Politique de cybersécurité

Auteur: **Jordan Quintelier**

Date: **10/11/2025**

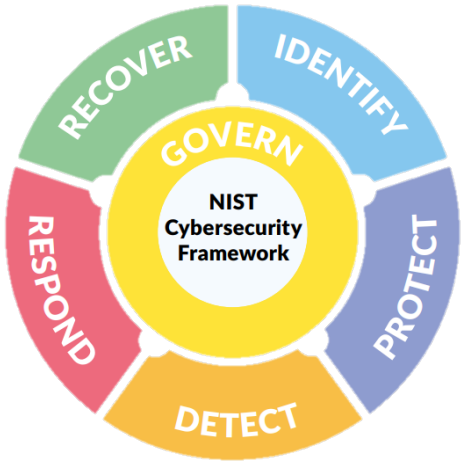
1 Introduction

Civadis fournit des services informatiques aux administrations locales belges, et développe et met en œuvre les applicatifs de soutien aux élections fédérales, européennes, régionales, provinciales et communales. Elle porte donc la lourde responsabilité d'assurer l'intégrité et la confidentialité des données administratives gérées et de garantir la continuité de ces services faisant partie de l'infrastructure critique de la société belge.

1.1 Comment est mise en place la sécurité chez Civadis

- Civadis poursuit une certification ISO/IEC 27001, pour laquelle une entreprise d'audit indépendante attestera de l'intégration de la sécurité dans l'organisation et de la mise en place des mesures nécessaires au maintien de la confidentialité, de l'intégrité et de la disponibilité des données.
- Civadis utilise le cadre mis en place par le CCB, lui-même basé sur le NIST CSF et d'autres standards de contrôle, pour s'assurer d'adresser tous les aspects pertinents de la sécurité.
- Civadis applique le niveau « Important » du CyberSecurity Framework du CCB.

CyFun®



1.2 Le cadre est basé sur 6 catégories

- **Gouverner** : Permettre à Civadis de savoir ce qui doit être fait pour atteindre et hiérarchiser les résultats des cinq autres catégories dans le contexte de sa mission et des attentes des parties prenantes.
- **Identifier** : Permettre à Civadis de comprendre ses actifs, ses fournisseurs et les risques qui leur sont associés. Identifier les pistes d'amélioration pour la gestion des risques de cybersécurité.
- **Protéger** : Mettre en place des mesures de protection permettant de prévenir ou de réduire la probabilité et l'impact des événements négatifs sur les actifs.
- **Détecter** : Découvrir et analyser les anomalies, les incidents et d'autres événements potentiellement négatifs qui peuvent indiquer que des attaques sont en cours.

- **Réagir** : Mettre en place les activités nécessaires pour contenir les impacts des incidents de cybersécurité.
- **Récupérer** : Mettre en place les activités nécessaires pour rétablir le plus rapidement possible les opérations de Civadis afin de réduire les impacts des incidents et de permettre une communication appropriée pendant le rétablissement.

1.3 Implémentation

En pratique, le cadre est mis en place chez Civadis selon une approche itérative d'amélioration continue.

Gouverner

- Un projet de certification ISO27001 est en cours afin de répondre aux obligations de la directive NIS2
- Des politiques et procédures de cybersécurité sont en place et revues régulièrement
- Une stratégie de cybersécurité définie et alignée sur les objectifs et les analyses de risques
- Les activités de Civadis sont conformes au RGPD, à la directive NIS2 et aux autres réglementations applicables
- Des rapports sont revus régulièrement par le Comité de Sécurité Informatique

Identifier

- Un inventaire d'actifs est tenu afin d'avoir une vue globale des dépendances et des impacts potentiels sur les systèmes.
- Une méthode d'analyse de risque est en place, inspirée de la norme ISO/IEC 27005
- Civadis évalue les risques de cybersécurité associés aux partenaires, fournisseurs et autres tiers, et met en place des mesures pour les gérer.
- Des pentests réguliers sont exécutés afin d'évaluer la maturité des processus de protection et de détection
- Une veille constante est assurée afin d'identifier de nouvelles menaces et de les intégrer dans nos outils et processus

Protéger

- Les locaux de Civadis sont protégés pour assurer un contrôle des accès ainsi qu'une protection physique des actifs
- Les datacenters utilisés par Civadis appartiennent à Keyes et sont conformes au niveau Tier III+, le niveau le plus élevé disponible en Belgique
- Les données sont sauvegardées et la confidentialité des sauvegardes est assurée via du chiffrement
- Le hardening et le patching sont assurés à travers le processus de gestion des vulnérabilités
- Tous les collaborateurs de Civadis suivent des formations régulières à la cybersécurité
- Les systèmes de Civadis sont protégés par des pares-feux et anti-malware, ainsi que par un contrôle d'accès rigoureux, incluant l'authentification multi-facteurs
- Les droits d'accès sont gérés selon des procédures rigoureuses

Détecter

- Le réseau, les systèmes et les locaux de Civadis sont surveillés de manière continue. Un comportement anormal génère une alerte.
- Les alertes sont analysées par l'équipe sécurité, qui en assure également le suivi
- Des audits techniques sont effectués de manière récurrente afin d'identifier les faiblesses potentielles

Réagir

- Un processus de gestion des incidents et des crises est mis en place pour traiter les incidents de manière efficace et assurer la continuité des activités
- Des procédures de communication sont mises en place pour informer les parties prenantes en temps adéquat
- Les incidents sont analysés et classés afin d'exécuter les plans d'actions, et permettre un apprentissage continu
- Les incidents sont confinés et résolus afin de limiter leurs impacts
- Des contacts avec les autorités compétentes sont maintenus pour permettre une réaction rapide et de qualité ainsi qu'un partage d'informations efficace

Récupérer

- Les actions nécessaires sont prises pour restaurer les services, les systèmes et les opérations critiques après un incident de cybersécurité
- Les contacts avec les parties prenantes et les autorités compétentes sont maintenus tout au long du processus de récupération pour assurer la transparence et la confiance.
- Après résolution et récupération, les incidents et les actions effectuées sont analysés afin d'améliorer les processus de gestion et les plans d'action