Le Centre pour la cybersécurité est né

FÉDÉRAL Le gouvernement a donné ce lundi le coup d'envoi du CCB

▶ Le Centre pour la cybersécurité Belgique devrait atteindre son régime de croisière dans les six mois.
▶ Il sera dirigé par Miguel De Bruycker, l'ex-patron de la cybersécurité au renseignement militaire.

Ce n'est pas un centre opérationnel, un machin « geek » et high-tech planqué dans un bunker. Le Centre pour la cybersécurité Belgique (CCB) est une « simple » (!) autorité de coordination, placée sous la tutelle du Premier ministre, constituée d'une dizaine de collaborateurs – qui ne sont pas encore tous recrutés – dont le budget annuel (700.000 euros) couvrira à peine les salaires et frais de fonctionnement. Son plan stratégique a été avalisé vendredi par le gouvernement et, dans les six mois, le centre devra s'installer dans ses nouveaux locaux, au 18 rue de la Loi, entre le Centre de crise et l'Ocam (Organe de coordination pour l'analyse de la menace). C'est dire si le vernissage a des odeurs de plâtre frais.

Mais dans un paysage belge particulièrement éclaté, face à une cybermenace mouvante, la coordination que la CCB va apporter pourrait bien être décisive. Le Centre reprend dans son orbite le Cert.be (l'équipe fédérale d'intervention d'urgence en sécurité informatique), et il servira par ailleurs à coordonner l'apport « cyber » des services de renseignement, de la police, de la Justice, de l'Intérieur, et à tracer une politique intégrée et coordonnée face à la cybermenace. Cela va de l'information et sensibilisation du public jusqu'aux avis et meilleurs pratiques adressées aux entreprises, en passant par les alertes précoces et la riposte aux cyber-incidents qu'essuieraient les secteurs vitaux du pays.

Le véritable coup de génie de ce CCB, c'est d'y avoir placé à sa tête, pour cinq ans, Miguel De Bruycker, l'ancien chef de la section Cybersécurité du SGRS, le service de renseignement militaire belge. Pourquoi ? Par nature, c'est le renseignement militaire qui est en première ligne pour les cyberattaques les plus sophistiquées (ils ont été cruciaux dans la gestion de la crise Belgacom), et c'est ce service qui a développé en Belgique, pour la Défense, la plus forte expertise en matière de détection des intrusions et des traces d'intrusion (*indicators of compromise*) dans les systèmes informatiques, d'attribution des attaques (que révèlent les signatures ?), d'analyse des malicieux (*digital forensics*) et, dans une phase d'adaptation et riposte, le partage automatisé d'informations sur les programmes malicieux.

Or cette expertise qu'a accumulée ces dernières années le SGRS est le résultat du travail personnel de Miguel De Bruycker lorsqu'il était lieutenant-colonel à la tête du Cyber & CIS Security. C'est dire si le nouveau directeur du CCB, rendu pour cinq ans à la vie civile, sait de quoi il retourne. De Bruycker aura par ailleurs la confiance du partenaire par nature le plus réservé – le renseignement militaire dont il provient –, ce qui devrait aider à réunir autour de lui les autres partenaires : public, privé, académique, belge et international.

Maturité à l'horizon 2020

Désigné le 17 juillet, accaparé par ce nouveau chantier depuis début août, l'homme est un pragmatique – il a mis sur pied un modèle pour la Défense, il semble s'en inspirer pour le CCB – mais aussi un stratège, qui tient à conserver une vision claire des menaces et qui valorise autant la riposte et la gestion immédiate des incidents que la sensibilisation des divers publics (grand public ou décideurs). C'est un grand écart pour une petite équipe, et on comprend qu'il ait phasé la montée en puissance du centre : dans les six mois, le centre disposera de ses locaux et de son personnel et ne vise la maturité qu'à l'horizon 2020.

Avertissement utile : le Centre est lancé mais ce n'est pas demain que les cyberattaques cesseront, préviennent en chœur le directeur du CCB et le Premier ministre Charles Michel. Le véritable défi sera de les détecter le plus rapidement possible et de limiter les dégâts envers les systèmes informatiques. ■

ALAIN LALLEMAND

MISSIONS

Coordination et convergence

Le Centre se fixe des objectifs distincts pour divers publics.

▶ La protection des secteurs vitaux requiert le développement d'un système d'alerte précoce (« early warning »), d'un soutien aux systèmes attaqués et d'une réponse aux incidents. La réponse inclut le traitement de l'incident mais aussi probablement le reporting et la sensibilisation du secteur à l'incident qui vient de se produire.

▶ Un autre public est celui des acteurs professionnels, entreprises, etc. Là, le CCB mènera des actions de sensibilisation, distribuera des informations notamment via un portail, développera aussi des partenariats (certainement avec la Belgian Cyber Security Coalition qui existe déjà) et valorisera les technologies fiables. Cela passera par la diffusion d'avis de sécurité et de *best practices*.

▶ Le grand public est lui aussi une cible, par la sensibilisation et la diffusion d'informations, l'encouragement des établissements d'enseignement et la sensibilisation des jeunes, etc.

▶ Au niveau international, le centre a déjà pris langue avec l'Enisa, l'Agence européenne chargée de la sécurité des réseaux et de l'information.