Les hackers éthiques : pourquoi vous avez besoin d'eux, et où trouver les meilleurs ?

Inutile de se voiler la face : partout dans le monde, les entreprises ont de plus en plus de mal à faire face à l'évolution rapide de la cybercriminalité, et à suivre l'évolution rapide des techniques imaginées par les pirates (qui sont, eux, de plus en plus motivés et de mieux en mieux rémunérés)

Et vu ce qui arrive sur le front des technologies, cette tendance n'est pas près de disparaitre d'elle-même : des technologies émergentes telles que l'Internet des objets (IoT) élargissent constamment les surfaces d'attaque exploitables, parfois même plus rapidement que les entreprises ne peuvent les identifier et s'organiser. Sans parler, bien sûr, du mouvement vers le Cloud, qui voit des volumes massifs de données et d'applications migrer de manière parfois chaotique en laissant au passage des « buckets » entiers de données non protégées et accessibles à tous.

L'une des approches que les entreprises mettent souvent en oeuvre pour comprendre ces risques et parvenir à suivre les innovations des cybercriminels, c'est de combattre le feu par le feu : mettre des pirates « éthiques » face aux pirates malveillants. On parle alors de White Hats (chapeaux blancs) pour désigner ces pirates éthiques, par opposition aux Black Hats, les pirates malveillants.

Car bien que les architectes de sécurité possèdent de vastes connaissances sur les meilleures pratiques de sécurité, ils manquent souvent d'expérience de terrain sur la façon dont les attaquants effectuent, par exemple, leur reconnaissance, enchaînent les attaques et pénètrent les réseaux de l'entreprise.

Et cela n'est bien sûr pas le cas du pirate éthique. Doté - on l'espère - de toutes les compétences et de la ruse de ses adversaires, il est légalement autorisé à exploiter les réseaux et les systèmes, en corrigeant au passage les vulnérabilités détectées lors de ses tests. Bien entendu un tel pirate éthique est également tenu de divulguer toutes les vulnérabilités découvertes durant sa mission, et pas uniquement celles qu'il a pu exploiter pour entrer !

Un marché en pleine expansion

Selon le rapport Hackers 2019 de la société HackerOne, la communauté des pirates éthiques a doublé en une année. Et il n'y a rien d'étonnant à cela quand on sait combien cette activité peut rapporter. En 2018, 19 millions de dollars ont ainsi été distribués en primes à des White Hats engagés pour rechercher des vulnérabilités, ce qui correspond presque au total des sommes versées au cours des six années précédentes combinées. Et le tout évidemment de manière légale, sans risquer de passer par la case prison.

Le rapport estime également que les pirates éthiques les mieux payés peuvent représenter jusqu'à quarante fois le salaire annuel médian d'un ingénieur en informatique dans leur pays d'origine, ce qui évidemment suscite des vocations...

Mais où trouver ces perles rares ?

Il reste cependant que les entreprises ont du mal à identifier et s'attacher les services de tels experts. Plusieurs options s'offrent à eux :

- Recourir à du crowd sourcing (Bug Bounty) public
- Embaucher un hacker
- Faire évoluer ses techniciens
- Repérer des talents au sein de l'entreprise

La méthode la plus courante pour travailler avec des White Hats compétents est d'instaurer un système de "prime aux bogues", fonctionnant de manière très encadrée à travers un programme de Bug Bounty.

De cette façon, n'importe qui peut, depuis Internet, rechercher et soumettre les vulnérabilités découvertes sur les systèmes sélectionnés par l'entreprise et avoir ainsi une chance de gagner une prime. Cela fonctionne généralement très bien pour les services accessibles au public, tels que les sites Web ou les applications mobiles. Les récompenses dépendent évidemment de la sévérité des vulnérabilités découvertes, après validation par l'entreprise.

Un tel recours au crowdsourcing et au paiement d'incitation présente des avantages évidents. Les pirates entretiennent leur réputation et/ou gagnent de l'argent de manière légale, sans aucun risque pour eux. En échange, l'entreprise bénéficie d'un influx de nouvelles idées, de nouvelles pratiques et de techniques de pointe pour évaluer sa sécurité. Tout le monde y gagne !

D'autres entreprises préfèrent, plutôt que de recourir à des pirates éthiques publics, embaucher directement des pirates informatiques. Bien qu'il puisse sembler contre-intuitif de faire appel à de futurs collaborateurs pouvant avoir des antécédents criminels, les entreprises qui font ce choix sont surtout attirées par leur grande expérience pratique. Toutefois, l'emploi d'un ex-cybercriminel est une décision risquée qui devrait être prise au cas par cas. Mais cela peut valoir la peine. Par exemple, il est peu probable qu'une personne accusée d'une attaque par déni de service à un jeune âge ait muté en un cybercriminel de carrure internationale. En fait, certains jeunes contrevenants deviennent souvent des consultants en sécurité et des leaders d'opinion respectés dans l'industrie.

Ne pas sous-estimer les talents internes

Les entreprises en recherche de cybertalents devraient également mieux exploiter les compétences des développeurs et autres spécialistes réseau qui bâtissent déjà leurs applications, développent leur code et font fonctionner leur infrastructure réseau.

Beaucoup de développeurs qui, certes, apprécient de bâtir des solutions, prennent encore plus de plaisir à les améliorer en y recherchant des failles ou tentant de « jouer » avec de manière créative. Ne pas proposer à de tels profils d'évoluer vers un poste de cybersécurité serait du gâchis.

Enfin, un autre terrain de chasse fertile pour de tels pirates éthiques pourrait s'avérer être partout ailleurs dans l'entreprise ! Car au-delà des développeurs et autres profils techniques, les meilleurs praticiens de la sécurité sont curieux, avec une passion pour le bidouillage, et en particulier pour démonter et remonter tout ce qui leur tombe sous la main. Ces gens-là, quel que soit leur rôle dans l'entreprise, devraient être identifiés et autorisés à se former à la cybersécurité.

Et cela tombe d'ailleurs plutôt bien car les moyens de les former existent désormais. Jadis jamais enseigné, le piratage éthique est aujourd'hui de plus en plus formalisé. Parmi les qualifications notables qui pourront accompagner vos futurs White Hats maison, citons le Certified Ethical Hacker (CEH), l'Offensive Security Certified Professional (OSCP) ou le Global Information Assurance

Certifications (GIAC).

Naturellement, de nombreux hackers chevronnés s'opposeront à de telles formations, mais il ne faut pas pour autant ignorer cette tendance. Le piratage éthique est appelé à devenir de plus en plus courant à mesure que les entreprises gagnent en maturité en matière de sécurité. Elles comprennent alors rapidement toute la valeur qu'elles peuvent tirer d'un pirate éthique capable de rechercher et d'exploiter leurs propres vulnérabilités avant qu'un Black Hat ne le fasse