20 mai 2021 -16:16

Une cyberstratégie 2.0 pour propulser la Belgique au rang des pays les moins vulnérables d'Europe

Le Conseil National de Sécurité (CNS) a validé ce jeudi les détails de la stratégie de cybersécurité 2.0. Cette stratégie cadre l'approche transversale de la Belgique en terme de cybermenace et d'opportunités pour notre pays. Elle doit propulser la Belgique au rang des pays les moins vulnérables d'Europe.

L'avènement d'une société de plus en plus numérique et le recours accru aux nouvelles technologies s'accompagne mondialement d'une recrudescence des cyberattaques mais également, comme les événements récents nous l'ont encore démontré, d'une intensification de la gravité et du degré de ces attaques.

L'évolution constante du cyberespace et de ses enjeux poussent notre pays à investir en continu dans son infrastructure et sa sécurité depuis plusieurs années. Dernier exemple en date : la cybersécurité est l'un des axes centraux du Plan National pour la Reprise et la Résilience remis par la Belgique à la Commission européenne fin avril.

La Belgique se dote aujourd'hui, sur approbation du Conseil National de Sécurité, d'une nouvelle stratégie de Cybersécurité particulièrement ambitieuse. Ce plan s'articule autour de six objectifs précis :

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

« La stratégie de cybersécurité 2.0 qui a été définie ambitionne de propulser la Belgique au rang des pays les moins vulnérables d'Europe dans le domaine de la cybersécurité à l'horizon 2025 », commente Miguel De Bruycker, directeur du Centre pour la Cybersécurité Belgique (CCB) qui sera chargé de la mise en œuvre de la stratégie de cybersécurité. Le CCB travaillera, pour ce faire, en étroite collaboration avec différents services publics pour qui la question de la cybersécurité est centrale.

Alexander De Croo, Premier ministre : « La cybersécurité est non seulement une priorité pour la Belgique, elle représente aussi une énorme opportunité pour nos entreprises et nos PMES qui détiennent énormément d'expertise en la matière. Nous allons continuer à investir pour protéger nos citoyens et nos systèmes contre les cybercriminels et tout faire pour développer, en parallèle, un écosystème propice à l'innovation en matière de cybersécurité chez nous ».

Annelies Verlinden, Ministre de l'Intérieur : "Dans les années à venir, je serai, en tant que ministre de l'Intérieur, étroitement impliquée dans la lutte contre l'un des risques majeurs en termes de sécurité pour notre pays : la cybercriminalité. Cette lutte sera une priorité absolue pour l'OCAM, la police intégrée et le Centre national de crise. Nous voulons donc renforcer dans tous ces services la lutte contre la

cybercriminalité au cours de cette législature. Nous le ferons en augmentant les effectifs, en attirant du personnel spécialisé et en misant sur la formation et les technologies."

Vincent Van Quickenborne, Ministre de la Justice : « Le nombre de cas de cybercriminalité a considérablement augmenté ces dernières années. Nous voyons de plus en plus de criminels se reconvertir en cybercriminels. Ils agissent de manière rapide, anonyme, organisée et à l'échelle internationale. Nous équipons la justice en conséquence pour qu'elle puisse mieux faire face à ce fléau. Nous mettons à disposition des cybermagistrats plus spécialisés dans les parquets et des spécialistes IT à la Police judiciaire fédérale et investissons 100 millions d'euros dans la numérisation de la justice. Avec Team Justice, nous voulons non seulement combattre les symptômes, mais aussi traquer et poursuivre les réseaux organisés à l'origine de cette criminalité. »

Ludivine De Donder, ministre de la Défense : « La nouvelle stratégie belge en matière de cybersécurité pose les bases d'un État plus résilient grâce à une infrastructure informatique à l'état de l'art. La Défense, dans la lignée de cette Stratégie Nationale, va développer au cours de cette législature une nouvelle composante : la Composante Cyber dédiée à la protection de nos systèmes, à la veille et à l'analyse du cyberespace, nouveau théâtre d'opération. Par le recrutement d'experts, celui de personnes intéressées par le domaine cyber devant être formées et par l'embauche de talents passionnés – geeks – j'ambitionne de doter la Défense d'un outil d'excellence au profit de la sécurité de tous. »

Petra De Sutter, ministre des Télécommunications : « Ces dernières semaines, nous avons assisté à une recrudescence des escroqueries par SMS, surtout après la fuite de données Facebook. Notre message reste le suivant : « Faites bien attention à ce que vous installez et à la provenance du message ». Mais en tant que gouvernement, nous avons aussi une grande capacité d'action. Grâce aux moyens du Plan de relance, nous allons pouvoir étendre et automatiser la lutte contre le phishing ou le smishing (fraude par SMS) en collaboration avec les opérateurs. Notre nouvelle loi sur les télécommunications, qui sera bientôt soumise au vote du Parlement, fournit le cadre juridique nécessaire. C'est une bonne chose que de plus en plus de personnes profitent des nombreux services en ligne : suivre un colis commandé, effectuer des paiements, remplir des documents officiels, etc. Il est donc également important que tout cela puisse se faire en toute sécurité. »

Sophie Wilmès, Ministre des Affaires étrangères : « Pouvoir attribuer formellement la responsabilité d'une cyberactivité malveillante est un outil de dissuasion important de notre stratégie de cybersécurité. C'est pourquoi le Conseil National de Sécurité a validé aujourd'hui une procédure d'attribution diplomatique qui permettra, concrètement, d'identifier l'éventuel acteur étranger impliqué dans des actes visant une organisation vitale de notre pays et de définir les réactions appropriées à y apporter. Cette procédure pourra également être activée dans le but de soutenir un pays allié victime de faits identiques. À l'heure où la cybersécurité est au sommet des priorités politiques au niveau de l'Union européenne ou de l'OTAN, par exemple, je pense qu'il était indispensable de compléter notre arsenal avec ce dispositif. »

Alexander De Croo, Premier ministre
Rue de la Loi, 16
1000 Bruxelles
Belgique
+32 2 501 02 11
https://premier.be
contact@premier.be