CENTRE FOR
CYBERSECURITY
BELGIUM 10Y

10 ANS D'EXISTENCE DU CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE

Centre for Cybersecurity Belgium
Sous l'autorité du Premier Ministre

.be

Éd. Responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur général
Rue de la Loi, 18

1000 Bruxelles

Recherche, interviews et rédaction
the content company

Rédaction finale
Katrien Eggers
Michele Rignanese

Photos
Archives personnelles CCB,
AdobeStock, Karakters, Cookiecutter
& Ron Lach for Pexels

Réalisation
Karakters.be

Impression
Imprimerie de la Chambre des
représentants

Dépot légal
D/2025/14828/006

Date de publication
31 octobre 2025

TABLE DES MATIÈRES

Chère lectrice, cher lecteur,

Il y a dix ans, avec la création du Centre pour la Cybersécurité Belgique (CCB), notre pays s'est doté d'un point de contact unique dans le domaine de la cybersécurité. L'histoire a débuté avec la publication d'un arrêté royal et le recrutement de deux pionniers motivés, pour évoluer en une autorité nationale respectée, soutenue par une équipe aux profils variés de près de 140 experts. En collaboration avec de nombreux partenaires, nous assurons jour et nuit la sécurité numérique des citoyens, des entreprises et des autorités.

Notre économie et notre société s'appuient de plus en plus sur les réseaux numériques, tandis que les cyberattaques deviennent de plus en plus sophistiquées et ciblées. La cybersécurité est donc une composante essentielle de notre société. Ces dernières années, l'Union européenne a renforcé le cadre réglementaire, notamment les directives NIS-1 et NIS-2, le règlement sur la cybersécurité et la législation sur la cyberrésilience. Chacune de ces initiatives entraîne des missions et des responsabilités supplémentaires, mais elles génèrent surtout des opportunités d'élever encore la barre en matière de cybersécurité.

Depuis notre rôle central, nous coordonnons le suivi des incidents, nous soutenons les secteurs vitaux et nous nous concentrons sur la prévention. Dès le premier jour, nous avons investi dans la technologie, l'expertise et les procédures, mais surtout dans la sensibilisation et l'implication des citoyens. C'est l'action collective des citoyens et des entreprises qui améliorera notre cyberrésilience. De mesures simples, comme l'authentification en deux étapes et la mise à jour rapide des logiciels, restent les moyens les plus efficaces de prévenir les problèmes.

Nous sommes donc fiers que Safeonweb soit devenu une source de confiance pour le grand public, offrant des conseils clairs et facilitant le signalement de messages suspects. Chaque signalement nous permet de réagir plus rapidement, de mieux cibler les informations et d'être plus forts ensemble. Grâce à Safeonweb@Work, avec ses directives pratiques et ses scans, nous aidons les entreprises à se préparer de manière plus efficace, étape par étape.

Entre-temps, notre écosystème s'est également professionnalisé. Une coopération étroite, basée sur la confiance entre les services publics, le secteur privé et le monde académique a permis à la Belgique de devenir, sous la coordination du CCB, un modèle européen en matière de cybersécurité.

Cette brochure revient sur une décennie d'apprentissage, d'expérimentation et d'ancrage des meilleures pratiques. Mais elle est aussi tournée vers l'avenir, car la progression de l'IA et la dynamique de la menace géopolitique nous posent de nouveaux défis. Toutefois, notre engagement et notre détermination restent assurés : prendre des mesures proactives pour protéger au mieux notre pays.

Ensemble, nous pouvons faire de la Belgique l'un des environnements numériques les plus sûrs d'Europe. Telle est notre ambition. Et cette responsabilité, nous ne pourrons l'assumer que si nous le faisons ensemble.

Miguel De Bruycker
Directeur général

Phédra Clouner
Directrice générale adjointe

L'AVANT

Le Centre pour la Cybersécurité Belgique (CCB) a été créé par l'arrêté royal du 10 octobre 2014 et a commencé ses activités au début de 2015. Avant cela, des initiatives avaient déjà été mises en place pour sécuriser le trafic Internet dans notre pays.

En 1993, Belnet a été lancé, un programme de recherche fédéral visant à développer un réseau permettant aux chercheurs de se connecter à distance à des superordinateurs. Belnet est devenu un carrefour Internet et a déployé des efforts pour garantir la qualité des connexions et les sécuriser.

En 2004, le Computer Emergency Response Team - CERT Belnet a été créé dans le giron de Belnet pour répondre aux questions sur les problèmes et incidents de sécurité des membres du réseau de la recherche scientifique.

En outre, la Belgian Network & Information Security Platform (BELNIS) a été lancée au sein des pouvoirs publics. Il s'agissait d'un organe de concertation au sein duquel tous les départements concernés par la sécurité numérique étaient représentés, dans le but d'aborder les problèmes de sécurité des réseaux et de l'information. L'organe ne disposant pas de pouvoir de décision ni de moyens financiers, cette plateforme n'a pas immédiatement donné lieu à des actions

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[2014/207006]

10 OKTOBER 2014. — Koninklijk besluit tot oprichting van het Centrum voor Cybersecurity België

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de Grondwet, de artikelen 37 en 107, tweede lid;

Gelet op het koninklijk besluit van 11 mei 2001 houdende oprichting van de Federale Overheidsdienst Informatie- en Communicatietechnologie;

Gelet op het advies van de inspecteur van Financiën, gegeven op 9 december 2013;

Gelet op het advies van de inspecteur van Financiën, gegeven op 13 december 2013;

Gelet op de akkoordbevinding van de Staatssecretaris voor Ambtenarenzaken, gegeven op 17 december 2013;

Gelet op de akkoordbevinding van de Minister van Begroting, gegeven op 17 december 2013;

Gelet op het protocol nr. 155/1 van 24 februari 2014 van het Sectorcomité I - Algemeen Bestuur;

Gelet op de vrijstelling van een impactanalyse op basis van artikel 8, § 1, 4°, van de wet van 15 december 2013 houdende diverse bepalingen inzake administratieve vereenvoudiging;

Gelet op het advies nr. 56.335/2 van de Raad van State, gegeven op 4 juni 2014, met toepassing van artikel 84, § 1, eerste lid, 2°, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973;

Op de voordracht van de Eerste Minister, de Minister van Begroting, de Minister van Financiën, belast met Ambtenarenzaken, de Staatssecretaris voor Modernisering van de Openbare Diensten en op het advies van de in Raad vergaderde Ministers,

Hebben Wij besloten en besluiten Wij :

Artikel 1. Bij de Federale Overheidsdienst Kanselarij van de Eerste Minister wordt het Centrum voor Cybersecurity België, hierna "CCB" genoemd, opgericht.

Het CCB staat onder het gezag van de Eerste Minister.

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[2014/207006]

10 OCTOBRE 2014. — Arrêté royal portant création du Centre pour la Cybersécurité Belgique

PHILIPPE, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la Constitution, les articles 37 et 107, alinéa 2;

Vu l'arrêté royal du 11 mai 2001 portant création du Service public fédéral Technologie de l'Information et de la Communication;

Vu l'avis de l'inspecteur des Finances, donné le 9 décembre 2013;

Vu l'avis de l'inspecteur des Finances, donné le 13 décembre 2013;

Vu l'accord du Secrétaire d'Etat à la Fonction publique, donné le 17 décembre 2013;

Vu l'accord du Ministre du Budget, donné le 17 décembre 2013;

Vu le protocole n° 155/1 du 24 février 2014 du Comité de Secteur I - Administration générale;

Vu la dispense d'analyse d'impact sur la base de l'article 8, § 1er, 4°, de la loi du 15 décembre 2013 portant des dispositions diverses concernant la simplification administrative;

Vu l'avis n° 56.335/2 du Conseil d'Etat, donné le 4 juin 2014, en application de l'article 84, § 1er, alinéa 1er, 2°, des lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973;

Sur la proposition du Premier Ministre, du Ministre du Budget, du Ministre des Finances, chargé de la Fonction publique, du Secrétaire d'Etat à la Modernisation des Services publics et de l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Article 1er. Auprès du Service public fédéral Chancellerie du Premier Ministre est créé le Centre pour la Cybersécurité Belgique, ci-après dénommé « CCB ».

Le CCB est placé sous l'autorité du Premier Ministre.

Arrêté royal portant création du Centre pour la Cybersécurité Belgique

2012 : La première cyberstratégie

Vu la recrudescence des incidents liés à la cybersécurité, il s'est révélé nécessaire d'élaborer une stratégie nationale globale. Elle a été définie en 2012 par Luc Beirens de la Federal Computer Crime Unit de la Police fédérale et Miguel De Bruycker, qui travaillait auprès du SGRS, le service de renseignement de la Défense en matière de cybersécurité. Cette première Stratégie de Cybersécurité poursuivait trois objectifs :

- La Belgique visera à garantir un cyberespace sûr et sécurisé dans le respect des droits fondamentaux et des valeurs d'une société moderne;
- La Belgique s'efforcera d'assurer une sécurité et une protection optimales des infrastructures critiques et des systèmes publics contre la cybermenace.
- La Belgique veut développer ses propres capacités de cybersécurité.

Dans le cadre des actions concrètes de mise en œuvre de la stratégie, cette note mentionnait explicitement la nécessité d'une approche centralisée et intégrée de la cybersécurité, par un pilotage central et le développement de partenariats public-privé étroits. Le projet de note évoquait pour la première fois l'idée de créer un centre indépendant de coordination de la cybersécurité en Belgique.

Au départ, ce centre de coordination n'a pas beaucoup enthousiasmé le monde politique. Cependant, plusieurs cyberincidents survenus en 2013 et l'arrivée d'un nouveau gouvernement fédéral fin 2014 ont contribué à placer la cybersécurité au sommet de l'agenda politique.

2013 : Le piratage de Belgacom

L'un des incidents les plus connus de cette période est le piratage de Belgacom. À l'été 2013, des cyberexperts néerlandais ont identifié des signes d'une intrusion numérique chez l'opérateur télécoms Belgacom. Ils ont découvert un logiciel espion sophistiqué dans les systèmes IT, probablement en place depuis 2011, capable d'intercepter les communications et les données de Belgacom et de sa filiale internationale BICS. Au lendemain de l'incident, Belgacom a investi massivement dans la cybersécurité. Des dizaines de millions seront consacrés au renouvellement de l'infrastructure informatique et à l'amélioration de la sécurité contre les cyberattaques.

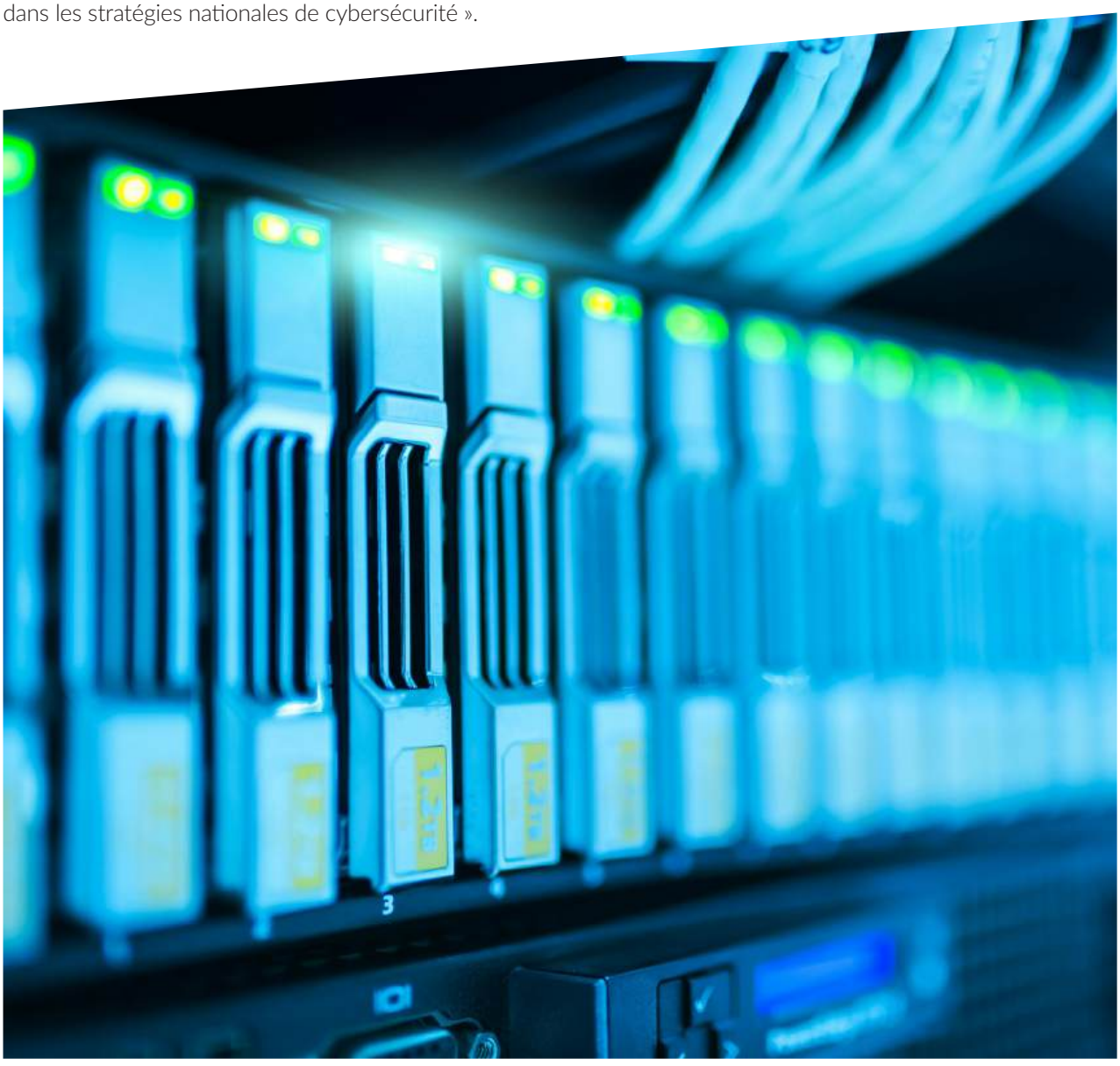
2013 : Une stratégie européenne de cybersécurité

La création du CCB ne peut pas non plus être dissociée des évolutions de la politique européenne en matière de cybersécurité. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) été créée en 2004. Mais ce n'est qu'en février 2013 que la Commission européenne a présenté sa première stratégie de cybersécurité, intitulée « An Open, Safe and Secure Cyberspace ». Cette stratégie prévoyait des initiatives législatives

visant à promouvoir la cybersécurité, soulignait l'importance de la sensibilisation dans les secteurs public et privé et insistait sur la nécessité d'investir davantage dans la R&D en matière de cybersécurité.

Dans le même temps, la Commission encourageait les États membres à mettre en place les structures nécessaires pour s'attaquer à la cyberrésilience, la cybercriminalité et la cyberdéfense, afin d'être mieux armés contre les cyberincidents. La stratégie préconisait « d'optimiser la coordination entre les ministères au niveau national et de définir les rôles et les responsabilités des différentes entités nationales dans les stratégies nationales de cybersécurité ».

"La création du CCB ne peut pas non plus être dissociée des évolutions de la politique européenne en matière de cybersécurité. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a été créée en 2004."



2014-2016

LA CRÉATION

La base juridique de la création du Centre pour la Cybersécurité Belgique a été établie à l'automne 2014. Le CCB s'est vu confier une mission claire par les autorités : surveiller, coordonner et renforcer la cybersécurité en Belgique.

Le centre coordonne ainsi la politique belge en matière de cybersécurité. Il suit la mise en œuvre, propose des initiatives et participe à l'élaboration de nouvelles réglementations. La sensibilisation est l'une de ses missions principales : informer les citoyens, les entreprises et les institutions publiques sur les risques en ligne et fournir des outils concrets pour y remédier. Sur la scène internationale, le centre représente la Belgique dans les organes européens de concertation. Eu égard à la portée transversale de sa mission, le CCB a été placé sous l'autorité directe du Premier Ministre, garant de sa responsabilité politique.

Le recrutement pour les postes clés a suscité un grand intérêt. Pour le poste de directeur, 16 candidats néerlandophones et 19 francophones se sont présentés. Pour le poste de directeur adjoint, il y a eu 27 candidats néerlandophones et 29 francophones. À l'issue de la sélection, Miguel De Bruycker (précédemment à la Défense) et Phédra Clouner (active à la Justice) ont été nommés directeur et directrice adjointe en août 2015, avec un mandat de cinq ans. Ils dirigent toujours l'organisation. L'équipe s'est progressivement agrandie, passant de deux personnes en août 2015 à plus de 140 aujourd'hui.

Premier plan stratégique du CCB

Pour orienter le développement de l'organisation, le CCB a élaboré un plan stratégique qui a été présenté au public le 26 octobre 2015. Le plan prévoyait un calendrier en trois phases : une phase de démarrage de six mois, suivie d'une phase de construction de trois ans et une phase de maturité sur cinq ans. Pour chacune de ces phases, des objectifs opérationnels distincts ont été définis, avec pour ligne directrice la mise en place d'une approche intégrée, coordonnée et axée sur l'action.

Dès le début, il a été décidé d'aligner la vision stratégique nationale avec des actions et services concrets du CCB. Avant l'élaboration du plan stratégique, quatre groupes cibles ont été définis: les citoyens, les entreprises, les organisations d'importance vitale (ce groupe a été systématiquement élargi par la suite, sous l'influence de la réglementation européenne NIS) et les services publics.

Cela a établi les fondements de l'approche orientée services qui caractérise l'organisation jusqu'à aujourd'hui. Les plans d'action indiquaient explicitement que le CCB s'attacherait en priorité à fournir des services à la population, par exemple à l'aide de campagnes de sensibilisation. Le raisonnement était que la notoriété auprès du grand public conduirait aussi immédiatement à une plus vaste publicité auprès des autres groupes cibles.

Parallèlement, l'élaboration d'un cyberplan d'urgence a été avancée comme une priorité urgente. Le plan déterminerait qui, en cas d'incident, pourrait prendre les commandes afin de limiter l'impact des cyberattaques. Cela devait conduire à une unité de commandement et à une lutte efficace contre les cyberattaques contre les principales cibles belges.

La Cyber Security Coalition a été créée en janvier 2015.

“Dès le premier jour, les attentes sont très élevées. La nécessité d’une cybersécurité renforcée et d’une approche coordonnée en Belgique apparaissent comme une évidence face à l’augmentation des cybermenaces entre 2014 et 2016. La coopération semble donc cruciale dès le début.”

Dans la phase initiale, le CCB est passé de deux à cinq employés.
En haut, de gauche à droite: Miguel De Bruycker, Phédra Clouner. En bas, de gauche à droite: Andries Bomans, Valéry Vander Geeten, Jo De Muynck.

Dès le premier jour, les attentes sont très élevées. La nécessité d'une cybersécurité renforcée et d'une approche coordonnée en Belgique apparaissent comme une évidence face à l'augmentation des cybermenaces entre 2014 et 2016. La coopération semble donc cruciale dès le début. La création de la Cyber Security Coalition en tant qu'asbl privée, le 26 janvier 2015, marque un progrès significatif.

Cette organisation rassemblera des acteurs institutionnels, des entreprises et des instituts scientifiques pour échanger des expériences, analyser les risques et développer des solutions. Ce réseau notamment permettra une accélération dans l'évolution du CCB, tant sur le plan stratégique qu'opérationnel, et il constitue l'épine dorsale de la cybersécurité belge actuelle.

Novembre 2015 : premier stress test

Le jeune CCB a rapidement été confronté à un défi majeur. En novembre 2015, des messages menaçants circulent sur YouTube et annoncent que des pirates informatiques vont détruire des sites Internet des autorités publiques belges. Ce premier test de résistance réel a de nouveau souligné l'importance de développer un plan d'urgence cyber détaillé.

L'équipe s'est rapidement mise au travail pour finaliser le plan d'urgence et assurer l'harmonisation nécessaire. Le plan d'urgence prévoit un système d'escalade par paliers, en fonction de la gravité de l'incident, et définit les services qui doivent intervenir. La rapidité, la coopération et la clarté de la communication sont au centre de ce processus.

Le plan qui a finalement été présenté a pris en compte de nombreuses sensibilités de terrain, et a aidé le CCB à revendiquer sa place dans l'écosystème au sens large. Le cyberplan d'urgence a créé une structure bien définie avec des engagements précis pour gérer les cyberincidents majeurs nécessitant une coordination nationale. Il a été développé et mis à jour progressivement.

2016 : élaboration d'un Early Warning System

En 2016, le CCB a renforcé son rôle de coordinateur de la stratégie belge de cybersécurité. Le centre a ainsi contribué au renforcement de la cyberrésilience transfrontalière, en préparation de la directive européenne NIS. Dans le même temps, une première version rudimentaire du système Early Warning (EWS) a été élaborée dans notre pays, permettant d'alerter rapidement les secteurs critiques en cas de nouvelles menaces.

Le EWS surveille les réseaux numériques de l'infrastructure belge et analyse les indicateurs techniques pouvant révéler une activité malveillante (tels que les réseaux de botnets, les IP malveillantes ou les domaines suspects). Le système est basé sur une combinaison de collecte de données automatisée, d'intelligence des menaces et d'alertes en temps réel. Les signaux sont traduits en avertissements pour des organisations spécifiques.

Des secteurs tels que les soins de santé, les finances et l'énergie ont été impliqués en priorité. Les avertissements varient d'un signalement de vulnérabilité dans une version logicielle spécifique à un avertissement concret pour des campagnes de phishing ciblées.

2017–2020

L'OPÉRATIONNALISATION : 2017-2020

À partir de 2017, le CCB a connu une forte croissance. La cybermenace sous toutes ses formes est devenue un phénomène bien connu de la société. Le développement de la maturité au sein du CCB n'a pas seulement été synonyme de croissance numérique, mais aussi de progrès stratégiques et substantiels.

CERT.be : développement d'une réponse performante aux incidents

Le 1er janvier 2017, la Cyber Emergency Response Team fédérale (CERT.be) a été officiellement intégrée au CCB. Il ne s'agissait pas seulement d'un remaniement administratif, impliquant le transfert du CERT de Belnet vers un autre service. Cet événement a marqué le début d'un ancrage fondamental de la réponse aux incidents dans la stratégie nationale plus large de cybersécurité.

Pour le CCB, il s'agissait d'un premier grand boost. Cette intégration a permis à l'organisation de se développer. Avec un avantage majeur : le fonctionnement du CERT a pu être entièrement repensé et intégré dans la stratégie que le centre était en train de déployer.

L'objectif était clair : étendre le fonctionnement de CERT.be, mieux structurer l'équipe et mieux l'adapter aux menaces accrues dans le cyberpaysage belge et international. Si CERT.be faisait déjà office de CSIRT (Computer Security Incident Response Team) au niveau national, l'ancrage dans la structure du CCB a néanmoins offert une occasion unique de professionnaliser davantage le service et de le relier à toutes les autres mesures prises pour renforcer la cybersécurité. CERT.be a eu accès à davantage de ressources, à un recrutement spécialisé et à un soutien stratégique.

L'une des principales priorités après l'intégration a été le déploiement d'une nouvelle équipe. Une composition plus pluridisciplinaire devait permettre à l'équipe non seulement de réagir aux incidents, mais également d'identifier préventivement les menaces, de formuler des recommandations et de faciliter la coordination nationale en cas d'incidents.

Cyber Europe: exercices de crise cyber 2018 et 2024

Fin 2018, une étape importante a été franchie : le CCB était désormais opérationnel en continu pour les opérateurs de services essentiels et les infrastructures critiques. Cette disponibilité permanente répond aux besoins économiques et renforce la préparation nationale aux cybercrises. Cette expansion a été réalisée en collaboration étroite avec le Centre de crise national (NCCN), qui a permis de garantir cette permanence 24 heures sur 24 et 7 jours sur 7.

Le service a travaillé sur la structuration des connaissances tout en faisant face au défi constant du recrutement et de la rétention de spécialistes de la cybersécurité, en raison de la pénurie de main-d'œuvre et de la concurrence internationale. Néanmoins, l'équipe a réussi à renforcer son expertise en investissant de manière ciblée dans la formation et en participant à des exercices internationaux tels que Cyber Europe, un exercice de cybercrise européen à grande échelle organisé par l'ENISA au cours duquel les pouvoirs publics, les entreprises et d'autres organisations collaborent pour mettre à l'épreuve leur résilience aux cyberincidents à grande échelle.

D'autres services publics ont par ailleurs reconnu la réputation et la professionnalisation acquises. Les évaluations et les collaborations ont montré que l'intégration de CERT.be au sein du CCB a conduit à une gestion plus efficace des incidents et à une meilleure coopération entre les différents acteurs fédéraux et sectoriels. La position renforcée de CERT.be est devenue un catalyseur pour des initiatives plus larges telles que la mise en œuvre de la directive NIS et le développement de la plateforme nationale de signalement.

Après les attentats terroristes de 2016, une partie de la « provision Terro » a été affectée à la cybersécurité

2016 : La « provision Terro » comme levier

Après les attentats terroristes de mars 2016 à Brussels Airport (Zaventem) et dans le métro de Bruxelles, le gouvernement fédéral a décidé de dégager des fonds structurels et non structurels supplémentaires pour des projets visant à lutter contre la radicalisation, le terrorisme et l'extrémisme violent. Bien que cette « Provision Terro » n'ait pas explicitement trait à la cybersécurité, ce cadre budgétaire particulier a néanmoins joué un rôle important pour le CCB.

Comme les réseaux terroristes exploitent également avec avidité le domaine numérique, le lien avec la cybersécurité s'est rapidement avéré indéniable. Dans ce contexte, le CCB a formulé des propositions visant à utiliser une partie de la Provision Terro pour renforcer la résilience numérique belge.

Ainsi, ces moyens ont permis de renforcer la coopération entre les administrations. La lutte contre les formes de terrorisme dans le domaine cyber requiert en effet une coopération entre le CCB, la Sûreté de l'État, la Police fédérale, la Défense, la Justice et les partenaires étrangers. Ces budgets ont permis de former du personnel commun, de construire des infrastructures partagées et de lancer des projets pilotes qui, autrement, auraient été difficiles à financer.

Threat intelligence

En 2020, le CCB a renforcé ses connaissances, ce qui conduit à la division du service CERT.be en deux équipes : Cyber Threat Research and Intelligence (CyTRIS) et CERT, cette dernière se concentrant davantage sur la réponse urgente aux cybermenaces. Ces deux facettes de la cybersécurité restent cruciales à ce jour et constituent l'activité principale du CCB : collecter et analyser les informations sur les menaces, et gérer les incidents.

La Cyber Threat Research & Intelligence Sharing team fournit différents services depuis 2018. Elle contrôle quotidiennement différentes sources, collecte et classe les informations qui peuvent être utiles pour alerter les victimes potentielles et effectue des analyses de cyber threat & intelligence approfondies, pour ensuite en faire rapport.

La CyTRIS envoie également des « spear warnings » (avertissements individuels) aux entreprises si une vulnérabilité particulière a été détectée au niveau de leur infrastructure informatique, si des logiciels malveillants ont été détectés ou si des identifiants ont été volés. Elle est également responsable de la première prise de contact avec les organisations qui signalent un incident au CCB en vue de lancer une enquête sur l'incident.

BePhish et le Belgian Anti-Phishing Shield (BAPS)

Le phishing a été une préoccupation majeure dès le départ et reste jusqu'à aujourd'hui l'une des formes les plus courantes de cybercriminalité, avec un impact important. Si les premiers mails étaient rédigés de façon maladroite et simpliste, ils sont au fil des ans devenus des messages très réalistes, diffusés via tous les canaux de communication possibles : mails, SMS, WhatsApp et médias sociaux.

Il est rapidement apparu que le modèle réactif traditionnel (intervention après le signalement d'une victime) ne suffisait pas. C'est pourquoi le CCB a développé le projet BePhish. Depuis 2019, les citoyens peuvent signaler toute communication suspecte 24 heures sur 24 et 7 jours sur 7 via suspect@safeonweb.be. Derrière cette boîte mail se cache un système d'analyse et de blocage automatisé. Il traite en moyenne 25 000 mails par jour.

Cette initiative a fourni au centre une large quantité d'informations sur les sites Internet malveillants. Pour lutter activement contre cette forme de criminalité, une deuxième initiative a été lancée : le Belgian Anti-Phishing Shield (BAPS), une défense supplémentaire contre ces pages Internet malveillantes. Les visiteurs qui cliquent sur ce genre de liens sont redirigés vers une page d'avertissement du CCB.

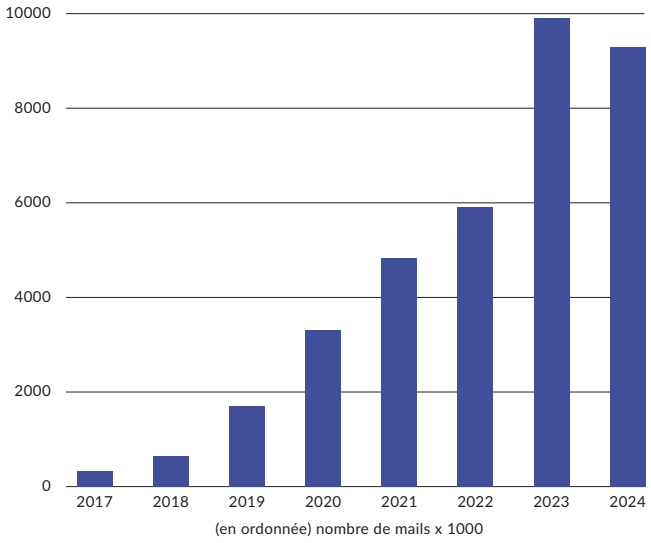
Page d'avertissement BAPS

Pour concrétiser cette idée sur le plan technique, une collaboration étroite avec les fournisseurs d'accès Internet a été nécessaire. Proximus a été le premier fournisseur à se lancer, suivi rapidement par Telenet. Actuellement, plus de 100 fournisseurs font partie de BAPS. En 2024, la page de redirection a été activée au moins 240 millions de fois.

L'Anti-Phishing Shield a permis de réduire le temps de réaction face aux sites Internet malveillants, qui est ainsi passé de plusieurs jours à quelques minutes. L'efficacité ne réside pas tant dans l'innovation technologique que dans l'implication des citoyens dès le départ, qui continuent de signaler massivement les messages contenant des URL suspectes. Grâce à un filtre anti-spam basé sur cette approche, le CCB et les fournisseurs de services empêchent également les messages malveillants d'atteindre les boîtes mail des citoyens et des entreprises.

Le tandem BePhish et BAPS est une contribution unique à la sécurité collective : grâce à tous les signalements, le CCB peut détecter rapidement les tendances et ensuite diffuser des avertissements via Safeonweb. L'idée quelque peu controversée d'une intervention active des autorités sur le trafic Internet est devenue un point central pour le CCB. Bien que les restrictions de la liberté de mouve-

Évolution des mails suspect@safeonweb / URL BAPS



ment dans le cyberespace aient suscité plusieurs plaintes, elles ont toujours été réfutées avec succès.

L'incident « NotPetya » et les Spear Warnings

Le 27 juin 2017, le CCB reçoit des messages de plusieurs pays européens concernant une vague de cyberincidents. Les attaques sont semblables à des rançongiciels (ransomware), mais concernent en fait des malware NotPetya. En d'autres termes, l'objectif n'était pas d'obtenir une rançon en échange de la restitution des données, mais plutôt de rendre les systèmes inutilisables à distance et de manière permanente. Il s'agissait d'une cyberattaque mondiale, ciblant principalement des entreprises en Ukraine.

Les attaquants ont créé un système capable de se propager très rapidement à travers d'autres réseaux. Face à une cyberattaque d'une telle ampleur, la société de transport danoise Maersk a été contrainte de neutraliser intégralement son infrastructure numérique afin d'endiguer la menace. Les employés ont dû revenir à l'utilisation du papier et du stylo.

Dans notre pays, le CCB a dû réagir très rapidement pour suivre l'incident. NotPetya a notamment été à l'origine du développement des Spear Warnings : lorsque des vulnérabilités sont identifiées sur un réseau informatique, le CCB est habilité à identifier l'adresse IP de l'organisation concernée. Il peut ensuite alerter les entreprises et autres organisations sur ces vulnérabilités. Cette attitude proactive permet donc de prévenir les cyberincidents.

Le virus NotPetya a marqué le début des Spear Warnings

Extension graduelle du Early Warning System

Afin de pouvoir réagir plus rapidement et de manière plus ciblée aux menaces numériques, le centre a misé dès 2018 sur le développement de son Early Warning System (EWS). Ce système d'alerte constitue depuis lors le radar technologique de la Belgique en matière de cybersécurité.

Durant cette période, le système a été progressivement étendu, tant en termes de portée que de profondeur. Le CCB a développé une méthodologie pour classer les notifications selon le risque et l'urgence, améliorant ainsi l'efficacité et la confiance dans le système. Le Early Warning System est devenu un élément crucial de la cybersécurité belge.

Quarterly Cyber Threat Report

En plus de fournir des informations en temps réel sur les menaces, le CCB a identifié le besoin de créer un modèle de rapportage structuré pour comprendre les tendances, les vulnérabilités et les risques émergents. C'est ainsi qu'est né le Quarterly Cyber Threat Report (QCTR), un événement trimestriel organisé depuis 2019, au cours duquel le CCB communique de manière transparente sur le contexte des cybermenaces en Belgique aux parties prenantes clés des secteurs critiques, aux décideurs politiques et à d'autres instances concernées. En les informant sur le paysage global des menaces, le CCB les aide à améliorer leur gestion des risques.

Chaque QCTR apporte des informations sur les vecteurs d'attaque dominants, les nouvelles vulnérabilités et les tendances sectorielles (telles que l'augmentation de l'activité dans le secteur des soins de santé ou dans les administrations communales), et des explications en cas d'incidents plus importants. L'objectif est le partage d'informations. À cette fin, le CCB collecte des données à partir des notifications d'incidents, de flux de renseignements internationaux sur les menaces et d'informations provenant de partenaires au sein de l'écosystème, y compris les partenaires commerciaux et les CSIRT.

Directive NIS-1

Entre 2017 et 2020, le CCB a joué un rôle clé dans la transposition de la première directive européenne sur la sécurité des réseaux et de l'information (NIS-1). Cette directive, officiellement adoptée en juillet 2016, a représenté une avancée majeure dans l'amélioration de la cybersécurité dans l'Union européenne. L'objectif était de renforcer la résilience numérique des infrastructures critiques et des services essentiels, de promouvoir la coopération transfrontalière et de garantir la stabilité du marché unique numérique.

Dès la phase préparatoire, le CCB a suivi de près cette trajectoire réglementaire. Dès qu'il est apparu clairement que la directive NIS allait voir le jour, le centre a pris des mesures pour mettre le cadre réglementaire belge en conformité avec les exigences européennes à venir. Pour s'attaquer à cette mission complexe, le CCB a renforcé ses capacités juridiques et techniques.

Outre la représentation active de la Belgique au sein du groupe de coopération européen NIS et du réseau CSIRT, le CCB a été chargé de préparer la législation nationale. Ce parcours a finalement donné lieu à la loi NIS du 7 avril 2019, qui a établi le cadre juridique pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, et à l'arrêté royal qui en a organisé l'exécution.

La mise en œuvre opérationnelle de NIS-1 a été confiée au CCB, qui a créé la Cyber Security Authorities Platform (CySSAP). Cette structure permet d'informer, de conseiller et de coordonner régulièrement les services publics et les autorités sectorielles concernées (telles que la FSMA pour le secteur financier ou l'IBPT pour les postes et télécommunications).

La Belgique a cependant été le dernier État membre de l'UE à transposer la directive NIS-1. La fragmentation du pouvoir de décision entre les différentes parties prenantes a posé des problèmes significatifs, car chaque secteur devait évaluer individuellement l'impact de NIS-1. Face à des défis nouveaux et complexes, certains secteurs ont retardé la mise en œuvre.

Enfin, le CCB a établi un point de signalement des incidents de cybersécurité, conformément à la directive NIS. La mise en œuvre de cette directive a non seulement renforcé le rôle institutionnel du centre, mais elle a aussi créé un nouveau catalyseur pour son développement.

Cette période a douloureusement mis en évidence la nécessité de réévaluer les relations entre le monde de la cybersécurité et les autorités sectorielles. Un remaniement, qui attribuait au CCB le rôle central de surveillance, a abouti à un modèle beaucoup plus performant. La mise en œuvre de NIS-2 allait également en attester plus tard : même si le nombre de secteurs critiques concernés est passé de 7 à 18, la Belgique allait devenir le premier État membre de l'UE à transposer la directive dans sa législation nationale.

Le centre ayant pleinement rempli son rôle, avec un déploiement efficace des ressources et une offre précieuse de services pratiques et d'assistance, les décideurs politiques ont peu à peu réalisé que le CCB était essentiel pour l'écosystème de sécurité en Belgique. De plus, pendant cette période, le centre a également pris l'habitude de lier sa stratégie et ses plans d'action à des budgets de projet clairs. Ce degré élevé de transparence sur le fonctionnement et le financement est resté inchangé jusqu'à présent.

Covid-19 et cyberrisques pour le système de soins

NIS-1 exigeait que chaque secteur identifie une liste des prestataires de services essentiels. En 2019, il a été décidé que le secteur des soins de santé ne comptait pas de tels prestataires, ce qui l'a exempté des obligations de la législation NIS et l'a exclu de la liste prioritaire du CCB.

Cependant, l'émergence de la pandémie de COVID-19 au printemps 2020 a radicalement changé la situation. Les hôpitaux sont devenus des cibles privilégiées des cybercriminels, qui cherchaient à exercer une pression sur le système de santé et à accéder aux données.

L'écosystème de la cybersécurité a apporté une aide collective. Le CCB a soutenu une « coalition de volontaires » composée de prestataires de services IT et cybersécurité, de sociétés de consultance et d'experts indépendants prêts à fournir gratuitement un soutien aux hôpitaux. Via le site Internet wehelpourhospitals.be, les établissements de soins ont pu faire appel à ces partenaires pour obtenir des conseils, une analyse de risques, une réponse à un incident, etc.

"Afin de pouvoir réagir plus rapidement et de manière plus ciblée aux menaces numériques, le centre a misé dès 2018 sur le développement de son Early Warning System (EWS). Ce système d'alerte constitue depuis lors le radar technologique de la Belgique en matière de cybersécurité. "

2020-2024

LA CROISSANCE

Malgré tous les efforts déployés, le nombre d'incidents signalés au CCB a continué d'augmenter fortement. Les rançongiciels, entre autres, ont eu un impact croissant, tant dans le secteur public que privé. À l'échelle mondiale, la cybercriminalité est désormais perçue comme le risque le plus important de dommages financiers majeurs. La mission du CCB reste donc pleinement d'actualité.

En août 2020, le mandat du directeur Miguel De Bruycker et de la directrice adjointe Phédra Clouner a pris fin. Le gouvernement fédéral a décidé de prolonger leurs mandats de cinq ans. Le CCB s'est vu confier la mission de faire évoluer sa vision et sa stratégie face à la menace croissante dans le cyberespace, tout en poursuivant ses missions existantes.

La Stratégie nationale de cybersécurité 2.0

Pour mener à bien cette mission, le CCB a élaboré la stratégie nationale de cybersécurité 2.0. Celle-ci comportait six objectifs stratégiques :

- renforcer l'environnement numérique et la confiance envers l'environnement numérique
- armer les utilisateurs et les gestionnaires IT et de réseaux
- protéger les opérateurs de services essentiels contre toutes les cybermenaces
- réagir à la cybermenace
- améliorer la coopération entre les secteurs public et privé et le monde universitaire
- prendre un engagement international clair

Le directeur général Miguel De Bruycker a présenté les détails de la nouvelle stratégie :

« Dans chaque société, il faut des règles contraignantes, et ce n'est pas différent dans le cyberespace. Nous devons donc trouver un nouvel équilibre entre un Internet totalement ouvert, libre et anonyme et un Internet fiable, dans lequel les règles et les lois nationales restent applicables. Toutefois, tout cela ne doit pas compromettre les possibilités de communiquer de manière libre et anonyme.

Un équilibre entre un cyberespace totalement ouvert et libre et un Internet dans lequel certaines règles juridiques peuvent être appliquées est, à mon avis, tout à fait possible. Trois concepts peuvent améliorer significativement la cybersécurité à moyen et à long terme : Trusted Sender, Trusted Publisher & Spear Warning.

Par exemple, il est possible de s'assurer, au niveau européen, que vous receviez un indicateur de validité lorsque vous accédez à un site Internet qui n'a pas de lien avec une organisation ou une entité enregistrée au niveau national.

La mise en œuvre belge du règlement de l'UE sur la cybersécurité doit être réalisée en priorité afin que notre pays dispose de la National Cybersecurity Certification Authority obligatoire d'ici juin 2021. Les ressources nécessaires pour y parvenir ont été calculées. Moyennant une décision politique, le plan élaboré avec le SPF Économie peut être mis en œuvre. »

La nouvelle stratégie a été approuvée par le gouvernement en 2021. Après avoir ouvert la voie à la création de partenariats et à l'amélioration de la coordination en matière de cybersécurité dans notre pays au cours de ses cinq premières années, et après avoir jeté les bases d'une approche plus intégrée de la sécurité, le CCB a eu pour objectif de développer davantage l'offre de services et de répondre encore davantage aux besoins et menaces concrets.

La volonté explicite des deux directeurs était de rendre la Belgique l'un des pays les moins cybervulnérables de l'UE. Toutes les actions entreprises durant cette période visaient cet objectif. En outre, l'organisation a reçu des responsabilités spécifiques qui ont renforcé son rôle de coordination.

Budget et équipe en hausse

Début 2020, le CCB employait environ 50 collaborateurs et disposait d'un budget annuel de fonctionnement d'environ 15 millions d'euros. Suite à la Cyberstratégie 2.0 et à l'obligation européenne de créer une National Cybersecurity Certification Authority (NCCA), une augmentation de 80 employés et un budget annuel d'environ 36 millions d'euros ont été envisagés.

National Cybersecurity Certification Authority

L'Union européenne s'est engagée dans de nombreux travaux réglementaires visant à renforcer la cybersécurité. En 2019, par exemple, le règlement sur la cybersécurité a été adopté, lequel a jeté les bases d'une certification commune des produits, services et processus ICT. L'UE voulait ainsi accroître la cyberrésilience de tous les États membres et renforcer la qualité et la confiance dans les produits cybersûrs par le biais de normes communes.

Dans chaque État membre, une autorité nationale de certification de cybersécurité (« National Cybersecurity Certification Authority », NCCA) devait superviser la certification et accompagner les entreprises. L'autorité a également pour mandat de publier des lignes directrices en matière de certification au niveau national. En Belgique, cette tâche a été confiée au CCB, qui a renforcé son rôle et élargi ses compétences.

La NCCA contrôle la certification et la conformité aux certificats délivrés par les organismes d'évaluation de la conformité (CABs). Il est aussi possible d'y faire appel en cas de plainte ou d'abus dans la certification des produits. La NCCA est également habilitée à agir pour assurer le respect de la réglementation.

Centre national de coordination de la cybersécurité pour la Belgique (NCC-BE) (2021)

Centre national de coordination de la cybersécurité

Un autre corollaire des initiatives européennes a été la création en 2021 du Centre national de coordination de la cybersécurité pour la Belgique (NCC-BE). L'UE souhaite utiliser les fonds qu'elle met à disposition pour la recherche et l'innovation dans le domaine de la cybersécurité de manière plus coordonnée. L'objectif est d'intégrer les priorités et besoins nationaux dans une approche européenne globale. Dans le même temps, l'UE souhaite mieux informer les chercheurs et les entreprises innovantes sur le soutien financier disponible, afin que les projets transfrontaliers soient plus nombreux. Le NCC-BE encourage le dialogue entre les entreprises, les universitaires, les chercheurs et les pouvoirs publics. Il aligne les politiques en matière de recherche, de développement et d'innovation et contribue à la réalisation de la Stratégie belge de Cybersécurité. Le NCC-BE relie les initiatives existantes et futures en matière de cybersécurité, crée des synergies et soutient les programmes éducatifs. En outre, le NCC-BE veille à ce que les régions, les communautés et l'autorité fédérale unissent leurs forces pour une approche uniforme des cybermenaces. Le NCC-BE soutient aussi les organisations dans l'accès au financement de l'UE et coordonne les investissements stratégiques.

Au niveau européen, le NCC-BE représente la Belgique et veille à ce que les intérêts en matière de cybersécurité de l'administration, de l'industrie et des universités belges soient toujours entendus.

Sous l'égide du Centre européen de compétences en matière de cybersécurité (European Cybersecurity Competence Centre, ECCC), le NCC-BE collabore avec un réseau de 29 centres nationaux de coordination. Cette initiative renforce l'innovation dans le domaine de la cybersécurité, soutient la politique industrielle et contribue à la souveraineté technologique de l'Europe.

Préparation de NIS2

En décembre 2020, la Commission européenne a annoncé la préparation d'une directive NIS-2 pour remplacer et améliorer NIS-1. L'objectif était de renforcer la cybersécurité et d'harmoniser l'approche au sein de l'UE. NIS-1 donnait aux États membres une certaine liberté dans la mise en œuvre des exigences européennes, ce qui a entraîné des interprétations et des variations dans leur application. NIS-2 vise à résoudre ce problème.

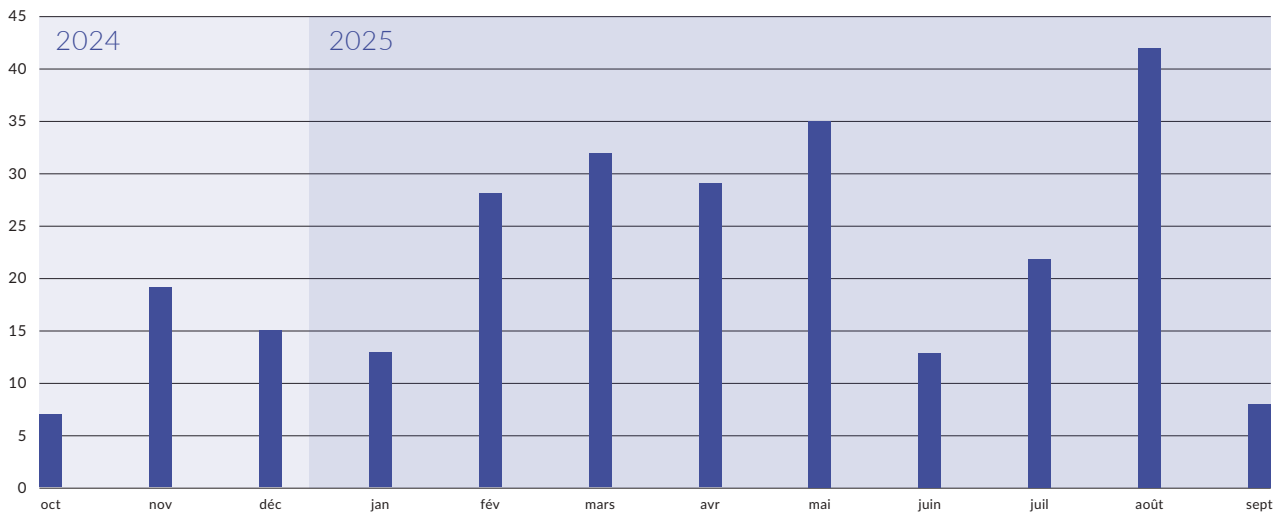
L'un des changements majeurs par rapport à son prédécesseur est l'élargissement du nombre de secteurs soumis aux obligations de NIS-2. En Belgique, NIS-1 concernait plus de 100 entités dans 7 secteurs, tels que l'énergie, les transports, la santé, les infrastructures numériques et les services. Après sa mise en œuvre, NIS-2 s'appliquera à plus de 4 000 entités dans 18 secteurs.

Le CCB a participé au niveau européen à la concertation sur l'interprétation de la réglementation NIS-2. Les travaux parlementaires (la transposition de la directive européenne en droit belge) ont été préparés dans le pays avec les administrations, la plate-forme CySSAP (dans lequel les autorités sectorielles sont représentées) et le niveau politique.

La loi NIS-2 est entrée en vigueur en Belgique en octobre 2024. Grâce à des discussions et préparatifs précoces, le CCB a pu facilement étendre son approche NIS-2, devenant l'organe central pour le suivi et le contrôle du respect de la loi, en collaboration étroite avec les autorités sectorielles.

Le CCB a réalisé un outil d'enregistrement pour les entités NIS-2 via la plateforme existante Safeonweb@work et a développé un système pragmatique de notification des incidents. En effet, la nouvelle directive impose aux organisations de signaler tout incident significatif au CCB immédiatement après sa découverte.

Notifications d'octobre 2024 à septembre 2025



Hack the Government, le tout premier événement de hacking éthique (2024)

Afin d'aider les entreprises à répondre aux exigences de NIS-2, le CyberFundamentals Framework (cadre des CyberFondamentaux ou CyFun®) a été créé. Ce guide pratique propose des mesures de cybersécurité adaptées à différents niveaux de maturité organisationnelle. Ainsi, le framework est également pertinent pour les entreprises et organisations en dehors des secteurs couverts par NIS-2. Le débat public sur NIS-2 a donc renforcé la sensibilisation à la cybersécurité au sein des entreprises belges.

Communication coordonnée des vulnérabilités (CVD)

En Belgique, une procédure légale de déclaration des vulnérabilités est en vigueur depuis 2023. Ce faisant, le CCB peut recevoir des signalements de chercheurs concernant des vulnérabilités potentielles relevant du droit belge. La communication coordonnée des vulnérabilités (CVD) est un processus par lequel les chercheurs, les entreprises et les autorités gèrent de manière structurée et sûre la détection et le rapportage des problèmes de sécurité dans les systèmes, produits ou services IT. L'objectif est de remédier aux vulnérabilités de manière rapide et réfléchie, sans qu'elles soient exploitées prématurément.

En novembre 2024, le CCB a organisé « Hack the Government », le tout premier événement de hacking éthique. Une manière de montrer que les hackers éthiques pouvaient aider à améliorer la cybersécurité en Belgique. Cette initiative sans précédent a rassemblé la communauté des hackers éthiques afin d'identifier les vulnérabilités des sites et systèmes des services publics.

"La volonté explicite des deux directeurs était de rendre la Belgique l'un des pays les moins cybervulnérables de l'UE. Toutes les actions entreprises durant cette période visaient cet objectif. En outre, l'organisation a reçu des responsabilités spécifiques qui ont renforcé son rôle de coordination."

Stop Phishing

Les efforts de prévention de la criminalité par le phishing, dans le cadre de l'approche globale du Belgian Anti-Phishing Shield (BAPS), se sont poursuivis sans relâche. En 2020, un nouveau projet « Stop Phishing » a vu le jour. L'objectif était d'empêcher que des mails ou des SMS contenant un lien malveillant ne parviennent aux citoyens et aux entreprises. Ils étaient interceptés avant même d'entrer dans la boîte mail ou la boîte de réception des SMS.

Ce projet s'est avéré un partenariat public-privé fructueux réunissant les opérateurs concernés, qui a reçu le soutien explicite du gouvernement. Il s'agis-

sait d'une nouvelle étape dans la stratégie proactive et préventive de BAPS. Les autorités ont financé par l'intermédiaire du CCB une partie du logiciel utilisé par les fournisseurs de services participants.

PhishNemo

PhishNemo est une extension du projet BAPS. Initialement développée par la Police judiciaire fédérale (PJF) du Limbourg, cette initiative s'est entre-temps muée en une collaboration entre la PJF et le CCB. Alors que le Belgian Anti-Phishing Shield s'appuie principalement sur les signalements de citoyens, depuis 2023, PhishNemo recherche de manière proactive les noms de domaine suspects qui pourraient être utilisés dans des campagnes de phishing.

Le système effectue un examen approfondi des nouveaux noms de domaine pour détecter des traces d'outils de phishing connus, appelées « empreintes digitales ». Cette méthode permet d'identifier les domaines malveillants avant l'envoi du premier mail de phishing. Les domaines repérés à un stade précoce sont immédiatement ajoutés au système BAPS, permettant leur déviation directe en collaboration avec les fournisseurs d'accès à Internet.

L'acquisition de ce système par la PJF du Limbourg a permis d'étendre davantage le projet. Dans ce cadre, le CCB collabore avec des partenaires privés qui assurent la maintenance des systèmes IT. Voilà comment PhishNemo joue un rôle actif dans le Belgian Anti-Phishing Shield.

Le hacktivisme à son paroxysme après l'invasion de l'Ukraine par la Russie

En février 2022, la Russie a envahi l'Ukraine ; le début d'une longue guerre. Bien que les cybercriminels soient surtout guidés par les gains financiers, il est clair maintenant qu'il existe un lien étroit entre la géopolitique et les cyberattaques. Au vu de ces évolutions dans le paysage géopolitique, le CCB compte aujourd'hui parmi les membres permanents du Conseil national de sécurité.

Cette adhésion à la concertation permanente des services de renseignement et de sécurité a constitué un jalon très important pour l'organisation. Désormais, le CCB est devenu incontournable s'agissant de l'architecture sécuritaire du pays. Grâce à cette adhésion, l'organisation dispose par ailleurs de moyens de fonctionnement supplémentaires provenant de la provision Ukraine.

En pratique également, le choix s'est avéré logique : au fil du temps, le nombre de groupes d'hacktivistes n'a cessé d'augmenter. Parmi leurs modes opératoires favoris figurent les attaques DDoS (Distributed Denial of Service), qui surchargent les sites Internet, et les opérations « hack-and-leak ». Depuis le début de la guerre en Ukraine, force est de constater une augmentation des attaques par rançongiciel contre les communes et les services publics dans plusieurs pays européens, dont la Belgique.

En raison du contexte géopolitique, une vigilance accrue a été nécessaire à l'approche des élections européennes, nationales et régionales de juin 2024, notamment en ce qui concerne les incidents de cybersécurité et l'augmentation des menaces. Les autorités fédérales, régionales et locales ont bénéficié des conseils et du soutien technique du centre. Lors des week-ends électoraux de juin et d'octobre 2024, le CCB a assuré une surveillance continue, avec une équipe d'urgence prête à intervenir.

Du reste, le centre avait déjà réalisé un audit de sécurité lors des scrutins précédents, formulant des recommandations qui ont significativement amélioré la sécurité des systèmes IT pour les élections. C'est en partie grâce à cela que les élections en Belgique n'ont jamais été affectées par des cyberattaques.

CYBERPROTECTION ACTIVE, UNE VISION PROACTIVE

Comme jamais auparavant, la numérisation ouvre le champ des possibles pour les citoyens, les entreprises et les autorités. Cependant, cette numérisation accrue augmente les risques de manière similaire. La cybercriminalité évolue à une vitesse fulgurante, les attaques sont toujours plus sophistiquées et l'impact sur notre société toujours plus grand. Pour contrer cette menace, sécuriser l'environnement numérique est crucial.

Depuis sa création, le CCB considère qu'il est de sa responsabilité de révéler les vulnérabilités (humaines et techniques) et d'agir pour y remédier. Plutôt que de réagir après un incident, le centre privilégie la prévention, la détection rapide et la réponse ciblée.

En 2024, nous avons désigné cette démarche proactive sous le nom de Cyberprotection Active (ACP). Cette idée regroupe une multitude de projets existants et récents qui visent à améliorer la cybersécurité avant qu'un incident ne survienne.

Le CCB a insisté pour que l'ACP soit intégrée dans la directive européenne NIS-2, qui est entrée en vigueur en Belgique en 2024. Cette réglementation contraint les entreprises actives dans une série de secteurs essentiels à adopter des principes de sécurité supplémentaires et à mettre en place des systèmes de gestion des risques.

La directive NIS-2 exige donc une attitude plus active de tous les États membres, tout en imposant la cyberprotection active au rang des exigences légales. La Belgique souhaitant jouer un rôle de pionnier en la matière, l'ACP constitue un pilier central de notre stratégie nationale de cybersécurité. Le CCB concrétise cette notion abstraite par une approche proactive, sur mesure, automatisée et participative :

- **Proactive :** ne pas attendre qu'un incident se produise, mais détecter et éloigner les menaces avant qu'elles ne causent des dégâts.
- **Sur mesure :** pas d'approche unique, c'est du cas par cas. La communication et la réponse sont adaptées aux besoins des organisations et des secteurs spécifiques.
- **Automatisée :** la rapidité d'action est cruciale. L'automatisation permet de réagir plus rapidement et compense le manque aigu d'experts en cybersécurité.
- **Participative :** la cybersécurité est une responsabilité partagée. Les collaborateurs, les partenaires et les citoyens doivent être activement impliqués.

Cette vision s'articule autour de cinq piliers stratégiques, qui constituent un cadre flexible en constante évolution, en fonction des tactiques toujours changeantes des cybercriminels.

PILIER I : AMÉLIORER LA SENSIBILISATION PAR L'IMPLICATION

Une politique forte en matière de cybersécurité commence par la sensibilisation du grand public. C'est, depuis le début, le fil rouge qui guide le CCB. En signalant les messages suspects, les citoyens peuvent contribuer activement à améliorer le niveau de cybersécurité du pays. Les initiatives de Safeonweb visent à armer les citoyens et les entreprises contre les menaces numériques. Voilà indéniablement la base de la vision proactive et, par extension, de la philosophie du CCB.

Pour les citoyens : Safeonweb@home

Safeonweb@home informe les citoyens des dangers actuels via un site Internet, de campagnes et des médias sociaux. L'application Safeonweb joue un rôle central à cet égard : elle avertit rapidement les utilisateurs des attaques de phishing et leur fournit des conseils de sécurité accessibles.

Une autre initiative couronnée de succès qui s'adresse aux citoyens est suspect@safeonweb.be, une adresse mail en quatre langues où ils peuvent envoyer les mails suspects. Rien qu'en 2023, près de 10 millions de mails ont été signalés à cette adresse. Un chiffre impressionnant qui souligne la valeur de la contribution des citoyens dans la lutte contre la cybercriminalité.

82 % de la population connaît Safeonweb

Pour les entreprises : Safeonweb@work

En 2023, Safeonweb@work est venu enrichir les moyens de communication du CCB. Il s'agit d'une plateforme conçue spécifiquement pour les entreprises belges qui regroupe des conseils précis et pratiques pour incorporer la cybersécurité dans leurs opérations de tous les jours, sans avoir à réaliser des investissements importants ou à instaurer des processus compliqués. Un portail en ligne permet aux entreprises d'enregistrer leur domaine et de recevoir automatiquement des alertes sur les vulnérabilités de leur infrastructure IT. La plateforme propose en outre des outils d'auto-évaluation, des lignes directrices de base et les meilleures pratiques dans le domaine, pour permettre aux organisations de renforcer leur niveau de sécurité à leur propre rythme. Le CCB soutient ainsi l'augmentation de la cybermaturité du paysage professionnel.

Campagne Safeonweb@work 2024

PILIER II : DÉTECTER ET SUPPRIMER LES INFRASTRUCTURES CRIMINELLES

Le deuxième pilier se concentre sur le cœur de la cybersécurité : les infrastructures utilisées par les criminels pour lancer des attaques, comme les sites de phishing ou les serveurs malveillants. Avec le projet **Belgian Anti-Phishing Shield (BAPS)**, le CCB vise à s'attaquer à la source de ces pratiques.

En collaboration avec les fournisseurs d'accès Internet belges, les sites Internet nuisibles sont automatiquement identifiés et supprimés, redirigeant immédiatement l'utilisateur vers une page sûre. Chaque jour, cette méthode permet de protéger quelque 100 000 Belges contre les sites Internet potentiellement malveillants.

La vitesse et l'automatisation font la force du système. Les URL malveillantes sont constamment mises à jour et directement intégrées dans les systèmes DNS des fournisseurs, ce qui permet d'intercepter les menaces en temps réel, souvent avant qu'elles ne causent des dommages. Le BAPS est donc l'exemple parfait d'une cyberprotection proactive : discrète en arrière-plan mais avec un impact mesurable.

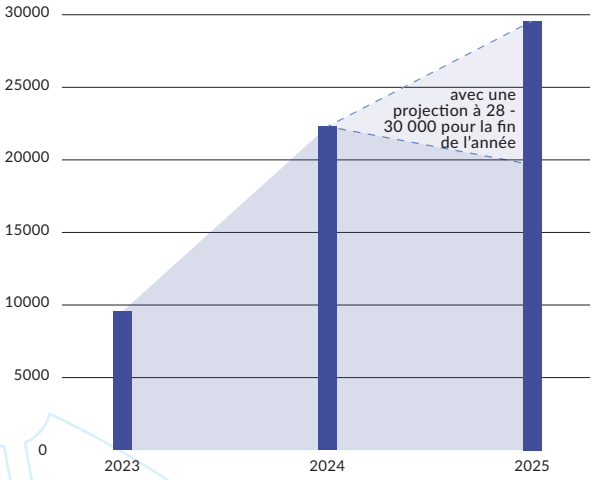
Cette approche n'est d'ailleurs pas passée inaperçue au sein de l'administration publique, du secteur financier et des services de police. Plusieurs organisations ont indiqué disposer de données précieuses dans leur propre domaine, comme des informations sur les boutiques en ligne frauduleuses ou sur la fraude à l'investissement. Elles n'ont toutefois pas la possibilité de rediriger les domaines de manière automatisée et au niveau national.

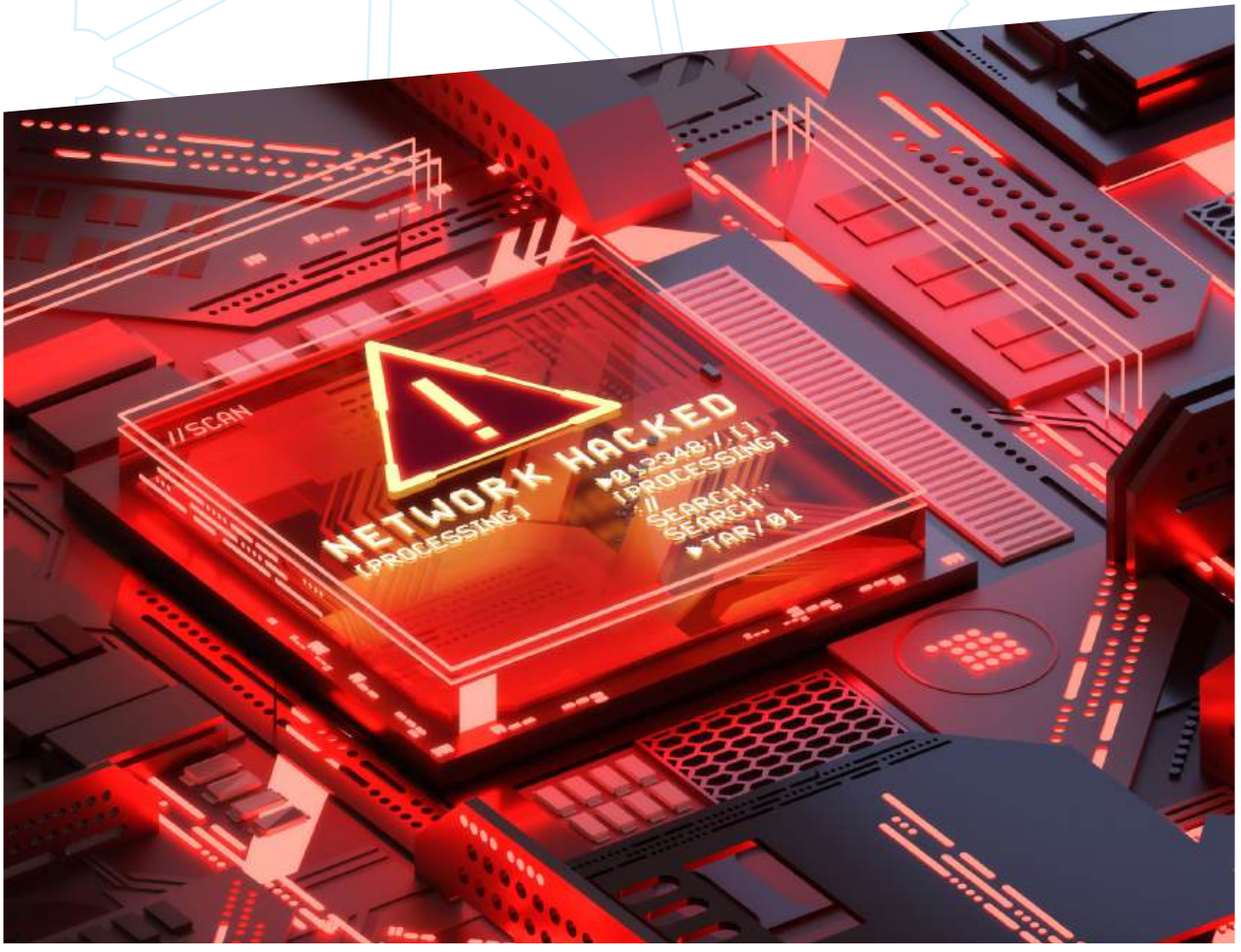
Le CCB a introduit le concept innovant de partenaires de confiance, permettant un accès sélectif et sécurisé au système BAPS à des partenaires soigneusement sélectionnés. Les partenaires fournissent les données, le CCB prend alors en charge le traitement pratique pour dévier les domaines suspects grâce à la collaboration avec les fournisseurs d'accès à Internet. Actuellement, le SPF Économie, la FSMA, Itsme et plusieurs banques belges, entre autres, participent en tant que partenaires de confiance à ce système.

PILIER III : SIGNALER LES MENACES DE MANIÈRE CIBLÉE

Les cybercriminels recourent fréquemment au « spear phishing » : des attaques ciblées contre des personnes spécifiques destinées à obtenir des informations sensibles. Le CCB suit la même approche, mais en faveur de l'utilisateur. Grâce à ces « spear warnings », le centre informe directement les organisations des vulnérabilités de leur environnement numérique.

Évolution chiffres « spear warnings »





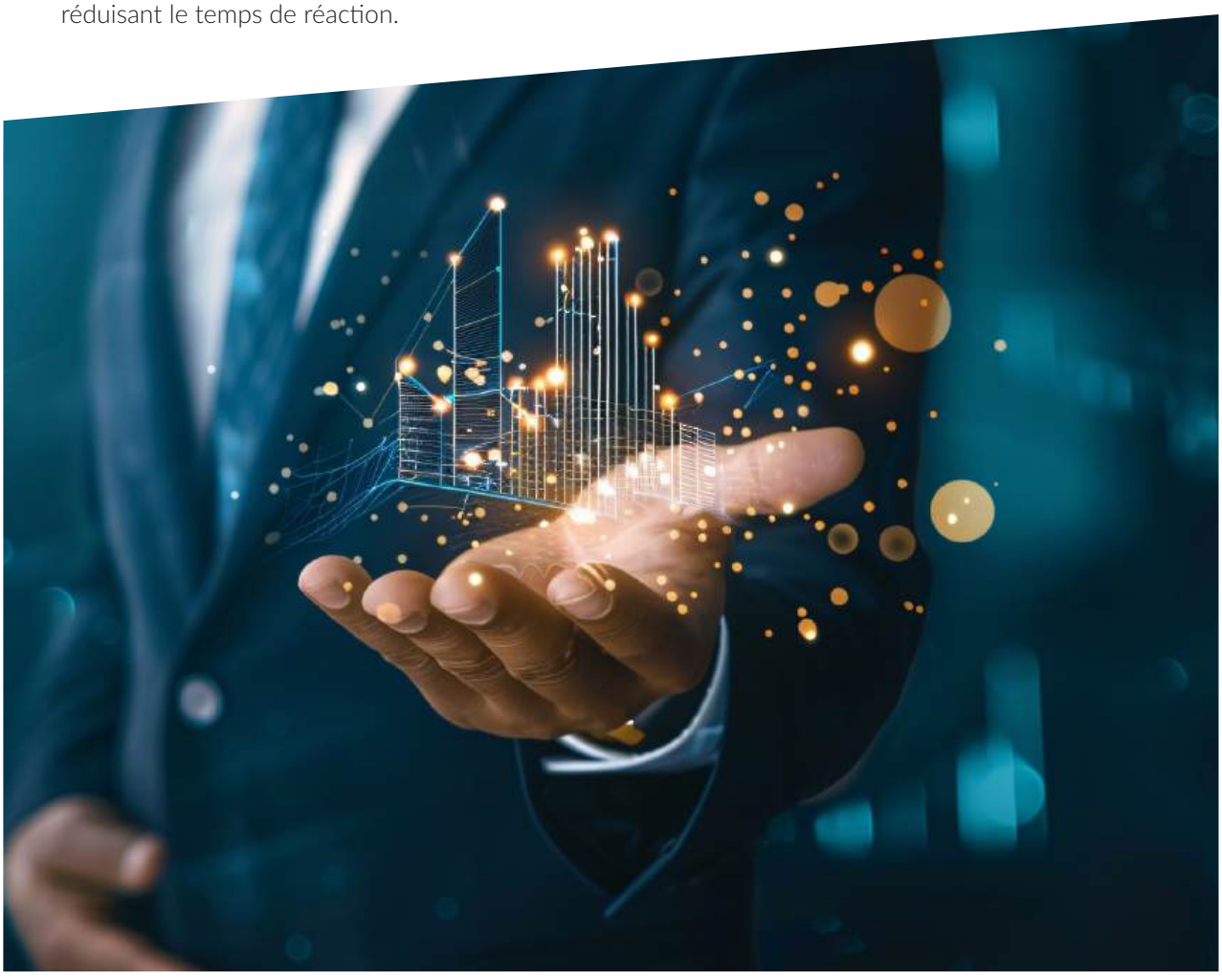
Cette approche permet aux organisations de réagir rapidement et de manière ciblée avant que les cyberpirates n'exploitent une vulnérabilité. L'initiative la plus connue est le « Early Warning System » (EWS), une plateforme ciblant spécifiquement les organisations dont l'infrastructure est critique ou vitale et qui sont soumises aux obligations de la directive NIS-2.

Grâce à ce portail, les analystes du CCB communiquent directement avec ces organisations essentielles. Pour elles, l'EWS fonctionne comme une paire d'yeux supplémentaire : il surveille les signaux numériques, détecte les risques et envoie des alertes de manière proactive. En outre, les organisations reçoivent des notifications personnalisées concernant, entre autres, les fuites de données ou d'informations de connexion et les systèmes peu sécurisés au sein de leur infrastructure.

Cette approche proactive permet d'éviter des incidents, tout en sensibilisant les entreprises et en réduisant le temps de réaction.

PILIER IV : ANCRER LA CYBERSÉCURITÉ AU SEIN DE L'ORGANISATION

Pour devenir réellement résilientes et résistantes, les organisations doivent intégrer la cybersécurité dans leur fonctionnement quotidien. Le CCB a donc développé le CyberFundamentals Framework : un référentiel pratique et évolutif qui aide les entreprises à renforcer progressivement leur protection numérique. Le cadre se compose de quatre niveaux (Small, Basic, Important et Essential), comportant chacun un ensemble de mesures concrètes. Le niveau « Small » guide les très petites organisations qui n'ont pas encore d'expérience en cybersécurité à prendre les premières mesures.



Les mesures des CyberFondamentaux ont été conçues pour contrer efficacement les cyberattaques courantes, leur pertinence étant confirmée par l'analyse des profils d'attaque du CERT. L'efficacité du modèle a entre-temps été prouvée :

- Le niveau « **Basic** » couvre environ 82 % des types d'attaque classiques.
- Pour le niveau « **Important** », ce pourcentage passe à 94 %.
- Les entreprises qui atteignent le niveau « **Essential** » se protègent même contre 100 % de ces attaques.

Le référentiel repose sur des normes internationales telles que NIST, ISO et IEC et est accessible à des organisations de toutes tailles. La certification par un organisme externe est possible, mais pas obligatoire.

Les CyberFondamentaux rendent la cybersécurité concrète, mesurable et accessible, même pour les PME ou les organisations sans département IT. Le modèle s'adapte aux risques, restant pertinent dans un monde numérique en constante évolution.

PILIER V: CRÉER UN ENVIRONNEMENT FIABLE

L'Internet offre une certaine liberté, laquelle permet aussi un certain anonymat. Bien entendu, cet anonymat est une épée à double tranchant. D'une part, il protège notre vie privée et notre liberté d'expression. D'autre part, il ouvre la porte aux abus. C'est précisément pour cette raison que le besoin de transparence et de validation numérique se fait de plus en plus pressant : pour rétablir la confiance et lutter contre les inconvénients de l'anonymat.

La recherche de ce nouvel équilibre entre anonymat et identité n'est pas un exercice facile. Il s'agit essentiellement d'un changement de comportement : les citoyens doivent s'habituer à l'idée que l'identification devient une partie intégrante de leur présence numérique. C'est la seule solution pour améliorer l'attribution et donc la sécurisation des activités en ligne.

"En collaboration avec les fournisseurs d'accès Internet belges, les sites Internet nuisibles sont automatiquement identifiés et supprimés, redirigeant immédiatement l'utilisateur vers une page sûre. Chaque jour, cette méthode permet de protéger quelque 100 000 Belges contre les sites Internet potentiellement malveillants."

Afin de renforcer la confiance des internautes envers les parties avec lesquelles ils sont en contact en ligne, le CCB a développé l'extension de navigateur Safeonweb. Elle affiche un code couleur clair à chaque visite de site Internet :

- **Vert** signifie que le propriétaire du site Internet est validé et donc fiable.
- **Orange** (ou ambre) signifie que le propriétaire est inconnu ou n'est pas validé. Dans ce cas, la prudence est de mise.
- **Rouge** indique un site Internet non sécurisé ou malveillant connu, qu'il est déconseillé de visiter, avec lequel il est préférable de ne pas partager de données.

L'extension a été conçue pour améliorer la sécurité et la facilité d'utilisation. Elle fonctionne automatiquement en arrière-plan et permet de vérifier rapidement si le partage de données personnelles est sécurisé. Ainsi, les surfeurs/utilisateurs peuvent être plus sûrs que le destinataire est fiable.

Le contenu d'un site Internet validé est tout de même suspect ? Dans ce cas, le statut du site changera immédiatement après la première notification, et passera du vert à l'orange, voire au rouge. Ainsi, le système reste à jour et fiable à tout moment.

LE CCB, UNE ORGANISATION POUR TOUS !

SENSIBILISATION : LE DÉFI NUMÉRO 1 DEPUIS LA CRÉATION

Dans les premières années de son existence, le Centre pour la Cybersécurité Belgique s'est heurté à un défi structurel : le spectre de la cybersécurité menaçait toujours plus la Belgique mais le grand public n'en avait pas encore conscience. Les citoyens, les entreprises et même certains services publics sous-estimaient alors le risque.

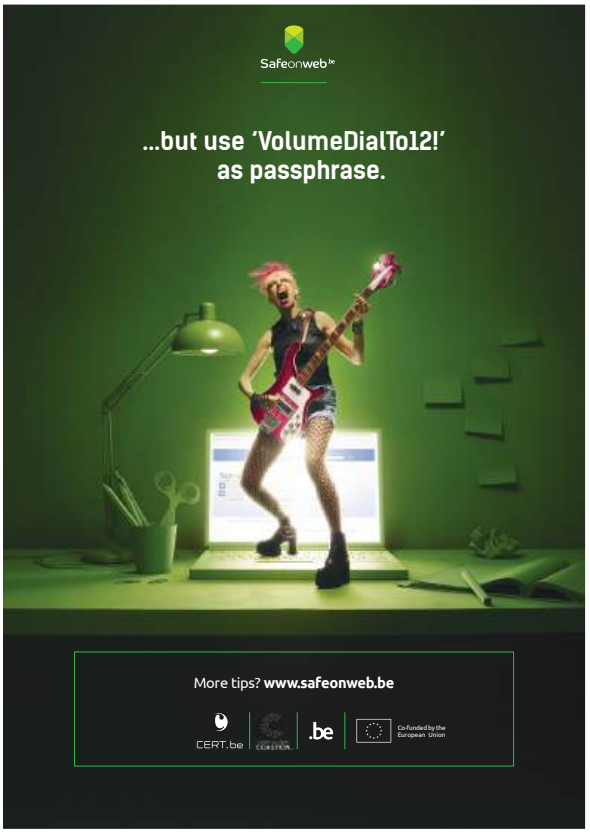
Conscients que la qualité de la sécurité dépend en fin de compte du facteur humain, nous avons décidé non seulement d'investir dans la détection et la réponse aux incidents, mais aussi de mener des campagnes de sensibilisation à grande échelle.

Les premières campagnes se sont concentrées sur des risques concrets : les mails de phishing, les mots de passe peu sûrs, la consultation de liens suspects et la nécessité de mettre régulièrement à jour les logiciels. Pour renforcer l'impact de ces actions, le CCB s'est attelé à mettre en place des collaborations avec des partenaires comme les banques, les entreprises de télécommunications et la Cyber Security Coalition. Les employeurs et les administrations locales ont été spécifiquement contactés pour stimuler la diffusion des informations.

En interne, ces campagnes ont par ailleurs jeté les bases d'une nouvelle manière multidisciplinaire de travailler au sein du CCB. Des spécialistes en communication et des équipes techniques ont collaboré avec des psychologues comportementaux et des spécialistes du marketing pour développer les premières campagnes. Une manière innovante et créative de s'attaquer à la sensibilisation pour une organisation publique !

Partie intégrante de la sensibilisation européenne

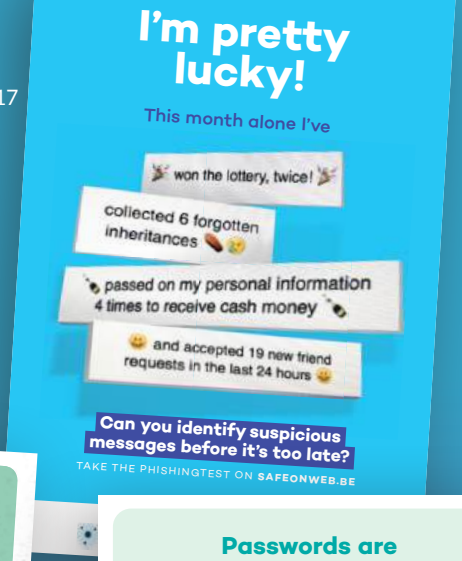
Le CCB organise sa campagne annuelle au mois d'octobre. Et ce choix n'est pas le fruit du hasard. En effet, le mois d'octobre a été désigné « Mois



Safeonweb campagne 2015.

2016

2017



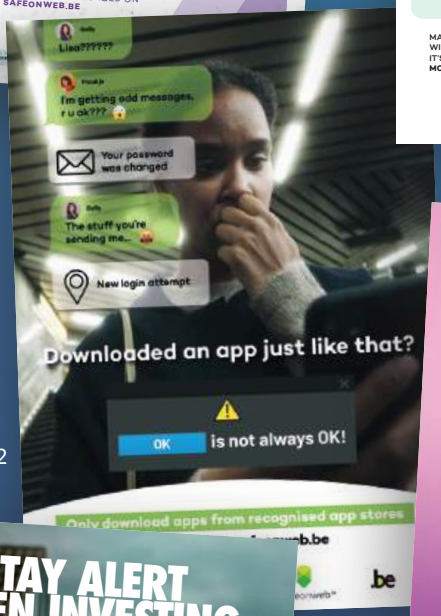
2018

2019

2020

2021

2022



2023

2024
2025

Visuels de campagne au fil des années.

européen de la cybersécurité », une initiative annuelle récurrente de la Commission européenne et de l'ENISA. Cette campagne vise également à améliorer la sensibilisation à la cybersécurité et à informer largement les citoyens et les organisations quant à la manière de renforcer leur sécurité en ligne.

Pour renforcer son impact, le CCB organise également des campagnes d'information intermédiaires, à des moments où les escrocs sont particulièrement actifs : autour des périodes de fêtes et de soldes ou en fonction de l'actualité.

Le centre participe au Safer Internet Day, dédié à la sensibilisation dans le monde qui se déroule chaque année en février et qui vise spécifiquement les écoles et les associations de jeunes.

Enfin, le CCB diffuse et renforce les campagnes des organisations partenaires sur le thème de la cyberprévention.

Les partenaires tendent la main

Le sujet de la campagne annuelle belge est choisi en fonction de l'actualité et des principales tendances. La campagne est déclinée dans les trois langues nationales et implique des acteurs de tous les secteurs.

Cette implication constitue un des points forts des campagnes de sensibilisation : d'une part, le CCB dispose d'une série de partenaires privilégiés comme le SPF Économie, la FSMA, la Police fédérale, Febelfin et la Cyber Security Coalition. Ces organisations font office de caisse de résonance et participent à toutes les étapes du développement de la campagne, tout en donnant leur avis : du choix du sujet, à la traduction, en passant par les images de la campagne ou encore la capacité de convaincre et d'inciter la population à adapter son comportement. Chaque partenaire apporte son savoir-faire et sa connaissance du terrain.

D'autre part, le centre peut également compter sur plus de 600 organisations qui s'engagent à diffuser la campagne. Étant donné que tous ces partenaires relaient la campagne, son impact est bien plus vaste et durable que le plan média payant prévu chaque année.

Une autre force réside dans la philosophie des campagnes, qui adoptent un ton léger, simple et clair. L'objectif est de convaincre le plus grand nombre de personnes qu'elles peuvent faire la différence (même celles qui éprouvent des difficultés en informatique ou qui craignent Internet). Cette approche positive est associée à un message axé sur les solutions, de sorte que la sensibilisation s'accompagne d'une solution concrète qui facilite la vie, comme l'adresse suspect@safeonweb.be. Enfin, les situations choisies permettent au public de s'identifier et sont abordées sur le ton de l'humour, comme la frustration ressentie au moment de trouver des mots de passe longs et complexes.

Résultats tangibles

L'un des principaux résultats de ces dix dernières années est que la plateforme globale Safeonweb.be est devenue une marque reconnaissable en matière de sécurité numérique en Belgique, grâce à des informations et des témoignages clairs et accessibles. Des études ont montré que 82 % de la population utilisait désormais safeonweb.be comme référence en matière de cybersécurité. La notoriété de cette marque a donc dépassé celle du CCB.

44 % des Belges déclarent avoir déjà signalé un mail ou un SMS suspect à suspect@safeonweb.be. Le système reçoit plus de 9 millions de messages par an. L'objectif du CCB est ainsi atteint : impliquer au maximum la population en tant que premier et principal public cible afin d'accroître la cyberrésilience.

LE COURONNEMENT

PRÉSIDENCE EUROPÉENNE 2024

Au premier semestre 2024, la Belgique a présidé le Conseil de l'Union européenne assumant des responsabilités internationales et défendant ses priorités. La cybersécurité a été un point central, offrant à la Belgique l'opportunité de se positionner comme leader mondial dans ce domaine.

Parmi les priorités majeures figuraient les négociations entre le Conseil de l'Union européenne (réunion des ministres compétents), le Parlement européen et la Commission européenne sur deux initiatives législatives : le règlement sur la cybersolidarité (Cyber Solidarity Act) et une modification du règlement sur la cybersécurité (Cybersecurity Act, qui datait de 2019). La délégation belge, composée de la représentation permanente auprès de l'UE et d'experts du CCB, est parvenue à conclure un accord politique sur les deux lois en un temps record, avant même la date butoir des élections européennes de juin 2024.

Le **règlement européen sur la cybersécurité** a jeté les bases d'un système européen de certification des produits, processus et services cybersécurisés en 2019. Grâce à lui, une seule certification est valable dans toute l'Union. Une modification de ce règlement a été votée sous la présidence belge. Il s'agissait notamment d'ajouter au système de certification des fournisseurs de services de sécurité gérés (« managed security services », comme les audits de sécurité, les tests de pénétration ou les réponses aux incidents). Cette certification renforce les garanties de qualité et de fiabilité pour les clients de ces prestataires de services, qui peuvent également vérifier leur chaîne d'approvisionnement.

Le **règlement sur la cybersolidarité** est entré en vigueur début 2025. Il a permis la création d'un système d'alerte européen pour les cybermenaces à grande échelle. Ce système rassemble les compétences des centres de cybersécurité nationaux et transfrontaliers afin de détecter, d'analyser et de contrer les attaques. Cet échange transfrontalier d'informations est fondamental pour pouvoir lutter avec succès contre les opérations cybercriminelles à grande échelle à l'aide d'une approche cohérente.

L'UE a par ailleurs décidé de prévoir dans ce règlement l'élaboration d'un mécanisme commun pour les situations d'urgence. Il s'agit d'actions dans trois domaines :

- une meilleure capacité de réponse dans des secteurs essentiels tels que les finances, l'énergie et les soins de santé. Les organisations de ces secteurs doivent être passées au crible afin de détecter les failles qui pourraient les rendre vulnérables aux cyberattaques.

- la création d'une réserve de cybersécurité de l'UE, composée d'une série de prestataires sélectionnés du secteur privé. Les États membres ou les institutions de l'UE (et même des pays tiers) pourraient faire appel à cette réserve pour faire face à des incidents de grande ampleur. L'ENISA a reçu pour mandat de mettre cela en œuvre au niveau européen au cours de l'été 2025.

- mise en place d'une assistance mutuelle : un État membre touché par un incident de cybersécurité peut donc compter sur le soutien des autres États membres.

Afin de renforcer la coopération entre les différents acteurs au sein des 27 États membres, le CCB a organisé en janvier 2024 le **Brussels Cybersecurity Summit**. Cet événement a réuni l'écosystème de notre pays avec des représentants des écosystèmes de la cybersécurité du reste de l'UE, dans différents domaines d'action : experts techniques, stratégiques et financiers. Les directeurs des autorités nationales et régionales en charge de la cybersécurité se sont par ailleurs réunis à l'occasion d'un sommet informel : une rencontre inédite !

Brussels Cybersecurity Summit (2024)

Un autre accomplissement concerne **EU-CyCLONe**, l'organisation qui fait le lien entre les autorités nationales des États membres pour la gestion d'une cybercrise. La création de cet organe était

inscrite dans la directive NIS-2. Sous la présidence belge, les premières procédures et règles ont été convenues au sein de l'EU-CyCLONe, concernant l'échange d'informations et la coordination des interventions. Ces procédures et le leadership du CCB ont pu être immédiatement mis à l'épreuve lors des élections européennes de 2024 et de « Cyber Europe », l'un des plus grands exercices internationaux de gestion des cyberincidents.

Outre l'EU-CyCLONe, le CCB a également présidé deux autres réseaux européens. Premièrement, le NIS Cooperation Group, qui réunit les États membres afin de concrétiser l'implémentation de la directive NIS-2 et ainsi de garantir des services essentiels dans l'UE. Le CCB a notamment pris l'initiative en faisant de la Belgique le premier État membre à transposer la directive. En outre, pendant 18 mois, le centre a présidé le réseau européen Computer Security Incident Response Team (CSIRT), une plateforme de concertation pour les équipes techniques d'urgence pour les cyberincidents.

Sous l'égide du CCB, une évaluation et un inventaire complets du paysage de la cybersécurité dans l'UE ont également été réalisés. Les conclusions du Conseil sur l'avenir de la cybersécurité, consignées dans un texte intitulé « Implement and Protect Together », ont été formellement adoptées par tous les ministres européens des télécommunications, à l'issue de négociations. Dans ce document, les 27 États membres ont notamment plaidé en faveur d'une réduction de la fragmentation de la législation, d'une clarification des rôles et des responsabilités, d'une coopération plus étroite avec les autorités chargées de faire appliquer la législation et d'une attention accrue à l'Active Cyber Protection. Cela a déplacé de facto l'accent de la politique européenne vers la mise en œuvre plutôt que l'adoption de nouvelles législations confirmant ainsi certaines priorités du CCB au niveau européen.

Reconnaissance internationale

La Belgique a été unanimement saluée à la fin de sa présidence européenne en juin 2024, avec des réalisations notables dans le domaine cyber contribuant à ce succès. L'approche transversale et la manière transparente dont les représentants du CCB ont préparé les dossiers avec la représentation permanente auprès de l'UE ont été fortement appréciées. Leur enthousiasme et leurs efforts pour réunir des experts et des décideurs politiques autour de réalisations concrètes ont porté leurs fruits.

Le CCB est désormais une voix respectée et écoutée sur la scène européenne. Ce qui a suscité un grand intérêt pour la stratégie belge en matière de cybersécurité et pour les différents projets dans le cadre du concept Active Cyber Protection. L'approche pensée par le CCB a ainsi fait tache d'huile :

- l'Union européenne érige le concept de cyberprotection active au rang des meilleures pratiques, et s'inscrit dans le cadre de la réglementation NIS2 (cyberrésilience accrue dans les secteurs critiques et essentiels).
- Dans l'intervalle, plusieurs pays mais aussi des entreprises privées ont mis en œuvre le CyberFundamentals Framework.
- Spear Warnings : plusieurs agences de cybersécurité étudient comment mettre en place un système d'alerte similaire dans leur propre pays.
- Belgian Anti-Phishing Shield : le Royaume-Uni a implémenté un système similaire pour les services publics et l'autorité française de protection des données et le centre de cybersécurité ANSSI étudient quant à eux la mise en place d'une version française ; au niveau européen, il y a un réel intérêt pour un déploiement plus large.

La réputation du CCB est également illustrée par sa communauté mondiale, liée à ses événements en ligne Connect & Share. Depuis 2020, plus de 8 000 professionnels de l'IT et cyberprofessionnels issus

de 70 pays ont pris part à ces séances, qui traitent de sujets à la fois techniques et stratégiques. Les intervenants internationaux sont ravis d'y contribuer.

Distinctions

En dix ans, la Belgique est indéniablement devenue un pionnier en matière de cybersécurité. L'ambition de faire de notre pays l'un des pays les moins cybervulnérables de l'UE a été atteinte. Les études comparatives et les classements internationaux le prouvent.

Grâce au travail et à la coordination du CCB avec ses partenaires nationaux, la Belgique est classée parmi les dix premiers pays dans les indices de cybersécurité renommés, où figurent le National Cyber Security Index (NCSI) et l'Indice de cybersécurité de l'UE. Dans le classement BitSight EU, la Belgique figure dans le top 3.

L'Union internationale des télécommunications (UIT) est l'agence des Nations unies pour les technologies de l'information et de la communication. Dans son Global Cybersecurity Index 2024, la Belgique est présentée comme un modèle de niveau 1 pour l'Europe. Cette étude évalue cinq domaines (réglementation, mesures techniques, organisation, niveau de coopération et développement des capacités). La Belgique obtient une note globale de 96,81 sur 100 et fait mieux que la moyenne européenne et mondiale dans tous les piliers.

Il s'agit d'une reconnaissance internationale des efforts fournis par le centre et l'ensemble de l'écosystème belge de la cybersécurité.

Les campagnes de sensibilisation annuelles belges attirent l'attention internationale: elles ont ainsi remporté en 2022 et 2024 l'European Cybersecurity Award pour la meilleure vidéo de sensibilisation.

En 2023, le projet Spear Warning a remporté un Publica Award

"En dix ans, la Belgique est indéniablement devenue un pionnier en matière de cybersécurité. L'ambition de faire de notre pays l'un des pays les moins cybervulnérables de l'UE est atteinte. Les études comparatives et les classements internationaux le prouvent."

LE CCB DANS LE MONDE

Dix ans après sa création, le CCB reste pleinement engagé face à un défi toujours aussi crucial : garantir la cybersécurité de notre pays, de ses citoyens, de ses entreprises et de ses institutions publiques.

L'environnement numérique évolue à grande vitesse, porté par les avancées technologiques, la montée en puissance des cybercriminels et un contexte géopolitique instable. Ces dynamiques entraînent une hausse constante et marquée des cyberattaques, ainsi que l'émergence continue de nouvelles formes de fraude.

Dans ce paysage en mutation, le CCB joue un rôle central. En tant que centre national de coordination, il assure une veille permanente sur la situation, prêt à réagir rapidement et efficacement face aux menaces

MENACES ACTUELLES VS MENACES « ANCIENNES »

Le paysage de la menace a encore évolué ces dernières années. C'est surtout la manière dont les criminels et les acteurs étatiques gèrent la situation qui a évolué. Nous distinguons trois grands groupes, qui ont chacun leurs propres méthodes.

Quelles sont les menaces ?

LES CYBERCRIMINELS ORGANISÉS

Alors que la cybercriminalité était autrefois principalement l'apanage de hackers individuels, force est de constater aujourd'hui l'émergence de groupes organisés à l'échelle internationale, qui œuvrent selon un business model bien rodé. Les attaques par rançongiciel, qui consistent à chiffrer des données et à ne les restituer qu'après paiement d'une rançon, sont devenues une industrie qui brasse des milliards. Les attaques sont par ailleurs désormais beaucoup plus ciblées.

Une attaque à grande échelle, comme Wannacry, qui a pris en otage des centaines de milliers d'ordinateurs à travers le monde pendant un court laps de temps, est moins fréquente aujourd'hui. Les attaques par rançongiciel sont maintenant mieux préparées et ciblent avec précision une ou plusieurs victimes.

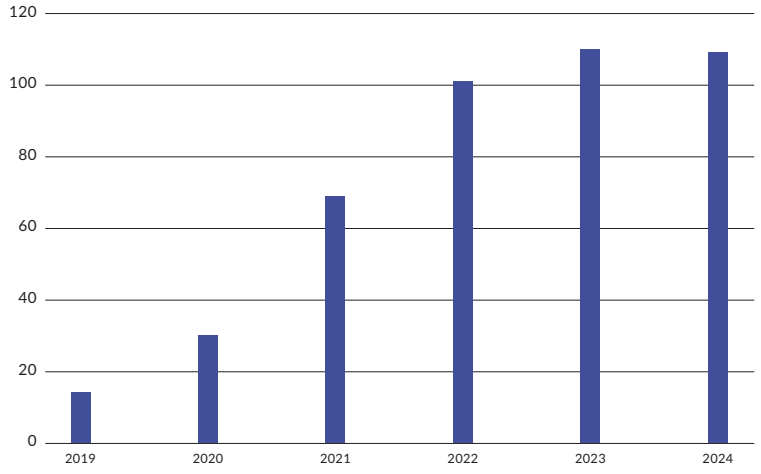
Dans le même temps, l'évolution technologique facilite les attaques par rançongiciel. Le ransomware-as-a-Service (RaaS) est un service par lequel des cybercriminels proposent un package complet de rançongiciel à d'autres criminels. Ainsi, le cyberpirate n'a plus besoin de disposer d'un bagage IT pour parvenir à s'en prendre à une organisation, ce qui augmente la fréquence et la diffusion des attaques.

LES HACKTIVISTES

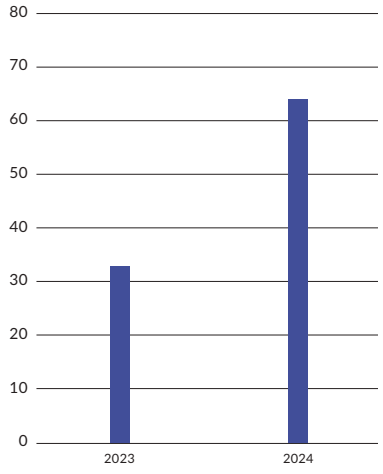
Les hacktivistes lancent des attaques pour des raisons idéologiques ou politiques. Leur action n'est pas guidée par l'appât du gain mais bien par la volonté de perturber les processus démocratiques d'une société ou de faire passer un message.

Dans la plupart des cas, ils ont recours à des attaques DDoS, qui leur permettent de rendre temporairement inaccessibles des sites Internet ou des services en ligne en les surchargeant. Si, à court terme, l'impact est en général limité, la valeur symbolique peut s'avérer importante. Cela dépend surtout de la situation et des tensions géopolitiques, qui entraînent des pics de ce type d'attaques. Le mode opératoire est resté généralement inchangé au fil des ans.

Evolution des attaques par rançongiciel



Evolution des attaques DDoS



LES ACTEURS ÉTATIQUES

Les acteurs étatiques agissent sur ordre ou pour le compte d'un État. L'objectif qu'ils poursuivent est différent de celui des hacktivistes et des groupes criminels. Ils disposent de davantage de ressources, d'une technologie de pointe et opèrent en toute discrétion. Leur objectif est généralement stratégique : exploiter des informations ou technologies sensibles et pénétrer dans des infrastructures critiques.

Bien que le nombre d'incidents visibles semble plutôt limité aujourd'hui, cela ne signifie pas qu'il n'y en a pas. Au contraire, c'est précisément parce que ce type d'attaques passent souvent inaperçues qu'il est difficile d'évaluer leur impact réel. En outre, les acteurs étatiques font parfois appel à des groupes criminels comme couverture, de sorte qu'il n'est pas toujours évident de savoir qui est à l'origine de l'attaque.

Fréquence des attaques : de sporadiques à quotidiennes

Le nombre de cyberincidents a indéniablement augmenté ces dernières années. Alors qu'il y a 20 ans, les attaques par rançongiciel et par phishing faisaient leur apparition à intervalles réguliers, elles sont devenues une réalité quotidienne. Une explication est que les compétences nécessaires pour lancer une attaque sont moindres, ce qui provoque une explosion du nombre d'acteurs.

De plus, les attaques se produisent de plus en plus rapidement, rendant la menace structurellement plus élevée qu'il y a quelques années. Les cyberattaques ne sont donc plus une exception, mais une réalité que toutes les organisations doivent prendre en compte.

Qui est aujourd'hui visé ?

En 2025, de nombreuses cyberattaques sont de nature opportuniste : les criminels recherchent le maillon le plus faible et frappent dès qu'ils en ont l'occasion. Néanmoins, des tendances claires se dessinent. Les services publics, les gestionnaires de réseau et les institutions financières restent une cible privilégiée, non seulement parce qu'ils disposent de données précieuses, mais aussi parce que ce sont des cibles symboliques.

Les instituts de recherche et les entreprises technologiques sont également de plus en plus souvent la cible de vols de propriété intellectuelle, de résultats de recherche sensibles ou de savoir-faire technologique. Les industries et le secteur logistique sont également plus exposés. Les attaques dans ces secteurs peuvent perturber les processus de production et les chaînes d'approvisionnement, ainsi que causer des dommages économiques considérables.

L'informatique comme arme géopolitique

Les tensions géopolitiques se sont répercutées dans le domaine numérique et, en raison de la rivalité croissante entre les blocs de pouvoir internationaux, le nombre de cyberattaques à motivation (géo)politique a sensiblement augmenté. Ce faisant, les États eux-mêmes ont toujours plus recours au cybersabotage et au cyberespionnage dans le cadre de leur politique étrangère, faisant de l'informatique une arme à part entière capable de perturber un pays, de mettre la pression sur des infrastructures critiques et de révéler des informations confidentielles.

Il est frappant de constater que les frontières qui séparent les groupes criminels et les acteurs étatiques sont de plus en plus ténues. Parfois, les criminels agissent pour le compte d'un régime, parfois les États utilisent les réseaux existants pour effacer leurs traces. Il en résulte un paysage de la menace dans lequel la géopolitique et la cybercriminalité sont de plus en plus étroitement liées.

L'impact des nouvelles technologies : IA et informatique quantique

Si les nouvelles technologies constituent une menace, elles offrent également des opportunités. L'IA en est un exemple criant. Par exemple, les criminels ont de plus en plus recours à l'IA pour rendre les mails de phishing plus convaincants, générer de fausses images ou vidéos (« deepfakes ») et automatiser les attaques. L'échelle et la vitesse à laquelle cela se produit rendent la détection plus difficile. Dans le même temps, l'IA peut aussi se révéler un allié : une technologie qui aide à reconnaître les attaques plus rapidement, à comprendre les motifs et à améliorer l'intelligence et l'efficacité des systèmes de défense.

Alors que l'IA constitue avant tout une percée pour les logiciels, la technologie quantique va révolutionner le matériel. Lorsque les ordinateurs quantiques seront au point, leur capacité de calcul sans précédent pourra craquer le codage classique et le chiffrage en un rien de temps. C'est pourquoi les chercheurs travaillent déjà activement à des solutions qui résistent à l'informatique quantique, comme la cryptographie post-quantique. Pour l'instant, il reste difficile de prédire quand cette technologie arrivera à maturité et quelle en sera l'ampleur.

Il faut donc faire preuve de vigilance face aux nouvelles avancées, tout en continuant à investir dans la recherche et l'expertise. Ceux qui parviendront à exploiter à temps la puissance de l'IA et de la technologie quantique prendront une longueur d'avance dans un monde numérique qui ne cesse de s'accélérer.

La Belgique comme pionnière de la sécurité numérique en Europe

La Belgique a beau être un petit pays, elle peut se targuer d'être pionnière en matière de cybersécurité et figurer au premier rang européen dans ce domaine. Et ce n'est pas un hasard : notre force réside dans une approche pragmatique et orientée vers les résultats, là où d'autres pays s'enlisent parfois encore dans des procédures et une bureaucratie sans fin.

> "Les différences entre hier et aujourd'hui ne résident pas tant dans le type d'attaques que dans leur professionnalisation, leur ampleur et leur interconnexion avec des motifs géopolitiques, criminels et idéologiques. Si le monde s'est rendu compte de la force dévastatrice d'une cyberattaque avec WannaCry et NotPetya, force est de constater que les attaques sont désormais plus subtiles et plus ciblées."

Un exemple frappant est la manière dont nous sommes parvenus à transposer la directive NIS2 dans un cadre national. Par ailleurs, le Early Warning System (EWS) que le CCB a mis au point pour détecter et partager rapidement les menaces est aussi une vaste réussite. Et le cadre CyberFundamentals, qui fournit des outils pour une meilleure cyberprotection, suscite un intérêt international.

La cybercriminalité reste un phénomène international par excellence. Une attaque contre notre infrastructure pourrait entraîner des conséquences considérables ailleurs. L'Europe reste donc le cadre principal pour coordonner la lutte contre la cybercriminalité et les menaces numériques. Les projets communs, le partage d'informations et la création de réseaux permettent aux écosystèmes nationaux et régionaux de se renforcer mutuellement. Notre pays choisit délibérément d'endosser le rôle de pionnier sur la scène européenne.

CENTRE FOR
CYBERSECURITY
BELGIUM 10Y

https://ccb.belgium.be