FOD Beleid & Ondersteuning
SPF Stratégie & Appui

Spending review - Cybersecurity

Groupe de travail : SPF BOSA (DG B&EP et DG S&D), Belnet, Belspo, CCB, SPF Finances, Smals, IBPT, SPF Economie, IF.

1. Executive Summary

Le Conseil des Ministres du 1er avril 2022 a décidé, afin d'améliorer la composition et l'efficacité des dépenses en matière de cybersécurité, d'élargir la spending review 2022 relative à la connectivité par la dimension étroitement liée qu'est la cybersécurité dans les départements fédéraux. La spending review devra être réalisée en collaboration avec le Centre pour la Cybersécurité Belgique (CCB) et la Direction générale Transformation Digitale du SPF Stratégie et Appui. Cette analyse permettra de formuler des options stratégiques et des synergies entre les départements et avec d'autres projets en cours.

Le Conseil des Ministres du 18 octobre 2022 a confirmé la spending review sur la cybersécurité comme sujet pour 2023.

Un groupe de travail mixte a été mis en place pour assurer l'exécution de la spending review.

Le groupe de travail a décidé de se baser sur les travaux déjà existants pour son analyse et notamment :

- La stratégie nationale « Cybersecurity 2.0 » du CCB ;
- La note cadre du CCB « CCB-2023-35 » ;
- Les rapports de Deloitte avec le soutien de la FIA ;
- La lettre aux Présidents du 22 décembre 2022 du Premier Ministre, de la Vice-Première Ministre De Sutter, du Secrétaire d'Etat Mathieu Michel et du CCB, concernant le déploiement de mesures d'hygiène de l'information dans toutes les entités fédérales.

Pour compléter ses informations, le groupe de travail a procédé à une enquête en deux phases :

- Envoi d'un premier questionnaire à l'ensemble des entités fédérales durant l'été 2022 en vue de constituer un inventaire global des dépenses actuelles dans le cadre de la cybersécurité ;
- Suite aux résultats de la première phase et aux difficultés rencontrées pour identifier de manière fiable les dépenses dans les systèmes de rapportage, un deuxième questionnaire a été envoyé à un échantillon représentatif composé de sept organisations fédérales afin d'approfondir l'enquête.

AS IS

Bien qu'il existe une stratégie nationale élaborée par le Centre pour la Cybersécurité Belgique (stratégie « Cybersecurity 2.0 »), l'analyse de la situation AS IS a démontré qu'il n'existe pas actuellement de stratégie fédérale commune en matière de cybersécurité.

En conséquence, des cyberattaques ciblant nos entités fédérales peuvent mettre en danger la sécurité de la population, de l'Etat et l'économie du pays.

L'analyse AS IS montre que des compétences existent et que certaines initiatives et marchés publics ont été développés et déployés par le passé. Il existe actuellement différentes solutions de sécurité offertes par différentes instances sous la forme « Security as a Service (SECaaS) ». Différentes entités ont des connaissances cyber et se protègent et soutiennent d'autres entités.

La première phase d'enquête auprès des entités fédérales concernant leurs dépenses de cybersécurité donne un aperçu des investissements déjà effectués en matière de cybersécurité Cependant, étant donné les difficultés rencontrées pour identifier et consolider de manière fiable les dépenses, certains constats et recommandations peuvent déjà être formulés à ce stade :

- Il est important de définir les notions de cybersécurité et de sécurité de l'information de la même façon au sein de toutes les entités fédérales ;
- Les dépenses de cybersécurité sont difficilement identifiables car il n'est actuellement pas possible de les distinguer des autres dépenses informatiques dans Fedcom. Une piste d'amélioration serait d'utiliser une sémantique commune afin de tenir une comptabilité analytique pertinente pour permettre des analyses approfondies, tout en garantissant le niveau de confidentialité approprié pour ces données ;

La deuxième phase d'enquête sur les dépenses de cybersécurité consistait en un « deep dive » sur sept organisations représentatives, sur base d'un questionnaire quantitatif portant sur 2020-2026 et un questionnaire qualitatif auxquels seules cinq entités sur les sept ont répondu.

TO BE

Tout d'abord, il est essentiel de développer une stratégie commune en matière de cybersécurité pour l'ensemble du fédéral, basée notamment sur la stratégie « Cybersecurity 2.0 » du CCB, la note cadre du CCB « CCB-2023-35 », les rapports de Deloitte avec le soutien de la FIA et les besoins exprimés par les entités questionnées dans l'enquête mentionnée précédemment.

L'objectif d'une stratégie fédérale commune est de pouvoir couvrir tout le spectre de la menace cyber, y compris les menaces futures, tout en maintenant un contrôle sur les dépenses. Pour cela,

il est essentiel de concentrer les efforts sur la protection des fonctions vitales, sur le renforcement des compétences en interne, sur la coopération entre organisations et sur une meilleure efficacité des investissements :

Une stratégie commune proposée en cinq axes d'intervention et huit objectifs stratégiques est proposée:

1. Focus 1 Stratégie : la cybersécurité comme priorité
2. Focus 2 Sécurité : des services publics sécurisés
3. Focus 3 Vigilance : être proactif à l'égard des menaces
4. Focus 4 Vigilance : capacité de réaction et/ou à se remettre face aux événements cyber défavorables
5. Focus 5 : des choix stratégiques et durables

En outre, l'analyse effectuée pour ce spending review montre incontestablement qu'une remise à niveau globale, et donc une augmentation des investissements, est inévitable en matière de cybersécurité si nous voulons couvrir le risque.

Sur base des informations reçues lors de la deuxième phase d'enquête, nous pouvons déduire les tendances d'investissements futurs. La courbe d'évolution sera importante en 2024-2025, entre autres suite à la mise en conformité requise par la directive NIS 2. Les investissements devront également être alignés pour assurer une réponse effective par rapport à l'évolution des menaces.

Les budgets futurs devront tenir compte des nouvelles menaces qui vont apparaitre et influencer notre posture de sécurité. Il s'agit entre autres du développement de l'Intelligence Artificielle (AI), des ordinateurs quantiques et de l'augmentation du nombre de machines de production (environnement connu sous le terme *Operational Technology* (OT) qui vont amener des défis et demander une réaction rapide et appropriée. Ces nouveaux risques devront être suivis, anticipés et provisionnés.

Etant donné qu'une stratégie fédérale commune est fortement recommandée et au vu de toutes les pistes d'optimisation identifiées par le groupe de travail, deux recommandations ont été développées :

1. **<u>La création d'une cellule transversale de sécurité de l'information (incluant le cyber) pour un soutient et coordination de activités de protection.</u>**

Celle-ci collaborera étroitement avec l'Audit Fédéral Interne supervisé par le Comité d'audit de l'administration fédérale.

Là où le CCB soutient au niveau national la protection cyber et contre les impacts des attaques, une nouvelle cellule transversale fédérale de soutien en matière de cybersécurité, accueillie au sein d'une structure existante, permettra la coordination et la coopération des institutions fédérales pour renforcer la protection de l'information. Elle permettra l'application de la stratégie commune et donc de couvrir le spectre de la menace cyber tout en maintenant un contrôle sur les dépenses.

Nous recommandons **que l'évaluation de la maturité cyber soit faite d'une manière régulière par la cellule de soutien (dont la position dans l'organisation fédérale sera à définir), l'entité de contrôle externe (la FIA), supervisée par le Comité d'audit de l'administration fédérale et le CCB.**

2. **Le renforcement des structures actuelles pour répondre à la menace.**

Il s'agit de renforcer les structures existantes. La proposition repose sur une bonne coordination et une utilisation optimale des compétences présentes et/ou à développer dans les organisations ou initiatives existantes (CCB, BOSA, GCloud) qui assistent déjà les institutions fédérales respectives dans l'exécution de leurs tâches.

Quelle que soit l'option choisie, il est recommandé de développer au plus vite le calendrier du renforcement des capacités - internes et externes - de l'organisation qui sera responsable de la coordination pour les entités fédérales et d'aligner suffisamment celui-ci sur le calendrier de mise en œuvre du NIS2.

2. Table of Contents

3. Introduction

3.1. Cadre et objectifs de la spending review

Le Conseil des Ministres du 1er avril 2022 a décidé, « afin d'améliorer la composition et l'efficacité des dépenses en matière de cybersécurité, d'élargir la spending review 2022 relative à la connectivité par la dimension étroitement liée qu'est la cybersécurité dans les départements fédéraux. Il est décidé également de réaliser la spending review en collaboration avec le Centre pour la Cybersécurité Belgique (CCB) et la Direction générale Digitalisation et Simplification du SPF Stratégie et Appui. Cette analyse permettra de formuler des options stratégiques et des synergies entre les départements et avec d'autres projets en cours. »

Le Conseil des Ministres du 18 octobre 2022 a confirmé la spending review sur la cybersécurité comme sujet pour 2023. Le rapport final validé doit être soumis au Conseil des Ministres pour le 30 juin 2023.

Le Comité de Monitoring, qui sert de comité de pilotage pour toutes les spending reviews, est responsable du suivi de l'exécution des spending reviews. Le comité de pilotage a validé la description des tâches pour la spending review Cybersecurity le 24 mars 2023 :

1. Beschrijving van de stand van zaken (AS IS) op het vlak van cybersecurity op federaal niveau:
   - Beschrijving van de voornaamste actoren;
   - Welke is de van toepassing zijnde reglementering en wat is de impact van komende wijzigingen aan de reglementering?
   - Établir un inventaire global des marchés publics actuellement utilisés dans le cadre de la cybersécurité (AS IS), ainsi que les montants totaux engagés pour les différents produits, services et prestations commandés dans ce domaine ;
   - Wat is de stand van zaken op het vlak van de cybersecuritystrategie op federaal niveau?
   - Welke zijn de huidige vormen van samenwerking en een evaluatie van deze samenwerking?

2. Het uitwerken van strategische opties om de efficiëntie en effectiviteit op het vlak van cybersecurity te verhogen, met onder meer:
   - De analyse van een gemeenschappelijke strategie op het vlak van cybersecurity (met een common baseline en specifieke elementen);
   - De impact op de uitgaven (het baseline scenario waarbij iedereen apart blijft werken vs. de te creëren synergiën);

- Wat zijn mogelijke synergiën (met bijkomend de impact op procurement).

Le chapitre 1 reprend le scope de la spending review, une introduction à la cybersécurité, les bases légales, directives, accords et règlementations applicables, les acteurs internes et externes concernés et un aperçu de la cybermenace en Belgique.

Le chapitre 2 dresse l'état actuel de la situation au niveau fédéral (AS IS) du point de vue des budgets, de la stratégie actuelle et des synergies existantes, afin de dégager des besoins communs et des propositions d'amélioration.

Le chapitre 3 élabore une vision stratégique pour accroître l'efficience et l'efficacité de la cybersécurité fédérale sur base des risques de non-conformité réglementaires, des cyber menaces et des contrôles communs à mettre en place.

3.2. Introduction à la cybersécurité

Définition de la cybersécurité[1]

> La cybersécurité est le résultat d'un ensemble de mesures de sécurité qui doivent minimiser le risque engendré par l'utilisation des systèmes d'information et de communication (TIC).

La cybersécurité englobe toutes les mesures destinées à protéger les TIC des citoyens, des entreprises, des organisations et des pouvoirs publics contre les risques engendrés par les cybermenaces.

Il s'agit de la protection des systèmes (tels que le matériel, les logiciels et les infrastructures connexes), des réseaux, ainsi que des données qu'ils contiennent et l'organisation périphérique. Les mesures visant à contrer l'exploitation des TIC, par exemple à des fins de fraude, d'incitation à la violence, ou de recrutement de terroristes, ne relèvent pas du présent rapport.

Cybersécurité versus sécurité de l'information

De manière générale, la sécurité de l'information s'applique aux 3 champs suivants :

- La sécurité logique (cyber)
- La sécurité des informations non-cyber (documents papier)
- Les contrôles administratifs (processus RH etc.)

Le scope de la "Spending Review" porte sur **la cybersécurité**, sans inclure d'autres éléments de la sécurité de l'information comme la sécurisation des documents papier ou des contrôles administratifs (processus RH etc.). Ceci sur base de la demande pour la visibilité sur les coûts de la cybersécurité et le temps attribué à cet exercice.

Nous nous limitons à :

- la sécurité procédurale (audit de sécurité, procédures informatiques…) ;
- la sécurité des systèmes d'exploitation.

[1] https://www.premier.be/sites/default/files/articles/CCB_Strategie%202.0_FR_DP2.pdf

3.3. Bases légales, directives, normes, règlementations et accords de coopération

Différentes règlementations sont d'application pour les entités fédérales. Par exemple, l'arrivée de la Directive NIS 2 (d'application sur toutes les entités fédérales) entraine une obligation du renforcement de la protection cyber sur base de normes minimales de sécurité.

Les principales bases légales et autres à considérer au niveau fédéral sont résumées ci-dessous.

NIS (2016) vs NIS Gov / NIS 2 (2022)[2]

La "Directive Network and Information Systems (Security)" NIS (-1) (Directive (EU) 2016/1148), actuelle est entrée en vigueur en 2016. Il s'agissait du premier texte législatif en matière de cybersécurité au niveau de l'UE. Le texte a ensuite été transposé dans le droit national belge par le biais de la loi NIS du 7 avril 2019. Tant qu'il n'y a pas de nouvelle loi belge NIS-2, toutes les obligations découlant de la directive NIS-1 restent en vigueur.

Suite aux nouvelles obligations découlant de NIS 2, les entités essentielles et importantes doivent prendre les mesures appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

Ces mesures sont fondées sur une approche « tous risques » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents.

Elles comprennent au moins:

- les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;
- la gestion des incidents ;
- la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;
- la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;

[2] https://ccb.belgium.be/fr/la-directive-nis2-que-cela-signifie-il-pour-mon-organisation

- la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;
- des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
- les pratiques de base en matière de cyber-hygiène et la formation à la cybersécurité;
- des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;
- la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;
- l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

Afin de sensibiliser le top management, les personnes physiques qui représentent des entités essentielles et importantes pourront être tenues responsables du non-respect des obligations de la directive.

Cyber Security Act (2019)[3]

Le "Cyber Security Act" établit le premier cadre de certification de la cybersécurité à l'échelle de l'UE afin de garantir une approche commune de la certification de la cybersécurité dans le marché unique européen et, à terme, d'améliorer la cybersécurité d'un large éventail de produits numériques (par exemple, l'internet des objets) et de services.

La directive sur la sécurité des réseaux et des systèmes d'information établit l'ENISA en tant que secrétariat des réseaux nationaux, des équipes nationales d'intervention en cas d'incidents de sécurité informatique (CSIRT). En Belgique ces taches sont assurées par le CCB.

Cyber Resilience Act (en cours)[4]

La proposition de règlement (discuté au sein du groupe de travail horizontal sur les questions cybernétiques le 26 avril 2023) relatif aux exigences de cybersécurité applicables aux produits comportant des éléments numériques, connue sous le nom de "règlement sur la cyber-résilience", renforce les règles en matière de cybersécurité afin de garantir une plus grande sécurité des produits matériels et logiciels.

[3] https://digital-strategy.ec.europa.eu/fr/policies/cybersecurity-act
[4] https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act

RGPD (2016)

Le règlement général sur la protection des données (2016/679, "GDPR") est un règlement du droit de l'UE sur la protection des données et de la vie privée dans l'UE et l'Espace économique européen (EEE). Le GDPR est une composante importante du droit de l'UE en matière de protection de la vie privée et du droit relatif aux droits de l'homme, en particulier l'article 8(1) de la Charte des droits fondamentaux de l'Union européenne.

European Electronic Communications Code – EECC[5]

La directive EECC a pour but de promouvoir les intérêts des citoyens de l'UE en offrant un maximum d'avantages en termes de choix, de prix et de qualité grâce à une concurrence efficace en maintenant la sécurité des réseaux et des services en assurant la protection des consommateurs par des règles spécifiques et en répondant aux besoins de groupes sociaux spécifiques, notamment les personnes handicapées, les personnes âgées et les personnes ayant des besoins sociaux particuliers.

Stratégie cybersécurité 2.0 (CNS du 20 mai 2021)[6]

Le 20 mai 2021, le Conseil National de Sécurité (CNS) a validé les détails de la stratégie de « Cybersecurity 2.0 » développée et proposée par le Centre pour la Cybersécurité Belgique (CCB). Cette stratégie cadre l'approche transversale de la Belgique en termes de cybermenace et d'opportunités pour notre pays. Elle doit propulser la Belgique au rang des pays les moins vulnérables d'Europe.

Ce plan s'articule autour de six objectifs précis :

1. Renforcer l'environnement numérique et accroître la confiance dans l'environnement numérique ;
2. Armer les utilisateurs et les administrateurs d'ordinateurs et de réseaux ;
3. Protéger les Organisations d'Intérêt Vital contre toutes les cybermenaces ;
4. Répondre à la cybermenace ;
5. Améliorer les collaborations publiques, privées et universitaires ;
6. Affirmer un engagement international clair.

[5] https://eur-lex.europa.eu/eli/dir/2018/1972/oj
[6] https://www.premier.be/sites/default/files/articles/CCB_Strategie%202.0_FR_DP2.pdf

Stratégie nationale de protection des infrastructures critiques (CES)

Cette stratégie définit la notion d'infrastructures critiques et détermine les secteurs et parties de secteurs considérés comme critiques en Belgique. Elle contient des mesures visant à améliorer la résilience de la Belgique sur le plan des infrastructures critiques.

eIDAS[7]

eIDAS est le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur (règlement eIDAS). Le règlement eIDAS aide les entreprises, les citoyens et les autorités publiques à réaliser des interactions électroniques sûres et transparentes.

NATO Cyber Defense Pledge[8]

En 2016, les membres de l'OTAN ont adopté un "Engagement en matière de cyberdéfense" qui décrit la manière dont les armées membres se préparent à faire face aux menaces futures.

ISO/IEC - NBN

ISO/IEC 27001 est la norme internationale pour la cybersécurité et permet de mieux maîtriser les risques cyber.

3.4. Stakeholders

Les acteurs externes les plus influents pour la cybersécurité au fédéral sont listés ci-dessous.

ENISA[9]

L'ENISA a été fondée par le règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information. ENISA supporte avec des conseils, de la documentation et procédures le renforcement de la cybersécurité des états membres.

[7] https://digital-strategy.ec.europa.eu/fr/policies/eidas-regulation
[8] https://www.nato.int/cps/en/natohq/official_texts_133177.htm
[9] ENISA (europa.eu)

Cyber Security Coalition

La Cyber Security Coalition est un partenariat entre des acteurs du monde universitaire, des autorités publiques et du secteur privé qui s'unissent dans la lutte contre la cybercriminalité[10].

OTAN[11]

Le mandat défensif de l'OTAN a été réaffirmé pour dissuader activement les cybermenaces, s'en défendre et les contrer à tout moment.

Les Alliés ont reconnu que l'impact d'activités cybernétiques cumulatives malveillantes importantes pouvait, dans certaines circonstances, être considéré comme une attaque armée. La nature du cyberespace exige une approche globale grâce à une unité d'action aux niveaux politique, militaire et technique.

3.5. La cybermenace contre la Belgique en 2023

Comme mentionné précédemment, la vision stratégique nationale, reprise dans le rapport du Centre pour la Cybersécurité Belgique (CCB) « Cybersecurity 2.0 – 2021-2025 » définit l'orientation stratégique fondamentale de la politique de sécurité de la Belgique. Dans ce but, le rapport dresse l'état des lieux de la cybermenace en Belgique et décrit les différents types de cybermenaces auxquels la Belgique est confrontée.

Le rapport souligne l'importance élevée et croissante des cybermenaces pour la politique de sécurité et leur évolution très dynamique. Tout porte à croire que les menaces vont s'intensifier encore davantage à l'avenir.

D'une manière générale, la transformation digitale augmente la surface d'attaque, l'intérêt des attaques et donc le risque. Les données échangées sont de plus en plus riches en valeurs ajoutées. Les machines sont de plus en plus puissantes et diversifiées et permettent des accès aux données par différents canaux (par exemple : 5G, IoT).

[10] Cyber Security Coalition | Cyber Security Coalition
[11] NATO - Cyberdéfense

Cette dépendance digitale de plus en plus forte augmente d'une manière exponentielle la pression et le besoin de sécuriser les flux et les infrastructures digitaux, ainsi que les logiciels métiers (business) utilisant ces mêmes données digitales.

Il reste néanmoins important de différencier les menaces dues à des actes illicites délibérés (cyberattaques) et les dangers dus à des événements provoqués de façon non intentionnelle (erreurs humaines et pannes techniques).

Cyberattaques

On a observé ces dernières années une forte augmentation des menaces dues aux cyberattaques. En Belgique et à l'étranger, des attaques réussies, aux conséquences parfois graves, ont montré que non seulement la fréquence et la complexité des cyberattaques augmentaient, mais encore que celles-ci étaient de plus en plus dirigées contre des États ou des entreprises.

Il est possible de distinguer cinq types de cyberattaques, étant entendu que celles-ci sont souvent combinées et présentent également des chevauchements :

- Cyber espionnage ;
- Cybercriminalité ;
- Cybersabotage et cyberterrorisme ;
- Désinformation et propagande ;
- Cyber conflits.

Erreurs humaines et défaillances techniques

Outre les cyberattaques ciblées et délibérées, il est également possible que des actes involontaires ou des événements liés aux conditions naturelles et techniques provoquent des dégâts touchant le cyberespace ou l'environnement physique. Ceux-ci sont dus à des erreurs humaines dans la préparation et l'utilisation de l'informatique (p. ex. utilisation inappropriée ou négligente des systèmes informatiques, mauvaises administration ou configuration, perte de supports de données, etc.) ou à des défaillances techniques dont les causes peuvent être multiples (par ex. vieillissement des infrastructures, phénomènes naturels, surcharge, défaut de conception ou entretien insuffisant).

Les cyber risques dus aux erreurs humaines ou aux défaillances techniques resteront très importants. En outre, la complexité croissante due à la mise en réseau des domaines les plus divers

permet mal d'apprécier et de délimiter les conséquences de ces événements involontaires. Une bonne préparation et une planification soigneuse vis-à-vis de tels incidents restent donc des éléments centraux de la gestion des cyber risques.

En plus des cyberattaques, le risque lié aux erreurs humaines et défaillances techniques devra être adressé également dans les campagnes de conscientisation liés à la cybersecurité.

4. Situation AS IS

Suite à la décision du Conseil des Ministres du 01/04/2022, un kick-off meeting a eu lieu avec les membres du g-Cloud COPB (Cloud Operations & Programme Board) le 21 juin 2022. Une équipe projet a été constituée avec Belnet et BOSA (DG S&D).

Durant le mois de juillet 2022, l'équipe projet BOSA-Belnet a proposé une 1ère phase exploratoire avec une approche globale en contactant l'ensemble des membres du groupe fédéral SIT, composé des responsables ICT des SPF, IPSS et OIP.

Cette approche visait à constituer un inventaire global des marchés publics actuellement utilisés dans le cadre de la cybersécurité (AS IS), ainsi que les montants totaux engagés pour les différents produits, services et prestations commandés dans ce domaine, via un questionnaire structuré sur une méthodologie de défense par couche en cybersécurité, reconnue mondialement, appelé Defense-in-Depth (DiD).

Ensuite il était prévu, dans un second temps, d'étendre l'analyse en permettant l'identification des futurs besoins (TO BE) en matière de cybersécurité par une approche d'analyse globale des risques, en regroupant et en consolidant, un top10 des cyber-risques et un top10 des risques de non-conformité liés aux obligations légales en matière de cybersécurité.

Pour cette deuxième phase « deep dive », un questionnaire en deux volets a été envoyé le 20 mars 2023 aux sept organisations sélectionnées :

- Un questionnaire en Excel concernant les dépenses réalisées et estimées pour la cybersécurité depuis 2020 jusque 2026, en engagement et en liquidation, ventilées en personnel, fonctionnement et investissement ; un questionnaire de maturité Yes/No a également été transmis à la demande du CCB sur base du Cyber Fundamental Framework développé par le CCB comme modèle de référence possible en vue du NIS 2;
- Un document Word avec des questions ouvertes concernant l'organisation et la maturité, les synergies existantes et possibles, les solutions cyber utilisées, les best practices à partager, les règlements à respecter, les besoins futurs, etc.

Des réunions ont ensuite été organisées séparément avec chacune des organisations pour affiner les réponses aux questionnaires et développer les chapitres AS IS et TO BE du présent rapport.

4.1. Budgets actuels

Résultats de la première phase d'enquête

Comme expliqué précédemment, un premier questionnaire avait été envoyé pendant l'été 2022 afin d'avoir une vue sur les dépenses de cybersécurité au niveau fédéral.

Cependant, les résultats obtenus suite aux réponses reçues sont très différents des chiffres présents dans FEDCOM, étant donné :

- Fedcom is het boekhoudprogramma van de FOD'S en de POD's, met inbegrip van de Federale Politie en Defensie. De cijfers van de andere federale instellingen (OISZ, ION, wetenschappelijke instellingen, bijzondere corpsen) ontbreken.
- L'interprétation divergente de la notion de cybersécurité et de la sécurité de l'information par les différentes organisations publiques fédérales ;
- L'absence de libellé spécifique (centre de coût) pour les dépenses CyberSécurité dans Fedcom. Alle IT-uitgaven (GL 610895,GL 615* voor de werkingskosten ; GL 202* en GL 24301* voor de investeringen) zijn dan ook lijn per lijn geanalyseerd en de uitgaven die verband houden met cybersecurity, geïnventariseerd.
- De resultaten van Fedcom betreffen enkel het eerste semester van 2022.

Résultats de la deuxième phase d'enquête (« deep dive »)

Comme expliqué, la deuxième phase d'enquête consistait en un « deep dive » auprès de sept entités sélectionnées en vue d'un échantillon représentatif. Cependant, seules cinq entités sur les sept ont répondu aux questionnaires envoyés.

4.2. Stratégie fédérale actuelle

L'existence de politiques différentes en matière de cybersécurité au sein des différentes entités fédérales a pour effet une gestion peu cohérente des cybers risques au niveau fédéral global. Soulignons que le niveau de protection à atteindre doit être aussi lié à l'activité de l'organisation

4.3. État de la protection des entités fédérales contre les cyber-risques

Rapport de Deloitte suite aux audits par la FIA (Audit 2019-2022)

Ces dernières années la FIA, en coopération avec Deloitte a effectué des audits sur les outils et organisations de cybersécurité dans différentes entités fédérales. Ces résultats ont été partagés durant un workshop le 19 avril 2023.

Prise en compte de tous les éléments de la sécurité de l'information

Sans tenir compte de l'entièreté des vulnérabilités à notre système de sécurité de l'information, une protection efficace ne sera pas possible. Au-delà de la spending review actuel, ceci devrait couvrir les trois éléments de la sécurité de l'information :

- Information contenue dans les systèmes d'informations (cyber protection) ;
  - Gestion des informations non-digitales (qui produit quoi, comment sont stockés les documents, cycles de vie etc.) ;
  - Organisation interne (par exemple : cycles RH des Joiner-Mover-Leaver sous contrôle).

4.4. Conclusion du AS IS

Constats et recommandations suite à la première enquête sur les dépenses actuelles en matière de cybersécurité au niveau fédéral

Suite à la première enquête visant à répertorier les dépenses fédérales en matière de cybersécurité, des recommandations peuvent déjà être formulées, étant donné les difficultés rencontrées pour identifier et consolider de manière fiable les dépenses de cybersécurité.

1. **Interprétation divergente de la notion de cybersécurité et de la sécurité de l'information par les différentes organisations publiques fédérales.**

Exemple : La sécurité physique est un élément important pour la sécurité de l'information, mais peut-être considéré comme une dépense intrinsèque à la Régie des Bâtiments. Par exemple, les cartes d'accès au bâtiment, les caméras ne sont pas toujours considérées comme faisant partie de la sécurité alors qu'il s'agit d'un élément essentiel de la protection physique.

2. **Difficulté pour identifier les dépenses CyberSécurité dans Fedcom**

L'état des lieux des dépenses relatives à la cybersécurité (et à la sécurité de l'information) est difficile car il n'est actuellement pas facile de les distinguer des autres dépenses ICT dans Fedcom.

Pour cette première phase d'enquête AS-IS, +- 18.000 lignes de dépenses pour le 1er semestre 2022 ont été analysées et catégorisées. Le contenu de ces dépenses est sujet à une interprétation très diverse selon le contexte et les organisations, notamment pour la partie ressources humaines. Il est difficile d'interpréter si un project manager travaille dans un contexte de projet de cybersécurité, idem pour les analyses et architectes de système d'information.

Une solution possible pour remédier à ce problème serait la mise en place d'une sémantique commune afin de facilité des analyses et rapportage dans la comptabilité analytique, en veillant à garantir le niveau approprié de confidentialité pour ces données.

Constats et recommandations suite à l'enquête « deep dive »

Vu le delta entre l'existant et nos besoins, un investissement sérieux est nécessaire. NIS 2 entrainera des normes minimales de protection, qui ne sont pas encore implémentées dans la plupart des entités.

Cet important investissement peut être atténué en partie et contrôlé par des mesures d'efficacité, comme une augmentation de connaissance interne, plus de coopération interdépartementale, une coordination des réponses et uniformisation des processus et outils. Ces mesures seront développées dans la partie TO BE.

Sans contrôle des investissements pour adresser le risque et sans contrôle des coûts des solutions et services actuels, les dépenses peuvent varier entre très faibles (ne couvrant pas le risque) et très importante avec des effets significatifs sur les budgets.

Conclusion stratégie AS IS

Avec sa structure étatique complexe, il est difficile en Belgique d'assurer la coordination d'une politique de cybersécurité pour les services publics. Les autorités fédérales disposent de services publics fédéraux horizontaux, verticaux et de programmation. Les régions et les communautés se déclinent en ministères et en directions. Le Centre pour la Cybersécurité Belgique (CCB) élabore des conseils et des directives qui sont à la disposition de tous les services publics.
La sécurité et la cybersécurité en particulier relèvent de la compétence fédérale et sont traitées au niveau national.
STRATÉGIE CYBERSECURITÉ BELGIQUE 2.0 – 2021-2025

Cette observation de la CCB se reflète dans la diversité en maturité au niveau de l'organisation fédérale actuelle dans sa réponse à la cybermenace.

Les risques que doivent gérer les différentes entités fédérales sont aussi divers que les missions qui leur sont attribués. Les attaques « cyber » se concentrent sur les points faibles de l'infrastructure transversale dans son ensemble et certaines applications spécifiques.

Toutes les entités font partie soit comme point final, soit comme partie d'une chaine d'information. Bien que certaines entités aient plus investi en cybersécurité, elles opèrent dans un paysage de maturités variées..

Au niveau de la formation des collaborateurs, les différentes entités ont des approches très différentes. La maturité des formations est diverse avec des programmes existants et suivis chez les uns, et non-existants chez les autres.

Une vision « risque » comme base :

Le mot « risque » est souvent utilisé, mais pas l'identification d'avoir une approche ou une méthodologie des risques cyber à communiquer / proposer / infuser aux organisations.

On met en avant le besoin d'une approche commune pour la cybersécurité, mais se limite souvent uniquement à l'implémentation des mesures de protection, et pas à une analyse de risques préalable. Sans ça, on ne peut garantir une gestion et priorisation efficace des risques à traiter, ni une bonne gestion des coûts que cela entraine.

L'investissement au niveau fédéral en un outil permettant aux organisations d'implémenter une gestion de risques (par exemple en accord avec ISO 27005 :2022 ou les Cyberfundamentals de CCB), serait fortement recommandé.

5. Options TO BE

5.1. Vision stratégique

Pour renforcer la cybersécurité dans les entités fédérales, nous proposons une stratégie basée sur plusieurs éléments fournis par le plan stratégique national « Cybersecurity 2.0 » élaboré par le CCB, la note cadre du CCB CCB-2023-35, les recommandations par Deloitte et la FIA et les besoins exprimés par les différentes entités questionnées.

VISION

La Belgique plaide en faveur d'un cyberespace ouvert, libre et sûr qui permette à nos citoyens et entreprises de s'épanouir pleinement et de s'engager sur la scène internationale, et qui sauvegarde et protège les droits fondamentaux. Afin de construire et d'assurer la confiance essentielle de la société dans le cyberespace, la cybersécurité joue un rôle inévitable et décisif. Il s'agit là d'une responsabilité partagée par tous les acteurs, qui exige une approche globale et donc une stratégie commune au niveau fédéral.

MISSION

La Stratégie Cybersécurité que nous proposons au niveau fédéral soutient l'ambition de faire de la Belgique l'un des pays les moins vulnérables d'Europe dans le domaine de la cybersécurité à l'horizon 2025. Elle s'articule autour de plans d'action destinés à protéger toutes les entités fédérales, en déployant les moyens nécessaires à la tâche, combiné avec une organisation inclusive, une approche transversale (ensemble), verticale qui tient compte des singularités des métiers (exemple IBZ) et pertinente.

Du fait que les cyber risques touchent simultanément divers domaines des entités fédérales, des mesures doivent être prises dans ces différents domaines. Pour que la stratégie reste cohérente malgré sa diversité, il est décisif de poursuivre une vision commune et de formuler des objectifs stratégiques supérieurs et mettre en place une coordination sur base de la vision stratégique nationale.

OBJECTIF

L'objectif du présent rapport est de développer, à la demande des autorités politiques, des options stratégiques et des synergies au niveau fédéral pour améliorer la composition et l'efficacité des dépenses en matière de cybersécurité.

Responsabilité de la cyberprotection

Dans la note cadre CCB-2023-035, le CCB fait plusieurs remarques :

Chaque entité fédérale est responsable de la mise en œuvre d'un niveau approprié de cybersécurité et du respect des normes de sécurité pertinentes au sein de son administration.

Le conseiller en sécurité de l'information (ou équivalent) de chaque service du gouvernement fédéral fait rapport au moins une fois par trimestre au Comité exécutif (ou équivalent) sur l'état de la cybersécurité de l'organisation.

Ce faisant rend compte au moins des principaux incidents de sécurité, des principales vulnérabilités, de la conformité à la norme de sécurité minimale et des domaines proposés.

Ce rapport est immédiatement suivi d'une décision formelle concernant les points d'amélioration proposés.

Gouvernance de la cybersécurité (note cadre CCB-2023-035)

Dans la note cadre CCB-2023-035, le CCB propose un suivi au fédérale par diverse entités :

En tant qu'autorité nationale de cybersécurité, le CCB administre la stratégie nationale de cybersécurité et approuve la politique générale de protection du public, des entreprises, des organisations d'importance vitale (telles que les infrastructures critiques) et du gouvernement. Le CCB élabore et tient à jour la norme minimale de cybersécurité (Cyber Fundamentals) pour la Belgique et met en place un système de certification pour cette norme. En tant que national Cyber Security Incident Response Team (CSIRT),

La réglementation NIS2 impose au gouvernement fédéral d'améliorer sa maturité cyber.

Pour ce faire, le CCB propose d'utiliser le cadre des cyberfondamentaux (https://ccb.belgium.be/en/cyberfundamentals-framework) pour tous les départements du gouvernement fédéral. Cela permettra de déterminer la maturité cybernétique cible de chaque organisation et de planifier sa réalisation et son suivi.

5.2. Couvrir tout le spectre de la menace Cyber

L'objectif d'une stratégie fédérale commune est de pouvoir couvrir tout le spectre de la menace cyber, tout en maintenant un contrôle sur les dépenses.

Pour cela, il nous semble essentiel de nous concentrer sur la protection des fonctions vitales, sur le renforcement des compétences en interne, sur la coopération entre organisations et sur une meilleure efficacité des investissements.

Protection robuste des fonctions vitales

La question clé à poser à tous les responsables des entités fédérales est :
« Comment fonctionneriez-vous sans service IT (pas 2h, mais 2 semaines, 2 mois) ? »

Renforcement des compétences en interne et du soutien du haut management

La cybersécurité et la sécurité de l'information doivent être engagées et soutenues par la haute direction, et les compétences internes doivent être renforcées. Cela s'applique à une vue d'ensemble des actifs, des vulnérabilités et de la connaissance des menaces potentielles. Une cellule fédérale de soutien dédiée à la coordination transversale fédérale et installée au sein d'une organisation fédérale existante permettrait de soutenir les présidents des entités dans le renforcement des protections des différentes entités.

Le renforcement de la connaissance interne, grâce à des recrutements et formations spécifiques évitera une dépendance trop importante aux instances externes. Les partenaires externes calculent le coût du support dans des cycles d'optimisation interne, risquant potentiellement une pression sur un service optimal.

Ce risque potentiel peut être couvert (ce qui existe déjà dans des programmes SECaaS) par :

- le maintien des connaissances cyber internes aux entités fédérales
- des SLA et KPI bien définis

- par des relations de partenariat avec les parties externes, plus qu'uniquement fournisseur/client.

Il est essentiel de coopérer en partenariat avec les fournisseurs de solutions de type « SECaaS » mais également de bien suivre les services rendus, et de proposer des adaptations pour répondre aux besoins des différentes missions des entités.

Renforcement de la coopération entre les entités fédérales

Les organismes fédéraux doivent coopérer plus étroitement et partager leurs connaissances et leurs expériences sur les menaces et les incidents. En pratique, différentes entités ont des grandes maturités et des compétences qui peuvent être partagées avec d'autre entités, voire de manière transversale dans toutes les entités fédérales.

Une meilleure diffusion des solutions existantes doit être soutenue. Ceci sur les solutions existantes mais également sur la gestion des informations au niveau des menaces.

Afin d'augmenter et de renforcer rapidement l'expertise interne - conformément au calendrier imposé par le NIS2 - et parce que la cybersécurité ne fait pas partie des fonctions principales de nombreuses administrations publiques, la CCB propose de s'appuyer sur un fournisseur compétent de services de sécurité (SecaaS).

Augmenter l'efficacité des investissements

L'analyse AS IS a montré qu'il existe déjà des solutions de sécurité développées par des organisations. La mise en commun de ces solutions, organisations et architectures existantes permettrait de mutualiser les investissements et d'en maximiser l'efficacité. La protection des organisations fédérales contre les attaques cyber dans son ensemble s'en trouverait renforcée.

Besoins en investissements structurels

Des importants investissements ont été fait dans le passé mais ceux-ci ne couvrent pas l'ensemble des risques, qui sont en constante augmentation. En effet, les investissements sont souvent effectués sur base d'un coût calculé par utilisateur mais sans prendre en compte le risque. Il existe dès lors un écart entre les investissements et les besoins de couverture des risques.

5.3. Axes d'intervention et objectifs stratégiques

La stratégie fédérale commune proposée en matière de cybersécurité peut se décliner en cinq axes d'intervention (focus) et en huit objectifs stratégiques.

FOCUS 1 STRATEGIE : LA SECURITE DE L'INFORMATION COMME PRIORITÉ

Pour les entités fédérales, la cybersécurité constitue un objectif stratégique en soutien à la réalisation de la mission de l'État et de ses cibles de transformation numérique. Elle repose sur un engagements et des moyens mis à disposition des plus hautes autorités du fédéral (par exemple au niveau des collèges des présidents et administrateurs généraux), l'instauration d'une gouvernance forte et intégrée de la cybersécurité et l'amélioration des comportements sécuritaires du personnel de ces entités.

FOCUS 2 SECURITE : DES SERVICES PUBLICS SÉCURISES

L'apparition de nouveaux risques de cybersécurité et à notre cyberspace représente un risque d'importance. La protection de l'information et la résilience des services publics sont de plus en plus actuels ; ceux-ci doivent être identifiés, traités et leurs impacts potentiels réduits à un niveau acceptable.

Pour adresser les risques de manière transversale nous devons stimuler la collaboration des entités fédérales dans l'implantation de moyens technologiques innovants pour la protection adéquate de l'information, en demeurant responsable à chacune des étapes du cycle de vie de celle-ci. Il en est de même pour la protection des échanges et des communications entre les entités fédérales et avec les partenaires.

FOCUS 3 VIGILANCE : ÊTRE PROACTIF A L'EGARD DES MENACES

La forme sans cesse renouvelée des cybermenaces constitue un enjeu de taille pour les entités fédérales.

La protection à l'égard des cybermenaces émergentes, souvent inconnues, est de plus en plus complexe. Devant celles-ci, les entités fédérales doivent augmenter les capacités institutionnelles

d'analyse des risques émergents et de prospective et mettre en place les mesures préventives appropriées de protection et de renforcement de la résilience de ses systèmes.

FOCUS 4 VIGILANCE : CAPACITE DE REACTION ET/OU A SE REMETTRE FACE AUX EVENEMENTS CYBER DEFAVORABLES

Pour réussir la sécurité des entités fédérales, il est nécessaire d'avoir une main d'œuvre hautement qualifiée en cybersécurité. Cette expertise doit évoluer en continu, au rythme des changements technologiques.

Nous pouvons compter sur l'expertise des partenaires fédéraux, des partenaires du secteur privé et du monde académique.

FOCUS 5 : DES CHOIX STRATEGIQUES ET DURABLES

Comme mentionné précédemment, pour couvrir les différents risques de manière transversale, nous suggérons de suivre une approche intégrale

5.4. Optimisation des ressources

L'analyse effectuée pour cette spending review montre incontestablement qu'une remise à niveau globale, et donc une augmentation des investissements, est inévitable en matière de cybersécurité si nous voulons couvrir le risque,

Cependant, une stratégie fédérale globale telle que nous le préconisons permettrait d'optimiser les ressources et de maximiser l'efficacité des investissements.

Nous avons identifié plusieurs pistes qui permettrait de garder un contrôle sur la croissance exponentielle des dépenses à politique inchangée.

Implémentation transversale NIS 2 pour les entités fédérales

Avec la venue de NIS 2, les entités fédérales actuellement non conformes doivent se mettre en conformité et restructurer leur posture de sécurité. Cette mise en conformité sera basée sur un « Framework » validé et reconnu par les autorités d'inspection.

Actuellement il existe plusieurs normes :

- La plus connue et utilisée est la norme ISO 27001 ;
- Le CCB a élaboré le cadre Cyber Fundamentals qui peut servir en premier lieu comme référence aux niveaux de maturité minimales à atteindre pour les entités fédérales. Une fois validé et reconnu, il pourra servir de guide pour la mise en conformité avec la législation.

Au niveau fédéral l'impact sera contrôlé par une approche commune et coordonnée. Pour faire face aux responsabilités des différentes entités sur leur cybersécurité, il est recommandé de créer une cellule de soutien avec les compétences cyber.

Protection des toutes les entités avec une stratégie centralisée

Pour protéger toutes les entités fédérales, tout en gérant les coûts, nous pouvons faire appel à des protections comme les solutions de type SECaaS. Certaines entités fédérales ont une expertise CISO, mais une grande partie n'ont pas ces connaissances en interne.

Nous recommandons de maintenir les structures actuelles dans lesquelles les CISO couvrent les risques inhérents à leurs entités, mais reçoivent un soutien centralisé. La diversité des objectifs et missions des entités fédérales, rendent une structure de CISO unique peu souhaitable. Une coordination centrale reste essentielle.

Les entités sans CISO pourraient faire appel aux compétences centralisées. La coordination centrale soutiendrait toutes les entités dans le déploiement des normes minimales liées au NIS 2 et dans le suivi d'évolutions futures.

Coopération trans-nationale

Une coopération et échanges d'information avec des partenaires fédéraux et des secteurs privés et académiques dans d'autre pays ayant les mêmes intérêts, peuvent apporter des idées sur une amélioration de notre organisation et des techniques et réduction de nos coûts de notre protection.

5.5. Se préparer à un environnement changeant.

Environnement législatif et gouvernance

Les menaces appellent à une approche plus coordonnée, mais l'environnement est également impacté par un environnement législatif changeant.

Comme déjà mentionné, la menace cyber est constamment en évolution et il est certain que cette évolution va encore s'accélérer dans les années à venir. Puisque les menaces changent de jour en jour, de manière prévisible ou imprévisible, il est primordial d'être agile face à celles-ci et de garder une marge de manœuvre dans notre capacité à répondre.

Facteurs technologiques

Cloud

La gestion de la cybersécurité dans un environnement virtuel continue á se développer ce qui engendre des nécessités d'investissements futurs qui ne sont pas actuellement chiffrables.

Intelligence Artificielle (A.I.)

L'intelligence artificielle est elle-même une technologie. En tant que telle, elle représente donc aussi une cible potentielle pour les cyberattaques. Et par rapport aux logiciels et aux appareils traditionnels, ses systèmes sont attaqués de manière non-traditionnelle. Les menaces qui pèsent sur les systèmes d'IA sont d'un tout autre niveau.

Quantum

Si l'ordinateur quantique n'est pas encore accessible sur le marché, les recherches sur le quantique et le post-quantique sont toujours en cours. Bien que la cryptographie post-quantique semble être nécessaire pour garantir une sécurité, il reste évident que les hackers tenteront de contourner ces systèmes.

Ces évolutions futures demanderont des efforts organisationnels, financiers et des compétences nouvelles. L'impact n'est pas encore mesurable, mais nous devons déjà en tenir compte.

5.6. Impact financier

Sur base des informations reçues lors de la deuxième phase d'enquête, nous pouvons déduire les tendances d'investissements futurs. La courbe d'évolution sera importante en 2024-2025, entre autres suite à la mise en conformité requise par la directive NIS 2.

5.7. Recommandations

Remarque

Suite aux discussions du groupe de travail, deux recommandations ont été proposées.

Recommandation 1 : Création d'une cellule transversale fédérale de coordination et soutien

Dans les précédents chapitres, nous avons vu qu'une stratégie fédérale commune est fortement recommandée dans la mesure où elle permettrait de couvrir entièrement le spectre de la menace cyber tout en maintenant un contrôle sur les dépenses. C'est pourquoi, nous recommandons logiquement la création d'une **cellule transversale fédérale de coordination et de soutien** de cybersécurité pour l 'application de cette stratégie fédérale commune :

- Vision commune cohérente pour toutes les entités fédérales ;
- Application transversale cohérente de cette vision commune des entités fédérales ;
- Meilleure coopération globale fédérale ;
- Réduction de la surface d'attaque globale et réponse aux vulnérabilités des entités fédérales ;
- Couverture globale de la menace ;
- Protection de l'ensemble des fonctions essentielles ;
- Application commune de la règlementation NIS 2 ;
- Gestion transversale de l'organisation interne (comme le cycle joiner-mover-leaver) ;
- Optimisation et renforcement des compétences interne ;
- Prévention et cyberhygiène communes;
- Coopération avec des partenaires stratégiques (gouvernement, CCB, Belnet, Collège des Présidents…) ;
- Veille législative et technologique et anticipation des nouveaux risques et menaces ;

- Optimisation des ressources et contrôle des coûts ;
- Echanges et coopération au niveau transnational.
- Méthodologie & plateforme de gestion des risques.
- Aide/support à opérationnaliser les mesures de sécurités à mettre en œuvre en matière de cybersécurité pour les organisations du fédéral qui n'ont pas les ressources suffisantes pour le faire.

Cette **cellule transversale fédérale de soutien** collaborerait (selon la position qu'elle aura au sein d'une organisation fédérale qui est à définir) avec le CCB et le FIA, et se focaliserait sur les objectifs de cette analyse tout en assurant un rôle significatif dans l'implémentation du cadre NIS2. Pour mieux le comprendre, nous proposons l'analogie suivante avec la gestion des incendies.

Analogie avec les risques incendie :

Là où la CCB a une fonction de pompier, de compétence des risques et centrale d'alarme, la cellule transversale fédérale se concentrera à soutenir les protections avec :

La prévention en identifiant les risques de feu
L'identification des vulnérabilités au feu de nos actifs
La détermination des protections avec la valeur des actifs,
L'augmentation de la connaissance interne des risques
Les actions à prendre en cas d'incendie
Les manières d'alerter les services internes et les pompiers
L'identification des meilleurs détecteurs incendie,
L'implémentation des recommandations et des bonnes pratiques (sur base du CCB) en matière de portes pare-feu
La signalisation des issues de secours,
L'installation des moyens de combattre le feu (extincteurs etc.),
La mise en place des systèmes d'alertes
La mise en place de systèmes de continuité des activités en cas de feu
L'organisation de tests de réactivité
Les activités d'inspection relatives à l'implémentation des mesures de sécurité

Tout ceci n'existe pas au niveau transversal des entités fédérales

Recommandation 2 : Contribution des IPSS

Comme l'ensemble des organisations fédérales et repris dans la première recommandation, les institutions publiques de sécurité sociale (IPSS) considèrent qu'il est important que la future organisation garantisse une approche efficace et efficiente de la cybersécurité. L'objectif doit être solidement atteint à un coût raisonnable, avec une valorisation et un déploiement maximaux des compétences existantes et à développer, mais sans fragmentation supplémentaire. Après tout, la cybersécurité exige une approche holistique.

C'est pourquoi l'IPSS formule la proposition d'organisation suivante.

Principes généraux

Les propositions formulées s'appuient sur les points suivants :

1. L'organisation de la sécurité de l'information doit être appropriée et proportionnelle aux cybermenaces et vulnérabilités des institutions ou groupes d'institutions au sein d'un même secteur.
2. L'utilisation des ressources doit être optimisée. Cela signifie que la préférence doit être donnée à l'utilisation des organisations existantes plutôt qu'à la création de nouveaux organismes.
3. Les propositions doivent permettre d'optimiser les conseils, de s'aligner sur l'infrastructure et les contrats actuels et de s'aligner sur les organisations qui en assurent l'application,
4. L'approche est holistique, mais les institutions restent responsables de l'organisation de la cybersécurité pour leur organisation.

Proposition

La proposition repose sur une bonne coordination et une utilisation optimale des compétences présentes et/ou à développer dans les organisations ou initiatives existantes qui assistent déjà les institutions fédérales respectives dans l'exécution de leurs tâches

Approche intégrée des différents aspects de la cybersécurité

La proposition implique un accompagnement plus intensif des différentes institutions dans la mise en place de leur cybersécurité. À cette fin, nous proposons d'élargir le mandat du CCB. Outre l'élaboration d'une vision et d'une stratégie, le CCB sera chargé d'apporter un soutien opérationnel aux institutions du gouvernement fédéral en matière de cybersécurité.

Soutien aux institutions en matière de sensibilisation des utilisateurs

Aujourd'hui, chaque institution mène des campagnes de sensibilisation auprès de ses employés et peut utiliser les services de formation du SPF BOSA.

Pour optimiser cela, nous proposons que le SPF BOSA fournisse les services suivants :

- Fournir un mécanisme de sensibilisation des utilisateurs

    - Les collaborateurs des institutions du gouvernement fédéral peuvent être inscrits dans un système qui prévoit une sensibilisation continue.
    - Les sujets peuvent être quasi-statiques pour l'introduction initiale (nouveaux collaborateurs).
    - De nouveaux thèmes devraient être proposés pour répondre à l'évolution des nouvelles menaces et techniques.

- Prévoir le développement des compétences

    Sur la base des contributions des différentes institutions, BOSA élabore un plan de formation qui commence régulièrement et de manière garantie (par exemple, tous les trimestres, sans limite inférieure pour les inscriptions).

    - Cette formation permettra à la fois
        - Une formation technique et approfondie pour les administrateurs de systèmes, les développeurs, etc.
        - Formation liée à la gouvernance (audit ISO27K, mise en œuvre, etc.)
        - Formation à la gestion telle que prescrite dans le NIS2

Pour ces deux axes, il est proposé que le CCB et le SPF BOSA fournissent les services nécessaires et participent activement aux divers groupes de travail sur la sécurité de l'information, qui traitent à la fois de la demande et de l'offre.

6. Conclusion

Dans le cadre des décisions des Conseil des Ministres du 1er avril 2022 et du 18 octobre 2022, mission a été donnée au groupe de travail d'examiner la composition et l'efficacité des dépenses de cybersécurité au niveau fédéral, afin de formuler des options stratégiques et d'identifier des synergies possibles entre les départements.

Bien qu'il existe une stratégie nationale élaborée par le Centre pour la Cybersécurité Belgique (stratégie « Cybersecurity 2.0 »), l'analyse de la situation AS IS a démontré qu'il n'existe pas actuellement de stratégie fédérale commune en matière de cybersécurité. Cela a pour effet une gestion peu cohérente des risques.

Des cyberattaques ciblant nos entités fédérales peuvent mettre en danger la sécurité de la population, de l'Etat et l'économie du pays. Outre une vaste palette de mesures renforçant la protection contre les cyber risques, il est ainsi nécessaire de disposer de capacités et ressources bien formées permettant de se sécuriser contre les attaques et de développer une protection apte à absorber des attaques multiples.

La première phase d'enquête auprès des entités fédérales concernant leurs dépenses de cybersécurité donne un aperçu des investissements déjà effectués en matière de cybersécurité. Cependant, étant donné les difficultés rencontrées pour identifier et consolider de manière fiable les dépenses, certains constats et recommandations peuvent déjà être formulés à ce stade :

- Il est important de définir les notions de cybersécurité et de sécurité de l'information de la même façon au sein de toutes les entités fédérales ;

  Les dépenses de cybersécurité sont difficilement identifiables car il n'est actuellement pas possible de les distinguer des autres dépenses informatiques dans Fedcom, afin de répondre à cette préoccupation, il est proposé d'utiliser une sémantique unique pour toutes les organisations afin de permettre de réaliser un suivi précis des dépenses grâce à la comptabilité analytique, en veillant à garantir le niveau approprié de confidentialité pour ces données ;

La deuxième phase d'enquête sur les dépenses de cybersécurité consistait en un « deep dive » sur sept organisations représentatives, sur base d'un questionnaire quantitatif portant sur 2020-2026 et un questionnaire qualitatif auxquels seules cinq entités sur les sept ont répondu.

Nous avons élaboré une proposition stratégique et des pistes d'amélioration possibles dans la partie TO BE du rapport.

Tout d'abord, nous plaidons en faveur d'une stratégie commune en matière de cybersécurité pour l'ensemble du fédéral, basée notamment sur la stratégie « Cybersecurity 2.0 » du CCB, la note cadre du CCB « CCB-2023-35 », les rapports de Deloitte avec le soutien de la FIA et les besoins exprimés par les entités questionnées dans l'enquête mentionnée précédemment.

Nous recommandons que la gouvernance suive globalement les recommandations émises par le CCB dans la note cadre CCB-2023-35 .

L'objectif d'une stratégie fédérale commune est de pouvoir couvrir tout le spectre de la menace cyber, y compris les menaces futures, tout en maintenant un contrôle sur les dépenses. Pour cela, il nous semble essentiel de nous concentrer sur la protection des fonctions vitales, sur le renforcement des compétences en interne, sur la coopération entre organisations et sur une meilleure efficacité des investissements :

Ensuite, nous avons décliné la stratégie commune proposée en cinq axes d'intervention et huit objectifs stratégiques :

Focus 1 Stratégie : la cybersécurité comme priorité

Focus 2 Sécurité : des services publics sécurisés

Focus 3 Vigilance : être proactif à l'égard des menaces

Focus 4 Vigilance : capacité de réaction et/ou à se remettre face aux événements cyber défavorables

Focus 5 : des choix stratégiques et durables

En outre, l'analyse effectuée pour ce spending review montre qu'une une augmentation des investissements est inévitable en matière de cybersécurité si nous voulons couvrir le risque, étant donné la maturité actuelle insuffisante des institutions fédérales.

Sur base des informations reçues lors de la deuxième phase d'enquête, nous pouvons déduire les besoins d'investissements futurs. La courbe d'évolution sera importante en 2024-2025, entre autres

suite à la mise en conformité requise par la directive NIS 2. Ensuite, les investissements devraient s'aligner sur l'évolution des menaces

Une stratégie fédérale globale telle que nous le préconisons permettra d'optimiser les ressources et de maximiser l'efficacité des investissements. Différentes pistes qui permettront de garder un contrôle sur la croissance exponentielle des dépenses à politique inchangée

Enfin, étant donné qu'une stratégie fédérale commune est fortement recommandée et au vu de toutes les pistes d'optimisation identifiées par le groupe de travail, nous proposons deux recommandations:

1. **La création d'une cellule transversale de sécurité de l'information (incluant le cyber) pour un soutient et coordination de activités de protection.**

Là où le CCB soutient au niveau national la protection cyber et contre les impacts des attaques, une nouvelle cellule transversale fédérale de soutien en matière de cybersécurité, accueillie au sein d'une structure existante (dont la position dans l'organisation fédérale sera à définir), permettra la coordination et la coopération des institutions fédérales pour renforcer la protection de l'information. Elle permettra l'application de la stratégie commune et donc de couvrir le spectre de la menace cyber tout en maintenant un contrôle sur les dépenses.

2. **Le renforcement des structures actuelles pour répondre à la menace.**

Il s'agit de renforcer les structures existantes. La proposition repose sur une bonne coordination et une utilisation optimale des compétences présentes et/ou à développer dans les organisations ou initiatives existantes qui assistent déjà les institutions fédérales respectives dans l'exécution de leurs tâches. Quelle que soit l'option choisie, il est recommandé de développer au plus vite le calendrier du renforcement des capacités - internes et externes - de l'organisation qui sera responsable de la coordination pour les entités fédérales et d'aligner suffisamment celui-ci sur le calendrier de mise en œuvre du NIS2.

En outre, nous recommandons **que l'évaluation de la maturité cyber soit faite d'une manière régulière par la cellule de soutien, l'entité de contrôle externe supervisée par le Comité d'audit de l'administration fédérale et le CCB.**

7. Glossaire

- **BCM : Business Continuity Management**
- **CCB**: Cybersecurity Centre Belgium
- **CES** : Stratégie nationale de protection des infrastructures critiques
- **CSIRT** : équipes nationales d'intervention en cas d'incidents de sécurité informatique
- **Cyber Fundamentals** : Cyber Fundamental Framework élaboré par le CCB
- **Cyber Resilience Act** : règlement relatif aux exigences de cybersécurité applicables aux produits comportant des éléments numériques
- **Cybersécurité** : La cybersécurité est le résultat d'un ensemble de mesures de sécurité qui doivent minimiser le risque engendré par l'utilisation des systèmes d'information et de communication (TIC).
- **Cyber Security Act (2019)** : certification de la cybersécurité
- **Cybersecurity 2.0 (CNS du 20 mai 2021)** : approche transversale de la Belgique en termes de cybermenace
- **DID** : Defense-in-Depth, défense en profondeur, consistant d'un multiple de cercles de défense.
- **EECC** : European Electronic Communications Code
- **eIDAS** : règlement sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur (règlement eIDAS) eIDAS= IDentification, Authentication and trust Services
- **ENISA** : agence européenne de cybersécurité
- **EWS**: Early Warning System du CCB
- **FISP** : Federal Information Sécurité Policy
- **IAM**: Identity and Access Management
- **ISO/IEC 27001 – NBN** : normes internationales pour la sécurité de l'information
- **Informations non-cyber** : tout autre transmission ou stockage d'information comme transmission orale, papier etc.
- **NATO Cyber Defense Pledge** : décrit la manière dont les armées membres se préparent à faire face aux menaces futures.
- **NIS (2016) / NIS 2 (2022)** : Directive Network and Information Systems (Security)
- **PAM**: Privileged Access Management
- **RGPD (2016)** : Le règlement général sur la protection des données (2016/679)
- **SECaaS** : Security as a Service: externalisation de solutions ou/et conseils en cybersécurité à travers de tierces parties
- **TIC** : Technologies des systèmes d'information et de communication

8. Sources consultées

- https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
- https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie/documenten/publicaties/2022/oktober/10/nlcs-2022
- https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/strategie/Bericht-Umsetzungsstand_NCS_2021_FR.pdf.download.pdf/Bericht-Umsetzungsstand_NCS_2021_FR.pdf
- https://en.digst.dk/media/27024/digst_ncis_2022-2024_uk.pdf
- https://www.dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf
- https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf
- https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024
- https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=4F5ABAF1C703DF8541301AD89A5173F5.1_cid340?__blob=publicationFile&v=4
- https://www.quebec.ca/gouvernement/ministere/cybersecurite-numerique
- https://www.quebec.ca/nouvelles/actualites/details/depot-du-plan-strategique-2023-2027-du-ministere-de-la-cybersecurite-et-du-numerique-48575
- https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
- https://www.enisa.europa.eu/publications#c3=2013&c3=2023&c3=false&c5=publicationDate&reversed=on&b_start=0&c2=National+Cybersecurity+Strategies
- https://www.enisa.europa.eu/publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity-strategies/@@download/fullReport
- https://www.csirt.es/index.php/es/
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf
- https://www.iso.org/standard/27001
- https://csrc.nist.gov/publications/sp800

9. Annexes

- Le document “Cybersecurity 2.0” élaboré par le Centre pour la Cybersécurité Belgique
- Note Cadre du CCB (CCB-2023-01-B)