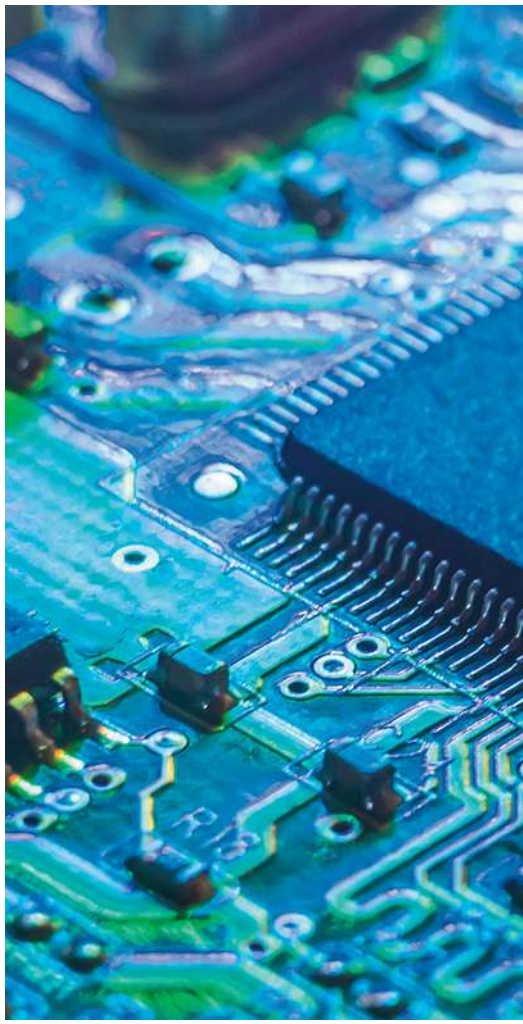
Les **chevaliers blancs** du cyberespace



Par **Thierry Fiorilli**

Ils s'infiltrent dans les systèmes informatiques, non pas pour en prendre le contrôle, mais pour en renforcer la protection. Infiltration dans le monde du hackisme éthique.

«La lutte contre la cybercriminalité vous passionne? Vous êtes d'accord avec l'adage "sois proche de tes amis et encore plus de tes ennemis"? Vous êtes convaincu que le piratage informatique peut être responsable et bienveillant, si tant est qu'il soit réalisé à bon escient? Et si vous deveniez hacker éthique?» Il n'y a pas à dire: en *punchline*, Guardia sait y faire. Guardia? Guardia Cyber School, une haute école française qui forme à la cybersécurité. En proposant notamment le *pentesting*, ou *pentest* –contraction de *penetration test*. C'est-à-dire tentative d'intrusion dans les systèmes informatiques. Du hacking, donc. Mais du hacking «éthique», son but étant de traquer les vulnérabilités d'un réseau, d'un serveur, d'un site, d'une application ou d'un logiciel, avant les pirates malveillants, pour que l'institution ou l'entreprise qui en dépend puisse y remédier.

Plusieurs établissements font pareil en Belgique. Dont l'Hénallux, haute école installée à Namur et première dans le pays à avoir proposé un bachelier en cybersécurité. C'était en 2017. Depuis, la section est devenue la plus importante de l'établissement: aujourd'hui, 400 étudiants (ultramajoritairement masculins), 200 dès la première année et entre 60 et 80 décrochant leur diplôme au bout des trois ans, y apprennent notamment le *pentest* –qui est au hacking éthique ce que la pratique est à la philosophie. Et le cadre, très strict, dans lequel il peut s'effectuer.

Une formation apparemment solide: ce sont trois de ses anciens étudiants en Sécurité des systèmes qui ont terminé aux trois premières places du concours Hack The Government organisé en novembre dernier par le Centre for Cybersecurity Belgium (CCB), à Zaventem. Sur la base d'une liste de sites web publics, des professionnels du secteur et une soixantaine d'étudiants d'universités et de hautes écoles étaient chargés d'identifier les failles. «Au final, résume Fabian Restiaux, directeur des Domaines des Sciences et des Sciences de l'ingénieur et technologie de l'Hénallux, tout le monde y gagne:

«On pense comme les hackers, mais on le fait au service de l'organisme pour lequel on travaille.»

GETTY

le gouvernement renforce sa cyberprotection et nos étudiants participent à un challenge d'envergure, intègrent une large communauté de hackers éthiques et ont la possibilité de gagner des formations de pointe très prisées dans le domaine de la cybersécurité».

A l'assaut

Domaine où travaille, depuis qu'il est sorti de la haute école namuroise, Célien Desteucq, 27 ans. Le vainqueur du Hack The Government, c'est lui. En juin 2022, son bachelier bouclé, il a été embauché par NVISO, gros cabinet de conseil en cybersécurité. Depuis ses bureaux bruxellois, Célien y officie comme *pentester*: il part à l'assaut des systèmes de clients, «privés et publics, industriels ou non, de Belgique, Allemagne, Autriche et Grèce. J'y fais principalement des tests d'intrusion dans des applications web et mobiles, dans le délai stipulé dans le contrat.»

Pourquoi y excelle-t-il tant? «Je suis curieux, perfectionniste et débrouillard. Il faut toujours aller farfouiller sur Internet, parce que les technologies et les failles évoluent sans arrêt, et c'est quelque chose que je ne fais pas mal. En plus, via le travail, je continue à apprendre. Et puis, je consacre un peu de mon temps libre, comme indépendant complémentaire, à du *bug bounty*, ces programmes, sites web ou plateformes qui regroupent des entreprises autorisant le test de la sécurité de leur système informatique et qui rémunèrent pour les failles détectées. N'importe qui peut s'y inscrire, mais pour gagner de l'argent il faut trouver une vulnérabilité qui n'a pas été identifiée avant. J'y teste des sites de sociétés qui ne sont pas clientes de mon employeur, évidemment.»

Question de déontologie. Indispensable. «Parce que la barrière entre hacker éthique et hacker mal intentionné est très faible. En réalité, je fais la même chose que le hacker mal intentionné, sauf que lui en abuserait et moi je le rapporte au client. Quand on fait du *pentest*, on pense comme les hackers mais on le fait au service de l'organisme pour lequel on travaille.»

Une mince ligne entre légalité et illégalité

Adrien Voisin, maître assistant et responsable de programmes pour la section Sécurité des systèmes à l'Hénallux, développe cet aspect, crucial: «L'objectif de jouer le rôle de l'attaquant, c'est d'avoir une vision différente pour identifier des vulnérabilités qu'on n'a pas relevées depuis l'intérieur. Cette façon de travailler, on l'appelle "hacking éthique", parce que c'est du hacking mais pour de bonnes raisons et surtout dans les bonnes conditions: à travers un contrat qui stipule ce qu'on peut faire ou non. Le hacking éthique ne sous-entend donc pas uniquement que l'intention est louable mais qu'il est contractuel, cadré. Hack The Government, c'est typiquement du hacking éthique, puisqu'on y donne la possibilité de hacker; mais si les participants faisaient pareil hors de ce cadre, on pourrait ...

… considérer qu'ils étaient hors la loi. Le CCB, l'organisme fédéral belge qui surveille le cyberespace, a sorti plusieurs textes juridiques sur lesquels on peut s'appuyer mais la limite entre légal et non légal n'est pas toujours très claire. Donc, on décourage fortement nos étudiants de faire du hacking s'ils n'opèrent pas sous couvert d'un contrat. Avec des sociétés qui leur demandent d'identifier les trous dans leur système informatique durant l'audit général de leur infrastructure.»

C'est la dimension la plus *touchy* de la démarche, confirme un responsable de la sécurisation des informations à la police fédérale: «C'est sûr que des données peuvent être volées par un hacker dit éthique mais, finalement, comme pourrait le faire un peintre qu'on laisse entrer chez soi. Le *white hacker* pourrait voler et revendre ce qu'il a trouvé –et ce sont des choses qui se font, évidemment– mais son intérêt est de gagner sa vie en sécurisant les réseaux de ses clients. C'est sa raison d'être. Le cadre est aussi très important pour que le hacker éthique comprenne la portée de son action: il va devoir utiliser des procédés qui sont d'office illégaux. Scanner toutes les adresses IP d'une société par exemple. Donc il doit pouvoir démontrer qu'il a l'accord de la société pour effectuer ce travail-là.»

En tout cas, c'est ça que souhaiterait Bryan Rivoux, 23 ans et en dernière année de sécurité des systèmes à l'Hénallux: «Je me verrais bien *pentester* au sein d'une boîte comme NVISO. Mais le forensique pourrait m'intéresser aussi: c'est le volet investigation, consécutif à un hacking malveillant. Le fait d'essayer de comprendre comment les hackers ont opéré.»

Maël, 27 ans, même promotion que Bryan et premier étudiant au Hack The Government de novembre, est plus décidé: «Je veux travailler dans le *bug bounty*. Des plateformes, comme Intigriti, HackerOne ou Bugcrowd , mettent en relation hackers éthiques et entreprises donnant accès à leur système pour qu'y soient décelées les failles. J'y officierais comme hacker éthique, à mon compte. J'adore! Dans un premier temps, on recueille toutes les informations sur "la cible": le système informatique. C'est l'étape de la reconnaissance. Puis, c'est celle de l'exploitation des vulnérabilités. En général, l'attaquant essaie d'en trouver plein de petites et d'en faire une chaîne, pour aller le plus loin possible dans le système et avoir un gros impact.»

«On fait la même chose, sauf que le hacker mal intentionné en abuserait, moi je le rapporte au client.»

Pour Maïko Tourre, 19 ans, en 2e bachelier, ce travail de *pentest* ressemble, un peu, «à une sorte d'*escape game* à l'envers: il faut être patient, persévérant et chercher partout non pas la sortie mais l'entrée du labyrinthe». Ce qui, selon Bryan, demande «un état d'esprit très spécifique, pas juste des compétences techniques. Il faut penser comme un hacker, pour que les automatismes se créent. On doit aussi avoir cette envie de creuser, encore et encore. Toujours plus loin. Et cette curiosité, pour savoir comment un programme est fait, de fond en comble. C'est indispensable pour pouvoir imaginer comment et par où il pourrait être victime d'attaques.»

Grande demande, grandes valeurs

Les cyberattaques se sont multipliés en 2025: en avril, contre le Service public de la Région wallonne; en septembre, contre Brussels Airport; en novembre, contre le service de renseignement militaire; en décembre (en cinq jours, 1.249 offensives et 64 cibles!), contre

HACKERONE

Des plateformes comme HackerOne mettent en relation hackers éthiques et entreprises.

la Chambre, les provinces de Liège et du Limbourg, Eneco, Elia, Luminus, Mega, Ecopower, des transporteurs au port d'Anvers... Par conséquent, on comprend, comme le relève Bastien Bodart, maître assistant en cybersécurité à la haute école, qu'«un bon nombre d'entreprises ont l'obligation légale d'élever leur niveau de sécurité informatique, d'autant que parmi celles qui sont hackées, une sur deux fait faillite l'année qui suit...» Et que la demande augmente continuellement: le secteur regroupe en Belgique 732 entreprises et organisations, comptait 9.750 emplois fin 2024 (+52% en trois ans) et en recherche 4.000 supplémentaires, au moins, d'ici à 2030, selon Agoria, la fédération belge des entreprises technologiques.

Dès lors, «95% de nos étudiants arrivés au bout de leur bachelier trouvent du boulot dès la sortie de leur stage (quatorze semaines en entreprise), sourit Bastien Bodart. Dans la consultance, le privé, le public, la police... Impossible d'y quantifier la proportion de *pentesters* ou de hackers éthiques mais, c'est clair: la cybersécurité est un excellent débouché.»

Excellent et exigeant: «Les techniques sont communes, dans le monde entier, souligne Bastien Bodart, mais les menaces changent: on découvre 5.000 vulnérabilités par an (les autres se vendent au marché noir). Conséquences: il faut, et singulièrement pour le hacking éthique, sans cesse se maintenir à jour. Nous, formateurs, en premier.» Comment? «En faisant beaucoup d'autoformation, avance Philippe Van Goethem, lui aussi enseignant à l'Hénallux. En ayant par ailleurs accès à des formations, avec certifications, et à certains groupes de travail au sein de la Cybersecurity Coalition, mise en place par le gouvernement et réunissant acteurs du privé, du public et de l'académique pour partager les bonnes pratiques en la matière.»

Célien Desteucq s'abreuve à d'autres sources: «Des personnes comme James Kettle, de chez PortSwigger, entreprise spécialisée dans la sécurité Web, publient sur Internet ou sur les réseaux (comme LinkedIn et X) lorsqu'elles trouvent de nouveaux types de vulnérabilités.» Maël s'accroche «aux plateformes d'entraînement en ligne: TryHackMe, Hack The Box, Root Me, PortSwigger Web Academy, PentesterLab... Et aux rapports de hackers de *bug bounty*.» Maïko, lui, est plutôt «YouTube, où on explique où on a découvert une nouvelle faille, comment elle a été exploitée, comment les Russes ont attaqué l'aéroport, etc.».

Au point, parfois, d'être tenté de passer du côté obscur de la force? «Chaque hacker a son code moral, ses valeurs, considère Maïko. Comme partout ailleurs dans la société. Certains peuvent donc verser dans l'illégalité, pour des raisons idéologiques ou financières, par besoin de reconnaissance, par plaisir aussi –parce que réussir à prendre le contrôle d'un site, par exemple, ça doit être quelque chose, quand même!» Maël ne le cache pas davantage: «On y a tous déjà pensé au moins une fois. Entrer dans le système d'une banque, par exemple, et réaliser un gros casse! Mais on a choisi de rendre service, de protéger. Le cours de déontologie sert à ça: poser le cadre de ce qu'on a le droit ou pas de faire et préciser le type de contrat qu'il faut passer avec le client.»

Parce qu'on a beau être un chevalier blanc, la croisade n'est pas bénévole pour autant. ●