Les systèmes IPS peuvent même prendre des mesures, par exemple en bloquant le trafic au niveau du pare-feu.

Les IDS/IPS doivent être envisagés pour les systèmes critiques et confidentiels si le risque l'emporte sur le coût.

## Politique de divulgation coordonnée des vulnérabilités CVDP (Important, Essentiel)

Les organisations qui atteignent le niveau d'assurance CyFun **Important** ou **Essentiel** doivent mettre en place une politique coordonnée de divulgation des vulnérabilités.

Il s'agit d'un ensemble de règles prédéterminées par [l'organisation] responsable des systèmes d'information qui permet aux participants (ou "hackers éthiques"), avec de bonnes intentions, de détecter d'éventuelles vulnérabilités dans ses systèmes, ou de lui fournir toute information pertinente à leur sujet. Ces règles, généralement rendues publiques sur un site web, permettent d'établir un cadre juridique pour la coopération entre l'organisation responsable et les participants à la politique. Ces règles doivent notamment garantir la confidentialité des informations échangées et encadrer toute divulgation de vulnérabilités découvertes de manière responsable et coordonnée.

Veuillez vous référer au Guide sur la politique coordonnée de divulgation des vulnérabilités préparé par le Centre for Cybersecurity Belgium lors de l'élaboration de ce CVDP.

[\*https://fr.wikipedia.org/wiki/Test\_d%27intrusion](https://fr.wikipedia.org/wiki/Test_d%27intrusion)

# Gestion des correctifs

Tous les serveurs, pare-feu, commutateurs et clients gérés doivent être mis à jour avec les derniers correctifs pertinents au moins tous les deux mois, sauf décision contraire explicite.

Les correctifs de sécurité doivent être installés dès que possible. Cela ne peut se faire qu'après une analyse d'impact approfondie sur l'environnement du correctif à installer.

Il doit exister un système ou un processus permettant de savoir quels sont les correctifs de sécurité disponibles et applicables.

Les correctifs de sécurité concernent les systèmes d'exploitation, les logiciels de serveur tels que les bases de données, les services et les applications.

**NOTE :** Si un système n'est pas en mesure d'appliquer les correctifs de sécurité, bien que les vulnérabilités soient connues, le système doit être isolé de l'internet et des autres systèmes connectés à l'internet et physiquement sécurisé.