Hacker éthique et cybersécurité, est-ce possible ?

Myriam QUEMENER
Magistrat honoraire
Docteur en droit

Amélie KOCKE
Consultante en criminalité financière

Face à une actualité particulièrement riche relative à des hackers majoritairement dépourvus d'éthique [1] , il apparaît important de cerner ces personnages de façon plus précise. En effet, les hackers sont encore dans l'ensemble souvent perçus comme des pirates informatiques qui à la fois fascinent et angoissent. Il faut relever que la plupart des hackers dont on parle dans les médias sont en fait des cybercriminels ou « black hat » qui ont attaqué des systèmes d'information ou exploité des failles de sécurité pour récupérer des milliers de données numériques revendues ensuite, y compris dans le Darkweb. Tel est le cas par exemple du mineur de 17 ans récemment interpelé et mis en examen pour avoir piraté de façon massive la base de données de Free, portant sur 19,2 millions de clients français dont 5,11 millions incluant un numéro d'IBAN. Cette base avait été mise en vente aux enchères sur un forum cybercriminel et le mineur, déjà connu pour des faits similaires avait perçu la somme de 10 000 euros pour cette action illicite.

Cependant, tous les hackers ne sont pas tous des cybercriminels [2] qui devraient d'ailleurs être dénommés plutôt crackers que hackers.

En effet, certains agissent pour le bien commun et la protection des systèmes d'information d'entreprises ou d'organisations par exemple et sont appelés « white hat » ou hackers éthiques [3] . Parfois, la frontière entre ces deux catégories de hackers peut être faible, certains d'entre eux apparaissant même « borderline », comme par exemple celui qui indique après avoir été cybercriminel être un hacker repenti[4] et avoir retrouvé le brouteur[5] c'est-à-dire l'auteur de l'arnaque au faux Brad Pitt[6] qui a dépouillé une Française d'une somme de 830 000 euros.

L'analyse juridique de ces hackers éthiques qui vient d'être publiée[7] tombe à point nommé en permettant de distinguer ces deux types de hackers et de décrypter l'éthique des hackers afin de comprendre le rôle qu'ils peuvent avoir pour contribuer à la cybersécurité des entreprises et des organisations. Il convient d'aborder en premier lieu le profil des hackers qui sont en fait des cybercriminels, puis le régime juridique des hackers éthiques.

Les hackers cybercriminels

Les hackers qui sont identifiés au terme d'une enquête peuvent faire l'objet de poursuites, notamment sur le fondement des infractions

[1] Le hacker Florent Curtet a été condamné à 2 ans de prison avec sursis pour association de malfaiteurs et complicité de tentative d'extorsion https://www.lemonde.fr/pixels/article/2024/12/16/le-hackeur-florent-curtet-condamne-a-deux-ans-de-prison-avec-sursis_6452291_4408996.html

[2] Ou « Black Hat »

[3] G.Goubin, L.Janaszewicz « le hacker éthique, votre meilleur ennemi ? », Dalloz IP/IT 2021, p.505

[4] https://www.lalsace.fr/faits-divers-justice/2025/01/18/faux-brad-pitt-cette-campagne-de-cyberharcelement-est-en-train-de-detruire-anne

[5] Escroc opérant sur Internet, notamment sur les réseaux sociaux. Le phénomène d'escroquerie en ligne ou « broutage » est apparu dans les années 2000.

[6] On évoque le terme de brouteur.

[7] M.Quéméner , A.Köcke , « Hacker éthique et cybersécurité, opportunités et défis » , Lextenso 2024

d'atteinte au fonctionnement et aux données contenues dans un système de traitement automatisé de données (STAD). L'entreprise victime de l'acte malveillant pourrait également se prévaloir, selon les circonstances, d'un abus de confiance commis à son préjudice. Selon l'article 323-1 du Code pénal « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 euros d'amende. Lorsqu'il en résulte soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 euros d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000€ d'amende. »

Ainsi, le simple fait d'accéder ou de se maintenir frauduleusement dans un système de traitement automatique de données peut être sanctionné par la loi pénale. Or, l'activité du hacker éthique consiste à s'introduire dans un système informatique sans droit d'accès afin de découvrir les éventuelles failles du système. En revanche, tous les hackers éthiques n'agissent pas forcément dans le cadre d'un bug bounty ou d'un audit de sécurité.

Aux termes de l'article 323-3-1 du Code pénal « le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ». Les hackers éthiques ne sont pas toujours à l'abri de poursuites sur cette base juridique, par exemple s'ils diffusent des failles de sécurité sans respecter une procédure bien définie avec le client afin d'éviter de nuire à sa réputation[8] numérique.

L'infraction de collecte frauduleuse des données personnelles, punie par l'article 226-18 du Code pénal, a parfois été retenue cumulativement soit avec l'accès frauduleux dans un système de traitement automatisé de données, soit avec l'extraction de données visée par l'article 323-3 du Code pénal. Il est aussi retenu les infractions d'association de malfaiteurs et complicité de tentative d'extorsion. En outre, par exemple dans la procédure Florent Curtet, ce dernier a été condamné à la peine complémentaire d'interdiction d'exercer dans le domaine de la cybersécurité pendant cinq ans, dont quatre avec sursis et des peines d'amende[9] .

Les hackers éthiques

Les hackers éthiques dénommés également chercheurs ou hunters par des entreprises craignant les confusions peuvent avoir une place de choix à prendre en matière de cybersécurité, à la condition de s'inscrire dans un dispositif contractuel bien défini pour rassurer les organisations et inspirer la confiance. En effet, l'activité des hackers éthiques consistant à signaler les vulnérabilités des systèmes informatiques afin de les corriger, renforce la cybersécurité. L'intérêt croissant de l'activité des hackers éthiques se reflète notamment avec le développement considérable des programmes de bug bounty.

Face à la complexification technique des cybermenaces, se passer des hackers éthiques semble être un risque pour la protection des systèmes d'information. Il n'est donc pas dans l'intérêt public de restreindre l'activité de ces véritables lanceurs d'alerte informatique.

[8] https://www.7mag.re/Un-ex-hacker-a-la-rescousse-de-la-victime-du-faux-Brad-Pitt_a19695.html

[9] Florent Curtet doit aussi s'acquitter d'une amende de 13 000 euros et verser, au total, 39 000 euros de préjudice aux différentes parties civiles.

En France, la signalisation spontanée de vulnérabilités à l'Autorité Nationale de la Sécurité des Système d'Information (ANSSI) par les hackers éthiques est encadrée par l'article L.2321-4 du code de la défense. Cet article réserve l'appréciation de la bonne foi du hacker ayant effectué une signalisation aux collaborateurs du CERT de l'ANSSI (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) sans toutefois en connaître précisément les critères.

Plusieurs propositions législatives ont été réalisées sans avoir été retenues, ce qui démontre la difficulté à concilier d'un côté la défense face aux risques d'abus des hackers d'un cadre juridique trop protecteur et de l'autre côté le manque de garantie d'une absence de sanction pour les hackers en cas de signalement.

Face aux cybermenaces grandissantes visant aussi bien les entreprises, les collectivités territoriales et même les hôpitaux, rechercher et opter pour des solutions efficaces est aujourd'hui une priorité pour l'ensemble des organisations.

Les bonnes pratiques du hacking éthique

Des solutions juridiques existent pour garantir un minimum d'encadrement pour les hackers éthiques. Il s'agit par exemple des contrats de pentests (tests d'intrusion) et des bug bounty. Il s'agit en cybersécurité d'un programme organisé par une entreprise ou une organisation invitant des hackers éthiques à identifier et signaler des vulnérabilités (ou bugs) dans leurs systèmes informatiques, applications, ou sites web. En échange, ces chercheurs reçoivent des récompenses financières ou autres avantages en fonction de la gravité des failles découvertes suite à des pentests [10] . Ces solutions ne couvrent cependant pas le signalement spontané de vulnérabilités qui devrait être davantage sécurisé juridiquement, dans l'intérêt à la fois du hacker et du destinataire de cette transmission qui peut être précise.

Actuellement, les hackers éthiques se font connaître aussi au niveau réputationnel par le biais de ce qu'on appelle des Hackathons[11] des concours de hacking encore peu connus des juristes[12] .

Les préconisations proposées dans l'ouvrage qui vient d'être présenté dans le cadre du CyberCercle résultent d'idées de différents professionnels de la cybersécurité interrogés et de l'analyse de réglementations étrangères comme par exemple la Belgique[13] et la Suisse qui encouragent le recours à ces sentinelles du numérique et qui a élaboré un guide de bonnes pratiques pour clarifier la mission des hackers éthiques. Le but est de préciser les conditions de signalement de vulnérabilités afin d'assurer une protection des hackers éthiques face à un risque de sanction.

Il est donc essentiel désormais, ainsi que l'a fait la Belgique, de définir une véritable doctrine de cybersécurité [14] pour les hackers éthiques qui ont toute leur place dans la protection des systèmes d'information des organisations, des entreprises et des collectivités territoriales. Ils peuvent en effet apporter des solutions pour faire face aux risques toujours croissants de cyberattaques.

[10] Test d'intrusion, contraction de l'anglais « penetration test » est une méthode d'évaluation de la sécurité d'un système informatique par la démonstration, par simulation des actions d'attaquants.

[11] Évènement au cours duquel des spécialistes se réunissent pendant plusieurs jours autour d'un projet collaboratif de programmation informatique ou de création numérique.

[12] F.Meuris - Guerrero, Les réunions nocturnes des hackers éthiques, Communication Commerce électronique n°9, septembre 2018, alerte 67

[13] https://www.lemonde.fr/economie/article/2024/12/05/en-belgique-l-essor-du-hacking-ethique_6431562_3234.html

[14] M.Quéméner, A.Köcke, Hacker éthique et cybersécurité , opportunités et défis, Lextenso 2024