Cybersécurité : quand l’État fait appel aux étudiants

La cybersécurité est un secteur en pleine expansion. Pourtant, son plus grand défi consiste aujourd’hui à trouver des talents qualifiés pour répondre à l’évolution rapide des menaces.

Wannacry, Not Petya, Mirai, Meltdown, Spectre… les vulnérabilités et cyberattaques se sont multipliées ces dernières années, confirmant, si besoin en était, que la cybersécurité reste une problématique préoccupante pour toute la société, de l’État aux entreprises françaises de toutes tailles.

En cause : une numérisation croissante aussi bien dans les foyers, que les lieux de travail, couplée à une augmentation de la menace, toujours plus compétents et toujours plus ingénieuse. Et ce n’est que le début, les cyberattaquants ne reculant devant rien pour espionner, saboter, manipuler de l’information ou encore usurper des identités, tout en évitant les détections . de nouvelles méthode de manipulation de l’information à grande échelle, l’utilisation de l’intelligence artificielle afin de cyberattaques seront sûrement parmi les moyens utilisés par les cyberattaquants en 2019.

La France s’organise

Mais alors, comment contrer cette menace, qui pèse tant sur la sécurité du numérique jusqu’à la sécurité nationale ? Les spécialistes de la cybersécurité

s’organisent, à grande échelle, pour lutter contre tout, des attaques étatiques aux catastrophes économiques, sociales et financières. Les professions liées à la sécurité numérique, elles, sont en plein essor face à la demande croissante des entreprises et des pouvoirs publics qui cherchent à dénicher des personnes capables de comprendre parfaitement le fonctionnement du cyberespace, sa géopolitique, les vulnérabilités et les techniques utilisées par les pirates et les erreurs courantes commises par les victimes.

Pourtant, de tels profils semblent encore aujourd’hui difficiles à trouver, tant la demande dépasse de loin l’offre. Seuls 1200 des 6000 postes ouverts dans la cybersécurité en 2016 auraient ainsi été pourvus, selon l’ANSSI.

Les écoles, un maillon critique de la cybersécurité française ?

Une pénurie bien réelle, à laquelle la France pourra répondre en allant chercher les talents en devenir là où ils se trouvent : à l’école. Plusieurs grandes écoles ont ainsi décidé, depuis quelques années déjà, d’intégrer des formations dédiées à la cybersécurité à leurs offres. Parmi elles : l’EPITA, l’école des ingénieurs en intelligence informatique, qui compte à ce jour un laboratoire Sécurité et Système, un centre de formation destinée aux professionnels des entreprises et une majeure spécialisée en cybersécurité dans son parcours éducatif.

Le premier, fondé en 1999, a posé l’une des premières pierres de l’offre « cybersécurité » de l’EPITA en offrant aux étudiants de l’école la possibilité de développer, en partenariat avec les équipes de la police (et plus particulièrement de l’O.C.L.C.T.I.C), des outils de recherche de preuves numériques au cœur d’un laboratoire entièrement dédié à la sécurité. Le second, baptisé SecureSphere, est lancé pour répondre aux besoins des entreprises en sécurité et propose à ces dernières des formations en sécurité numérique pour leurs salariés, leurs cadres et leurs dirigeants. Parmi ses clients : des fonds d’investissement, des banques, ou encore des constructeurs automobiles. Enfin, la troisième, appelée SRS (système, réseau et sécurité), est proposée aux étudiants de l’EPITA dès la deuxième année d’étude afin leur permettre de maîtriser tous les maillons de la cybersécurité technique et organisationnelle. Les diplômés sont en mesure d’évaluer la sécurité, détecter – caractériser – réagir face à une cyberattaque.

DEFNET, la fiction au service de la

réalité

Et c’est à cette dernière que le ministère des Armées fait appel, chaque année depuis 2014, pour participer à l’exercice inter-armées DEFNET. L’objectif : s’initier, sur deux semaines aux côtés des militaires et d’une dizaine d’écoles d’ingénieurs, à la résolution d’incidents de sécurité informatique perpétrées contre une entreprise fictive.

Un exercice grandeur nature partie intégrante de la réserve de cyberdéfense et des besoins de recrutement, piloté par le commandement de la cyberdéfense. De quoi permettre à l’État de s’assurer d’avoir des talents opérationnels à disposition en cas d’attaque réelle, mais aussi aux étudiants d’affiner leur formation : *« Ça nous permet de prendre conscience de ce que vouloir travailler dans la cybersécurité implique, de nous sentir plus concernés »*,

explique Maxence Duchet, étudiant en 5e année de la majeure SRS à l’EPITA, avant d’ajouter que *« c’est de la pratique supplémentaire. Les cours, c’est théorique. Il est important d’avoir un oeil sur l’extérieur pour gagner en maturité »*.

Et DEFNET n’est pas le seul exercice proposé aux étudiants. Depuis 2014, la majeure Système Réseau et Sécurité organise le challenge de forensic (investigation numérique) du forum international de la cybersécurité (FIC). Les ingénieurs aujourd’hui doivent savoir faire preuve de professionnalisme et acquérir des expériences dès le cursus. De nombreux concours sont organisés pour leur permettre de s’entraîner aux défis d’aujourd’hui et de demain, à l’image de la nuit du hack, Greyhack, le concours SemEval-2018 ou encore le concours DEFT. *« Notre chef de majeur, Sébastien Bombal, est le conseiller de l’officier général au commandant de la cyberdéfense, il nous pousse à participer à beaucoup de concours et d’événements externes pour que l’on se fasse la main »*, raconte Maxence Duchet. Le tout, toujours sous l’œil des experts du secteur, à la recherche des futures pépites de la cyberdéfense française.

Téléchargez le livre blanc « Cybersécurité et Innovations »

Maddyness, partenaire média de IONIS Group.

Article écrit par MADDYNESS, AVEC IONIS GROUP