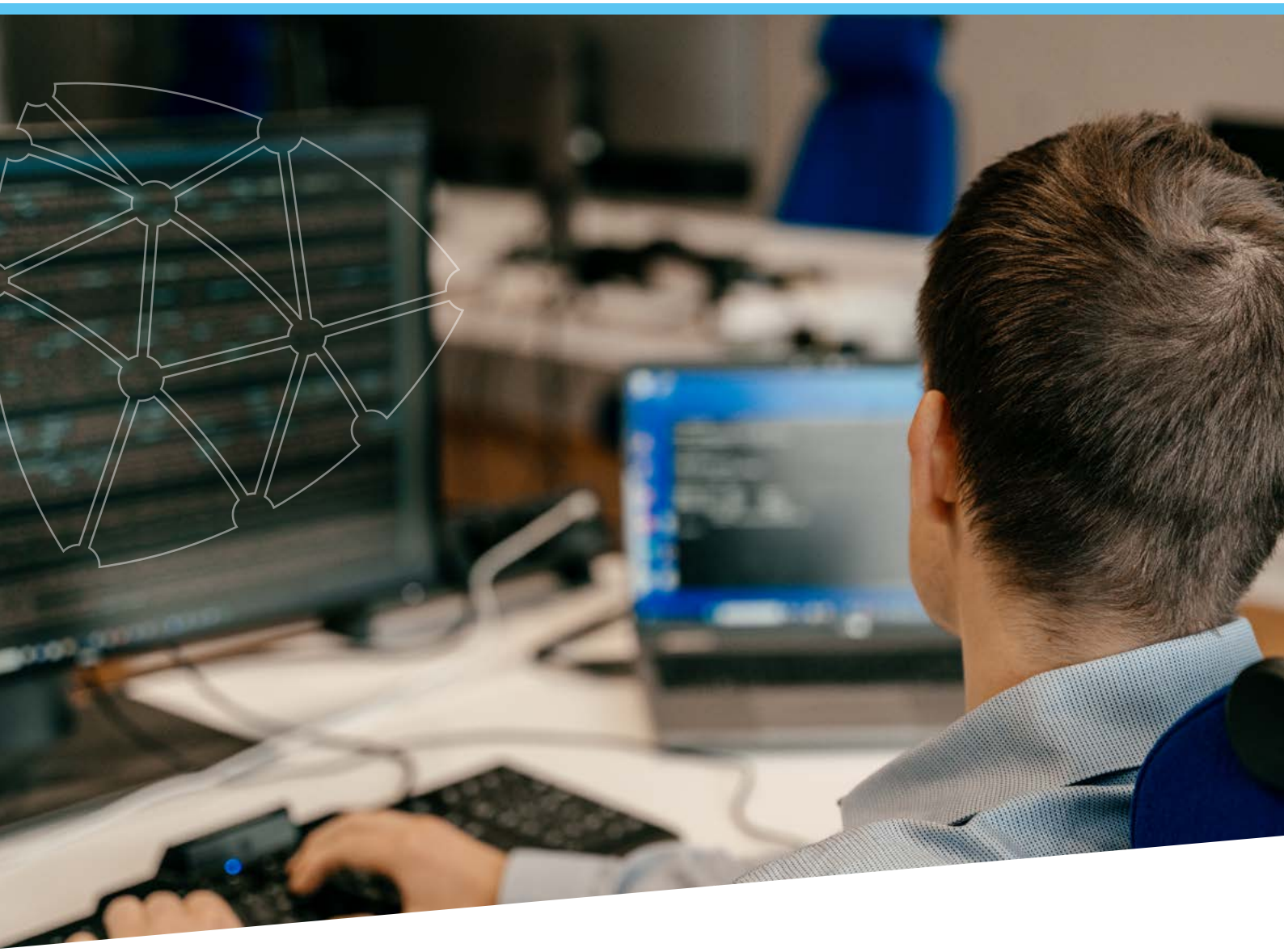
CENTRE FOR
CYBERSECURITY
BELGIUM



MISER SUR LA CYBERSÉCURITÉ

RAPPORT CCB 1/1/2023 - 30/9/2023

Centre for Cybersecurity Belgium
Sous l'autorité du Premier Ministre

Table des matières

Le mot du directeur

Améliorer la cybersécurité nationale et réduire le niveau de vulnérabilité d'un pays est une mission des plus complexes. Le cyberespace est presque entièrement un environnement privé. Dès lors, les autorités rencontrent des difficultés pour sa protection, la détection et la réponse aux menaces et aux incidents.

Comme dans la plupart des pays, le Centre pour la Cybersécurité Belgique (CCB) s'efforce de renforcer la résilience par la collaboration nationale et internationale, les partenariats public-privé, le partage d'informations, le renforcement des capacités et la formation, la sensibilisation, la recherche, la détection et la réponse basées sur l'IA, la cryptographie *Quantum ready*, les exercices nationaux de cybersécurité, etc. Si toutes ces actions sont indispensables et utiles, elles ne sont pas suffisantes. Malgré toutes ces mesures, la cybercriminalité et la fraude en ligne continuent d'augmenter.

Ces mesures semblent être trop générales et, souvent, ne débouchent ni sur des actions, ni sur des résultats concrets et ne sont pas traduites en projets et services de plus petite échelle, plus concrets et plus ciblés. Vous n'êtes marathonien qu'après le dernier kilomètre ! Voici notre ambition au CCB : courir ce dernier kilomètre pour tous ces concepts et initiatives essentiels. Nous voulons nous demander à chaque projet :

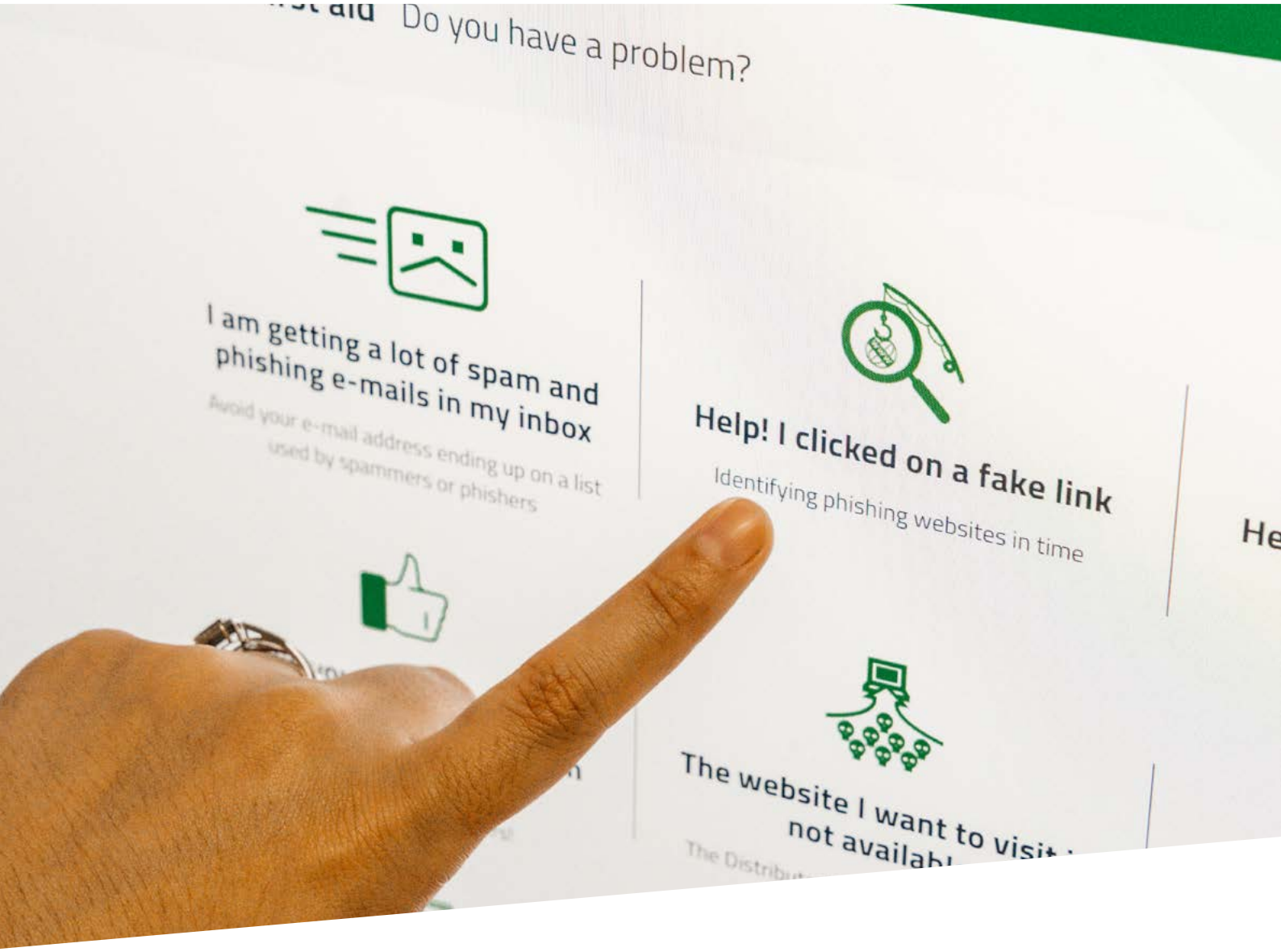
> Quel est l'impact réel sur les citoyens, les entreprises, les autorités ou les infrastructures critiques ?

Pour parvenir à courir ce dernier kilomètre, nous avons mis sur pied une nouvelle initiative : l'Active Cyber Protection (ACP), qui s'articule autour de cinq sous-domaines. Nous voulons impliquer les propriétaires des systèmes ou des comptes menacés, filtrer les communications avec des infrastructures 100% malveillantes au niveau national, faire de la cybersécurité un domaine accessible à toutes les entreprises, identifier les systèmes vulnérables en Belgique et avertir directement leurs propriétaires (*Spear Warning*) et, enfin, contribuer au développement de services validés afin que toute personne recevant des informations via Internet puisse vérifier si l'identité de l'expéditeur a été validée ou non.

Évaluer le paysage des cybermenaces, en constante évolution, et y répondre par des projets concrets en collaboration avec nos partenaires ; telle est la raison d'être du CCB. Nous devons nous assurer que nos partenaires nous voient arriver, courir ce dernier kilomètre pour passer la ligne d'arrivée.

Miguel De Bruycker
Directeur général,
Centre pour la Cybersécurité Belgique

Bruxelles, décembre 2023


Do you have a problem?
I am getting a lot of spam and phishing e-mails in my inbox
Avoid your e-mail address ending up on a list used by spammers or phishers
Help! I clicked on a fake link
Identifying phishing websites in time
The website I want to visit
not availab

PROJETS NATIONAUX ET PRIORITÉS INTERNATIONALES

Grâce à ses projets et initiatives visant à améliorer la cybersécurité et la résilience des institutions publiques, des entreprises, du monde universitaire et des utilisateurs finaux, le Centre pour la Cybersécurité Belgique, en tant qu'autorité nationale de cybersécurité, participe activement à faire de la Belgique l'un des pays européens les moins vulnérables en termes de cybersécurité d'ici 2025.

La présidence tournante du Conseil de l'Union européenne

Du 1er janvier au 30 juin 2024, la Belgique assure la présidence tournante du Conseil de l'UE.

Durant cette période, le CCB assumera ses responsabilités internationales et jouera un rôle de premier plan dans la promotion des priorités belges et du programme de la présidence dans le domaine de la cybersécurité auprès des autres États membres et au-delà, dans le but de promouvoir l'objectif 6 de notre Stratégie nationale de cybersécurité : maintenir l'engagement international clair de la Belgique dans le domaine de la cybersécurité.

LA PRÉSIDENCE ENGENDRE DES OBLIGATIONS ET DES OPPORTUNITÉS

Le CCB assure la présidence tournante de plusieurs réseaux européens officiels de cybersécurité au sein desquels il est le représentant officiellement désigné de la Belgique (tels que le groupe de coopération NIS, le EU Cybercrisis Liaison Network – EU-CyCLONe, et le réseau EU-CSIRTs). Le CCB assurera le suivi des responsabilités légales de ces réseaux, présidera, établira l'ordre du jour et accueillera les réunions de tous ces groupes aux quatre coins de la Belgique afin de mettre en valeur notre pays.

À l'heure où la transposition de la directive NIS2 dans la législation nationale entre dans sa phase finale, une coordination de qualité au sein de tous ces réseaux est essentielle. La Belgique et le CCB ont également pour tâche de finaliser au sein du réseau EU-CyCLONe le premier rapport au Conseil et au Parlement européen.

En cas d'incidents de cybersécurité majeurs, le CCB devra également jouer un rôle majeur dans la coordination de la réponse européenne, tant au sein du réseau CyCLONe que du réseau EU-CSIRTs.

Le CCB jouera également un rôle de premier plan dans les travaux législatifs et politiques menés au sein du groupe de travail du Conseil sur les questions de cybersécurité. Nous soutiendrons les attachés belges au Conseil pour atteindre les objectifs belges et pour faire avancer ou finaliser les travaux sur des dossiers importants tels que la loi sur la cyber-résilience, la loi sur la cyber-solidarité ou les amendements de la loi sur la cybersécurité. Nous les soutiendrons également dans l'organisation d'un bilan européen sur l'état de la politique de cybersécurité de l'UE, qui débouchera sur des conclusions du Conseil sur l'avenir de la cybersécurité.

ET LES ÉLECTIONS

La présidence belge sera marquée non seulement par les élections nationales et régionales, mais aussi par les élections européennes, qui se tiendront du 6 au 9 juin 2024. Compte tenu du contexte géopolitique, ces élections peuvent donner lieu à des événements liés à la cybersécurité ou à des menaces accrues ayant un impact sur l'UE, ce qui nécessitera une coopération renforcée au niveau de la gestion de crise ainsi que sur le plan technique.

NIS 2 : Impact sur les secteurs et entités belges

Afin de faire face à l'expansion du paysage des cybermenaces et à l'émergence de nouveaux défis, l'Union européenne a adopté un nouvel acte législatif concernant des mesures pour un niveau commun élevé de cybersécurité au sein de l'Union (directive 2022/2555 du 14 décembre 2022 – dite « directive NIS2 »), qui remplace la « directive NIS1 » (directive 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union).

La directive NIS2 a introduit des changements importants par rapport à la directive NIS1 : élargissement du spectre des secteurs et des entités couverts, nouvelles méthodes de sélection et d'enregistrement, davantage d'exigences en matière de cybersécurité, nouveaux délais pour la notification des incidents, renforcement des mécanismes de contrôle.

La directive NIS2 vise également à améliorer les capacités et les politiques de cybersécurité nationales. En ce qui concerne les politiques nationales, il s'agit notamment de la stratégie nationale de cybersécurité, des cadres nationaux de gestion des cybercrises, des rôles des autorités compétentes et de la coopération nationale ou internationale.

COORDINATION ET MISE EN ŒUVRE DE LA DIRECTIVE NIS 2

En tant qu'autorité nationale de cybersécurité, le CCB jouera un rôle clé dans la coordination et la mise en œuvre de cette directive. Le CCB assure les tâches d'autorité compétente pour tous les secteurs (en coopération avec les autorités sectorielles potentielles), de CSIRT national, de point de contact unique national, de représentant au sein du groupe de coopération, du réseau CSIRT et du réseau CyCLONe.

En ce qui concerne les mesures de gestion des risques liés à la cybersécurité, les entités essentielles et importantes doivent prendre des mesures techniques, opérationnelles et organisationnelles appropriées et propor-

tionnées pour gérer les risques liés à la sécurité du réseau et des systèmes d'information qu'elles utilisent pour leurs opérations ou pour la fourniture de leurs services et pour prévenir ou minimiser l'impact des incidents sur les destinataires de leurs services. Ces mesures reposent sur une approche tous risques, pour laquelle le CCB a fourni des orientations claires en adoptant le CyberFundamentals Framework. À cette fin, les organisations bénéficieront d'une présomption de conformité si elles obtiennent une certification ou un label CyberFundamentals ou ISO/IEC 27001.

En tant que CSIRT national, le CCB sera informé des incidents importants par des entités NIS afin de limiter la propagation potentielle des incidents, de permettre aux entités de demander de l'aide, de gérer les situations de crise de la meilleure façon possible et de partager les informations techniques pertinentes avec d'autres entités.

Enfin, le CCB, par l'intermédiaire de son service d'inspection (en coopération avec les autorités sectorielles potentielles), jouera également un rôle dans la supervision des entités concernées.

Le CyberFundamentals framework

Dans le domaine de la cybersécurité, il existe des cadres ou « framework » internationaux et diverses normes internationales. Les organisations belges connaissent ces cadres, mais ils sont généralement difficilement applicables à la situation belge spécifique et restent fort généraux. Cela signifie que les mesures que les organisations peuvent prendre doivent être déterminées en fonction des risques, ce qui pose des difficultés spécifiques pour les organisations qui ne disposent pas nécessairement de cyberspécialistes ou qui n'en emploient pas.

Afin de donner corps à la mission de la Stratégie nationale belge de cybersécurité 2.0, laquelle est également du ressort du CCB – à savoir faire de la Belgique l'un des pays les moins cybervulnérables d'Europe d'ici 2025 –, l'Autorité de certification CCB a développé le CyberFundamentals framework, ou « cadre des cyberfondamentaux ».

RÉDUIRE LE RISQUE DE CYBERATTAQUES

Ce cadre vise à protéger nos données, à réduire considérablement le risque de cyberattaques et à accroître la résilience des organisations belges.

Grâce à cette approche holistique basée sur les risques, nous entendons renforcer la confiance dans la numérisation de la société en partageant nos connaissances et en fournissant un aperçu des différentes cybermenaces. Pour ce faire, nous intégrons des données réelles que nous recevons du CERT (Belgian Cyber Emergency Response Team) et nous utilisons ces données, ainsi que d'autres méthodologies, pour valider le cadre.

Le cadre repose sur le NIST-CSF framework, de renommée mondiale, et incorpore divers éléments des normes ISO 27001 et ISO 62443, qui sont largement utilisées en Belgique, ainsi que des éléments du CIS Security Framework. Les fonctions Identify, Protect, Detect, Respond et Recover constituent le fil conducteur du cadre, qui est rédigé sous la forme d'un système d'évaluation de la conformité permettant de démontrer la conformité ou non avec les mesures du cadre.

NIVEAUX D'ASSURANCE

En outre, le cadre respecte les niveaux d'assurance de la loi sur la cybersécurité et comprend trois niveaux d'assurance : « Basic », « Important » et « Essential », assortis d'un niveau initial « Small ». De cette manière, et en partie en incorporant une approche de maturité, le cadre vise à fournir une réponse proportionnée aux besoins des petites et grandes organisations, afin qu'elles puissent améliorer progressivement leur niveau de cybersécurité.

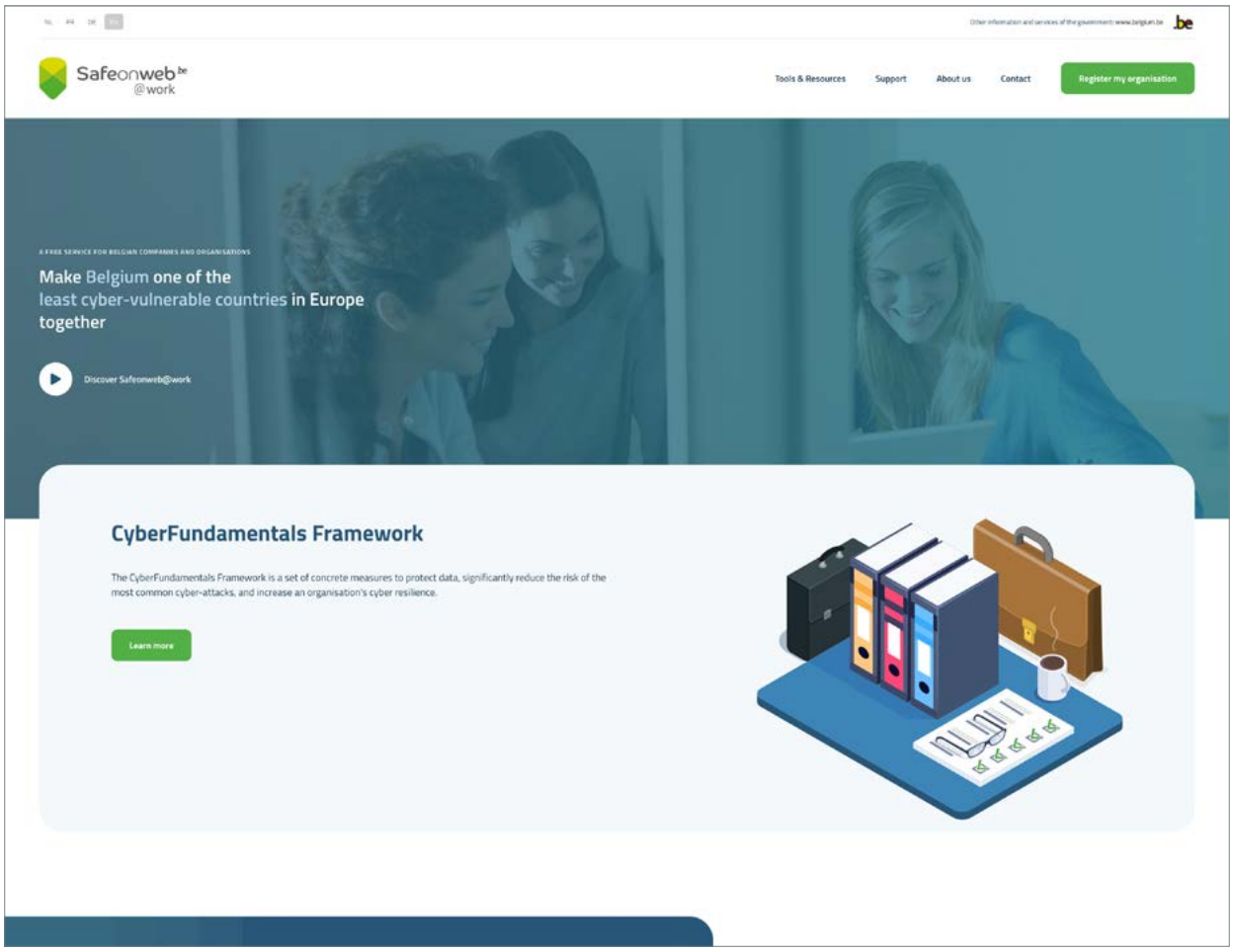
Enfin, pour soutenir la mise en œuvre de ce cadre, le CCB propose plusieurs outils parmi lesquels une analyse de risque pour la détermination du niveau d'assurance requis par la NIS2, ainsi qu'un outil d'auto-évaluation et même une cartographie des différents cadres et normes qui sous-tendent ce cadre.

Le cadre et les outils sont disponibles gratuitement.

www.cyfun.be

Safeonweb @work

Safeonweb@work est une initiative destinée aux organisations et entreprises belges. Son objectif est de renforcer leur niveau de cybersécurité en leur fournissant des conseils, des recommandations et des outils pour leur permettre d'identifier et de réduire les vulnérabilités de leurs systèmes et d'être sensibilisées aux cybermenaces. Grâce à ces différents services, les organisations peuvent mettre en œuvre de manière proactive les mesures appropriées pour réduire de manière significative le risque de cyberattaques, et ainsi participer à notre objectif de faire de la Belgique l'un des pays les moins cybervulnérables d'Europe d'ici 2025.



LES SERVICES SAFEONWEB@WORK INCLUENT :

Cyber Threat Alerts
Un service d'alerte précoce en cas de menaces pour le réseau. Safeonweb@work envoie une alerte spécifique si une vulnérabilité ou une infection a été signalée sur le réseau enregistré sur la plateforme.

Quick Scan Report
Un service permettant de recevoir un rapport offrant une vue d'ensemble des actifs de l'organisation, et identifiant les vulnérabilités potentielles et les recommandations pour y remédier.

Policy templates
Un ensemble de documents de politiques de cybersécurité personnalisables et modifiables pour faciliter la mise en œuvre de la gestion de la sécurité de l'information au sein d'une organisation.

Self-assessment
Un questionnaire d'auto-évaluation permettant de jauger le niveau de maturité d'une organisation en matière de cybersécurité et de recevoir des recommandations pratiques pour combler les lacunes.

Ressources
Actualités, conseils, avertissements, webinaires, recommandations sur les meilleures pratiques en matière de cybersécurité et les principales menaces, ainsi que divers outils visant à améliorer le niveau de cybersécurité d'une organisation.

atwork.safeonweb.be

Extension de navigateur Safeonweb

Le CCB a développé l'extension de navigateur Safeonweb pour aider les citoyens et les organisations à évaluer si l'identité du propriétaire d'un site Internet a été validée ou non. Ces informations permettent d'évaluer la fiabilité du site Internet. L'extension est gratuite et fournit des informations concernant la vérification du propriétaire du site Internet et non son contenu.

COMMENT L'EXTENSION DE NAVIGATEUR SAFEONWEB FONCTIONNE-T-ELLE ?

L'extension attribue un score aux sites web que vous visitez :

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 le propriétaire du site est enregistré sur atwork.safeonweb.be (uniquement pour les organisation belges).

Donc :
- Vous devriez pouvoir continuer à surfer sur ce site Web.
- Il devrait être acceptable de partager des données sur ce site Web.

Orange (!)
scores de 1 à 3 sur 4 : le propriétaire du site Web dispose d'un Certificat « Organisation Validation » ou d'un Certificat « Domain Validation » délivré par une autorité de certification, et le site Web n'est pas enregistré sur atwork.safeonweb.be

Donc :
- Vous devriez pouvoir continuer à surfer sur ce site Web.
- En cas de doute, évitez de partager des données sur ce site Web.

Rouge (X)
score de 0 sur 4 : le site Web ne dispose pas de fonctionnalités de sécurité de base ou est reconnu comme étant malveillant. Le propriétaire du site Web ne possède pas de Certificat et n'a donc pas été validé.

Donc :
- Nous vous déconseillons de naviguer sur ce site Web et de partager des données.

Vous trouverez de plus amples informations sur le projet et sur les instructions d'installation à l'adresse suivante :

- https://safeonweb.be/en/safeonweb-browser-extension
- https://atwork.safeonweb.be/protect-my-organisation/safeonweb-browser-extension

Promouvoir l'innovation en matière de cybersécurité pour les PME belges : Soutien financier à des tiers

Le soutien financier à des tiers (Financial Support for Third Parties, FSTP) est un projet mis en œuvre par le Centre national de coordination - Belgique (National Coordination Centre Belgium, NCC-BE) au sein du CCB. Cette initiative vise à faire valoir les investissements de l'UE, tels que le FSTP, pour permettre aux start-ups, aux PME et aux entreprises de taille moyenne de renforcer leurs capacités en matière de cybersécurité, contribuant ainsi à rendre l'environnement numérique plus sûr.

RENFORCER LA CYBER-RÉSILIENCE DES PME

Le FSTP n'est pas qu'un simple acronyme, c'est votre passeport pour la cyber-résilience.

Connu sous le nom de « financement en cascade », le FSTP est un mécanisme-clé utilisé par la Commission européenne pour soutenir les start-ups et les PME dans la promotion de la cybersécurité. Le NCC-BE utilise le FSTP pour diffuser des solutions de cybersécurité de pointe et renforcer ainsi la cybersécurité de la Belgique.

L'IMPACT DU FSTP : PLUS FORT, PLUS SÛR, PLUS INTELLIGENT !

L'initiative FSTP devrait produire des résultats significatifs qui auront un impact positif sur la cybersécurité en Belgique de la manière suivante :

- Amélioration de la cyber-résilience : Les PME auront davantage accès à des solutions innovantes en matière de cybersécurité, ce qui renforcera leur capacité à faire face à l'évolution des cybermenaces.
- Favorisation de l'innovation : Encourager l'innovation dans le secteur des PME permettra de développer des technologies de pointe en matière de cybersécurité, ce qui améliorera considérablement la capacité de la Belgique à lutter contre les cybermenaces sophistiquées.
- Coopération public-privé : La collaboration entre le NCC-BE et les PME privées améliorera le partage d'informations et favorisera une approche cohérente de la cybersécurité, ce qui profitera à la cyber-résilience globale du pays.
- Croissance économique : En renforçant le niveau de cybersécurité des PME, le programme FSTP contribuera à la croissance économique en protégeant les actifs numériques essentiels et en favorisant un environnement propice aux opérations commerciales.

Le FSTP, initié par le NCC-BE, est essentiel pour que la cybersécurité en Belgique reste alignée sur les objectifs européens en matière de cybersécurité. Pour plus d'informations et d'actualités, n'hésitez pas à suivre les canaux du CCB et du NCC-BE.

Funding & tenders (europa.eu)

PAYSAGE DES CYBERMENACES EN 2023

Le niveau de cybermenace actuel

LE PAYSAGE DES CYBERMENACES MONDIAL

En 2023, le paysage mondial des cybermenaces a été à nouveau marqué par des cyberattaques menées par différents acteurs malveillants, comme des groupes d'hacktivistes, des groupes d'opérateurs de ransomware et des groupes de pirates informatiques parrainés par des États. Si les cybercriminels sont surtout intéressés par les gains financiers, il existe un lien étroit entre la géopolitique et les cyberattaques menées par des hacktivistes et des acteurs parrainés par des États.

Le conflit Ukraine-Russie

Le conflit Ukraine-Russie, qui a débuté en 2022, a réactivé l'hacktivisme et montré que les groupes d'hacktivistes pouvaient représenter une capacité de nuisance importante et un moyen efficace d'attirer l'attention pour soutenir les opérations physiques et idéologiques en période de conflit. En 2023, les agissements des hacktivistes se sont principalement articulés autour du conflit entre l'Ukraine et la Russie. Dès le début du conflit, de nombreux groupes d'hacktivistes sont apparus sur la scène numérique et ont fortement accru leur activité pour soutenir les intérêts et la politique de l'une des parties impliquées dans le conflit. Leurs modes opératoires favoris consistent en des attaques par déni de service distribué (DDoS), l'utilisation de défacements de sites Internet et des opérations de *hack-and-leak*.

Les groupes d'hacktivistes pro-russes ont ciblé l'Ukraine, mais aussi de nombreux autres pays d'Europe, dont la Belgique. Leurs cibles étaient principalement des entités gouvernementales et militaires, mais aussi des organisations des secteurs de l'énergie, du transport (ports et aéroports), de la logistique, des banques, des télécommunications et même des soins de santé. Les attaques ont été menées en représailles au soutien militaire, financier, humanitaire ou politique des pays européens envers l'Ukraine et ont toujours reflété les objectifs stratégiques de la Russie. Hormis l'activité hacktiviste liée au conflit entre l'Ukraine et la Russie, l'hacktivisme s'est également développé dans différentes zones du globe, car ces groupes réagissent constamment à l'évolution des questions politiques et sociétales ainsi qu'aux conflits dans le monde entier. En résumé, les questions politiques et les tensions sociales, ainsi que les conflits en cours dans différentes zones du monde, ont influencé l'activité hacktiviste en 2023.

L'activité cybercriminelle a été influencée par les changements macroéconomiques et a connu des transformations et des développements significatifs en ce qui concerne l'augmentation des capacités et des tactiques utilisées et l'ajout de nouveaux types de cibles, telles que les organismes gouvernementaux, les institutions publiques et les organisations des secteurs critiques.

Ransomware

L'attaque par ransomware est restée l'activité cybercriminelle la plus importante affectant les organisations, y compris les infrastructures critiques, en Europe et aux États-Unis. Les opérateurs de ransomware ont principalement ciblé les secteurs suivants : l'industrie, les logiciels et les technologies de l'information (IT), les soins de santé, l'éducation, les services commerciaux et de conseil, le droit, la finance et le secteur bancaire. Depuis le début de la guerre en Ukraine, nous avons observé une augmentation des attaques par ransomware contre les municipalités et les institutions du secteur public dans les pays européens, y compris la Belgique.

Campagnes APT et cyberespionnage

La géopolitique demeure le principal moteur de développement des campagnes APT (Menace Avancée Persistente), dont l'objectif premier reste le cyberespionnage (exfiltration et collecte de données sensibles). Les attaques APT ont été principalement menées par des groupes de hackers parrainés par des États et ont eu un impact significatif sur les infrastructures ciblées. Tout au long de l'année, les entreprises de cybersécurité et les autorités nationales ont fait état de multiples campagnes de cyberespionnage ciblant principalement l'environnement gouvernemental, mais aussi certains secteurs stratégiques.

Des groupes de hackers bien connus, parrainés par des États, tels que APT 28 (Fancy Bear), APT 29 (Cozy Bear), Emissary Panda, APT 33, Charming Kitten ou Lazarus Group, pour n'en citer que quelques-uns, sont restés actifs au niveau mondial. Des rapports font également état d'une activité intense contre différentes

cibles européennes de la part de nouveaux groupes tels que Storm-0978, signalé par Microsoft, qui a mené une campagne de phishing contre le sommet de l'Organisation du traité de l'Atlantique Nord (OTAN) cette année, ou Storm-0558, un acteur malveillant également repéré par Microsoft, qui cible principalement les agences gouvernementales d'Europe occidentale et se concentre sur l'espionnage, le vol de données et l'accès à des données d'identification. Les acteurs malveillants parrainés par des États ont également développé et déployé de nouveaux outils et de nouvelles capacités contre leurs cibles, afin de maintenir leur mainmise et d'éviter d'être détectés pour atteindre leurs objectifs.

LE PAYSAGE DES CYBERMENACES BELGE

En 2023, si les organisations belges ont été principalement victimes de ransomware et d'attaques DDoS, elles ont également été touchées par d'autres catégories de cyberincidents comme les fraudes au CEO ainsi que les fuites de données sur le dark web et les forums spéciaux sur lesquels sont publiées les données volées et les adresses IP belges compromises lors de cyberopérations.

Ransomware

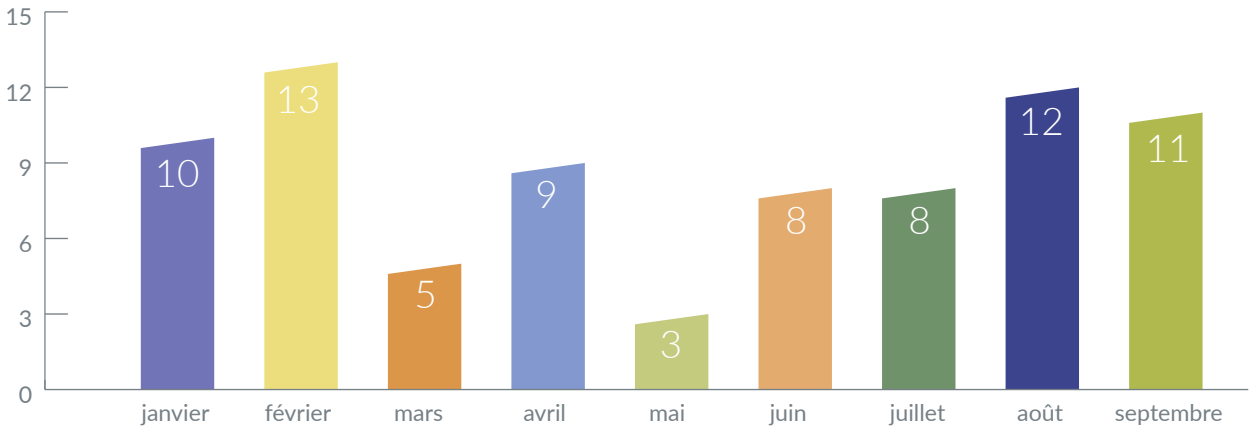
Comme dans d'autres pays européens, le ransomware est resté la cybermenace la plus importante et la plus constante, tant en termes de nombre que d'impact. Les organisations belges ont été attaquées par différents groupes de ransomware, dont les plus connus sont LockBit, Play ou Cl0p.

Selon nos données, c'est LockBit qui a fait le plus grand nombre de victimes belges, ce qui est cohérent avec les opérations du groupe à l'échelle mondiale.

Par ailleurs, l'exploitation massive de la vulnérabilité critique MOVEit par le gang du ransomware Cl0p s'est hissée au sommet de la hiérarchie des acteurs malveillants dans le domaine du ransomware.

Ces attaques ont visé des entités privées et publiques de différents secteurs, notamment les autorités, les administrations locales, les soins de santé, l'industrie, les technologies de l'information, l'alimentation et les boissons. Leur impact a été de faible à élevé en fonction de l'organisation ciblée, de son infrastructure de cybersécurité et des pratiques et politiques en place. Dans certains cas, les cybercriminels se sont livrés à une double extorsion et les attaques par ransomware ont été suivies de fuites de données et de leur exposition sur les Data Leak Site appartenant aux groupes de ransomware. Dans ces situations, l'impact est toujours plus important car les attaques affectent non seulement la disponibilité des infrastructures mais aussi l'image publique des entreprises ciblées. Au cours des trois premiers trimestres de l'année, des entités publiques ou privées en Belgique ont signalé au CCB 79 cas de ransomware.

Attaques par ransomware : Janvier – Septembre 2023



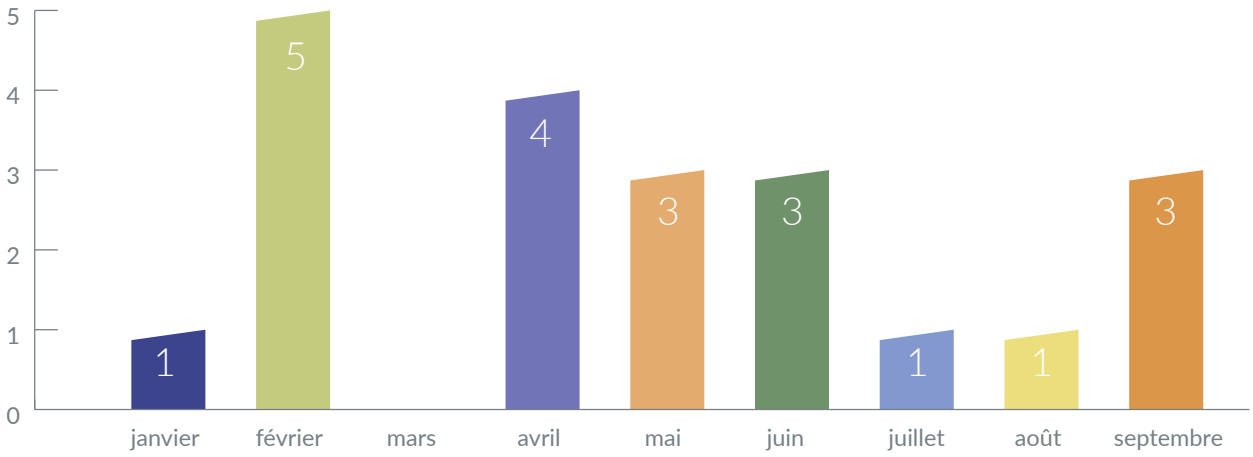
DDoS

Les attaques DDoS menées contre des entités belges ont constitué une menace constante mais de faible impact. Les attaques ont temporairement entravé la disponibilité de certaines ressources ou de certains services des organisations ciblées. En général, les situations ont été gérées correctement et les services sont redevenus disponibles et fonctionnels rapidement. Certaines de ces attaques ont été revendiquées par les groupes d'hacktivistes pro-russes KillNet, NoName057(16) et NET-WORKER ALLIANCE et étaient liées aux positions officielles de l'État belge concernant l'évolution du conflit Ukraine-Russie ou au soutien militaire offert par notre pays à l'Ukraine.

Il est important de préciser que les attaques DDoS menées par les hacktivistes pro-russes sont en général associées à des opérations de désinformation ou des opérations dont le but est d'attirer facilement l'attention des médias. Ainsi, l'indisponibilité apparente de services ou l'impact surestimé de l'attaque pourrait nuire à la réputation de l'entreprise et avoir, à long terme, un effet bien plus grave.

D'autres attaques DDoS, non revendiquées par des groupes hacktivistes pro-russes, ont été menées principalement contre des entités publiques, ce qui porte à 21 le nombre total d'attaques signalées entre janvier et septembre 2023.

Attaques DDoS : Janvier – Septembre 2023



Et en 2024 ?

Les attaques par ransomware resteront l'une des cybermenaces les plus fréquentes et les plus lourdes de conséquences pour la Belgique.

En fonction de l'évolution des conflits en cours et de la situation géopolitique, ainsi que des décisions et des mesures prises par la Belgique, le risque d'attaques DDoS par des groupes d'hacktivistes contre des cibles belges persistera.

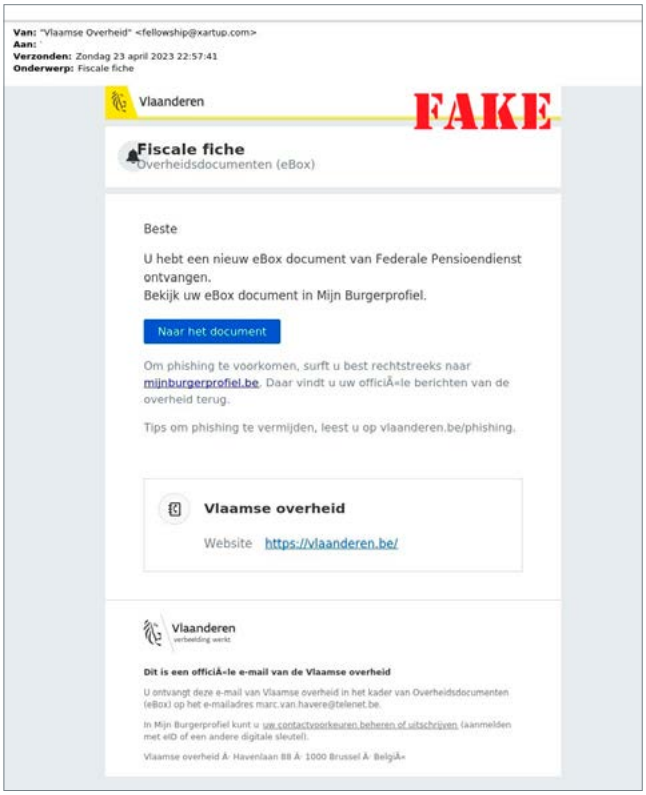
La Belgique restera une cible d'intérêt pour le cyberespionnage, avec Bruxelles comme capitale et abritant de nombreuses entreprises et organisations internationales ainsi que des institutions de l'UE.

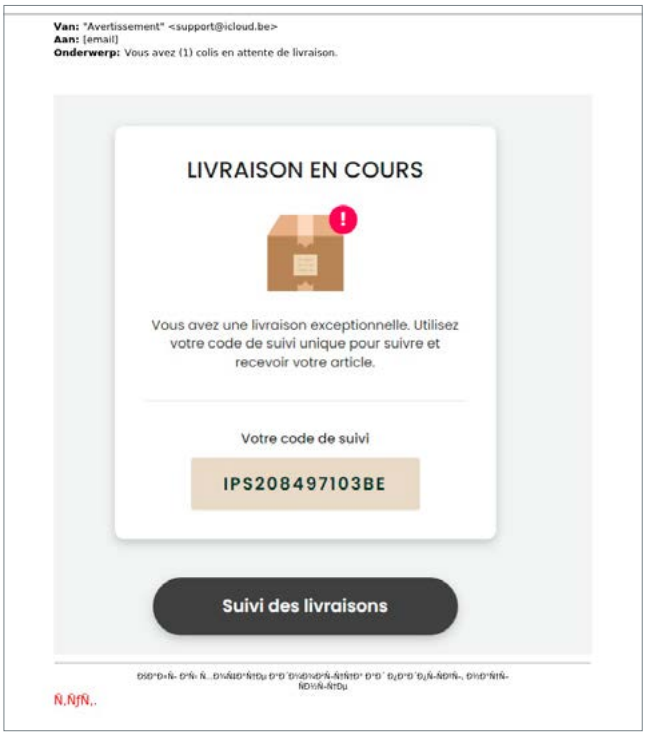
Exemples d'attaques contre des organisations belges : Janvier - Octobre 2023

	Type	Description ou activité
12/03/2023	Ransomware	Une entité active dans le secteur des soins de santé a été touchée par un ransomware
11/05/2023	Ransomware	Une entité active dans le secteur des soins de santé a été victime d'un ransomware
20/06/2023	DDoS	Des pro-russes ont mené une attaque DDoS contre des entités belges du secteur maritime. NoName057(16) est à l'origine de l'attaque.
27/06/2023	DDoS	Le gouvernement fédéral belge a été la cible d'une attaque DDoS
14/07/2023	Ransomware	Une commune belge a été victime d'une cyberattaque
2/08/2023	Ransomware	Une association belge a été victime d'une attaque par ransomware
22/08/2023	Ransomware	Une infrastructure liée à une commune belge a été la cible d'une cyberattaque
24/08/2023	Cyberattaque	Le gouvernement a été touché par une attaque DDoS
12/10/2023	DDoS	NoName057(16) a visé des entités gouvernementales belges en représailles à la promesse d'un soutien militaire et financier à l'Ukraine.

Le projet anti-phishing

Phishing est resté l'un des principaux **vecteurs d'attaque** utilisés par les acteurs malveillants pour installer des logiciels malveillants dans un système ciblé, mais aussi l'un des **types d'attaques les plus utilisés pour voler des données**, telles que des informations personnelles et des données d'identification. Ces données sensibles seront ensuite exploitées pour mener des activités de cyberfraude. Les attaques par phishing s'appuient largement sur des **techniques d'ingénierie sociale** qui reposent sur l'erreur humaine plutôt que sur des vulnérabilités techniques et représentent **un risque à la fois pour les organisations belges et pour les particuliers**.





Van: Proximus <r[redacted]@lureldkq.yangtaie.com>
Datum: 3 november 2023 om 15:03:16 CET
Aan: [redacted]
Onderwerp: Procédez à la conversion de vos points de fidélité avant le 10/11/2023.

Le service clients Proximus

Cher(e) Client(e) ,

Nous tenons à vous informer que depuis votre souscription, vous avez cumulé un total de 61 890 crédits de fidélité. Veuillez noter que ces crédits expireront après le 10 Novembre 2023.

Nous vous invitons donc à **échanger vos points de fidélité** pour vous offrir un **samsung Galaxy S23 gratuit**. Une fois que vous aurez confirmé votre **adresse et payé les frais d'expédition, votre samsung Galaxy S23 sera expédiée.**

En acceptant cette offre, votre compte sera **débité de 55 365 points**. Aucun abonnement ne sera souscrit sans votre accord préalable .

CONFIRMER & CONTINUER

*** Aucun abonnement ne sera souscrit sans votre accord préalable.**

Les sujets et les appâts que les pirates informatiques utilisent dans les messages et les mails de phishing pour voler des données aux victimes belges étaient principalement liés à des sujets d'intérêt pour les citoyens (communications bancaires, colis et autres services postaux) et étaient influencés par le contexte socio-économique, la période de l'année ou les circonstances géopolitiques.

Les acteurs malveillants se sont également très souvent fait passer pour des autorités officielles et des institutions publiques. Bien que certaines tentatives de phishing soient réalisées de manière très professionnelle, de nombreux mails et messages de phishing sont encore faciles à repérer. **Par exemple**, outre les thèmes « traditionnels » liés aux colis, aux rappels finaux pour différents paiements obligatoires, etc. 2023 a vu apparaitre des messages traitant de **subventions énergétiques** et de **contribution fiscale**, tandis que les anciens sujets liés à au COVID-19 sont tombés en désuétude.

L'objectif principal des campagnes de phishing étant de collecter les données des victimes, les **cinq malwares les plus utilisés disposaient de capacités de vol d'informations** : Agent Tesla, xloader, remcos, snake keylogger, Loki password stealer.

Top 10 des familles de malware

Famille de malware	Total
agent tesla	545
xloader	124
remcos	68
snake keylogger	57
loki password stealer (pws)	46
cloudeye	41
blustealer	40
dbatloader	29
upatre	25
ave maria	22

Source : CCB, 2023

Agent Tesla[1], le malware le plus actif en 2023, est un **remote access trojan (RAT)** avancé qui se spécialise dans le vol d'informations sensibles sur les machines infectées (« **infostealer** »). Il est apparu pour la première fois en 2014 et a été largement exploité dans le cadre de campagnes de phishing sur le thème du COVID-19.

Agent Tesla envoie des mails contenant des fichiers *.zip*, *.gz*, *.cab*, *.msi* et *.img*, ainsi que des documents Microsoft Office contenant des macros Visual Basic Application (VBA) malveillantes, afin de compromettre les systèmes ciblés. Ces campagnes de phishing sont connues pour reproduire précisément le ton de communication et l'identité visuelle d'une entreprise légitime, y compris jusque dans l'utilisation des logos et des polices de caractères de ladite entreprise.

Le logiciel malveillant peut collecter différents types de données, notamment les frappes au clavier, les identifiants de connexion utilisés dans les navigateurs internet, les logiciels de messagerie, les profils sans fil et d'autres informations sensibles.

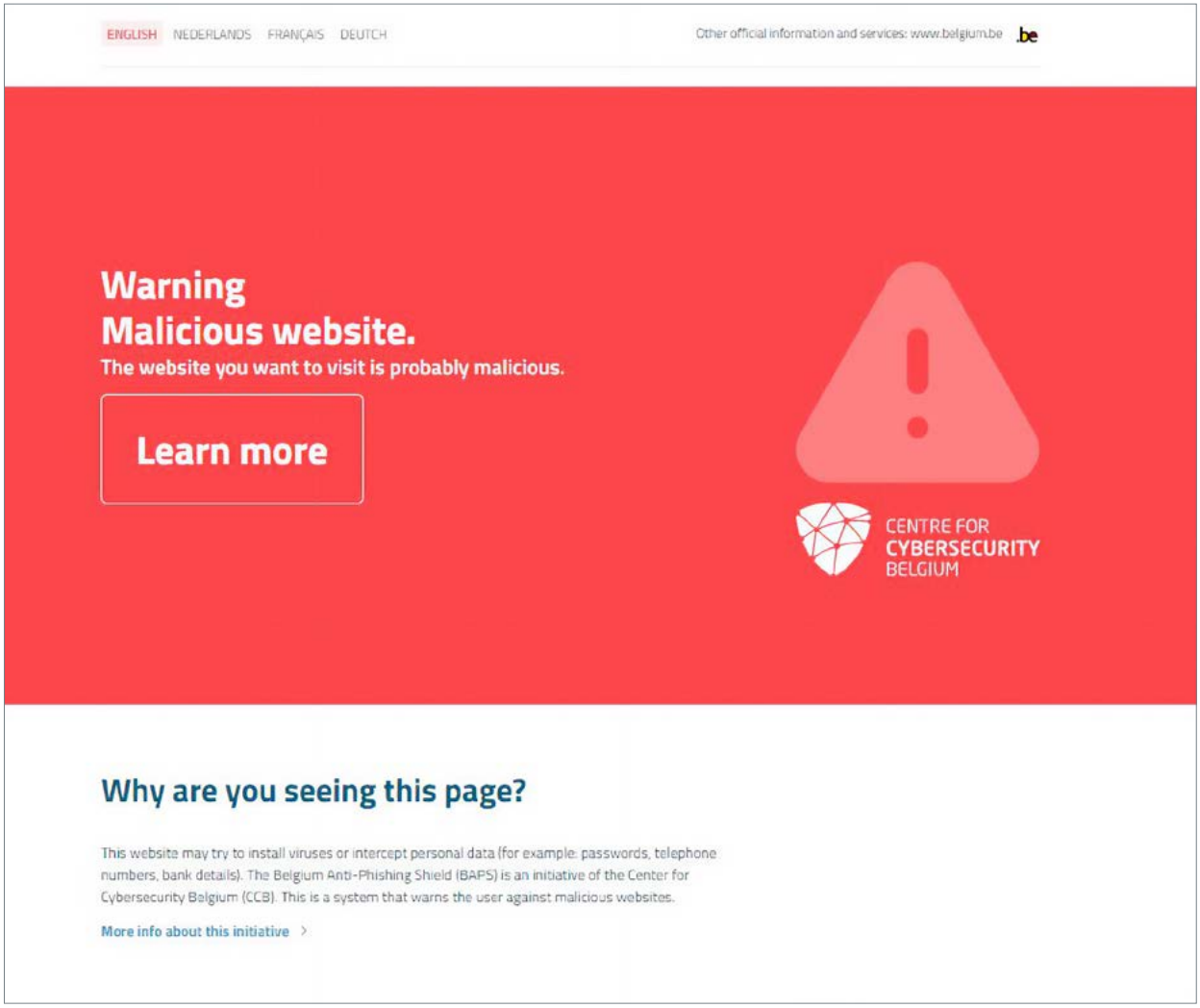
1 https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/agent-tesla
https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/agent-tesla-malware

SAFEONWEB ET LE BELGIAN ANTI-PHISHING SHIELD

Pour aider le public belge à assurer sa sécurité en ligne et à mieux se protéger contre les cybermenaces et les vulnérabilités, le CCB propose un service appelé Safeonweb qui dispense des informations actualisées essentielles et des campagnes d'information spéciales sur un sujet spécifique. La stratégie belge de cybersécurité 2.0 stipule que « L'Internet appartient à tout le monde et est accessible à tout un chacun. Sa sécurité est donc également le fruit d'un effort commun. C'est pourquoi la population est encouragée à prendre activement part à sa sécurisation ».

Safeonweb est un très bon exemple de coopération constructive entre les institutions publiques, les citoyens et le secteur privé, car il offre la possibilité de lutter contre les activités de phishing en signalant les liens et les messages suspects à suspect@safeonweb.be. Sur la base de ce service, le CCB a créé, dans le cadre de l'approche Active Cyber Protection, l'initiative Belgian Anti-Phishing Shield (BAPS), qui met en garde les internautes en Belgique contre les sites Internet dangereux (tels que ceux utilisés lors de tentatives de phishing) et redirige les liens suspects signalés sur notre page d'avertissement.

Au cours des trois premiers trimestres de 2023, plus de 7 millions de messages (7.207.167) ont été envoyés à l'adresse suspect@safeonweb.be, contre près de 4 millions de messages au cours de la même période l'année dernière (3.954.641 en 2022), ce qui témoigne de l'étendue de la portée et de l'engagement civil. Grâce à ces messages, le CCB a pu rediriger 633.361 URL uniques et 163.736 domaines uniques considérés comme malveillants. Entre janvier et septembre 2023, le système BAPS a averti les citoyens belges 5.736.374 fois qu'ils essayaient de consulter un site Internet ou un serveur malveillant.

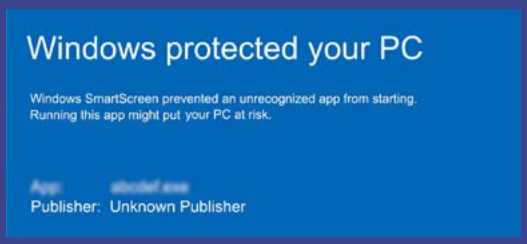


Source : https://baps.safeonweb.be/

Belgisch Anti-Phishing Shield (BAPS)

Comment fonctionne-t-il ?

1. Le CCB reçoit des informations sur des sites Internet potentiellement malveillants lorsque des internautes transmettent des messages suspects à suspect@safeonweb.be.
2. Les pièces jointes et autres liens sont alors extraits des messages suspects. Les URL sont également extraites des captures d'écran et des codes QR.
3. Le bouclier (le « Shield ») analyse l'URL/le lien/la pièce jointe et s'il s'avère qu'il s'agit d'un site malveillant, il est ajouté à la liste de sites malveillants transmise à nos partenaires (tels que les ISP, Google Safe Browsing et Microsoft SmartScreen).



4. Lorsqu'un internaute clique sur un lien menant à un site malveillant, le fournisseur de services Internet concerné compare la requête DNS à la liste des sites malveillants.
5. L'utilisateur est redirigé vers une page d'avertissement et ne peut pas consulter le site malveillant.

Active Cyber Protection – spear warnings

Le Centre pour la Cybersécurité Belgique (CCB) a introduit le concept de Spear Warning début 2021. L'objectif principal des Spear Warnings est d'informer les entreprises et les particuliers d'une cybermenace en temps opportun afin qu'ils puissent agir à temps et éviter une cyberattaque. Le terme « Spear Warning » (SW) est un jeu de mots lié au « Spear Phishing », un mode opératoire utilisé par les cybercriminels consistant à envoyer des mails de phishing très ciblés à des victimes potentielles, généralement dans l'intention de les inciter à fournir des informations personnelles. Les Spear Warnings relèvent également du concept d'Active Cyber Protection (ACP), qui figure désormais dans la directive NIS2 de l'UE.

Le concept de Spear Warning vise à contacter les internautes (entreprises ou utilisateurs finaux) de manière « active », par mail, lettre ou même téléphone (la méthode de contact la plus rapide et la plus efficace en cas de menace imminente). Ils peuvent ainsi être informés à temps et de manière proactive des cybermenaces ou des vulnérabilités. Le fait que ce message personnel émane directement du CCB devrait, en principe, attirer efficacement l'attention.

EMPÊCHER LE CYBERCRIMINEL DE PASSER À L'ACTION

En envoyant des Spear Warnings, le CCB cherche à empêcher l'acteur malveillant d'atteindre ses objectifs, comme compromettre des systèmes, les rendre indisponibles ou exfiltrer des données.

Les Spear Warnings du CCB font souvent partie de campagnes à long terme et concernent principalement :

- des systèmes IT vulnérables connectés à Internet et pouvant être facilement compromis/attaqués/exploités par des cybercriminels ;
- des vulnérabilités critiques qui pourraient avoir un impact sur les organisations belges ;
- des fuites de données d'identification et des accès non autorisés aux données d'entreprises belges mis en vente sur des forums de cybercriminels et pouvant être utilisées pour d'autres campagnes de spear phishing ;
- des systèmes infectés par des logiciels malveillants qui pourraient être utilisés pour une cyberattaque plus importante, comme c'est le cas lorsque des infrastructures belges sont compromises par des logiciels malveillants utilisés comme précurseurs d'attaques par ransomware ;
- des certificats et des enregistrements de domaines suspects ;
- des notifications d'actifs compromis.

LE PROCESSUS

L'une des parties les plus importantes du concept de Spear Warning est la détection des cybermenaces et des vulnérabilités pour l'ensemble du cyberespace belge et c'est l'une des missions principales du CCB. Le CCB utilise diverses techniques pour les « processus de collecte d'informations » : solutions techniques, sources d'information (ouvertes et commerciales) et partenariats. En ce qui concerne les vulnérabilités, le CCB a lancé un projet national de « gestion des vulnérabilités » afin de classer les vulnérabilités par ordre de priorité et de déterminer celles qui feront l'objet d'une alerte Spear Warning. Une fois qu'une vulnérabilité a été sélectionnée, le processus de Spear Warning démarre et permet d'informer les organisations concernées en leur fournissant les éléments suivants :

- une analyse des risques et de l'impact de la vulnérabilité,
- des actions recommandées,
- l'exploitation active par les cybercriminels.

Une autre version du concept de Spear Warning consiste à envoyer des messages automatisés au sujet des vulnérabilités et des infections de l'infrastructure IT aux organisations qui souscrivent à ce service et partagent leur(s) plage(s) IP avec le CCB, car aucune identification d'IP n'est nécessaire dans ce cas. Avec le lancement du projet safeonweb@work, toute entreprise pourra souscrire à ce service.

Parfois, comme dans le cas d'incidents majeurs, les Spear Warnings font partie d'une procédure d'escalade plus large qui comprend également les communiqués de presse, la publication d'avis sur les sites Internet, l'envoi d'alertes par l'intermédiaire d'un système d'alerte précoce et même l'organisation de webinaires spécifiques. Les Spear Warnings contribuent fortement à la mission officielle du CCB de faire de la Belgique l'un des cyberespaces les moins vulnérables de l'UE. En étant mieux informées, les organisations peuvent accroître considérablement leur niveau de cybersécurité. Leurs systèmes IT sont ainsi moins exposés aux attaques des cybercriminels, qui choisissent invariablement la voie de la moindre résistance.

Il arrive souvent que des organisations reçoivent un Spear Warning du CCB et qu'elles admettent ne pas être au courant du problème de sécurité, de la vulnérabilité, de la violation de données ou de l'infection de leurs systèmes IT. Dans certains cas, l'attaque était en cours ou en pleine préparation au moment où la victime a reçu un avertissement du CCB et a donc pu réagir à temps.

Le Centre pour la Cybersécurité Belgique (CCB) est fier d'annoncer qu'il a remporté les Publica Awards dans la catégorie « Security & Safety » avec son projet pionnier « Spear Warning ». Les Publica Awards récompensent l'excellence des projets publics et le CCB est ravi d'avoir remporté cette prestigieuse compétition, qui s'est déroulée à Bruxelles le 16 novembre 2023.

« Nous sommes extrêmement heureux et reconnaissants d'avoir reçu cette récompense des Publica Awards. Ce prix confirme l'impact et le côté innovant du projet Spear Warning. Il montre que des mesures proactives comme celle-ci jouent un rôle crucial dans le renforcement de la résilience numérique de notre société. Nous poursuivrons nos efforts pour améliorer la cybersécurité et protéger nos citoyens et nos entreprises contre les cybermenaces en constante évolution. »

Miguel De Bruycker, Directeur général CCB

SPEAR WARNING – HAFNIUM : LE PREMIER GRAND CAS D'UTILISATION

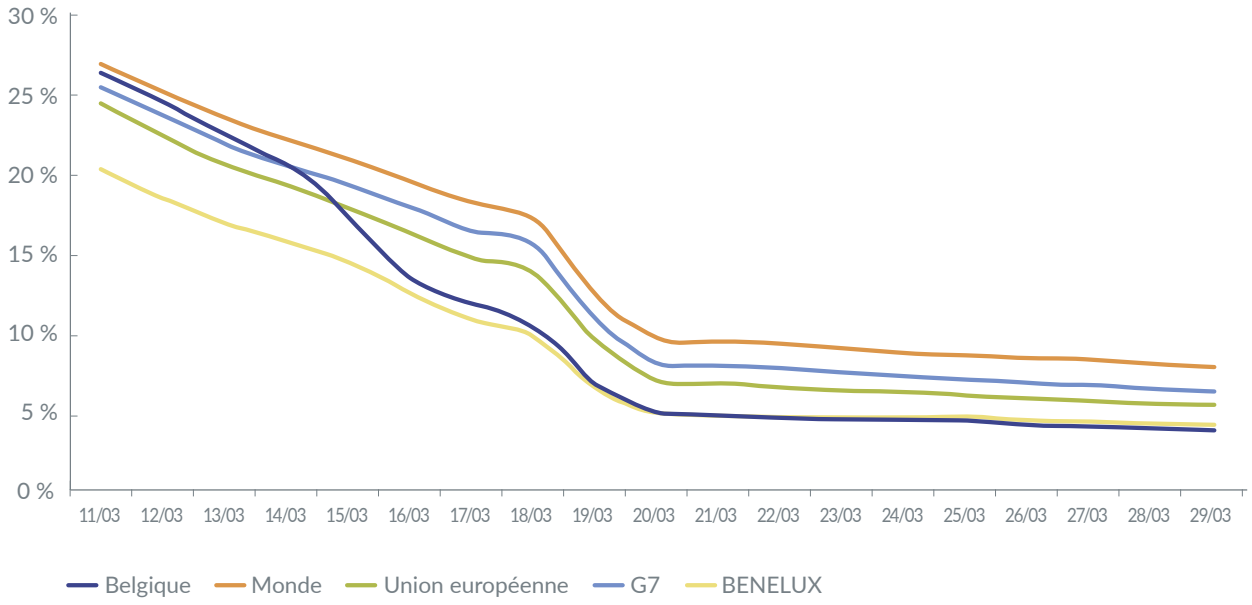
Hafnium. Cet acteur a exploité une faille dans Microsoft Exchange et, à l'époque, un grand nombre d'installations Exchange belges étaient vulnérables et exposées à Internet. La Belgique affichait le pourcentage le plus élevé de systèmes Microsoft Exchange vulnérables et exposés. Cependant, l'introduction du système de Spear Warnings a marqué le début d'une évolution positive. Le premier Spear Warning envoyé aux victimes potentielles a entraîné une réduction notable du nombre de systèmes vulnérables.

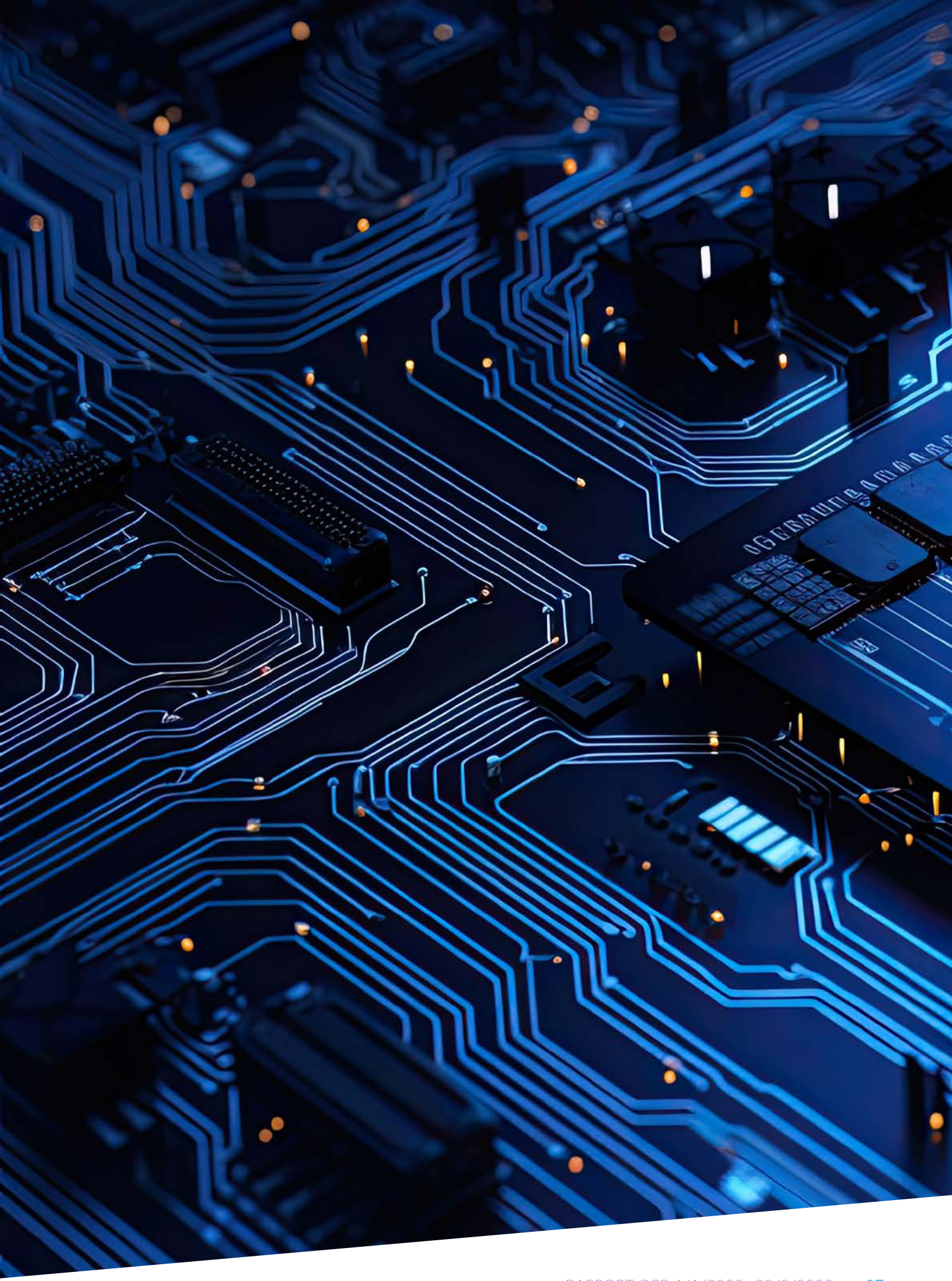
La situation s'est encore améliorée avec le deuxième Spear Warning, ce qui a entraîné un revirement remarquable. La Belgique est passée du plus grand nombre de systèmes vulnérables au plus petit nombre, démontrant ainsi l'efficacité avérée du système de Spear Warnings.

- Planification et direction : Formulation d'un plan stratégique et préparation de l'identification des vulnérabilités ayant l'impact le plus important sur le cyberespace belge.
- Collecte : Réalisation d'un scan complet pour détecter les systèmes vulnérables en Belgique.
- Traitement et exploitation : Identification des propriétaires de ces systèmes vulnérables.
- Analyse et production : Lancement d'une communication pour informer les propriétaires de systèmes de leurs vulnérabilités.
- Diffusion : Après une certaine période, réévaluation des systèmes pour déterminer s'ils restent vulnérables.
- Feedback : Envoi de rappels aux propriétaires des systèmes si nécessaire.

2021

Notifications envoyées à 1259 organisations vulnérables
Notifications envoyées à 355 organisations concernées
Plusieurs rappels ont ensuite été envoyés





VULNÉRABILITÉS CRITIQUES

Vulnérabilités critiques qui ont marqué le paysage des cybermenaces entre janvier et septembre 2023

Des acteurs malveillants ayant des intérêts différents exploitent des vulnérabilités critiques durant leurs attaques. Ils sont de plus en plus rapides pour exploiter les vulnérabilités « zero-day » à leur avantage, ce qui leur permet de devancer les organisations qui doivent mettre à jour leurs mesures de cybersécurité. Il a également été observé que les acteurs malveillants continuent d'exploiter avec succès des vulnérabilités préexistantes dans des logiciels non corrigés lorsque les entreprises appliquent des mesures de sécurité laxistes ou inadéquates.

CVE signifie Common Vulnerability Exposures. Chaque fois que des chercheurs ou des organisations spécialisés en sécurité découvrent de nouvelles vulnérabilités, ils les ajoutent à la liste CVE tenue par la MITRE Corporation. Un numéro d'identification CVE est attribué à la vulnérabilité afin qu'il soit plus facile de l'identifier et de s'en protéger.

Voici cinq des vulnérabilités les plus critiques ayant également été exploitées par des acteurs malveillants en 2023 :

CVE-2023-0669

CVE-2023-0669, une vulnérabilité zero-day dans l'outil GoAnywhere Managed File Transfer (MFT) de Fortra, une plateforme centralisant le contrôle des transferts de fichiers internes et externes, qui a été activement exploitée par des acteurs malveillants, y compris des groupes de ransomware. Cette vulnérabilité permet l'exécution de code malveillant à distance (remote code execution, RCE), ce qui peut compromettre les systèmes affectés ou entrainer de vastes violations de données et des extorsions financières. Le logiciel de transfert de fichiers géré d'une victime peut être utilisé pour infecter d'autres victimes en envoyant des fichiers malveillants et une intrusion réussie pourrait conduire à une attaque massive de la chaîne d'approvisionnement. Le groupe de ransomware Clop a spécifiquement ciblé environ 490 000 personnes, compromettant leurs informations personnelles grâce à l'exploitation de cette vulnérabilité.

CVE-2023-2868

La vulnérabilité CVE-2023-2868 dans les dispositifs Barracuda Email Security Gateway permet aux entrées utilisateur d'être exécutées en tant que commande système, ce qui donne aux cyberpirates la possibilité de manipuler à distance les commandes système avec des privilèges potentiellement élevés. La faille a été exploitée lors de vastes campagnes, depuis octobre 2022 jusqu'à mai 2023, par un acteur malveillant hautement qualifié, repéré par Mandiant sous le nom de UNC4841. Près d'un tiers des organisations touchées identifiées étaient des agences gouvernementales réparties dans toutes les régions. Mandiant estime qu'il s'agit d'une activité liée à la Chine et que, d'après le profil de ciblage observé, il pourrait s'agir d'une campagne d'espionnage.

CVE-2023-34362

CVE-2023-34362 est une vulnérabilité zero-day critique dans MOVEit Transfer, une solution de transfert de fichiers. Cette vulnérabilité, qui peut entraîner une élévation des privilèges et un accès non autorisé à l'environnement, a été exploitée massivement par le groupe de ransomware Cl0p pour voler des données aux organisations ciblées. Les auteurs du ransomware Cl0p ont affirmé avoir eu accès aux informations de « centaines » d'entreprises utilisant le logiciel MOVEit et ont commencé à dresser la liste des victimes sur leur Data Leak Site (DLS).

CVE-2023-23397

Une autre vulnérabilité très exploitée par les acteurs malveillants est la CVE-2023-23397, une vulnérabilité critique d'augmentation des privilèges dans toutes les versions prises en charge du client de messagerie Microsoft Outlook pour Windows. Cette faille permet aux acteurs malveillants de contourner les mesures d'authentification, facilitant ainsi l'accès non autorisé à des données confidentielles et permettant l'usurpation d'identité d'utilisateurs au sein des organisations ciblées.

CVE-2023-38831

CVE-2023-38831 est une faille de sécurité dans l'outil d'archivage WinRAR pour Windows, qui permet aux cyberpirates d'exécuter un code arbitraire lorsqu'un utilisateur tente de visualiser un fichier anodin dans une archive ZIP. Cette vulnérabilité a été largement exploitée par des organisations cybercriminelles et des acteurs malveillants parrainés par des États, comme APT 28, Sandworm, DarkPink ou encore APT40 afin de réaliser une exploitation de code à distance.

Le CCB publie toujours des avis techniques, avertissant de l'exploitation possible des vulnérabilités et recommandant les actions recommendées pour réduire les risques, y compris l'application de correctifs.

Dans le cas de vulnérabilités critiques présentant un risque élevé d'impact sur la Belgique, le CCB émet des Spear Warnings, informant directement les organisations belges de la menace et de la nécessité urgente d'appliquer des correctifs. Cette approche proactive permet de protéger les victimes belges et de prévenir avec succès les attaques imminentes, telles que les attaques par ransomware utilisant des vulnérabilités exploitables.

Aperçu des Belgium Cyber Metrics en 2023

2023	Q1	Q2	Q3
PHISHING			
Mails reçus	2.695.345	2.381.106	2.130.716
URL uniques qualifiées de malveillantes	186.792	237.740	211.031
Domaines uniques qualifiés de malveillants	12.382	93.481	59.727
BAPS			
Nombre de visites sur la page d'avertissement	2.031.888	2.464.489	1.239.997
WAARSCHUWINGEN			
Avis techniques publiés sur www.cert.be	35	39	41
Tweets techniques	67	67	79
Spear warnings			
Traités automatiquement	1.193	863	1.221
Traités manuellement	1.653	946	1.255
Total	2.846	1.809	2.476
INCIDENTS			
Ransomware (signalés)	28	20	31
Denial of Service	6	10	5
COMMUNICATION			
Websites			
Sessions www.safeonweb.be	674.243	615.379	450.365
Actus sur Safeonweb	22	19	16
Événements CCB			
Évènements Connect & Share	2	2	0

BELGIUM CYBER METRICS EN 2023

Sensibiliser et construire une communauté solide d'experts en cybersécurité

Dans le cadre de l'initiative Connect & Share du CCB, qui vise à sensibiliser et à construire une communauté en réunissant des professionnels de la cybersécurité pour partager leurs réflexions sur les différentes cybermenaces en Belgique et dans le monde, plusieurs événements ont été organisés en 2023, avec une forte participation, en présentiel ou en version hybride :

12 JANVIER 2023 – ÉVÉNEMENT QUARTERLY CYBER THREAT REPORT Q4 2022

Les experts du CCB, en collaboration avec des experts d'entreprises spécialisées dans la cybersécurité, ont examiné le paysage de la cybermenace en mettant l'accent sur la sécurité du cloud et le secteur de l'énergie.

19 JANVIER 2023 – ÉVÉNEMENT ICS RAPID RESPONSE

Cet événement, organisé par SANS et le CCB, a permis à des spécialistes ICS expérimentés, ainsi qu'à des non-spécialistes ICS, d'assister à des présentations sur une série de sujets, incluant par exemple : Cinq contrôles critiques, Architecture défendable, Visibilité OT, Threat Intelligence et OSINT.

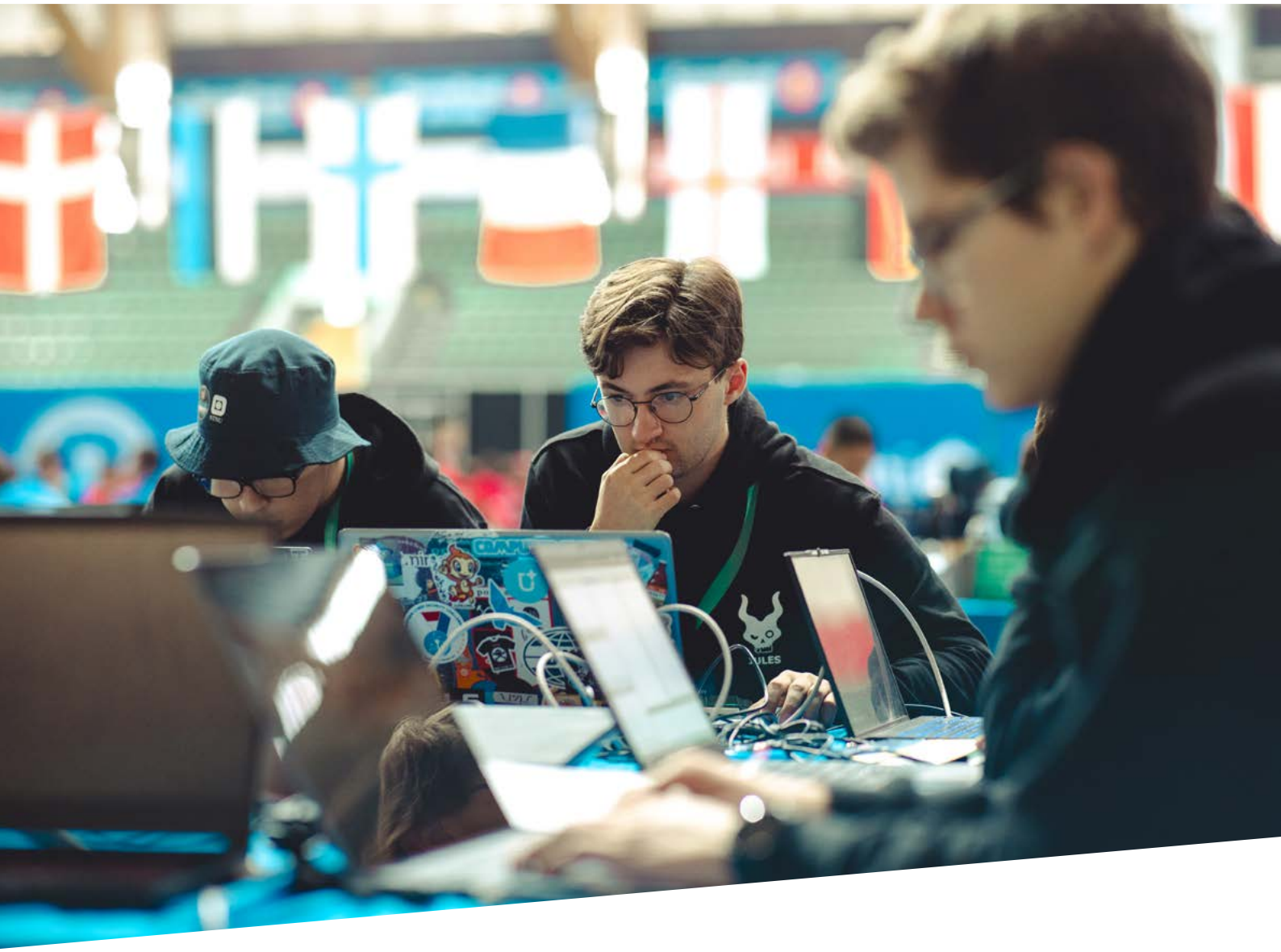
20 AVRIL 2023 – ÉVÉNEMENT QUARTERLY CYBER THREAT REPORT Q1 2023

Le CCB a organisé un nouvel événement pour passer en revue les observations du premier trimestre 2023 et discuter de sujets tels que les attaques DDoS, la sécurité Wi-Fi, les logiciels malveillants et les dernières observations en matière d'espionnage et d'hacktivisme. Ce fut également l'occasion pour les experts de partager leurs dernières recherches.

25 MAI 2023 – 11e EU MITRE ATT&CK® COMMUNITY WORKSHOP

Le CCB a co-organisé un événement hybride avec MITRE Engenuity pour présenter des mises à jour sur l'utilisation du cadre ATT&CK® pour faire progresser la défense basée sur les menaces. Des experts du CCB, de MITRE Engenuity et d'autres développeurs de systèmes et d'outils soutenant le cadre ATT&CK® ont fait des présentations lors de l'événement.

CONNECT & SHARE EVENTS



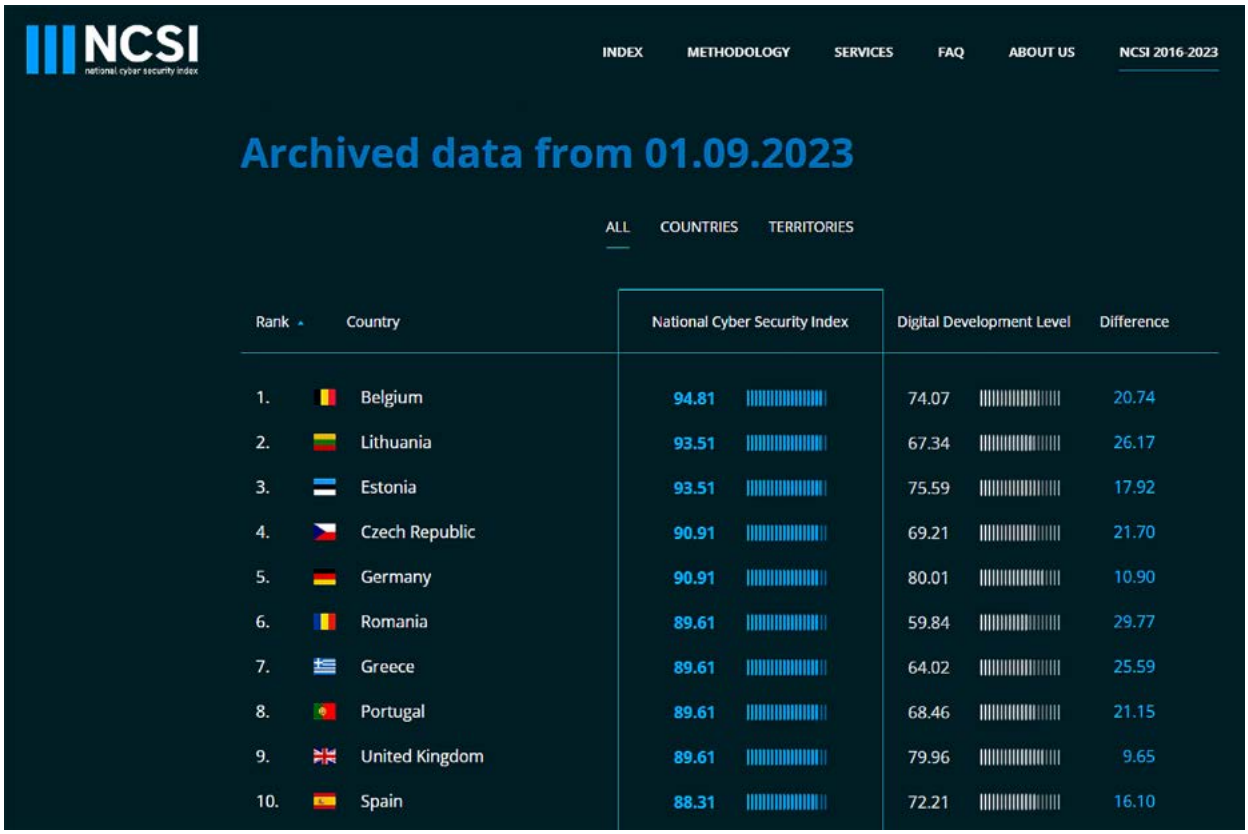
LA BELGIQUE DANS LE MONDE

La cybersécurité belge dans les classements

La très bonne position générale de la Belgique en matière de cybersécurité et la préparation à la prévention des cybermenaces et à la gestion des cyberincidents affectant les organisations nationales se reflètent également dans le classement de la Belgique en matière de cybersécurité.

En 2023, la Belgique a atteint la première place mondiale selon le National Cyber Security Index, l'indice mondial live, qui mesure la préparation des pays à prévenir les cybermenaces et à gérer les cyberincidents.

Le score NCSI indique le pourcentage que le pays a reçu par rapport à la valeur maximale des indicateurs considérés sur la base de la méthodologie utilisé.



Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Belgium	94.81	74.07	20.74
2.	Lithuania	93.51	67.34	26.17
3.	Estonia	93.51	75.59	17.92
4.	Czech Republic	90.91	69.21	21.70
5.	Germany	90.91	80.01	10.90
6.	Romania	89.61	59.84	29.77
7.	Greece	89.61	64.02	25.59
8.	Portugal	89.61	68.46	21.15
9.	United Kingdom	89.61	79.96	9.65
10.	Spain	88.31	72.21	16.10

Source : https://ncsi.ega.ee/ncsi-index/?archive=1

Les cyberchampions belges : Les Red Deamons à l'ECSC 2023

En octobre 2023, l'équipe des Red Daemons s'est rendue à Hamar, en Norvège, pour représenter fièrement la Belgique lors de la 8e édition annuelle du European Cyber Security Challenge (ECSC). En compétition avec des équipes de 29 autres nations européennes, les Red Daemons ont, trois jours intenses durant, relevé des défis liés à la sécurité, accumulant des points pour leurs solutions. C'était la sixième participation de la Belgique à cet événement international prestigieux.

Comme d'habitude, les dix cybertalents ont été sélectionnés parmi les équipes victorieuses du Cyber Security Challenge Belgium (CSCBE), qui s'est tenu au mois de mars de la même année. Au cours des sept dernières années, le Cyber Security Challenge Belgium a suscité l'intérêt de milliers d'étudiants belges désireux de tester leurs compétences, d'apprendre et de s'engager dans le monde passionnant de la cybersécurité.

La demande d'experts en cybersécurité dans les entreprises, les organisations et les forces de sécurité et de police est en hausse. La participation des Red Daemons est rendue possible grâce à un effort de collaboration entre le CCB et NVISO. Chaque année, ces partenaires sont responsables de l'organisation de l'événement, du sponsoring et de l'organisation d'ateliers préparatoires.

La compétition nationale (CSCBE) est organisée tous les ans par NVISO, avec le soutien du CCB.

Des événements tels que l'ECSC et le CSCBE jouent un rôle crucial puisqu'ils encouragent les jeunes à poursuivre des carrières dynamiques dans le domaine de la cybersécurité.

Suivez les Belgian Red Daemons sur les médias sociaux :

- X : @BelRedDaemons
- Instagram : @belgianreddaemons
- Facebook : https://www.facebook.com/BelRedDaemons

CYBER SPOTLIGHT : IA & CYBERSÉCURITÉ

Cyber Spotlight : IA & cybersécurité

Derrière l'engouement actuel que l'on observe autour de l'IA dans le monde de la tech, il existe une véritable tendance de fond qui consiste à envisager l'utilisation de l'IA dans tous les secteurs. La cybersécurité ne fait pas exception et sa proximité avec l'innovation et sa transversalité à de nombreuses technologies en font un sujet de choix pour les applications de l'IA. Pour mieux appréhender les interactions entre ces deux sujets, il est possible de définir **trois grands domaines de convergence** comme suit :

- l'IA au service de la cybersécurité : comment les experts en cybersécurité peuvent-ils utiliser l'IA pour améliorer la protection de leurs systèmes ? (analyse des logiciels malveillants et détection des attaques, p. ex.)
- l'IA « contre » la cybersécurité : comment un hacker peut-il tirer parti de l'IA pour améliorer ses techniques et ses tactiques ? (deepfake et recherche de vulnérabilités, p. ex.)
- la sécurité des applications de l'IA : les applications de l'IA présentent-elles des vulnérabilités et comment les protéger ? (empoisonnement des données et évasion des modèles, p. ex.)

Ces différentes approches sont riches et en constante évolution et nous ferons de notre mieux pour les aborder dans une série d'articles. Le premier traitera de la tendance des chatbots et des Large Language Models (LLM). Nous avons décidé de nous concentrer sur la troisième approche, la sécurité de l'IA, du point de vue d'un utilisateur moyen.

CONSIDÉRATIONS GÉNÉRALES POUR UNE UTILISATION SÛRE ET RESPONSABLE DES TECHNOLOGIES D'INTELLIGENCE ARTIFICIELLE (IA) CONVERSATIONNELLE

Les technologies d'IA conversationnelle telles que ChatGPT et Bard, basées sur des LLM, ont gagné en popularité et de nombreux Belges les ont adoptées pour améliorer leur productivité. Dans ce contexte, le CCB a reconnu l'importance de définir clairement les problèmes que posent ces technologies.

Nous souhaitons présenter ici une première liste de « bons réflexes » à adopter pour une utilisation sûre et responsable de ces technologies.

En préambule, même si cela semble relever du bon sens, il est essentiel de ne jamais se fier aveuglément aux réponses fournies par les agents conversationnels et de toujours garder un esprit critique. Les réponses fournies par ces outils étant imparfaites, elles doivent toujours être relues et corrigées. De plus, les agents conversationnels manquent généralement de raisonnement logique ; ils sont « probabilistes » dans le sens où ils sont entraînés à générer des séquences de mots avec un haut degré de probabilité.

En outre, une attention particulière doit être accordée aux aspects suivants :

- Protégez les données confidentielles : évitez de partager des informations sensibles, car les agents d'IA conversationnelle peuvent stocker et réutiliser ces données. Désactivez l'enregistrement de l'historique des conversations dans la mesure du possible.
- Détection des erreurs : les agents d'IA conversationnelle commettent des erreurs ; ne leur confiez donc que des tâches pour lesquelles vous disposez de connaissances suffisantes (afin de pouvoir vérifier et contrôler les résultats).
- Fact-checking : vérifiez les faits de manière indépendante (fact-checking), car les agents conversationnels omettent souvent les sources.
- Problème de l'automatisation : en les utilisant trop souvent, il est possible de favoriser les résultats générés par les agents d'IA et de leur accorder une confiance excessive alors que, comme nous l'avons vu, dans de nombreux domaines, les humains sont plus compétents.
- Limites et préjugés : les agents conversationnels peuvent être entachés de préjugés et sont limités dans leurs connaissances par leurs données de formation. Confrontez-les à diverses sources pour obtenir un contexte objectif et complet.
- Transparence : privilégiez une utilisation transparente des agents conversationnels. N'essayez pas de dissimuler leur utilisation, mais signalez-la plutôt pour renforcer la confiance et la responsabilité.
- Droits d'auteur : les réponses fournies par les agents conversationnels peuvent enfreindre les règles liées aux droits d'auteur ; il convient donc d'être prudent lors de leur utilisation à des fins académiques ou commerciales.
- Humanité : n'oubliez pas que les agents conversationnels sont dépourvus de conscience et d'émotions. Méfiez-vous de la manipulation émotionnelle.

En tenant compte de tous ces aspects, nous pensons que les utilisateurs peuvent utiliser efficacement les agents conversationnels tout en comprenant leurs limites et en agissant de manière responsable.

QUI SOMMES-NOUS ?

Qui sommes-nous ?

Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale en charge de la cybersécurité en Belgique. Institué par l'arrêté royal du 10 octobre 2014, le CCB relève de l'autorité du Premier ministre.

Grâce à un échange d'informations optimal, les entreprises, les autorités, les opérateurs de services essentiels et les citoyens peuvent compter sur une protection adéquate.

Le CCB supervise, coordonne et veille également à la mise en œuvre de la stratégie belge en matière de cybersécurité, approuvée par le Conseil national de sécurité en 2021. Sa mission est de faire de la Belgique l'un des pays les moins cybervulnérables d'Europe d'ici 2025.

Le CCB joue un rôle clé en aidant la Belgique à atteindre cet objectif en menant à bien ses tâches, telles que l'information et la sensibilisation aux principales cybermenaces et à la manière de s'en prémunir.

Suivez le Centre pour la Cybersécurité Belgique sur les médias sociaux et son site Internet :

- X : @CCBbelgium
- X : @CCBAlerts
- LinkedIn
- www.ccb.belgium.be

Éditeur responsable
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur général
Rue de la Loi, 18
1000, Bruxelles

Dépôt légal
D/2024/14828/003