Sécurité informatique des entreprises : bientôt un « Campus Cyber » lillois ?

Dans un monde numérique de plus en plus complexe et dangereux, les enjeux de cybersécurité sont devenus prioritaires pour protéger les données d'un pays, des entreprises, des citoyens. La métropole lilloise souhaite créer un « Campus Cyber », lieu de formation, de recherche et d'accompagnement.

PAR JEAN-MARC PETIT
jmpetit@lavoixdunord.fr

LILLE. Malwares (virus), ransomwares (blocage des données contre rançon), pourriels (courriels infectés), phishing (hameçonnage)… Tous ces mots sont devenus le quotidien de nos sociétés ultra-connectées, et la bête noire des entreprises et administrations nombreuses à être victimes d'intrusions ou de piratages dans leurs systèmes informatiques. Dernière en date, la société lilloise de BTP Rabot-Dutilleul, qui s'est vu réclamer 8 millions d'euros par des pirates informatiques ayant bloqué les données du groupe.

« *Le marché mondial de la cybersécurité est estimé à 150 milliards d'euros d'ici à 2023* », explique Ludovic Delaire, directeur général du CITC, le Centre d'innovation des technologies sans contact à EuraTechnologies Lille. Ce centre s'est vu confier par la Métropole européenne de Lille (MEL) et la Région Hauts-de-France le pilotage de la pré-configuration d'un « Campus Cyber » sur la métropole.

FORMATION, RECHERCHE, ACCOMPAGNEMENT

« *Nous nous sommes mis dans le sillage de la mission nationale Campus Cyber présentée en janvier dernier lors du FIC (Forum international de la cybersécurité) à Lille* », explique Akim Oural, en charge de la stratégie numérique à la MEL. L'objectif est de créer des lieux dédiés aux enjeux de la sécurité numérique. Un premier Campus Cyber doit ouvrir à Paris en 2021, Rennes s'est positionné pour accueillir un campus dédié à la cyberdéfense, Lille souhaite accueillir un même campus dédié aux entreprises et collectivités.

> ***« Près de 10 000 emplois pourraient être créés en région dans le domaine de la cybersécurité d'ici à 2025. »***

En s'appuyant sur l'écosystème existant et les entreprises leaders du secteur *(voir ci-dessous)*, ce campus proposerait à la fois de la formation dédiée, de la recherche et innovation, un observatoire de la menace numérique et un accompagnement spécifique pour les entreprises et administrations.

« *L'enjeu est d'abord de protéger nos entreprises*, explique Ludovic Delaire. *La période du confinement a vu une recrudescence des attaques numériques, alors que la moitié de la population avait basculé en télétravail avec le risque d'ouvrir des failles dans les systèmes informatiques des entreprises. L'enjeu est aussi économique. Près de 10 000 emplois pourraient être créés en région dans le domaine d'ici à 2025. Il est indispensable d'attirer les talents, d'où l'enjeu de la formation, et les entreprises pour identifier notre région comme territoire de référence.* »

Le CITC a lancé un grand questionnaire de pré-configuration de ce Cyber Campus, afin de connaître les attentes et besoins. Un cahier des charges sera rédigé à partir d'octobre pour une première présentation en fin d'année. Le parc technologique de la Haute Borne de Villeneuve-d'Ascq est souvent cité pour accueillir ce futur campus. Mais toutes les options sont encore sur la table. ■

Le marché mondial de la cybersécurité est estimé à 150 milliards d'euros d'ici à 2023. PHOTO PIB

L'ÉCOSYSTÈME CYBER

Les quatre grands groupes soutenant le Cyber Campus France ont tous d'importants sites en région (campus cyberdéfense d'Orange à Villeneuve-d'Ascq, branche R&D cyber d'Atos à Seclin, Thalès à Lambersart et Capgemini à EuraTechnologies).

Au total, 73 entreprises spécialisées dans la cybersécurité, représentant 6 500 emplois spécialisés, sont également présentes en métropole, dont quelques leaders (Stormshield, VadeSecure, OVH, Dhimyotis, aDvens, etc.).

22 formations dédiées à l'intelligence artificielle et la cybersécurité sont délivrées en Hauts-de-France (IMT Lille-Douai, université de Lille, université d'Artois, université polytechnique Hauts-de-France et UTC Compiègne). Quatre laboratoires (Cristal, IRCICA, CRIL-LAMIH, INRIA) et trois plateformes de transfert de technologies (CITC, InTech et CEA Tech) complètent les équipements de recherche.

« Aider les entreprises à se protéger »

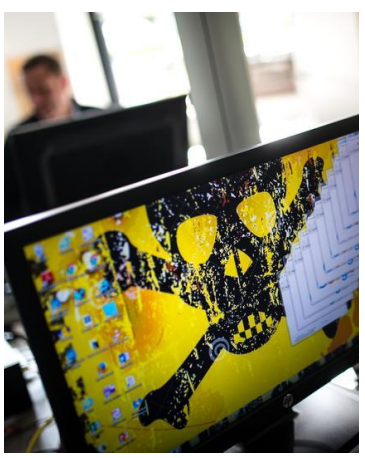
NOYELLES-GODAULT. Après avoir dirigé plusieurs années le CITC (Centre d'innovation des technologies sans contact), Chekib Gharbi dirige aujourd'hui la filiale cybersécurité de Luxant à Noyelles-Godault. C'est désormais du côté du privé qu'il mesure les enjeux et attentes des entreprises vis-à-vis de la création d'un « cyber campus ».

« *Un patron de PME n'est pas forcément technophile. Beaucoup d'entreprises, mais aussi les collectivités locales, sont très fragiles par rapport aux enjeux de cybersécurité. Beaucoup sont équipées de systèmes peu fiables. Il est indispensable de les aider à se protéger des vols de données en interne comme en externe.* »

« FORMER LES TALENTS DE DEMAIN »

La première attente des entreprises en matière de « cyber campus », concerne les moyens et les ressources. « *On a quelques formations en région, mais il faut absolument préparer le territoire à former les talents de demain en matière de cybersécurité, pas encore assez prise en compte dans les formations informatiques classiques. Un plan cyber a été lancé il y a deux ans par la Région, avec un audit des entreprises. Cet enjeu de la formation est récurrent.* »

La seconde attente concerne la mutualisation des moyens. « *Des infrastructures technos peuvent être mutualisées entre des acteurs privés, des systèmes collaboratifs. D'où la nécessité de créer cet écosystème fort qui permettra de reconnaître le territoire comme un acteur essentiel de la cybersécurité.* » ■ J.-M. P.



La cybersécurité n'est pas encore assez prise en compte dans les formations informatiques classiques. PHOTO PASCAL BONNIÈRE