La mutualisation informatique
au service des pouvoirs locaux

Séance d'information - Cybersécurité

Prenez le pouvoir
sur votre informatique.

Isnes, 16 avril 2024

Contexte

Augmentation des cyberattaques et des menaces numériques
Arrêté du GW du 16 décembre 2021

Le plan fédéral relatif à la Stratégie cybersécurité 2.0 2021-2025 précise que la cybermenace peut être utilisée dans le cadre de la menace hybride pour amplifier les effets d'autres méthodes d'attaque. En cas de menace, la combinaison, par exemple, d'une attaque physique et d'une série de cyberattaques peut sérieusement augmenter l'impact et **semer temporairement une atmosphère de chaos**.

Objectif du GW

Fournir un soutien financier à l'ensemble des communes et des centres publics d'action sociale afin de les **équiper**, de les **conscientiser** à la nécessité de s'équiper de manière structurelle et de **former** les agents dans le cadre de la cybersécurité.

Il faut en effet œuvrer à rendre le cyberespace plus sûr en vue de sauvegarder et de protéger les droits fondamentaux et démocratiques de nos institutions.

Subside du GW

Audits (750.000 euros) finalisés le 31 mars 2023

Évaluer la maturité en cybersécurité au sein des Pouvoirs locaux en Wallonie

Mesures (1.750.000 euros) 15/10/2023 au 30/6/2024

Fournir des outils pour la renforcer

Méthodologie

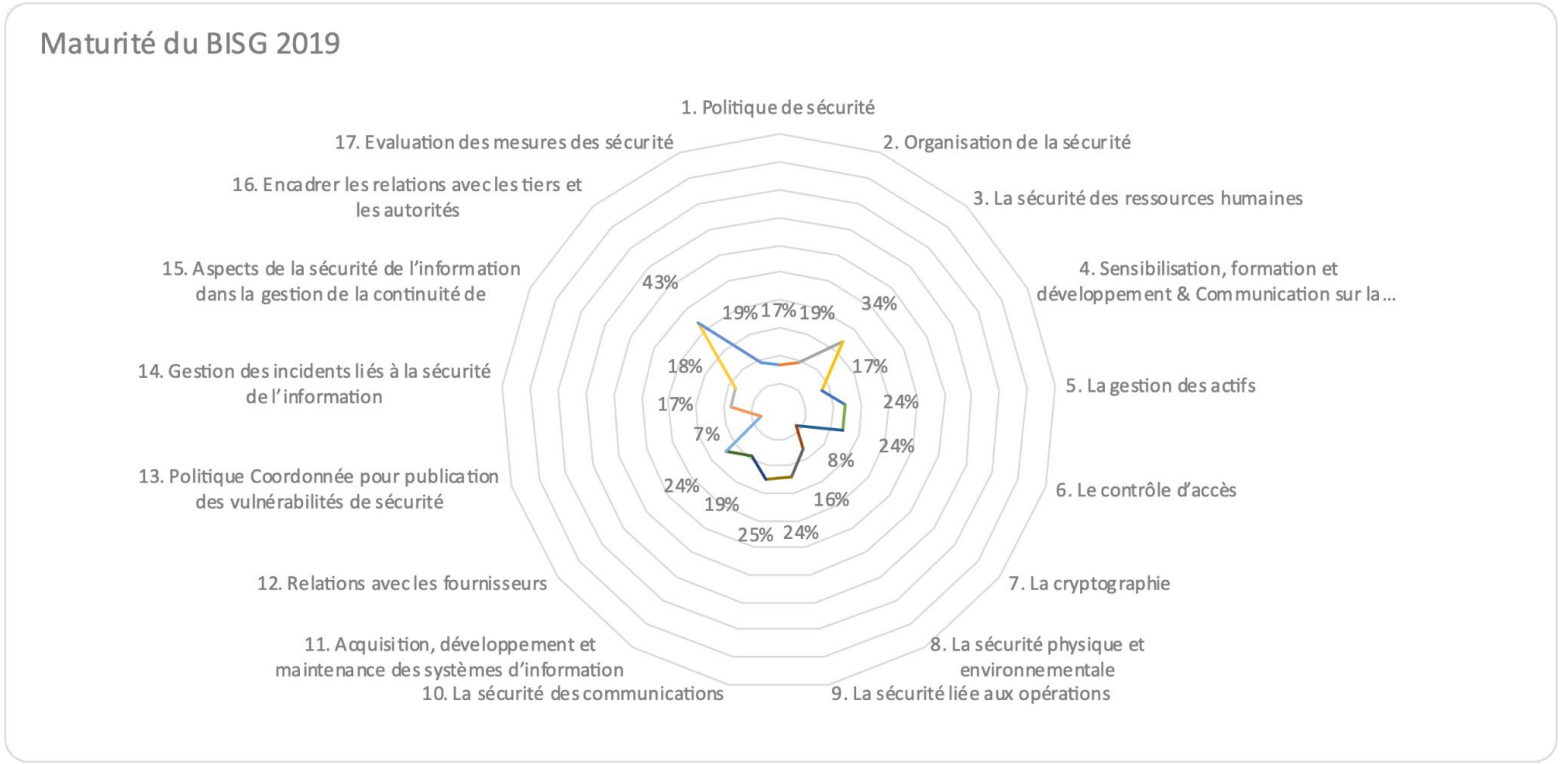
Audit de maturité (octobre 2022 → mars 2023) de 60 communes et 40 CPAS

Indicateurs identiques fédéraux & internationaux imposés :

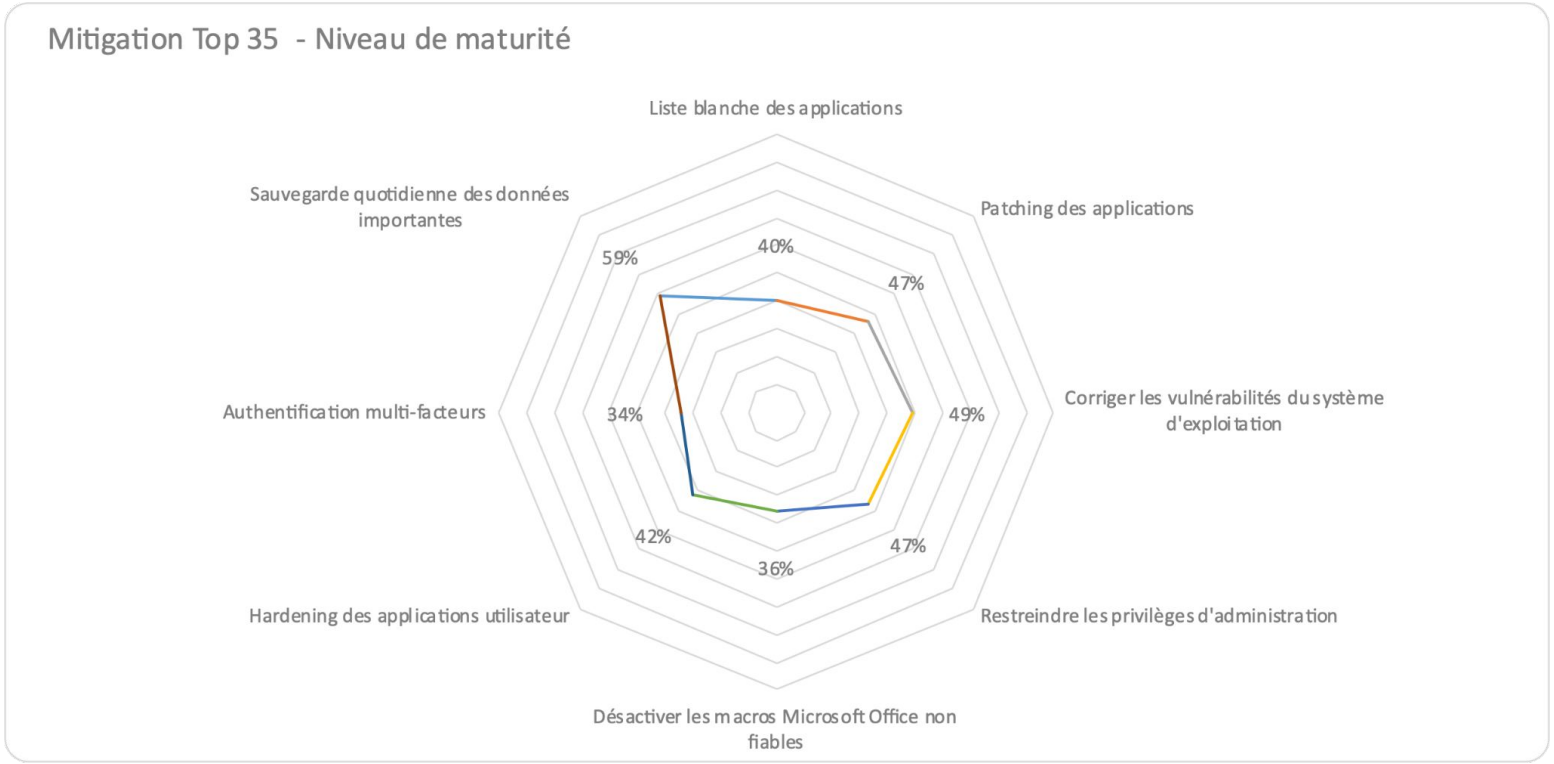
- Recommandations du CCB s'inspirant de la norme ISO 27001 (bonnes pratiques), 103 points de contrôle
- Liste de contrôle technique (Top 35)

Analyse sur base de preuves

Indicateurs normalisés (fédéral)



Indicateurs normalisés (fédéral)

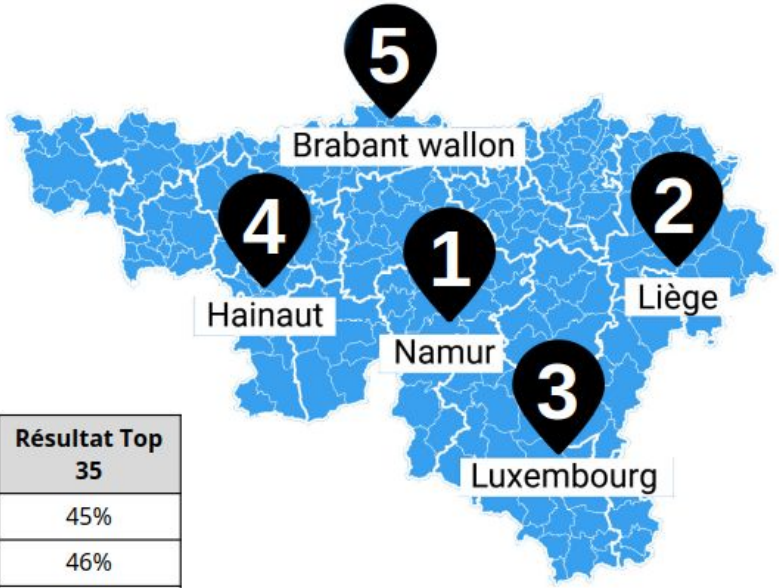


Chiffres clés

- 20 experts, 6 sociétés
- 100 CPAS et Administrations Communales audités
- 92% ne dépassent pas 35% de maturité de conformité avec les standards

Un impact sur près de 1,300,000 citoyens, soit près de 40% de la Wallonie
4 PL de très grande taille (supérieur à 50000hab.)
14 PL de grande taille (entre 20000 et 50000hab.)
25 PL de taille moyenne (entre 10000 et 20000hab.)
40 PL de petite taille (entre 4000 et 10000hab.)
17 PL de très petite taille (inférieur à 4000)

Résultats



Province	Résultat Agrégé	Résultat ISO	Résultat Top 35
Hainaut	**32%**	19%	45%
Liège	**34%**	23%	46%
Luxembourg	**34%**	24%	44%
Namur	**36%**	26%	47%
Brabant Wallon	**27%**	16%	37%

Résultats

91% des agents et des élus déclarent ne pas avoir été sensibilisés à la sécurité informatique
81% pensent que le risque est faible ; inexistant ou ne savent pas l'évaluer
96% des pouvoir locaux interrogés ne sont pas en conformité avec le RGPD
94% des Pouvoir Locaux ont déclaré partager un ou plusieurs mots de passe
57% des Pouvoir Locaux ont déclaré ne pas savoir qui contacter en cas d'incident de sécurité de grande ampleur.
83% externalisent la totalité de la gestion de leur parc informatique.
18% des Pouvoir Locaux audités déclarent avoir eu un problème de continuité de l'activité après le départ/l'arrêt surprise d'un collaborateur ou d'un prestataire externe.

Résultats

Pas de culture du risque

Usurpation d'identité : des agents se partagent des mots de passe.
Exploitation du manque de culture sécurité d'un collaborateur via une attaque de type social engineering.
L'absence de test des backups
Accès facile aux bâtiments et infrastructures
Recommandations de rapports précédents ne sont pas souvent mises en œuvre
Mise en défaut de l'administration par rapport à des obligations réglementaires
Absence de fiche de fonction, d'attribution d'objectifs et d'évaluation.
Pas d'inventaire d'actifs
Stratégie de mots de passe pas en phase avec la réalité du paysage cyber
Absence de feuille de route cybersécurité
Fuite de données sensibles via un accès non autorisé aux serveurs.

Recommandations

- Renforcer la **gouvernance**
  - *Absence d'une politique de sécurité*
  - *Rôles et responsabilités non clairement définis.*
  - *Absence d'une stratégie de communication*
- Développer les **compétences** cybersécurité

Recommandations

- Promouvoir la collaboration entre les Pouvoirs locaux, les autorités régionales et fédérales pour **mutualiser** les ressources et les compétences en matière de cybersécurité
- Forcer l'**adoption d'un cadre de cybersécurité** contraignant reconnu, tel que l'ISO 27001
- Assurer la **conformité aux réglementations** applicables, telles que le RGPD, en mettant en place des processus et des contrôles adaptés.

Centrale de marché “mesures”

- **Marché public mesures cybersécurité** : L'objectif est de mobiliser des ressources externes spécialisées pour aider à renforcer les capacités de cybersécurité des Pouvoirs locaux. Ce marché fournira un point de départ significatif pour la cybersécurité. Néanmoins, il ne doit pas être perçu comme une solution universelle. Une supervision rigoureuse et un suivi continu seront essentiels pour garantir l'efficacité de ce projet.

Offre de service

https://www.imio.be/cda/cybersecurite/offres-de-service

https://www.imio.be/cda/cybersecurite

Lots pour l'accompagnement

- A1 : Rédaction et accompagnement des politiques de sécurité

  Accompagnement relatif à la définition de votre stratégie et la feuille de route à mettre en œuvre pour protéger les données de l'organisation

- A2 : Évaluation des vulnérabilités et pen test

  Outils et de méthodologies pour fournir une analyse détaillée des vulnérabilités cachées dans les systèmes d'information du pouvoir local et des risques associés ; former les agents à comprendre et agir et fournir un service de suivi des corrections

- A3 : Campagne de test de phishing/vishing/social engineering

  Campagnes de sensibilisation et formations des agents aux bonnes pratiques; des tests afin de vérifier la vulnérabilité des agents aux tentatives de cyber intrusion; des actions de correction et évaluation de leur efficacité

Pen test et bug bounty

Test de pénétration (pentest) et programme de bug bounty pour applications web, clients lourds et cloud native. Marché séparé initié et exécuté par iMio.

Le lot 1 concerne un exercice de test de pénétration exhaustif -> Civadis

Ce pentest est conçu pour évaluer en profondeur la robustesse des serveurs et applications les plus couramment utilisées chez les prestataires des pouvoirs locaux dans le cadre d'une infrastructure locale, donc non cloud-native (prestataire : Approach Belgium).

Le lot 2 concerne un programme de bug bounty dans le cadre d'applications cloud-native -> iMio

Ce programme entend mobiliser la communauté des chercheurs en sécurité autour d'une démarche collaborative, mettant en lumière les vulnérabilités potentielles (prestataire : Privacy Praxis/Intigriti)

Lots pour l'accompagnement

- A4 : Cyber Threat Intelligence

  Collecte, analyse et diffusion sur les menaces actuelles et émergentes (y compris sur le dark web). Recommandations pour les contrer. Mesures préventives consistant à identifier les acteurs malveillants et leurs techniques, méthodes et outils. Mise en place d'un système d'alerte et d'un portail web reprenant les menaces en temps réel.

- A5: Accompagnement DPD/DPO à la demande.

  Service permettant de se conformer aux exigences réglementaires en matière de protection des données à caractère personnel. Assistance d'experts pour la mise en place d'une politique de protection des données à caractère personnel, formation des agents, suivi et évaluation continue des pratiques mises en place.

- A6 : RSSI as a service

  Le Responsable Sécurité du Système d'Information (RSSI) a pour objectif de fournir des services de conseil et d'expertise en sécurité de l'information : accompagnement dans la définition de la politique de sécurité, proposition de mesures, amélioration des dispositifs, veille règlementaire…

Lots pour l'équipement

- M1 : Produit MFA (authentification multifacteurs)

  Sélection d'un dispositif d'authentification à deux facteurs pour protéger les comptes utilisateurs contre les tentatives d'accès non autorisés. Les services fournis comprennent la personnalisation de la solution, le déploiement, le support technique et les mises à jour.

- M2 : pare-feu

  Sélection d'un environnement technique permettant de protéger l'infrastructure informatique contre les risques de sécurité. Ce système, adapté à la taille de l'organisation et à son environnement (y compris l'installation locale ou cloud), inclut les fonctionnalités les plus récentes en termes de détection de la menace, de chiffrement et de performance. Des services d'installation, support - maintenance et formation sont prévus.

- M3 : Sauvegarde des données sécurisées

  Ce lot concerne la sélection d'un système (cloud ou local) destiné à sauvegarder et restaurer toutes les données du Pouvoir local (applications métier, bases de données, postes de travail, documents, systèmes de fichiers) sur plusieurs types de médias (disques externes, bandes magnétiques,...). Un accompagnement pour mettre en place une stratégie de sauvegarde sécurisée est prévu, de même que la maintenance de la solution.

Lots pour l'équipement

- L1 : Journalisation des événements

Logiciel permettant d'enregistrer les événements survenant dans un réseau informatique (incidents de sécurité, problème applicatif, saturation de serveurs, ...) et de permettre leur consultation via une interface de visualisation unique. Il est capable de récupérer les informations provenant de tous les composants du système informatique (pare-feu, applications, systèmes d'exploitation) pour les traiter de manière unifiée afin, par exemple, d'alerter en temps réel l'utilisateur sur un incident critique.

- L2 : Gestion de l'authentification et à l'identification numérique

Solutions de management et d'authentification de l'ensemble des utilisateurs d'une organisation et de leurs données.

- L3 : Filtrage des messages électroniques

Logiciel (cloud ou local) permettant d'assurer la sécurité et la confidentialité des messages électroniques en identifiant les messages indésirables (spam, ...) et les menaces de sécurité (virus, phishing, ...).

Lots pour l'équipement

- L4 Antivirus/antimalware/EDR/XDR

Logiciel permettant de se protéger contre les virus, malwares et attaques externes, y compris sur base de déviances comportementales (XDR : eXtended Dectection Response)

- L5 : Gestion des mots de passe

Logiciel de gestion sécurisée des comptes et des accès utilisateurs permettant à ces derniers de changer et de récupérer facilement leur mot de passe tout en respectant la politique de sécurité du Pouvoir local.

Dispositions contractuelles

- Centrale d'achats :
  - Restreinte aux PL ayant une déclaration d'intérêt dans le lot
  - Limite 4 M€, tous lots confondus, subside durant la première année
  - Procédure d'adhésion doit être respectée
- Accord cadre pour les lots d'accompagnement :
  - Pluri-attributaires
  - cascade selon résultats CA procédure initiale
  - 1j ouvrable pour répondre à la demande de démarrage selon date souhaitée par le PAB pour débuter la mission

Utilisation de la centrale

Pour pouvoir prétendre au subside Cyber, il est nécessaire que :

- Le demandeur doit avoir au préalable marqué son intérêt à la centrale lors de l'appel à candidature et adhérer formellement à la Centrale.
- La commande doit être effectuée au plus tard pour le 30 juin 2024
- Une copie de la facture doit être transmise à iMio (par le fournisseur) au plus tard pour le 31 août 2024 afin de justifier le subside.
- Le paiement du subside interviendrait en octobre 2024 après approbation du dossier par l'autorité de tutelle.

Utilisation de la centrale

Comment s'assurer de bien bénéficier du subside ?

- Chaque PAB a reçu l'information du subside potentiel octroyé
- Le subside est décompté lors de la réception de la commande via le portail.
- Le PAB est prévenu si le subside est épuisé **AVANT** que la commande ne soit traitée par le prestataire, afin d'éventuellement l'annuler ou modifier l'offre.
- Un formulaire va être mis en ligne pour l'information du subside disponible avant de passer l'acte au collège.

Utilisation de la centrale

Calcul du subside en fonction du nombre d'utilisateurs déclaré dans les marques d'intérêt

Catégorie	Nombre d'utilisateurs	Montant du subside
Cat1	< 50	10.000 €
Cat2	50 à 100	15.000 €
Cat3	100 à 500	25.000 €
Cat4	>500	35.000 €

Utilisation de la centrale

Comment s'assurer de bien bénéficier du subside ?

Montant du subside	1.400.000 €	
Montant réservé via devis	438.000 €	
Reste	962.000 €	

Montant du subside	1.400.000 €	
Montant réservé via commandes	191.371 €	
Reste	**1.218.629 €**	

Questions pratiques (1)

Comment la centrale peut-elle compléter une solution existante déjà acquise par le pouvoir local ?

Toutes les solutions proposées par notre centrale sont standardisées et prévues pour s'insérer dans une solution cloud déjà en place.
Les prestataires doivent s'assurer de la complémentarité de leur offre avec les autres lots du marché.

Questions pratiques (2)

Si le subside est valable pour 2024, qu'en est-il sur des missions planifiées sur les années ultérieures ou des licences pluriannuelles ?

Le marché a une durée de 4 ans. Seule la première année est subsidiée. iMio a démarché le cabinet Collignon pour renouveler le subside pour les autres années

Questions pratiques (3)

Sur quelle durée de disponibilité des produits et services peut-on contractualiser ?

Sur la durée du marché (4 ans).
Sauf disposition particulière du marché subséquent.

Questions pratiques (4)

Comment s'assurer de la compatibilité entre les lots si par exemple des missions d'accompagnement doivent être réalisées en même temps que de l'acquisition de logiciels et/ou matériels ?

Le cahier des charge se base sur les standards reconnus, que ce soit pour l'accompagnement (CCB, ISO 27000, …) ou pour les équipements.

Les critères de sélection et d'attribution sont similaires pour tous les lots

Questions pratiques (5)

Quel est la réactivité prévue en cas de commande urgente ?

Pour les lots d'accompagnement, la réponse à une demande de devis est de 24h par prestataire (cascade)
Pour les lots d'équipement, aucun délai n'est imposé, mais la plateforme en ligne permet la traçabilité des échanges. iMio intervient pour une latence de +de 2 semaines.
Indiquez l'urgence dans la description de la mission !

Questions pratiques (6)

Des missions liées au marché précédent comme les audits, peuvent-elle encore être réalisées dans le cadre de ce marché ?

Oui, via les lots d'accompagnement.

Questions pratiques (7)

Peut-on avoir accès à une documentation plus complète avec listes de prix détaillées avant d'introduire une demande de devis ?

Oui, les offres de services (équipement) et les grilles tarifaires ont été publiées sur
https://www.imio.be/cda/cybersecurite/documents-prestataires-par-lot
(Demander un accès)

Comment introduire une demande

Utiliser le portail pour introduire une demande de devis

https://my.imio.be/cyber/