La cyberdéfense contre-attaque

Lutte contre le piratage, protection des données... Des formations apprennent à sécuriser un espace numérique et à riposter

Chaque année, plusieurs centaines de millions de cyberattaques ont lieu en France. Un phénomène en expansion lié à la diffusion des outils numériques – croissance des réseaux, apparition des objets connectés... – et à l'obsolescence de certains systèmes informatiques qui deviennent plus vulnérables.

Résultat : *« La sécurité devient une préoccupation croissante des entreprises »*, affirme Olivier Blazy, responsable de la deuxième année du master Cryptis de l'université de Limoges. Créé il y a trente ans, celui-ci forme des experts en sécurité informatique et en cryptographie : *« Il s'agit de trouver le bon compromis pour garantir la sécurité et l'authenticité d'un message, tout en facilitant le processus d'utilisation dans un contexte professionnel »*, explique-t-il.

Dans ce contexte, nombre d'établissements ont développé des cursus ou spécialisations en sécurité informatique. Jusqu'ici, les formations reconnues par l'Etat étaient répertoriées par l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui recensait notamment une vingtaine de masters.

Pour aller plus loin, l'agence vient de lancer un label baptisé SecNumEdu, visant à garantir que la formation *« répond à une charte et des critères définis par l'Anssi en collaboration avec les acteurs et professionnels du domaine »*. En particulier, les responsables de formation doivent s'assurer que *« lorsque des aspects concernant la sécurité offensive sont abordés, les contre-mesures correspondantes sont également présentées, avec leurs limites éventuelles »*. Autrement dit, les étudiants sont formés au « hacking éthique ».

Un secteur qui embauche

Diplômé du master Secrets (Sécurité des contenus, des réseaux, des télécommunications et des systèmes) de l'université Versailles Saint-Quentin-en-Yvelines, Andrei Dumitrescu est ce que l'on appelle un *« white hat »* (« chapeau blanc »), par opposition aux pirates que sont les *« black hats »*. Consultant en sécurité informatique chez Lexsi, il fait partie du pôle chargé de réaliser des tests d'intrusion. Un poste qui lui permet de combiner le *« plaisir du hacking »*, en s'amusant de *« voir jusqu'à quel point on peut exploiter une faille dans un système »*, avec *« la satisfaction de contribuer à améliorer la sécurité du client »*.

Avec Conix, Bull ou Worldline, ce type d'entreprises spécialisées dans la sécurité informatique constituent les premiers recruteurs des diplômés de master. *« Les PME n'ont pas les moyens d'avoir une équipe sécurité en interne, tandis que les grands groupes voient difficilement le retour sur investissement*, explique Olivier Blazy. *En effet, avoir un pôle sécurité, ce n'est pas de l'argent qu'on gagne, mais de l'argent qu'on ne perd pas »*. Et de citer Google qui *« a une* Red Team *capable de réagir en cas d'attaque, mais ne se préoccupe pas de faire de la prévention »*.

Autre débouché possible : le ministère de la défense et la Délégation générale à l'armement. *« Les institutions publiques embauchent davantage depuis trois ans »*, observe Gilles Zémor, responsable du master Cryptologie et sécurité informatique à l'université de Bordeaux, qui note *« une prise de conscience du politique. La protection contre la cybercriminalité est devenue un enjeu de sécurité nationale et le secteur est globalement porteur »*, souligne-t-il. *« 80 % des étudiants de master 2 sont recrutés directement après leur stage »*, évalue Olivier Blazy, confirmant la bonne insertion professionnelle dans un secteur où les salaires d'embauche s'établissent entre 30 000 et 35 000 euros bruts par an. ■

SOPHIE BLITMAN