CENTRE FOR
CYBERSECURITY
BELGIUM

LA CYBERPROTECTION ACTIVE (ACP)

Document d'orientation, juin 2024

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Table des matières

Table des visuels

Table des Tableau

1. Vision pour l'avenir

Le monde n'en est qu'au début de la transition numérique. Pour profiter pleinement des opportunités que cette transition offre à notre société et à notre économie, il est crucial que nos citoyens, nos entreprises et nos gouvernements puissent maintenir leur confiance dans l'environnement numérique. Pour garantir cette confiance, la cybersécurité est essentielle.

Ces dernières années, de nombreux efforts nationaux et internationaux ont été déployés pour améliorer la cybersécurité des organisations et autres victimes potentielles. Cependant, bien que ces efforts soient essentiels pour renforcer la résilience d'un pays, les tendances récentes indiquent qu'ils restent insuffisants, car les incidents de cybersécurité, la cybercriminalité et la fraude en ligne continuent d'augmenter. Selon le Centre pour la Cybersécurité Belgique (CCB), les vulnérabilités, qu'elles soient humaines ou techniques, en sont la cause. En tant qu'agence nationale en charge de la cybersécurité, nous considérons qu'il est de notre devoir d'aider les organisations et les citoyens à vaincre ces vulnérabilités.

Au cours des dernières années, le CCB a développé plusieurs projets visant à remédier à ces vulnérabilités par une approche proactive, que nous avons initialement décrite à travers le concept de cybersécurité active, et qui est désormais dénommée **cyberprotection active (ACP en abrégé pour « *Active Cyber Protection* » en anglais)**. Une étape politique importante a été franchie lorsque la directive européenne NIS2 a reconnu l'importance d'une approche proactive et a fait de l'ACP une exigence légale dans la définition des stratégies nationales de cybersécurité. Par conséquent, il est désormais impératif que les États membres de l'UE intègrent dans leurs stratégies nationales de cybersécurité des politiques qui mettent en œuvre l'ACP dans le cadre d'une stratégie globale de prévention et de résilience. Cette évolution souligne l'importance des mesures proactives pour sauvegarder les infrastructures cyber et garantir la sécurité des communications numériques dans l'UE.

Le CCB est convaincu de l'importance de promouvoir la cyberprotection active et souhaite encourager non seulement les États membres de l'UE, mais aussi d'autres pays, à adopter des politiques d'ACP. Dans ce guide, nous souhaitons expliquer notre définition du concept d'ACP et partager certaines de nos expériences, afin qu'elles puissent bénéficier à d'autres et faciliter la collaboration.

2. Introduction

Le concept de cyberprotection active (ACP) est mentionné – pour la première fois sur le plan juridique – dans la directive NIS2 (directive européenne 2022/2555 concernant des mesures destinées à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union), au considérant 57 et à l'article 7.

La directive précise que « *dans leur stratégie nationale en matière de cybersécurité, les États membres devraient adopter des politiques de promotion de la cyberprotection active dans le cadre d'une stratégie plus large de cybersécurité.* »[1] La directive NIS précédente exigeait déjà des États membres qu'ils adoptent des stratégies nationales de cybersécurité, définissant des objectifs et des priorités stratégiques. Aujourd'hui, l'**ACP promet de devenir un point clé pour les autorités nationales et les décideurs politiques chargés de réviser, d'actualiser et d'adopter des stratégies nationales de cybersécurité dans le cadre de leurs obligations de mise en œuvre de NIS2**.

Cependant, comme les États membres de l'UE sont encore en train de transposer NIS2 en droit national, il n'y a pas encore de compréhension commune, ni de définition commune, de ce que signifie exactement l'ACP, et de la manière dont la ou les politique(s) ACP pourrait(ent) être transposée(s) au niveau national. **Dans ce document d'orientation, le CCB souhaite exposer sa compréhension du concept et partager quelques bonnes pratiques pour sa mise en œuvre**.

Le considérant 57 de la directive NIS2 décrit l'ACP comme suit:

> ***« Plutôt que de d'agir de manière réactive, la cyberprotection active consiste en la prévention, la détection, la surveillance, l'analyse et l'atténuation actives des violations de la sécurité du réseau, combinées à l'utilisation de capacités déployées à l'intérieur et en dehors du réseau de la victime. Il pourrait s'agir d'États membres offrant des services ou des outils gratuits à certaines entités, y compris des contrôles en libre-service, des outils de détection et des services de retrait (TakeDown Services). La capacité de partager et de comprendre rapidement et automatiquement les informations et les analyses sur les menaces, les alertes de cyberactivité et les mesures d'intervention est essentielle pour permettre une unité d'effort dans la prévention, la détection, le traitement et le blocage des attaques ciblant des réseaux et systèmes d'information. La cyberprotection active repose sur une stratégie défensive qui exclut les mesures offensives. »***

Le CCB, l'autorité nationale pour la cybersécurité en Belgique, est responsable de la coordination des obligations internationales et de la représentation européenne en matière de cybersécurité. Nous définissons l'ACP comme une approche proactive, sur mesure, automatisée et participative de la cybersécurité.

[1] Considérant 57 de la directive NIS2.

Tableau 1 Caractéristiques de l'approche du CCB en matière d'ACP

Proactive	Plutôt que de se contenter de réagir aux attaques cyber, il s'agit de les prévenir en cherchant proactivement les menaces et vulnérabilités potentielles afin d'éviter que les systèmes vulnérables ne soient exploités à grande échelle. L'ACP contribue ainsi à la prévention des atteintes majeures à la cybersécurité dans les organisations.
Sur mesure	Parce qu'il n'existe pas de solution unique, l'ACP préconise des solutions personnalisées qui tiennent compte des différents besoins et de la posture cyber des parties prenantes, qu'il s'agisse de particuliers, de petites organisations, de grandes entreprises ou d'administrations publiques. Les mesures d'ACP s'adaptent à la nature du secteur et à la configuration des systèmes. L'ACP encourage, par exemple, le partage d'informations et une offre de services adaptée à chaque acteur plutôt que des avertissements généraux qui créent une surcharge d'informations.
Automatisée	Des solutions automatisées, de préférence à grande échelle, doivent être développées pour protéger les systèmes contre des attaques automatisées de plus en plus nombreuses. Cette automatisation et cette évolutivité de la protection peuvent également contribuer à remédier à la pénurie croissante de personnel compétent en matière de cybersécurité.
Participative	L'ACP encourage la participation active de tous les acteurs, des particuliers aux grandes organisations, pour identifier et corriger les vulnérabilités d'une manière qui profite à la société dans son ensemble. Plutôt que de se limiter à constater qu'il suffit d'un seul maillon faible pour permettre une attaque, l'ACP chercher à inverser cette logique: il devrait suffire d'un seul citoyen vigilant pour contribuer à la protection d'un système. Chacun peut jouer un rôle dans la protection de tous.

Le CCB met donc l'accent sur l'aspect actif de l'ACP. Cela signifie qu'en tant que CSIRT national, le CCB cherche **activement à impliquer et à aider les utilisateurs dans le renforcement de l'environnement numérique, contribuant ainsi à augmenter leur confiance dans les services numériques**. Avant tout, les citoyens et les entreprises devraient être impliqués dans leur propre protection, car une approche proactive mène à une meilleure collaboration. La vision belge de l'ACP vise à informer les utilisateurs sur les menaces concrètes qui les concernent. Cette approche s'appuie sur une base solide consistant à fournir des orientations et des lignes directrices, à publier des alertes, et à renforcer l'expertise et les capacités.

3. Les piliers du projet actuel de cyberprotection active en Belgique

Le CCB considère l'ACP comme un concept fiable qui englobe sa stratégie de protection proactive. Celle-ci s'aligne sur les initiatives en cours dans plusieurs États membres de l'UE, mises en œuvre par les agences de cybersécurité nationales. **La mission principale du CCB est de faire de la Belgique l'un des pays les moins vulnérables d'Europe sur le plan cyber**. Pour atteindre cet objectif, le CCB **développe des projets nationaux qui s'attaquent non seulement aux vulnérabilités techniques telles que les codes malveillants, mais aussi aux vulnérabilités humaines telles que l'hameçonnage.**

Ces **projets sont actuellement regroupés autour de cinq piliers opérationnels:** l'identification et le démantèlement des infrastructures malveillantes, l'implication des utilisateurs, l'alerte rapide, la cybersécurité comme routine et les services validés.

Illustration 1: Les cinq piliers représentant les projets actuels du CCB en matière d'ACP

Avant d'examiner ces piliers plus en détail, il est important de préciser que l'**approche du CCB en matière d'ACP n'est pas statique. Son objectif n'est pas fini. Il s'agit au contraire d'un effort constant et dynamique**. Constamment révisé et affiné, l'approche ACP est une trajectoire plutôt qu'un projet avec une ligne d'arrivée. L'objectif du CCB est de créer un cadre général pour promouvoir la flexibilité nécessaire pour répondre aux nouvelles méthodes de cyberattaque. Cette attitude proactive est essentielle pour garder une longueur d'avance dans le domaine en constante évolution des cybermenaces. Les cinq piliers actuels seront sans aucun doute adaptés à l'avenir.

Pilier I - Identification et démantèlement des infrastructures malveillantes

Les projets de segmentation de l'infrastructure IT impliquent l'identification systématique des systèmes utilisés par les acteurs malveillants. Cette identification permet de fournir des alertes en temps utile sur les infrastructures malveillantes. Par la suite, des mesures appropriées sont mises en œuvre pour filtrer les menaces lorsque cela est jugé nécessaire. Cette approche de "segmentation" est centrée sur la compréhension des activités des acteurs malveillants, ce qui permet une protection plus ciblée des systèmes en Belgique.

L'une des initiatives clés du CCB dans le cadre de ce pilier est le **bouclier anti-hameçonnage belge** (BAPS pour *Belgian Anti-Phishing Shield* en anglais, plus de détails en annexe). Lancé en 2021, BAPS lance des alertes sur les sites web malveillants au niveau du DNS belge, s'alignant ainsi sur la dimension d'"atténuation active" décrite dans NIS2.

Le projet vise à identifier les liens malveillants. En cas de requête par un internaute d'un site web figurant sur une liste de liens suspects (la liste est tenue à jour par le CCB), l'utilisateur est redirigé vers une page d'avertissement grâce à une collaboration avec les principaux fournisseurs d'accès à Internet (FAI) belges. Cette collaboration public-privé a permis d'éviter pas moins de 13 millions de clics vers des sites web suspects en 2022, soit l'émission d'environ 25 alertes aux internautes belges par minute. Au cours du premier trimestre 2024, BAPS a donné lieu à 3 039 84 visites sur sa page d'accueil, soit une moyenne quotidienne de 97 838 visites. Grâce à ce système, chaque jour, près de 98 000 Belges qui ont cliqué sur un lien suspect sont protégés contre une infrastructure malveillante. Le projet est donc proactif, automatisé, et participatif.

Pilier II - Participation des utilisateurs

Les projets regroupés autour du pilier de l'implication des utilisateurs se concentrent sur le renforcement de la confiance de la population belge (c'est-à-dire les médias, les entreprises, les citoyens, etc.) dans l'environnement numérique, notamment grâce à la sensibilisation à la cybersécurité. Les projets du CCB regroupés sous le nom de Safeonweb et visent à la fois le grand public (@Home) et les organisations (@Work).

- **Safeonweb@home** utilise un ensemble d'outils de communication pour informer rapidement les citoyens belges et les conseiller sur la sécurité en ligne et les menaces numériques afin de réduire le risque d'être victime d'escrocs et de cybercriminels. Le site web safeonweb.be offre un accès permanent à des conseils en matière de cybersécurité. Ces conseils sont également diffusés par l'intermédiaire des réseaux sociaux, de la presse et de plus de 500 partenaires. Lors de la campagne de sensibilisation annuelle Safeonweb en octobre de chaque année, le CCB implique des représentants de tous les secteurs – public, privé, universitaire. Nos partenaires privés, tels que la Belgian Cybersecurity Coalition et Febelfin, contribuent notamment à l'élaboration du contenu de la campagne. Leur expertise sur le terrain permet au CCB d'affiner son message afin qu'il atteigne un maximum de personnes. La communication

autour de l'hameçonnage, véritable fléau de notre époque, est souvent au premier plan.
    - L'application mobile Safeonweb est l'un des services de Safeonweb. Elle permet d'informer rapidement les internautes des nouvelles tentatives d'hameçonnage et d'envoyer des conseils de sécurité (voir l'annexe pour plus de détails).
- Plus récemment, le CCB a lancé **Safeonweb@work**. L'objectif de cette initiative est de s'assurer que les organisations belges soient à la pointe dans un monde de plus en plus numérisé. En numérisant leur organisation et leurs méthodes de production, les entreprises belges tentent de réduire leurs coûts d'investissement et d'optimiser leurs processus pour se rapprocher de leurs clients. En réaction à cette transformation, les systèmes informatiques sont de plus en plus connectés et interdépendants, ce qui augmente la surface de vulnérabilité des organisations et créé de nouveaux défis. La mise en œuvre de mesures de cybersécurité est donc indispensable pour protéger les activités et les investissements des organisations. En s'appuyant sur le succès de la marque Safeonweb.be auprès du grand public, le CCB a lancé en novembre 2023 une plateforme ciblant les organisations nommée Safeonweb@work (voir https://atwork.safeonweb.be). Via cette plateforme, les organisations belges peuvent enregistrer leurs noms de domaine et leurs adresses IP afin de bénéficier de services dédiés. Safeonweb@work propose notamment une version light du système d'alerte précoce développé par le CCB pour les organisations d'intérêt vital. Ce système permet aux organisations de recevoir des alertes ciblées, basées sur les informations techniques qu'elles ont renseignées dans la plateforme. Sur le portail, les organisations peuvent par ailleurs évaluer leur niveau de maturité en matière de cybersécurité et trouver différents documents de référence, des outils, modèles et repères pour les aider à renforcer leur niveau de cybersécurité.

L'un des projets phares au cœur de Safeonweb.be est le **projet BePhish** de lutte contre le phishing (voir annexe). Depuis de nombreuses années, le CCB peut compter sur la participation des citoyens qui lui signalent des messages suspects. Grâce à l'adresse électronique suspicious@safeonweb.be (dont des déclinaisons existent dans les trois langues nationales en plus de l'anglais: néerlandais, français, et allemand), les citoyens peuvent transmettre une copie des messages suspects qu'ils ont reçu, que ce soit par email ou par SMS. Chaque jour, le CCB reçoit ainsi des milliers de messages suspects.

La participation de la population aux projets Safeonweb, et en particulier à BePhish, est une véritable illustration de l'ACP et de sa dimension participative, telle qu'elle est évoquée dans la directive NIS2. En 2021, 4 500 000 messages ont été transmis à suspicious@safeonweb.be. En 2022, ce chiffre est passé à 7 millions de messages, ce qui a permis de détecter plus de 660 000 URL suspects, soit une moyenne de 15 000 messages analysés par jour. En 2023, ce chiffre a encore augmenté pour atteindre près de 10 millions, soit une moyenne de 27 000 messages par jour. Tous les liens transférés sont ensuite utilisés par le CCB pour alimenter d'autres projets, tels que BAPS.

Pilier III – Le *spear warning*

Alors que le *spear phishing* est utilisé avec succès pour envoyer des messages ciblés à des individus dans le but de s'introduire dans leur système informatique, le CCB renverse cette approche en l'utilisant dans un but de protection – ce que nous appelons le « *spear warning* ».

La **détection des menaces en temps réel** est un élément important de l'ACP. L'identification en amont permet aux organisations de réagir rapidement et de minimiser les dommages potentiels. Les projets d'alerte sont spécifiquement conçus pour aider les organisations à identifier les systèmes vulnérables.

Le CCB collecte systématiquement des informations sur les systèmes vulnérables, y compris les menaces, les vulnérabilités et les intrusions. Cela permet de tenir à jour une liste des systèmes vulnérables les plus susceptibles d'être exploités en Belgique. Sur la base de cette liste, le CCB cherche à identifier proactivement les propriétaires des systèmes vulnérables. Une fois qu'un propriétaire est identifié, le CCB lui envoie un avertissement individuel et personnalisé en utilisant des processus automatisés pour une notification rapide et directe. **Cette approche contribue activement à la réduction de la surface d'attaque des organisations. Cela permet de rendre l'exploitation des vulnérabilités plus difficile pour des attaquants potentiels.** Le CCB a remarqué à plusieurs reprises que les avertissements ciblés augmentent de manière significative le degré d'action des organisations vulnérables.

Illustration 2 : Les quatre phases distinctes de l'ACP

En outre, le **système d'alerte précoce** du CCB (EWS pour *Early Warning System*, voir annexe) est une autre initiative phare complémentaire au *spear warning*. L'EWS a été conçu pour fournir des alertes aux organisations d'intérêt vital telles que les opérateurs NIS, les infrastructures critiques, les opérateurs de centrales nucléaires et l'agence de protection des données, ainsi qu'aux organisations d'intérêt particulier au niveau national en Belgique. L'EWS contribue à la mise en œuvre de l'ACP et s'inscrit parfaitement dans le concept d'« atténuation active » décrit dans la directive NIS2.

Le processus d'alerte dans le cadre de l'ACP se déroule en quatre phases distinctes: priorisation, scanning, identification, alerte et information. Plus précisément:

- **Priorisation:** en collaboration avec son partenaire commercial Recorded Future, le CCB évalue les vulnérabilités les plus susceptibles d'être exploitées.
- **Scanning:** le CCB procède ensuite à une analyse approfondie des adresses IP belges afin d'identifier les principaux systèmes affectés par des vulnérabilités classées par ordre de priorité. Nous disposons pour cela d'un mandat légal. Comme les pays n'ont pas de frontières claires en matière d'adresses IP, nous pouvons analyser uniquement les adresses IP qui peuvent être considérées avec un haut degré de certitude comme étant en Belgique. Ce qui peut être considéré comme « l'espace belge des adresses IP » a certes des contours flous, mais la part des systèmes qui ne peuvent pas être scannés pour cette raison est en pratique assez limitée.
- **Identification:** l'étape suivante consiste à identifier les propriétaires de systèmes vulnérables. La plupart du temps, nous devons segmenter les listes d'adresses IP en fonction des *timestamps* et demander les coordonnées des propriétaires des systèmes concernés aux FAI.
- **Avertissement et information:** la dernière étape consiste à envoyer des avertissements ciblés aux propriétaires des systèmes vulnérables. Cette opération est facilitée par des processus automatisés permettant une communication rapide. Les emails sont généralement envoyés aux responsables informatiques des systèmes vulnérables.

Le CCB a constaté que les avertissements, ciblés et sur mesure ont plus d'impact que les avertissements génériques sur les vulnérabilités. Néanmoins, tous les propriétaires avertis n'appliquent pas immédiatement les mises à jour logicielles nécessaires et urgentes. Très souvent, des vulnérabilités activement exploitées ne sont pas corrigées pendant trop longtemps en raison d'un manque d'urgence ressenti au niveau du responsable informatique. C'est pourquoi le CCB envoie parfois également des lettres papier signées par son directeur général afin de sensibiliser directement le PDG ou autre représentant légal de l'organisation concernée.

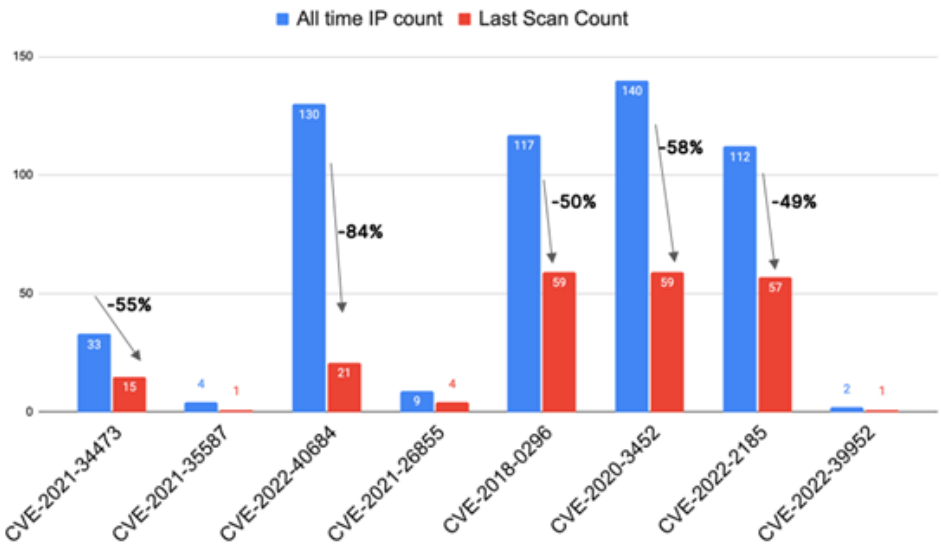

Illustration 3: Taux de réduction des vulnérabilités à la suite d'une procédure d'alerte

Au cours du premier trimestre 2024, 5 757 avertissements ont été envoyés à des organisations et à des particuliers belges. Par ailleurs, en plus des avertissements relatifs aux vulnérabilités, le CCB a commencé à envoyer des avertissements relatifs aux fuites d'informations personnelles/de données d'accès et aux infections par des logiciels malveillants susceptibles d'entraîner des dommages importants. Ce type d'infections conduit souvent à des attaques par ransomware. On peut donc supposer que grâce aux avertissements du CCB, certains incidents liés à des ransomwares ont pu être évités, même si nous n'en connaîtrons jamais le nombre exact.

Compte tenu de ces chiffres et de ces actions, il n'est pas surprenant que le projet *spear warning* ait reçu la première place des Publica Awards en 2023, dans la catégorie « Security & Safety ».

Pilier IV - La cybersécurité comme routine

Tout comme la sécurité incendie et la protection contre les intrusions font partie de la « routine sécurité » des organisations, le **CCB estime que les normes de cybersécurité devraient faire partie de la routine de sécurité de chaque organisation**. Pour les organisations qui sont déjà soumises à des exigences réglementaires strictes en matière de cybersécurité, la mise en œuvre de mesures ACO peut les aider à respecter les normes de conformité. Pour les organisations dont les exigences en matière de cybersécurité ne sont pas obligatoires, la mise en place d'une routine avec des normes, des contrôles, des labels et/ou des certifications peut les aider à améliorer leur niveau de cybersécurité.

Le CCB a développé un cadre appelé CyberFundamentals, reposant sur quatre niveaux, afin d'instaurer des normes de sécurité standard, des contrôles externes et des certifications pour toutes les parties prenantes à tous les niveaux. Pour faciliter l'utilisation internationale de ce

cadre, aucune référence spécifique n'a été incluse en ce qui concerne la législation nationale. Le modèle CyberFundamentals se compose de quatre niveaux: Small, Basic, Important et Essential. Chaque niveau suit la même structure cohérente mais comprend un nombre différent de contrôles à mettre en place, en fonction de la taille et de la criticité de l'organisation. En outre, les **cyberfondamentaux s'articulent autour de cinq fonctions essentielles:** identifier, protéger, détecter, répondre et rétablir.

- **Identifier:** cette fonction permet à l'organisation de comprendre comment gérer les risques de cybersécurité liés aux systèmes, aux personnes, aux biens, aux données et aux capacités.
- **Protéger:** cette fonction est axée sur l'élaboration et la mise en œuvre des mesures de sauvegarde nécessaires pour atténuer ou contenir un risque cybernétique.
- **Détecter:** cette fonction a pour but d'assurer la détection en temps utile des événements liés à la cybersécurité.
- **Répondre:** cette fonction concerne les contrôles qui permettent de réagir aux incidents de cybersécurité. Elle permet de contenir l'impact d'un éventuel incident de cybersécurité.
- **Rétablir:** cette fonction se concentre sur les mesures de protection qui contribuent à maintenir la résilience et à rétablir les services qui ont été affectés par un incident de cybersécurité.

Grâce aux CyberFundamentals, la cybersécurité peut devenir une routine. Une boîte à outils supplémentaire a été créée pour guider les organisations dans la mise en œuvre du cadre. Les CyberFundamentals se basent en grande partie sur le cadre de cybersécurité du National Institute of Standards and Technology (NIST/CSF) des Etats-Unis, complété par des éléments pertinents provenant d'autres normes, notamment ISO 27001/ISO 27002 (pour l'établissement d'un système de gestion de la sécurité de l'information), IEC 62443 (cybersécurité pour la technologie opérationnelle dans les systèmes d'automatisation et de contrôle), et CIS Critical Security Controls (ETSI TR 103 305-1). Le cadre CyberFundamentals est validé par l'équipe fédérale d'intervention en cas d'urgence cyber, CERT.be. CERT.be a en effet fourni des informations (anonymisées) sur les cyberattaques dans le monde réel afin d'estimer la façon dont les mesures du cadre CyberFundamentals peuvent contribuer au taux de couverture contre les attaques cyber. Le cadre CyberFundamentals continuera d'être mis à jour et amélioré à l'avenir pour tenir compte des réactions des parties prenantes, de l'évolution des risques liés à des menaces de cybersécurité spécifiques, de la disponibilité de solutions techniques et de l'évolution des connaissances.

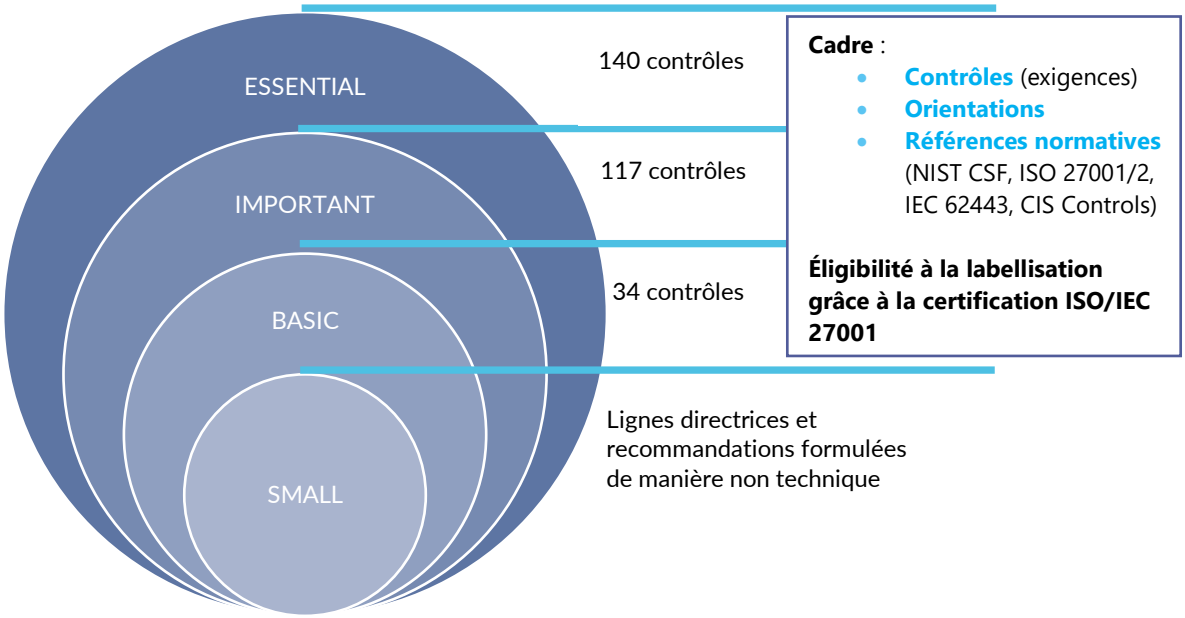

Illustration 4: Vue d'ensemble du cadre CyberFundamentals

Sur base des données historiques du CCB, un *rétrofit* a été effectué sur les cyberattaques réussies en utilisant des données anonymes. La conclusion est la suivante:

- les mesures du niveau d'assurance Basic sont capables de couvrir 82% des attaques,
- les mesures du niveau d'assurance Important permettent de couvrir 94% des attaques,
- les mesures du niveau d'assurance Essentiel sont capables de couvrir 100% des attaques.

Les attaques analysées ont en effet permis d'identifier des mesures clés à chaque niveau afin de hiérarchiser les contre-mesures de protection contre les cyberattaques connues et pertinentes pour chaque niveau d'assurance (plus d'informations en annexe).

Pilier V – Les services validés

L'Internet offre l'anonymat à ses utilisateurs. Mais l'anonymité en ligne est une arme à double tranchant. Si elle peut donner un sentiment de libération, elle peut aussi favoriser les activités malveillantes. En l'absence de responsabilité, les individus peuvent exploiter l'anonymat pour se livrer à des activités nuisibles. D'où le besoin croissant d'une certaine validation pour contrecarrer ces aspects négatifs. Alors que les technologies de prévention de la fraude deviennent de plus en plus sophistiquées, les tactiques de prise de contrôle des comptes donnant accès à des systèmes IT suivent le même rythme. Selon les chercheurs, les attaques de prise de contrôle de comptes continuent d'augmenter, ce qui représente un problème en termes de pertes monétaires et de perte non quantifiable de crédibilité et de confiance pour les victimes.

En outre, les technologies récentes, telles que l'IA générative, semblent amplifier les techniques antérieures telles que l'ingénierie sociale fine, le phishing et d'autres types d'attaques. Elles donnent aux pirates un accès inégalé aux informations personnelles et leur permet de prendre

le contrôle de comptes d'utilisateurs. C'est pourquoi l'authenticité devient de plus en plus complexe à prouver.

C'est ce problème spécifique – comment s'assurer que ce qui apparaît en ligne est sûr et validé – qui a conduit le CCB à s'interroger sur la manière de sécuriser la présence des individus et des organisations en ligne. En raison de l'augmentation du nombre de sites web frauduleux utilisés à des fins d'hameçonnage (c'est-à-dire des sites qui cherchent à obtenir les données personnelles à des fins illégales), le CCB a créé le **pilier « Services validés » de l'ACP.**

L'un des aspects fondamentaux d'un environnement en ligne sûr est la recherche d'un équilibre entre l'anonymat et la validation. Il est important que **la liberté qu'offre l'anonymat ne s'oppose pas au besoin croissant de validation en ligne à des fins de sécurité**. Il est également important d'introduire des niveaux de responsabilité pour fournir des services validés. Des mécanismes de validation doivent être mis en œuvre lorsque des informations personnelles, sensibles et/ou critiques sont utilisées, à la fois pour des raisons de confidentialité et de sécurité. Les identités numériques liées à des références réelles peuvent dissuader les acteurs malveillants et établir un environnement de confiance et de crédibilité.

Dans le cadre du projet de sites validés, le CCB a développé l'**extension de navigateur Safeonweb** pour indiquer aux utilisateurs le niveau de fiabilité des sites web qu'ils visitent (validation forte de l'éditeur, pas de validation de l'éditeur propriétairecou site web malveillant connu). L'objectif est d'atteindre 90% d'expérience de feu vert en Belgique lors de la navigation en ligne (voir l'annexe pour plus de détails). Ce projet est directement lié à la dimension de confiance évoquée pour définir l'ACP dans la directive NIS2. Le projet est par ailleurs conforme au règlement EUid, qui révise le précédent règlement européen eIDAS sur l'identité électronique. Par ce règlement, l'UE a pour objectif de promouvoir les services d'authentification de sites web comme moyen de renforcer la confiance dans les services en ligne, en donnant aux utilisateurs l'assurance qu'une entité authentique et légitime se trouve derrière le site web qu'ils visitent.

4. Conclusions et perspectives d'avenir

La cybersécurité n'est pas un projet, c'est une trajectoire. Il s'agit un processus continu qui exige une adaptation et une collaboration permanentes. Dans le monde interconnecté d'aujourd'hui, les cybermenaces évoluent constamment et exigent une approche dynamique et proactive. Les organisations et les individus ne doivent pas considérer la cybersécurité comme une entreprise ponctuelle avec un point final défini, mais plutôt comme une expédition permanente vers la résilience et un haut niveau de préparation. Le présent document de référence donne un aperçu du cadre stratégique adopté par le CCB. À cet égard, il souligne l'importance de **projets proactifs, sur mesure, automatisés et participatifs reposant actuellement sur cinq piliers.**

Le **CCB reconnaît le rôle significatif joué par les agences nationales de cybersécurité qui prennent des mesures proactives et soutiennent les utilisateurs dans l'identification et la rectification des vulnérabilités face aux cybermenaces**. Prenant en compte les obligations réglementaires définies dans la directive NIS2 et la définition complète de l'ACP, **le CCB reconnaît que cette entreprise ne peut être poursuivie de manière isolée**. Les agences doivent travailler ensemble, non seulement avec le secteur privé, mais aussi entre elles. Il est donc essentiel d'intégrer une dimension internationale aux initiatives ACP et de reconnaître leur rôle dans la promotion de collaborations internationales dans le domaine cyber. Ces collaborations offrent d'ailleurs des opportunités de renforcer les projets ACP existants.

Dans cette perspective, le CCB **invite ses partenaires internationaux, des secteurs public comme privé, à s'engager dans cet effort collectif et à réfléchir à des stratégies innovantes**. Le CCB encourage toutes les parties intéressées à prendre contact avec ses équipes, en exprimant leur intérêt pour une collaboration ou un partage d'informations sur les principes énoncés dans ce document.

L'annexe fournit des informations détaillées sur les projets spécifiques du CCB qui font partie intégrante du cadre ACP. Elle constitue en quelque sorte un répertoire succinct des meilleures pratiques et offre des pistes de coopération potentielle. En parcourant la description des différents projets, toute personne intéressée peut se faire une idée des initiatives en cours au CCB, facilitant ainsi l'échange d'expertise. Nous espérons que cette ressource sera utile à tous ceux qui cherchent à approfondir leur engagement avec le cadre ACP pour renforcer la cyber résilience à l'échelle nationale et internationale.

En favorisant un environnement de collaboration et de partage d'expertise, la **Belgique vise à renforcer sa cyber résilience et à contribuer aux efforts mondiaux de lutte contre les cybermenaces**.

Annexe

LE BOUCLIER ANTI-HAMEÇONNAGE BELGE (BAPS - BELGIAN ANTI-PHISHING SHIELD)	
Page web	BAPS.Safeonweb.be
Objectif	Réduire le taux de clics sur des sites web malveillants dans le cyberespace belge
Descriptif	Le bouclier anti-hameçonnage belge (BAPS) a été lancé en 2021 pour avertir les internautes de la présence de sites web malveillants au niveau du DNS belge. Si un site web demandé par un internaute figure sur une liste de liens suspects maintenue par le CCB, l'utilisateur est redirigé vers une page d'avertissement.
Comment cela fonctionne-t-il ?	BAPS est basé sur le projet BePhish (voir ci-dessous). Les liens web suspects sont identifiés grâce aux messages envoyés au CCB via l'adresse électronique suspicious@safeonweb.be. Le contenu des sites est vérifié et, si aucun contenu n'est trouvé, les liens sont inclus dans la « liste BAPS » des sites web malveillants. Les URL suspects sont transmises à Google Safe Browsing et à Microsoft SmartScreen. Les navigateurs utilisent ensuite ces informations pour avertir les internautes de la présence de sites web malveillants. Comme le CCB n'a aucun contrôle sur la vitesse avec laquelle Google et Microsoft réagissent à sa liste de liens malveillants, le CCB et les principaux fournisseurs belges d'accès à Internet (Belnet, Proximus, Telenet et Orange) ont mis au point une procédure pour avertir les internautes en temps réel. Chaque fois qu'un utilisateur clique sur un lien, une requête DNS est envoyée au fournisseur d'accès à internet (FAI). Grâce à BAPS, le serveur DNS du FAI compare le site web demandé avec la liste des sites web malveillants. **Si le site demandé figure sur cette liste, le serveur DNS du FAI redirige l'utilisateur vers une page d'avertissement**. La liste des sites web malveillants est continuellement alimentée par les messages transférés reçus via le projet BePhish.
Chiffres	La collaboration avec la population belge a permis d'éviter pas moins de 13 millions de clics vers des sites web suspects en 2022, soit environ 25 avertissements aux internautes par minute. Au cours du deuxième trimestre 2023, BAPS a donné lieu à 2 064 378 visites sur sa page d'accueil, soit une moyenne quotidienne de 33 842 visites.

LE SYSTÈME D'ALERTE PRÉCOCE (EWS - EARLY WARNING SYSTEM) ET SPEAR WARNING	
Objectif	Réduire le nombre de vulnérabilités et la durée des menaces pour les organisations d'intérêt vital et d'intérêt particulier en Belgique
Descriptif	Le système d'alerte précoce (EWS) est une plateforme en ligne créée pour alerter rapidement et de manière standardisée les organisations d'intérêt vital et d'intérêt particulier en Belgique sur les vulnérabilités, les intrusions et autres cybermenaces ou attaques qui sont pertinentes pour leur secteur ou même leur organisation. Une équipe spécialisée dans le partage d'informations

	sur les cybermenaces surveille quotidiennement le dark web pour détecter les vulnérabilités telles que les fuites de données d'accès. Les alertes émises sont basées sur les renseignements reçus par le CCB en provenance d'un large éventail de partenaires publics et privés, nationaux et internationaux. Après filtrage, ces informations sont partagées de manière générique et/ou ciblée. • Une fois inscrites sur la plateforme, les organisations peuvent consulter librement un référentiel contenant des rapports stratégiques et opérationnels et des notifications pertinentes pour leur secteur. Un rapport général sur les menaces est également publié quotidiennement sur le portail. Les notifications concernant les nouvelles informations disponibles sont envoyées par e-mails aux utilisateurs, avec l'option de les recevoir en temps réel et sous forme résumée. • De manière ciblée, des alertes, des indicateurs de compromission (IoC) et des rapports sont envoyés directement aux organisations d'importance vitale ou d'intérêt particulier. Ces alertes permettent aux intéressés d'obtenir rapidement des informations pertinentes auprès d'une source fiable et d'agir aussi vite que possible pour se protéger contre les menaces actives.
Cadre juridique	L'un des aspects les plus difficiles pour mettre en place un service d'alerte précoce et de *spear warning* au niveau national consiste à obtenir les dispositions légales nécessaires au déploiement du service. Le CCB a dû déployer des efforts considérables pour trouver le bon équilibre et convaincre les autorités politiques d'adapter le cadre réglementaire. Le CCB a désormais pour mission légale la détection des cybermenaces et des vulnérabilités qui pourraient conduire à des cyberattaques et à des dommages importants. Dans le respect du principe de proportionnalité, le CCB ne collecte que les informations nécessaires à l'identification des vulnérabilités, dans le seul but d'informer immédiatement les propriétaires de systèmes vulnérables. Le CCB procède à des analyses non discriminatoires et non intrusives. Par ailleurs, des changements législatifs ont été nécessaires pour permettre au CCB d'obtenir des informations sur l'identité des propriétaires de systèmes vulnérables. Grâce à un nouveau cadre juridique et à une collaboration constructive avec les FAI, le CCB peut désormais identifier et notifier la plupart des organisations exposées à des risques dans les quelques jours qui suivent la détection de la vulnérabilité.
Chiffres	Le CCB a envoyé 8 000 avertissements de *spear warning* au cours des trois premiers trimestres de l'année 2023. En fonction des cas, on constate une réduction rapide de la vulnérabilité identifiée allant de 50 % à 90 % en quelques jours, plutôt qu'en quelques semaines ou mois en l'absence de *spear warning*. L'effet est significatif, même pour les vulnérabilités plus anciennes pour lesquelles plusieurs avertissements généraux ont déjà été publiés. Outre les avertissements sur les vulnérabilités, le CCB envoie également des avertissements sur les fuites d'identifiants/données d'accès, ainsi que sur les

	infections par des logiciels malveillants susceptibles d'entraîner des dommages importants.

SAFEONWEB@HOME: L'APPLICATION SAFEONWEB	
Page web	Safeonweb.be
Objectif	Les principaux traits humains exploités par les cybercriminels sont l'ignorance et la crédulité. Avec Safeonweb.be, le CCB souhaite sensibiliser le grand public au phishing et aux escroqueries en ligne en montrant que l'on ne peut pas faire confiance à tous les messages et que l'on n'est jamais totalement sûr de l'identité de l'expéditeur d'un message. L'envoi régulier d'un avertissement efficace sur les menaces immédiates peut faire une différence significative, sans pour autant vouloir susciter une peur et une méfiance excessives.
Descriptif	L'application mobile Safeonweb envoie des alertes sur les cybermenaces réelles en Belgique d'une manière comparable aux applications de flashs d'information. L'application est disponible gratuitement pour iOS (App Store) et Android (Google Play Store).

BEPHISH	
Page web	Qu'est-ce que suspect@safeonweb.be ?
Objectif	Les citoyens sont encouragés à être attentifs aux e-mails suspects, mais aussi à prendre des mesures. Chaque individu peut transmettre des e-mails ou des SMS suspects à l'adresse électronique du CCB suspect@safeonweb.be. Cette activation de la population permet de maintenir l'attention sur les messages d'hameçonnage plus longtemps et de manière plus engagée. L'objectif de BePhish est de sensibiliser la population aux dernières campagnes d'hameçonnage et de réduire autant que possible le taux de réussite de l'hameçonnage.
Descriptif	Le CCB encourage les internautes à envoyer tout message suspect à l'adresse électronique suspect@safeonweb.be (disponible en français, néerlandais, allemand et anglais). Outre les e-mails, il est également possible de transmettre des captures d'écrans de SMS ou de codes QR suspects (la technologie utilisée par le CCB permettant d'extraire un URL d'une capture d'écran). À partir des messages reçus, le CCB extrait les pièces jointes et les liens pour les analyser de manière automatisée. Dans le cas des pièces jointes, un système de bac à sable (« sandbox ») est utilisé pour éviter toute infection informatique. Les listes de liens suspects alimentent par ailleurs le projet BAPS (mentionné plus haut). Si l'analyse montre qu'une URL est malveillante, elle est transmise à Google Safe Browsing et à Microsoft Smartscreen. Ces listes de sites web malveillants sont utilisées pour fournir un avertissement au niveau du navigateur. De cette manière, les internautes moins attentifs qui cliquent sur le lien sont protégés grâce à une page d'avertissement.
Chiffres	En 2021, 4 500 000 messages ont été transmis à suspect@safeonweb.be. En 2022, ce chiffre est passé à 7 millions de messages, ce qui a permis de détecter plus de 660 000 URL suspectes. En 2023, le CCB a reçu près de 10 millions de messages de la population, soit une moyenne de 27 000 e-mails

	par jour. Cela a permis de détecter près de 1,3 million d'URL suspectes.

SAFEONWEB@WORK	
Page web	Safeonweb@work
Objectif	Le projet Safeonweb@work vise à améliorer le niveau de cybersécurité des entreprises et autres organisations belges en leur fournissant du contenu, des outils et des services tels que la détection de vulnérabilités, des alertes, des modèles de documents et des conseils.
Descriptif	La plateforme Safeonweb@work est divisée en deux parties: un site web et un portail avec une connexion sécurisée. • Le site web est accessible au public et rassemble des outils et des services permettant aux organisations belges d'effectuer des évaluations de maturité cyber et de trouver des outils, des conseils ou encore des modèles de documents personnalisables pour gérer leur sécurité informatique. Une auto-évaluation leur permet d'identifier d'éventuelles lacunes en matière de cybersécurité et leur fournit des références pour augmenter leur niveau de cybersécurité à court et à long termes. • Le portail sécurisé dispose d'un mécanisme d'authentification basé sur l'eID (appelé « ItsMe » en Belgique) et s'appuie sur le Service fédéral d'authentification. Une fois authentifiées sur le portail, les organisations belges peuvent indiquer leurs coordonnées et les informations relatives à leurs réseaux (noms de domaine, adresses IP, etc.). Le portail propose une version « allégée » du système EWS qui envoie des alertes en fonction des informations techniques fournies par les organisations. Une fois l'inscription terminée, les utilisateurs peuvent activer des services spécialisés tels que les alertes sur les cybermenaces (ils reçoivent des alertes par email lorsqu'une vulnérabilité ou une infection est détectée sur leur réseau) ou le rapport d'analyse rapide (un aperçu annuel des noms de domaine et des réseaux de l'organisation identifiant les menaces les concernant et décrivant les mesures prendre pour réduire les risques).

LE CADRE CYBERFUNDAMENTALS	
Page web	Cadre des CyberFundamentals | CCB Safeonweb@work
Objectif	Le cadre CyberFundamentals vise à accroître la résilience des organisations, à réduire considérablement le risque des cyberattaques les plus courantes et à protéger les données, en veillant à ce qu'un maximum d'organisations se conforment aux principes fondamentaux de la cybersécurité.
Descriptif	Le cadre CyberFundamentals a été développé sur la base de normes internationales existantes dans le domaine des TIC et de la cybersécurité industrielle. La mise en œuvre des CyberFundamentals aide les organisations dans leur mise en conformité réglementaire tout en augmentant le niveau de confiance dans leurs systèmes. Le cadre s'articule autour de 4 niveaux et peut être utilisé par toute

	organisation, indépendamment de sa taille, de son secteur ou de sa maturité en matière de cybersécurité. Chaque niveau suit une structure cohérente et se distingue par un certain nombre de contrôles à mettre en œuvre. Les CyberFundamentals permettent d'augmenter le niveau de maturité cyber d'une organisation au fil du temps, de sorte que les ressources investies se traduisent par une augmentation du niveau de résilience. • **Le niveau d'assurance SMALL** fournit des orientations de départ pour les micro-entités ou les entités qui n'ont pas d'expérience en matière de cybersécurité. • **Le niveau d'assurance BASIC permet** de couvrir 82% des attaques, • **Le niveau d'assurance IMPORTANT** permet de couvrir 94% des attaques, • **Le niveau d'assurance ESSENTIEL** peut couvrir 100% des attaques, sur la base de données historiques. Le cadre CyberFundamentals du CCB s'articule par ailleurs autour de 5 fonctions essentielles: identifier, protéger, détecter, répondre et rétablir. Ces fonctions permettent, quels que soient l'organisation et le secteur d'activité, de promouvoir la communication autour de la cybersécurité entre les experts techniques et les décideurs afin que les risques cyber puissent être intégrés dans la stratégie globale de gestion des risques de l'organisation. La certification ou la labellisation est possible par l'intermédiaire d'organismes d'évaluation de la conformité accrédités, impartiaux et compétents, qui effectuent des audits de vérification (BASIC/IMPORTANT) ou de certification (ESSENTIAL). Les CyberFundamentals peuvent également être utilisés comme outil pour démontrer la conformité d'une organisation avec les exigences de cybersécurité dans le cadre de la directive NIS2.
Comment cela fonctionne-t-il ?	Les CyberFundamentals se basent en grande partie sur le cadre de cybersécurité du National Institute of Standards and Technology (NIST/CSF) américain. Il y ajoute d'autres éléments pertinents provenant d'autres normes, notamment ISO 27001/ISO 27002 (pour l'établissement d'un système de gestion de la sécurité de l'information), IEC 62443 (pour la cybersécurité des technologies opérationnelles dans les systèmes d'automatisation et de contrôle) et les contrôles de sécurité critiques CIS (ETSI TR 103 305-1). • **Le niveau de départ Small** permet à une organisation de procéder à une première évaluation. Il est destiné aux micro-organisations ou aux organisations ayant des connaissances techniques limitées. • **Le niveau Basic (**34 contrôles de sécurité) contient des exigences standards en matière de sécurité de l'information pour toutes les entreprises. Ces exigences fournissent une valeur de sécurité efficace à partir des technologies et processus déjà disponibles. Lorsque cela se justifie, les mesures sont adaptées et affinées. 82 % des profils d'attaques observés par CERT.be sont couverts par les exigences du niveau BASIC. • **Le niveau Important** (117 contrôles de sécurité) est conçu pour minimiser les risques de cyberattaques ciblées par des acteurs

	disposant de compétences et de ressources communes, en plus des risques connus en matière de cybersécurité. 94% des profils d'attaques observés par CERT.be sont couverts par les exigences du niveau IMPORTANT. • **Le niveau Essential** (140 contrôles de sécurité) va plus loin et répond également au risque de cyberattaques avancées menées par des acteurs disposant de compétences et de ressources étendues. 100 % des profils d'attaques observés par CERT.be sont couverts par les exigences du niveau ESSENTIAL.

L'EXTENSION DE NAVIGATEUR SAFEONWEB	
Page web	Extension de navigateur Safeonweb
Objectif	L'extension de navigateur Safeonweb fournit aux internautes une indication du niveau de confiance qu'ils peuvent avoir dans les sites web qu'ils visitent. Un internaute sera ainsi plus susceptible de partager des données personnelles sur un site avec un haut niveau de confiance. Lorsqu'un site web n'est pas en mesure de prouver l'identité de son propriétaire, la prudence est de mise.
Descriptif	Pour chaque site web visité par un internaute, l'extension de navigateur Safeonweb indique si l'identité du propriétaire du nom de domaine a été validée (vert) ou non (orange). Il est recommandé de ne pas partager de données sensibles avec les sites web de niveau orange. Si un pirate informatique place un contenu malveillant sur un site web dont le propriétaire a été validé, l'état de validation passera du vert à l'orange ou au rouge dès la première notification. Les sites web malveillants ou peu sûrs sont marqués en rouge.
Comment cela fonctionne-t-il ?	L'extension attribue une note à chaque site web: • Vert (OK) - score de 4 sur 4: Le propriétaire du site web dispose d'un certificat Extended Validation délivré par une autorité de certification, ou bien le propriétaire du site est enregistré sur atwork.safeonweb.be (pour les organisations belges uniquement). Il ne devrait pas y avoir de problème en principe pour partager des données sur ce site web. • Orange (!) - score de 1 à 3 sur 4: Le propriétaire du site web dispose d'un certificat de validation au niveau de l'organisation ou du domaine, délivré par une autorité de certification, mais le site web n'est pas enregistré sur atwork.safeonweb.be. En cas de doute, il est recommandé de s'abstenir de partager des données sur ce site. • Rouge (X) - score de 0 sur 4: Le site web ne présente pas les caractéristiques de sécurité de base ou est réputé malveillant. Le propriétaire du site n'a pas de certificat et n'a donc pas été validé. Il est fortement déconseillé de naviguer sur le site et de partager des données.

	Ce score est basé sur trois variables:
	• Le **score du type de certificat**, qui reflète le niveau de validation du certificat obtenu par le propriétaire pour son site web. Ce score est calculé comme suit:
	  ○ 3/3 quel que soit le type de certificat si le site web est enregistré sur le portail safeonweb@work, ou bien en cas de certificat de validation étendue,
	  ○ 2/3 en cas de certificat de validation de l'organisation,
	  ○ 1/3 en cas de certificat de validation de domaine, ou
	  ○ 0/3 si aucun type de certificat n'a été obtenu pour le site web.
	• Le **score de l'autorité de certification** est un score de 1 ou 0 selon que l'autorité de certification qui a délivré le certificat du site web est un acteur connu sur le marché et référencé dans les bases de données du CCB.
	• Le **score du domaine** indique si le domaine est enregistré comme malveillant, auquel cas votre score total est ramené à 0.

Chiffres	Comme ce projet est encore récent, les chiffres sont limités. D'octobre à fin novembre 2023, l'extension de navigateur web avait été téléchargée plus de 12 000 fois.

Clause de non-responsabilité

Ce document et ses annexes ont été préparés par le Centre pour la Cybersécurité Belgique (CCB), une administration fédérale créée par l'arrêté royal du 10 octobre 2014 et placée sous l'autorité du Premier ministre.

Le CCB n'assume aucune responsabilité quant au contenu de ce document.

Les informations fournies:

- sont exclusivement de nature générale et n'entendent pas prendre en considération toutes les situations particulières,
- ne sont pas nécessairement exhaustives, précises ou à jour sur tous les points.

Editeur responsable:
Centre pour la Cybersécurité Belgique
M. De Bruycker, directeur général
Rue de la Loi 18
B-1000 Bruxelles.

Dépôt légal:
D/2024/14828/006