PÔLE D'EXCELLENCE
CYBER

HACKING ÉTHIQUE ET SOUVERAINETÉ NUMÉRIQUE : Les nouveaux acteurs de la sécurité

Mars 2026

Région Bretagne

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS

SOMMAIRE

Préface 8

Anne Le Henanff
Ministre déléguée auprès du ministre de l'Économie, des Finances et de la Souveraineté industrielle, énergétique et numérique, chargée de l'Intelligence artificielle et du Numérique 9

Sabine Thillaye
Députée d'Indre et Loire 11

Introduction 14

Brunessen Bertrand 14

Partie 1. Les enjeux du hacking éthique 16

Éthique et cybersécurité
Noobosaurus R3x 18

Une définition du hacking éthique
Nicolas Bottero, Security Manager, Capgemini 22

Le statut d'hacker « éthique »
Mélanie Romano, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool 24

Ethical hacking, perspective d'un CISO
Laurent Guérin, CISO CMA CGM 30

Hacking éthique : le piratage légal et responsable
Christèle JACQ-ARNOULT, Stéphane SZYMANSKI, Damien HARDY 32

Le statut de chercheur en cybersécurité
Mélanie Romano, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool 35

La protection des enfants est-t-elle inclue parmi les objectifs de l'éthique « Hacking » ? De l'empowerment à la sécurité by design.
Stefania Attolini, Docteur en droit 38

Partie 2. Le cadre juridique du hacking éthique en France 40

Approche juridique de la notion de hacking éthique 42
ASC Eve TOURNY, DC DIRISI/DIV NUMO/SD CYBER

Renforcer le statut des lanceurs d'alerte numérique "hackers éthiques" en droit français 44
Fabien Lemarchand, Président de Hack4Values

L'importance du contrat dans le cadre du pentest 46
Jules Cooper, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

Le statut juridique du lanceur d'alerte « numérique » 51
Titouan Le Blé, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

Partie 3. Le cadre juridique du hacking éthique à l'étranger 60

Étude comparée du droit des hackers « éthiques » 62
Elyes Hakmouni, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

Hacking éthique aux États-Unis : entre risque judiciaire permanent et émergence d'un statut protecteur 64
Kamel El Hilali, Docteur en Droit, Chercheur Associé, Information Society Project, Yale Law School

Perspectives 68

Proposition d'amélioration du cadre juridique des hackers éthiques 70
Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

Conclusion 73

Brunessen Bertrand 73

Livre blanc

HACKING ÉTHIQUE

PRÉFACE

Par Anne Le Hénanff, Ministre déléguée auprès du ministre de l'Économie, des Finances et de la Souveraineté industrielle, énergétique et numérique, chargée de l'Intelligence artificielle et du Numérique.

À l'ère du numérique, la cybersécurité est devenue un enjeu stratégique majeur pour les entreprises, les institutions et les citoyens.

Chaque jour, de nouvelles menaces émergent, exploitant les vulnérabilités des systèmes et mettant en péril la confidentialité, l'intégrité et la disponibilité des données. Le panorama de la cybermenace publié par l'ANSSI pour l'année 2025 souligne que la menace cyber est toujours plus présente, exercée par des attaquants d'origines étatiques ou criminelles et visant une grande diversité de cibles. En 2025, 2 209 signalements et 1 366 incidents ont été portés à la connaissance de l'Agence. Face à ces défis, une figure particulière se distingue : le hacker éthique.

Loin de l'image du pirate informatique aux intentions malveillantes, le hacker éthique est un acteur clé de la protection numérique. Son rôle est d'identifier les failles avant qu'elles ne puissent être exploitées par des cybercriminels, contribuant ainsi à renforcer la résilience des infrastructures informatiques. Cependant, ce métier qui apporte une contribution précieuse et essentielle, demeure entouré d'un flou juridique oscillant entre nécessité de sécurité et cadre légal contraignant.

Ce livre blanc, fruit du travail d'experts en cybersécurité, juristes et chercheurs, sous la houlette de Brunessen BERTRAND de l'université de Rennes qui a piloté, depuis deux ans, un groupe de travail au sein du Pôle d'excellence cyber sur le statut des hackers éthiques, et de l'amiral Arnaud COUSTILLIÈRE, se veut une contribution éclairée à la réflexion sur le hacking éthique.

Il explore ainsi ses enjeux, ses implications éthiques et son encadrement juridique en France et à l'étranger. Il met en lumière la nécessité d'un statut clair et protecteur pour ces professionnels de l'ombre, tout en proposant des pistes d'amélioration du cadre légal.

Alors que le Parlement examine le projet de loi Résilience qui transpose la directive européenne NIS 2, qui permettra d'élever le niveau global de cybersécurité des entités qui y seront assujetties, ce livre blanc constitue une contribution essentielle à la réflexion générale sur la cyber-protection de notre pays.

En France, la loi a permis d'encadrer partiellement le statut des hackers éthiques. L'article 47 de la loi du 7 octobre 2016 pour une République numérique a introduit une mesure visant à apporter une protection aux hackers éthiques, sous conditions strictes. Cette loi prévoit que pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule ANSSI une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système d'information. L'ANSSI doit préserver la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que les conditions dans lesquelles celle-ci a été effectuée. Cette disposition protège ainsi les hackers éthiques contre les poursuites.

Il s'agit d'un sujet important, qui mérite de faire l'objet d'une réflexion approfondie, nuancée et équilibrée. C'est tout l'objet de cet ouvrage, dont je salue la très grande qualité.

PRÉFACE

Par Sabine Thillaye, députée d'Indre et Loire

Ce livre blanc du hacking éthique est une excellente initiative au moment où les cyberattaques se multiplient et deviennent le lot quotidien tant d'entreprises, de collectivités comme de particuliers.

Dans un monde aux menaces protéiformes, tous les leviers doivent être utilisés face aux cyberattaques massives, de plus en plus sophistiquées, y compris en facilitant la coopération entre entreprises et hackers dits « éthiques ». Cela demande entre autres de renforcer la protection juridique de ces derniers, véritables « lanceurs d'alerte numérique ».
Ce document propose de réfléchir aux enjeux du hacking éthique, présente le cadre juridique en France et à l'étranger et propose des améliorations du cadre juridique.
Les termes « hacking » et « éthique » paraissent, à première vue, totalement antinomiques. Beaucoup réduisent le hacking à une activité illégale simplement exercée par des cybercriminels animés par l'appât du gain ou directement par des États dans un objectif de déstabilisation. Le hacker éthique existe pourtant bel et bien. Il est de bonne foi, animé par des intentions « bienveillantes » mais en utilisant des moyens « illégaux » afin de s'introduire dans les systèmes d'information. Son activité vise à identifier, tester et corriger les vulnérabilités des systèmes informatiques.

Cela nécessite aussi des définitions claires afin de faire la distinction entre hacking éthique, hacking malveillant et hacking de recherche.

Les hackers éthiques utilisent leurs compétences pour protéger les données et renforcer les infrastructures numériques, plutôt que de les compromettre en identifiant les failles. De nombreuses entreprises et institutions publiques y ont recourt pour renforcer la sécurité de leurs systèmes d'information. Depuis 2021, la direction interministérielle du numérique (DINUM) a mis en place avec YesWeHack - une plateforme de mise en contact avec des hackers éthiques- un programme visant à renforcer la sécurité de FranceConnect en encourageant les hackers éthiques à signaler les failles de sécurité qu'ils pourraient identifier.

Depuis la loi pour une République numérique de 2016, les hackers sont protégés par l'article L2321-4 du code de la Défense, à condition qu'ils transmettent de bonne foi toute information sur une vulnérabilité à l'autorité nationale de sécurité des systèmes d'information. Cette protection a donné naissance à la communauté de hackers « éthiques », bien que, comme déjà souligné, leur appellation puisse sembler paradoxale, relever de l'oxymore, puisqu'ils s'introduisent par des moyens illégaux dans les systèmes afin de détecter les failles. Avec l'avènement des programmes de bug bounty, cette communauté a grandi, mais cela a également augmenté les risques d'infiltration par des individus moins compétents ou malveillants, motivés par la notoriété ou le volume des découvertes plutôt que par une réelle expertise.

Il est donc nécessaire d'établir des standards et des bonnes pratiques dans le domaine, de sensibiliser le plus grand nombre aux enjeux de la sécurité informatique dans un contexte de transition numérique et de favoriser la collaboration entre acteurs de la cybersécurité.

Dans un contexte d'augmentation du nombre de hackers éthiques, il serait intéressant de mettre en place une charte d'engagement impliquant l'élaboration de règles déontologiques flexibles et réactives servant de référence pour les bonnes pratiques en matière de signalement des vulnérabilités et de coopération avec les entreprises.

J'ai eu l'occasion de me pencher sur le statut juridique du hacker éthique et les protections légales dont il bénéficie. Celles-ci sont récentes et datent des lois Sapin II de 2016, renforcée ensuite par la loi Waserman de 2022. Ces deux lois protègent les lanceurs d'alerte, et couvrent partiellement le cas très spécifique des hackers éthiques. La loi Godfrain de 1988 permettait la répression du piratage informatique sans faire de distinction entre le cybercriminel et l'internaute bienveillant. La jurisprudence appliquait jusqu'alors strictement la loi, condamnant les personnes de bonne foi souhaitant alerter de l'existence d'une faille de

sécurité.

Si le hacker éthique bénéficie aujourd'hui d'un cadre juridique plus protecteur, des avancées restent nécessaires, notamment sur la possibilité de faire remonter des failles de sécurités directement vers les responsables des systèmes informatiques sans nécessairement passer par un intermédiaire comme l'ANSSI, comme le propose l'un des contributeurs au livre blanc.

Pour assurer une sécurité juridique plus robuste au hacker éthique, il est crucial d'intégrer dans le code pénal la distinction entre hacker « éthique » et hacker « malveillant » en reprenant notamment la notion de « bonne foi ». Le hacker éthique devrait par ailleurs être considéré comme un lanceur d'alerte et pouvoir bénéficier des mêmes protections, y compris la possibilité de se tourner vers le Défenseur des droits qui l'accompagnerait dans le processus de signalement des vulnérabilités découvertes.

Ce livre blanc du hacking éthique dirigé par Brunessen Bertrand constitue un outil précieux pour le législateur.
Dans un domaine en perpétuelle évolution, il permet un éclairage afin d'adapter au mieux notre législation aux défis croissants de la cybersécurité.

INTRODUCTION

Brunessen BERTRAND, Professeure à l'Université de Rennes, Membre de l'Institut universitaire de France, cotitulaire de la Chaire Cybersécurité, protection des données et droits fondamentaux

La transformation numérique des sociétés contemporaines a profondément modifié les enjeux de la protection des données, des infrastructures critiques et plus largement des interactions économiques et sociales. Cette numérisation croissante draine avec elle de nouvelles vulnérabilités, les systèmes d'information étant devenus des cibles privilégiées pour des acteurs malveillants. Dans ce contexte, les enjeux de cybersécurité se complexifient et s'amplifient, mettant ainsi en avant la question de la détection préventive et de la remédiation rapide des failles de sécurité. C'est précisément dans cet espace stratégique qu'intervient le hacking éthique, discipline souvent mal comprise mais dont l'importance dans les dispositifs contemporains de cybersécurité est désormais incontestable.

Le hacking éthique désigne l'ensemble des pratiques consistant à simuler des attaques informatiques dans un cadre légal et contrôlé, afin d'identifier les vulnérabilités d'un système avant qu'elles ne soient exploitées de manière malveillante. Ces pratiques, qui mobilisent des compétences techniques avancées, s'inscrivent dans une démarche proactive, reposant sur une autorisation explicite et sur une déontologie rigoureuse. Les hackers éthiques contribuent ainsi à renforcer la résilience des systèmes d'information, en jouant un rôle stratégique dans l'écosystème global de la cybersécurité.

Aussi importante soit-elle, cette fonction recouvre cependant des enjeux complexes, tant sur le plan éthique que juridique. Où se situent les frontières entre légitimité et illégalité, entre curiosité technique et violation de la confidentialité ? Dans quelle mesure les cadres normatifs existants permettent-ils d'encadrer efficacement ces pratiques ? Quelle place le hacking éthique occupe-t-il dans les stratégies nationales de cybersécurité ? Enfin, comment repenser la figure du hacker au sein de l'imaginaire collectif, entre mythe subversif et acteur responsable de la sécurité numérique ?

Cet ouvrage se propose d'examiner de manière approfondie les multiples dimensions du hacking éthique. À travers une approche pluridisciplinaire, l'objectif est d'analyser les fondements, les pratiques, les enjeux et les perspectives de cette activité singulière. L'enjeu étant de définir selon quelles modalités le hacking éthique peut s'affirmer comme une réponse légitime, structurée et nécessaire aux défis contemporains de la cybersécurité.

Les enjeux éthiques et juridiques du hacking éthique

Si le hacking éthique s'impose aujourd'hui comme une composante de la cybersécurité préventive, il demeure une pratique ambivalente, dont la légitimité repose sur un équilibre fragile entre liberté d'intervention et respect du cadre juridique. Cette ambivalence soulève plusieurs questions fondamentales : peut-on « attaquer » un système de manière éthique ? À quelles conditions une intrusion peut-elle être considérée comme légitime ? Quels sont les risques d'une pénalisation de ces activités ou, à l'inverse, d'une absence de régulation ?

La frontière entre la curiosité technique, souvent présentée comme un moteur de l'innovation informatique, et la violation délibérée de systèmes protégés est parfois ambiguë. L'histoire du hacking est en effet marquée par une tension constante entre exploration des systèmes informatiques et transgression des limites fixées par leurs concepteurs ou exploitants. Certains actes, bien qu'animés d'intentions non malveillantes, peuvent être interprétés juridiquement comme des intrusions non autorisées, passibles de sanctions pénales.

Cette zone grise est d'autant plus problématique que l'acte de tester un système implique par définition d'y accéder, parfois sans l'autorisation explicite du propriétaire ou de l'administrateur. Or, le cadre juridique interdit et sanctionne l'accès non autorisé à un système informatique, indépendamment de

l'intention de nuire. Cela crée une difficulté pour le hacking éthique : comment contribuer à la sécurité sans risquer des poursuites judiciaires ?

Des initiatives comme les programmes de bug bounty ou de responsible disclosure policies par les entreprises visent précisément à encadrer cette pratique, en définissant des modalités d'intervention autorisées, des périmètres d'analyse, et des mécanismes de rémunération ou de reconnaissance. Cependant, tous les acteurs n'adoptent pas ces dispositifs, et les divergences entre les législations nationales rendent encore difficile l'uniformisation des pratiques.

La question de l'intention et du consentement

L'un des principes fondamentaux du hacking éthique est l'obtention du consentement explicite du propriétaire du système visé. Ce consentement constitue la principale ligne de démarcation avec le black hat hacking (hacking malveillant). Toutefois, dans la pratique, cette exigence pose plusieurs défis. D'une part, certaines failles de sécurité affectent des systèmes interconnectés, dont les propriétaires sont multiples ou indéterminés, rendant l'obtention du consentement complexe, voire impossible. D'autre part, des hackers agissant de manière indépendante peuvent découvrir fortuitement des vulnérabilités dans des systèmes sans avoir été mandatés pour le faire, dans l'objectif supposé de prévenir une exploitation criminelle. Dans ces situations, l'intention bienveillante ne suffit pas et pose la question de l'articulation entre consentement, intérêt général et proportionnalité des moyens employés. Faut-il tolérer, voire encourager, certaines formes de hacking non autorisé si elles visent à renforcer collectivement la sécurité numérique ? Ou doit-on au contraire préserver une stricte légalité, au risque de limiter des compétences parfois nécessaires à la protection des systèmes ?

Les incertitudes du cadre juridique

Sur le plan juridique, la situation des hackers éthiques varie considérablement d'un pays à l'autre alors même qu'appliquer un principe de territorialité à ces activités est souvent un défi. Certains États ont organisé des procédures pour encourager la divulgation responsable de vulnérabilités alors que d'autres disposent d'un cadre plus répressif, dans lequel le hacking, même à visée éthique, peut entraîner des poursuites.

Cette incertitude juridique a des conséquences négatives. Des chercheurs en sécurité, craignant des représailles, choisissent de ne pas divulguer certaines failles découvertes, ou de le faire de manière anonyme. Cela prive potentiellement les organisations de retours nécessaires pour améliorer leur cybersécurité. C'est la raison pour laquelle certains acteurs plaident aujourd'hui pour la création de statuts juridiques spécifiques, de chartes de bonne conduite permettant de distinguer clairement le hacking éthique des actes malveillants, sans pour autant légaliser les intrusions.

Vers un cadre déontologique ?

Au-delà des aspects juridiques, se pose la question d'un cadre éthique propre à la profession de hacker éthique. Plusieurs initiatives émergent pour codifier des principes déontologiques : intégrité, transparence, respect de la vie privée, minimisation des dommages, devoir de signalement… Ces principes visent à construire une culture professionnelle autour du hacking éthique, comparable à celle des médecins ou des avocats, et à renforcer la confiance du public dans ces acteurs techniques.

Mais là encore, une tension subsiste entre encadrement normatif et liberté d'innovation. Si les règles sont trop rigides, elles risquent de freiner l'efficacité des hackers éthiques, dont l'essence repose justement sur une forme de créativité. Si elles sont trop souples, le risque est de voir apparaître des dérives ou des justifications a posteriori d'actions douteuses.

Un équilibre doit donc être trouvé entre responsabilité éthique, sécurité juridique et souplesse consubstantielle à l'exercice de cette activité. Cela suppose un dialogue constant entre les juristes, les chercheurs, les entreprises, les institutions publiques et les communautés de hackers. C'est précisément l'objet des travaux entrepris dans le cadre du Pôle d'excellence Cyber, à la demande de l'Amiral Arnaud Coustillière.

Brunessen
BERTRAND


01

LES ENJEUX DU HACKING ÉTHIQUE

- Éthique et cybersécurité
- Une définition du hacking éthique
- Le statut d'hacker « éthique »
- Ethical hacking, perspective d'un CISO
- Hacking éthique : le piratage légal et responsable
- Le statut de chercheur en cybersécurité
- La protection des enfants est-t-elle inclue parmi les objectifs de l'éthique. « Hacking » ?
  De l'empowerment à la sécurité by design

ÉTHIQUE ET CYBERSÉCURITÉ

Noobosaurus R3x

Éthique et Cybersécurité

La cybersécurité ne se réduit pas à des aspects purement techniques, elle implique également des considérations éthiques fondamentales qui influencent les décisions et les comportements des professionnels du domaine. Nous aborderons, dans cet article, la notion d'éthique en cybersécurité, afin de distinguer éthique et légalité, et nous examinerons des dilemmes éthiques potentiels auxquels ces professionnels sont confrontés.

Définition de l'éthique en cybersécurité

L'éthique se définit comme l'ensemble des principes et valeurs qui guident les comportements humains au sein de la société. En cybersécurité, elle concerne spécifiquement la manière dont les professionnels gèrent les données et les systèmes qui leur sont confiés, tout en tenant compte du bien-être des individus et de la société dans son ensemble.
Il est crucial de distinguer l'éthique de la légalité. La légalité se réfère aux lois et réglementations en vigueur, tandis que l'éthique s'intéresse aux principes du bien et du mal, qui peuvent ou non être couverts par la loi. En cybersécurité, un comportement peut être légal sans être éthiquement justifiable. L'éthique, subjective par nature, peut varier considérablement d'une personne à l'autre, et d'une culture à une autre, ce qui pose des défis particuliers dans un domaine aussi global et interconnecté que la cybersécurité.

Donc, cette éthique, en cybersécurité, est intrinsèquement subjective, car les perceptions de ce qui est moralement acceptable varient considérablement selon les normes culturelles, les expériences personnelles, et les objectifs stratégiques des individus et des organisations. Cette diversité éthique peut engendrer des conflits lorsqu'il s'agit d'élaborer des politiques de cybersécurité qui respectent les différentes attentes des parties prenantes.

Conflits éthiques en cybersécurité : cas pratiques

Les professionnels de la cybersécurité sont fréquemment confrontés à des dilemmes éthiques qui nécessitent une réflexion approfondie. Ces dilemmes ne sont pas de simples théories, mais des réalités pressantes qui testent les principes moraux des individus impliqués. Ces dilemmes ne sont pas un jeu de l'esprit ou une abstraction pour la réflexion mais une réalité tout à fait commune dans le monde de la cybersécurité.

Découverte de données ou d'activités illégales lors d'un test d'intrusion

Prenons l'exemple d'un pentester engagé pour évaluer la sécurité d'une entreprise et découvrant des preuves d'activités illégales, telles que des transactions frauduleuses ou des contenus illicites. Ce professionnel se trouve donc face à un dilemme éthique complexe : doit-il dénoncer ces activités aux autorités ou respecter la confidentialité stipulée par son contrat ?

L'éthique impose de considérer plusieurs aspects de cette situation. D'un côté, le pentester est lié par un accord de non-divulgation garantissant la confidentialité des informations découvertes. Rompre cet accord pourrait compromettre sa carrière et miner la confiance dans ses relations professionnelles futures. Il ne faut pas négliger la pression qui peut reposer sur les épaules d'un salarié face à un tel dilemme. De l'autre, ignorer ces activités criminelles pourrait avoir des conséquences graves pour les victimes potentielles et la société en général. Sans parler de l'obligation légale de dénoncer un crime dont vous auriez pu avoir connaissance.

Pour résoudre ce dilemme, une approche nuancée est nécessaire. La première étape consisterait à faire part de la trouvaille à son supérieur hiérarchique et consulter un conseiller juridique pour clarifier les obligations légales et évaluer les risques de chaque option. Ensuite, un dialogue transparent avec le client pourrait permettre à l'entreprise de prendre des mesures correctives tout en respectant les obligations contractuelles du pentester. Cette approche équilibrée tente de concilier responsabilité légale et morale avec les contraintes professionnelles inhérentes au métiers de la cyber.

Conservation d'une Zero-Day par une équipe de Red Team

Considérons un autre scénario : une équipe de Red Team découvre une vulnérabilité Zero-Day dans un logiciel largement utilisé. Au lieu de signaler immédiatement cette vulnérabilité au développeur pour correction de la faille, l'équipe décide de garder cette information secrète pour l'exploiter dans de futurs contrats, lui permettant d'avoir un point d'entrée facilité sur des systèmes d'informations. Ce choix, motivé par des considérations commerciales, soulève de sérieuses questions éthiques.

La rétention d'une vulnérabilité expose potentiellement des millions d'utilisateurs à des risques de sécurité, ce qui va à l'encontre de la responsabilité sociale des professionnels de la cyber. La tentation de prioriser le profit commercial sur la sécurité publique révèle un conflit d'intérêts fondamental. De plus, si cette équipe a pu découvrir cette faille, rien ne prouve qu'une équipe de cybercriminels ne l'exploitent pas déjà. L'éthique exige ici une introspection rigoureuse : quel est le véritable rôle d'un professionnel de la cybersécurité ? Est-ce de maximiser le profit à tout prix ou de protéger la société contre les menaces numériques ?

La solution éthique à ce dilemme réside dans la divulgation responsable. L'équipe devrait informer le développeur de la vulnérabilité trouvée, permettant ainsi sa correction avant que l'information ne soit rendue publique. Adopter et adhérer à des codes de conduite stricts peut également prévenir de tels dilemmes à l'avenir, en instaurant des normes claires sur la gestion des vulnérabilités.

Utilisation de l'OSINT dans une campagne de cyberattaque

Enfin, troisième exemple, imaginons une situation où une équipe offensive, engagée pour mener une campagne de reconnaissance contre une cible spécifique, utilise l'Open Source Intelligence (OSINT) pour collecter des informations. Au cours de cette collecte, l'équipe découvre des informations sensibles et privées sur des employés de l'organisation cible, comme des détails personnels, des habitudes de vie ou des communications privées accessibles via des réseaux sociaux et d'autres sources publiques.

Les membres de l'équipe sont alors confrontés à un dilemme éthiquement complexe : doivent-ils utiliser ces informations pour affiner leur attaque et maximiser son efficacité, ou doivent-ils respecter la vie privée des individus et s'abstenir d'exploiter ces données personnelles ?

D'un côté, utiliser ces informations peut permettre à l'équipe d'atteindre ses objectifs de manière plus efficace et démontrer la vulnérabilité de la cible, justifiant ainsi l'engagement de l'équipe par leur client. Cependant, exploiter ces données personnelles soulève des questions éthiques importantes, notamment le respect de la vie privée et les conséquences potentielles pour les individus concernés.

Pour résoudre ce dilemme, l'équipe offensive devrait adopter une approche éthique en accord avec la nature offensive de leur mission. Une première étape consisterait à évaluer la nécessité et l'impact de l'utilisation de ces informations personnelles dans le cadre de cette opération. Ensuite, il serait pertinent de consulter les régulations et les normes éthiques en vigueur, s'il en existe déjà, ainsi que les politiques internes de l'organisation employant l'équipe, pour déterminer les limites légales et éthiques de leur action.

Une approche équilibrée pourrait consister à utiliser les informations collectées pour sensibiliser la cible à ses vulnérabilités sans exploiter les données personnelles de manière invasive. Cela peut inclure la création de scénarios d'attaque simulant les découvertes sans révéler explicitement les informations personnelles collectées.

Ces différents scénarios n'ont pas pour but d'indiquer un comportement ou une réaction exclusive et déterminée à un problème éthique donné. Il faut cependant bien prendre en compte la diversité des problèmes rencontrés, des situations professionnelles et de la subjectivité de l'éthique de tous les acteurs impliqués. Il n'est pas possible, à notre niveau, d'indiquer quelle serait la seule et unique démarche à entreprendre face à un problème éthique soulevé lors d'un engagement en cybersécurité.

Gérer la subjectivité éthique

La complexité éthique de la cybersécurité implique de reconnaître que la certitude est souvent absente et que les réponses simples sont rares. La subjectivité éthique ne constitue pas une faiblesse à surmonter, mais une réalité à embrasser. Chaque décision dans ce domaine est imprégnée de valeurs, de jugements et de conséquences. Pour gérer cette subjectivité, il est nécessaire de disposer d'outils robustes et de pratiques adaptatives permettant de naviguer à travers les nuances et les contradictions inhérentes à ce secteur.

Développement de codes de conduite

Le développement de codes de conduite doit être perçu non pas comme un simple exercice bureaucratique, mais comme un acte de concertation éthique. Ces codes devraient émerger d'un dialogue profond et

continu entre toutes les parties prenantes, incluant les professionnels, les entreprises, les régulateurs, et même les utilisateurs finaux. Ce processus vise à établir un consensus éthique, un socle de valeurs partagées transcendant les différences culturelles et contextuelles.
Il est toutefois crucial que ces codes de conduite demeurent flexibles. La rigidité des normes éthiques peut conduire à des impasses morales, incapables de s'adapter aux nouvelles réalités technologiques et sociales. La flexibilité permet de répondre aux variations culturelles et aux contextes spécifiques sans perdre de vue les principes fondamentaux. Cette adaptabilité est essentielle pour maintenir la pertinence et l'efficacité des pratiques éthiques dans le monde de la cybersécurité, monde mouvant et en perpétuel changement.

Formation et sensibilisation continues

La formation et la sensibilisation ne sont pas des tâches ponctuelles, mais des engagements permanents. Former les professionnels de la cybersécurité, qu'ils soient novices ou expérimentés, est une tâche qui exige rigueur et profondeur. Il ne suffit pas de transmettre des connaissances techniques, il faut aussi cultiver une conscience éthique. Il faut se rendre compte, avant toute chose, de l'avancée de la réflexion sur l'éthique du futur professionnel en cybersécurité. Avant même de suivre une formation techniques très poussée, les futurs professionnels de la cyber doivent avoir la fibre éthique bien ancrée en eux. Et donc, cette éducation doit commencer dès les premiers jours de formation académique et se poursuivre tout au long de la carrière professionnelle.

Pour les élèves et futurs professionnels, les programmes éducatifs doivent intégrer des modules d'éthique de la cybersécurité. Les étudiants devraient être confrontés à des dilemmes moraux réels et hypothétiques, encourageant ainsi la réflexion critique et le débat. Ces exercices aident les étudiants à développer une boussole éthique personnelle qui les guidera dans leurs futures décisions professionnelles et leur permettra de confronter leur éthique avec celles des autres.

Pour les professionnels actuels, la formation continue est indispensable. Les cybermenaces évoluent rapidement, tout comme les outils et techniques pour les contrer. De même, les implications éthiques de ces nouvelles technologies doivent être comprises et intégrées dans les pratiques quotidiennes. Les formations régulières, les ateliers de sensibilisation et les discussions de cas concrets ou hypothétiques peuvent renforcer la cohérence des pratiques et préparer les professionnels à gérer les dilemmes éthiques avec discernement et responsabilité.

Mécanismes de résolution de conflits

Dans un domaine aussi complexe que la cybersécurité, les désaccords éthiques sont inévitables. Il faut donc mettre en place des mécanismes de résolution de conflits clairs et accessibles. Ces mécanismes doivent être transparents et justes, permettant à chaque partie de s'exprimer et de défendre son point de vue. Ils doivent également favoriser des solutions constructives et respectueuses des principes éthiques établis auparavant.

Un environnement de travail transparent et responsable ne peut être maintenu que si les conflits éthiques sont gérés de manière proactive et réfléchie. Cela inclut la création de comités d'éthique, la mise en place de protocoles de médiation et l'encouragement à la communication ouverte et honnête. Ces initiatives visent non seulement à résoudre les conflits, mais aussi à prévenir leur apparition en cultivant une culture d'éthique et de responsabilité.

Les comités d'éthique devraient jouer un rôle crucial dans la gestion des conflits éthiques en cybersécurité. Composés de professionnels expérimentés et de représentants des différentes parties prenantes, ces comités auraient pour mission d'évaluer les situations conflictuelles de manière impartiale, de fournir des recommandations basées sur les principes éthiques établis et de garantir que toutes les parties concernées puissent s'exprimer.

La médiation, quant à elle, est un outil puissant pour résoudre les conflits éthiques. Les protocoles de médiation doivent inclure la désignation de médiateurs neutres et formés, des procédures claires pour initier et mener à bien les sessions de médiation, ainsi qu'un cadre de discussion visant à trouver des solutions acceptables pour toutes les parties impliquées.

Pour prévenir les conflits éthiques, il est fondamental d'encourager une communication ouverte et honnête au sein des organisations. Cela inclut la promotion d'un environnement où les employés se sentent en sécurité pour exprimer leurs préoccupations éthiques sans crainte de répercussions de leur hiérarchie. Organiser régulièrement des forums de discussion et des ateliers sur l'éthique, ainsi que mettre en place des canaux de communication confidentiels pour signaler les problèmes éthiques, contribue à renforcer cette culture de transparence et de responsabilité.

Aux décideurs politiques

Les décideurs politiques, à tous les niveaux, jouent un rôle crucial en définissant le cadre légal et éthique dans lequel opèrent ces professionnels de la cybersécurité. Il est essentiel que les régulations intègrent les

dimensions éthiques de la protection des données et des systèmes d'information, comme cela a été fait avec le RGPD. Cela implique d'élaborer des lois qui ne se contentent pas de prescrire des mesures techniques, mais qui établissent également des standards éthiques clairs et applicables.

La coopération internationale est également indispensable. Les cybermenaces étant globales par nature, les réponses doivent l'être également. Promouvoir des standards éthiques internationaux et encourager la collaboration entre les nations pour harmoniser les régulations et partager les meilleures pratiques est essentiel. Cette coopération internationale peut s'appuyer sur des accords, des conférences et des forums internationaux dédiés à la cybersécurité pour créer une base commune d'éthique et de régulations. La tâche est vaste mais pas inaccessible. Il faut profiter de l'interconnexion des multiples communautés en cyber afin de faire avancer ces idées.

Aux professionnels de la cybersécurité

Pour les professionnels de la cybersécurité, l'intégration de l'éthique dans la pratique quotidienne est essentielle. Il ne suffit pas de suivre les lois à la lettre, il faut également adopter une perspective éthique qui guide les décisions au-delà de la simple conformité. Chaque action technique doit être évaluée non seulement en termes de son efficacité, mais aussi de ses implications morales. Cette approche holistique garantit que les décisions prises respectent les principes éthiques tout en répondant aux exigences de sécurité.

La formation continue joue un rôle central dans cette approche. Les professionnels doivent être régulièrement exposés à des dilemmes éthiques réels et hypothétiques, encouragés à réfléchir de manière critique et à débattre des meilleures façons de résoudre ces situations. Ce processus de réflexion et d'éducation doit commencer dès la formation académique et se poursuivre tout au long de la carrière professionnelle. Les programmes de formations continues devraient inclure des modules sur l'éthique appliquée à la cybersécurité, avec des études de cas concrets et des simulations de scénarios éthiques complexes.

Conclusion

En conclusion, la cybersécurité ne peut être efficacement gérée sans une profonde intégration des considérations éthiques. Les dilemmes éthiques auxquels les professionnels sont confrontés soulignent l'importance de développer une approche nuancée et réfléchie, où les décisions techniques et morales s'entrelacent pour garantir la sécurité et la confiance publique.

Les décideurs politiques ont la responsabilité de créer un cadre légal qui non seulement régule les aspects techniques mais aussi intègre des standards éthiques robustes et applicables. Et il faut insister sur cette notion d'applicable. Cette régulation doit être soutenue par une coopération internationale, car les cybermenaces ne connaissent pas de frontières. Harmoniser les régulations et promouvoir des standards éthiques globaux est essentiel pour une réponse coordonnée et efficace aux défis posés par la cybersécurité.

Les professionnels de la cybersécurité, quant à eux, doivent s'engager à adopter une perspective éthique dans leur pratique quotidienne de leur travail. Cela implique une évaluation constante des implications morales de leurs actions et une formation continue pour rester informés des évolutions technologiques et éthiques. L'éducation éthique doit commencer dès les premiers jours de formation académique et se poursuivre tout au long de la carrière, afin de développer une boussole morale capable de guider les décisions professionnelles dans des situations complexes.

La cybersécurité ne peut être efficacement gérée sans une profonde intégration des considérations éthiques.

La gestion de la subjectivité éthique nécessite des outils et des structures adaptés. Les codes de conduite doivent être élaborés de manière participative, et des mécanismes clairs de résolution de conflits éthiques doivent être mis en place. Comités d'éthique, protocoles de médiation et forums de discussion ouverts sont autant de moyens pour assurer que les questions éthiques peuvent être discutées et résolues de manière juste et transparente.

Un environnement de travail transparent et responsable est indispensable pour naviguer dans les complexités éthiques de la cybersécurité. Les défis éthiques influencent non seulement la sécurité, mais aussi la vie privée et la confiance publique. Il est impératif que les décideurs politiques et les professionnels de la cybersécurité reconnaissent et abordent ces défis avec rigueur et discernement. En fin de compte, une approche éthique solide en cybersécurité contribue non seulement à protéger les systèmes et les informations, mais aussi à renforcer la confiance et la sécurité de la société dans son ensemble.

UNE DÉFINITION DU HACKING ÉTHIQUE

Nicolas BOTTERO, Security Manager, Capgemini

L'ère numérique dans laquelle nous vivons impose un haut niveau de sécurisation de nos systèmes informatiques et de l'accès à nos données professionnelles et personnelles.

Dans ce contexte, le hacking éthique joue désormais un rôle primordial dans la protection de nos actifs numériques en identifiant et en permettant de corriger les vulnérabilités afin d'empêcher tout acteur malveillant de les exploiter.

Cette contribution vise à poser un cadre pour définir le hacking éthique, ses méthodologies, ses avantages et ses limites afin de permettre aux organisations d'envisager les meilleures pratiques.

Le hacking éthique, de quoi s'agit-il ?

Aujourd'hui, la différence technique entre le hacking éthique et le piratage est nulle. La différence morale est cependant essentielle. A partir de ce constat la différenciation entre un hacker éthique et son contraire, le hacker malveillant, est une question de morale et de perspective.

En effet, le terme « hacker » désignait à l'origine un programmeur ou un utilisateur informatique enthousiaste, très doué techniquement et capable de trouver des moyens de contourner ou détourner l'utilisation d'un système. Désormais le terme a pris un nouveau sens et désigne un individu qui pénètre illégalement dans des systèmes informatiques à des fins personnelles. Le terme de hacker a continué d'évoluer dans la littérature et il est aujourd'hui associé à différents qualificatifs.

On parle ainsi de « Black hats » pour désigner des hackers animés par des intentions malveillantes et préjudiciables. Par opposition, il existe les « white hats » qui correspondent à nos hackers éthiques mettant à profit leurs compétences pour protéger et défendre les systèmes. Nous avons également les « grey hats » dont les motivations sont plus opportunistes car capables d'agir de manière éthique ou non en fonction des circonstances. Les « hacktivistes » et les « cyber terroristes » sont quant à eux animés par la volonté de promouvoir une cause sociale, politique ou religieuse. Enfin les « script kiddies » utilisent des ressources existantes à des fins de piratage mais n'ont pas les compétences pour développer leurs propres outils, ils peuvent appartenir à l'une des trois catégories citées précédemment, « black », « white » ou « grey hats ».

Par opposition aux hackers malveillants dont les motivations sont criminelles, le hacking éthique consiste à utiliser des techniques de piratage afin d'évaluer la sécurité des systèmes informatiques et de leurs réseaux. De ce fait, le hacking éthique est mis en œuvre avec l'autorisation du propriétaire du système ciblé, car il a pour but d'améliorer la sécurité plutôt que de causer des dommages. Dans ce contexte, le hacking éthique regroupe principalement les « pentesters » et les chercheurs en sécurité.

Le hacking qu'il soit éthique ou pas repose sur la même méthodologie articulée autour de 5 phases :

- La reconnaissance qui vise à collecter les informations sur la cible, telles que l'infrastructure réseau, les systèmes d'exploitation, les applications utilisées. Des techniques passives comme la collecte d'informations sur Internet ou l'ingénierie sociale ainsi que des techniques actives comme le balayage des ports ou l'analyse du trafic réseau peuvent être mises en œuvre ;

- Le balayage grâce à des outils permettant la recherche de vulnérabilités dans les systèmes et les réseaux permet d'identifier les ports ouverts, les services en cours d'exécution ainsi que les faiblesses de configuration potentiellement exploitables ;

- La phase d'accès permet l'exploitation des vulnérabilités exposées afin d'obtenir une ou des entrées non autorisées dans les systèmes.

- Le maintien de l'accès aux systèmes permet d'établir une persistance, d'une part pour se créer une deuxième porte d'entrée si l'accès initial n'est plus disponible et d'autre part se donner l'opportunité d'étendre la compromission à d'autres systèmes.

- L'effacement des traces consiste à supprimer toutes les preuves de présence dans les systèmes une fois les tests terminés.

Reposant sur cette méthodologie, différents types de tests de hacking éthique sont envisageables. Chaque type correspond à la simulation d'une attaque particulière :

- Les tests en boite noire qui nécessitent aucun accès préalable aux informations sur le système ciblé, simulant ainsi une attaque par un hacker externe ;

- Les tests en boîte blanche qui grâce à un accès complet aux informations sur le système ciblé permettent de simuler une attaque par un initié ;

- Les tests en boîte grise qui via un accès partiel ou limité aux informations simulent une attaque réalisée par un employé ou un individu disposant de privilèges limités.

Si par nature les actions des hackers sont illégales, celles réalisées dans le cadre du hacking éthique peuvent être considérées comme leur antithèse. En effet là où le piratage va laisser derrière lui des dégâts (systèmes paralysés, vols de donnés, espionnage industriel, préjudices commerciaux, atteintes à l'image et à la réputation), le hacking éthique a lui pour vocation à empêcher ou limiter ces risques.
Ainsi et par définition le hacking éthique s'inscrit dans une perspective d'amélioration de la sécurité. L'identification et la correction de failles avant qu'elles ne puissent être exploitées permet en effet de fournir des recommandations pour renforcer la sécurité et prévenir les cyberattaques. Le hacking éthique permet également d'aider les organisations à se conformer aux différentes réglementations et à leurs évolutions.

L'association du terme éthique à la notion de hacking n'est pas un oxymore. Néanmoins cela soulève des implications morales fondamentales telles que la confidentialité et la responsabilité, qui tant qu'elles sont respectées sont les garantes de la bonne définition du hacking éthique.

Afin de garantir le caractère éthique et responsable des actions de hacking, celles-ci doivent être en permanence encadrées. L'autorisation de tests est un des prérequis indispensables car elle définit clairement la portée des tests, notamment le périmètre des systèmes et des applications à tester. En outre, l'utilisation d'outils et de techniques appropriés, reconnus par l'industrie et conformes aux normes éthiques est également une condition sine qua non garantissant le caractère éthique du hacking. La documentation des résultats des tests, incluant les vulnérabilités identifiées ainsi que les recommandations proposées doit faire l'objet d'une traçabilité exhaustive et rigoureuse. Enfin la détention de certifications donne certaines garanties quant à la volonté d'inscrire cette démarche dans un caractère éthique (CEH « Certified Ethical Hacker », OSCP « Offensive Security Certified Professional »).

En conclusion, outil puissant et seul rempart véritable pour protéger les actifs numériques d'une organisation, le hacking éthique joue un rôle clef pour améliorer la sécurité des systèmes informatiques. S'il est essentiel de prendre en compte les implications morales qui vont définir les comportements et les actions des hackers éthiques, un garde-fou du caractère éthique est son encadrement via la réglementation.

Néanmoins cette dernière incarnée par la législation nécessaire pour encadrer cette pratique ne doit pas devenir un frein ou un obstacle susceptible de décourager les hackers éthiques. Elle doit en priorité continuer à les protéger tout en leur donnant les moyens d'exercer leurs activités et avoir ainsi un impact réel sur l'accroissement de la sécurité des systèmes informatiques. Aujourd'hui plus que des compétences et un état d'esprit, le hacking éthique doit évoluer vers un statut juridique.

Nicolas
BOTTERO

Sources

- Loi n° 2026-1321 du 07 octobre 2016 pour une République numérique
- Certified Ethical Hacker (CEH) – EC – Council
- Offensive Security Certified Professional (OSCP)
- Penetration testing: a hands-on introduction to hacking par Georgia Weidman
- OWASP top 10 (Open Web Application Security Project)
- NIST Cybersecurity Framework (National Institute of Standards and Technology)

LE STATUT D'HACKER « ÉTHIQUE »

Mélanie ROMANO, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

Le statut d'hacker « éthique »

De prime abord, il est nécessaire de signaler qu'il n'existe pas de définition du hacker en droit.
En pratique, le « hacker éthique » (aussi appelé « white hat » ou « bidouilleur ») peut être défini comme une personne physique[1] , agissant de sa propre initiative (sans contrat) dans le but de trouver des vulnérabilités au sein d'un système automatisé de traitement des données (ou « STAD »). Si la définition s'arrêtait ici, rien ne permettrait de distinguer le « hacker éthique » d'un cybercriminel. Il est donc important de noter que dans cette entreprise, le hacker éthique se doit de faire preuve de bonne foi et d'agir dans l'intention d'aider l'entreprise à qui appartient ce système automatisé de traitement des données (ci-dessous « STAD »).

Si dans le cadre de contrats de pentest, d'audit ou de « bug bounty » le périmètre est clairement défini en amont de la recherche de vulnérabilité, dans le cadre d'un hacker, le périmètre de ses recherches n'existe tout simplement pas. De même, ce n'est pas l'entreprise qui fait appel au hacker, mais le hacker lui-même qui décide de son propre chef de sa cible.
Parmi les hackers éthiques, il est possible de trouver des professionnels ou même des particuliers. Lors d'entretiens avec des professionnels juridiques et techniques, les hackers éthiques ont été décrits comme des personnes qui agissent bénévolement tiennent en haute estime le fait de respecter une éthique, au point même que pour certains le terme hacker éthique n'a pas lieu d'être étant donné qu'un hacker est éthique par nature, sinon il est un cybercriminel.
Les cybercriminels sont désignés quant à eux comme des personnes qui cherchent à obtenir « des renseignements personnels afin de les exploiter ou de les revendre (données bancaires, identifiants à des sites marchands, etc.) »[2] . Il semble donc que ce qui distingue un hacker éthique d'un cybercriminel est l'intention de leurs actes. Ils peuvent aussi parfois être différenciés par leurs pratiques ou modes opératoires (l'éthique ou principes moraux).

Distinctions sur l'éthique, l'intentionnalité et la bonne foi

L'éthique

Il est possible de définir l'éthique par « une réflexion sur les valeurs qui orientent et motivent nos actions. Cette réflexion s'intéresse à nos rapports avec autrui et peut être menée à deux niveaux. Plus généralement, la réflexion éthique porte sur les conceptions du bien, du juste et de l'accomplissement humain. […] Les règles, cependant, sont générales et ne peuvent couvrir toutes les situations où des choix d'actions sont nécessaires »[3]. Cette définition est une définition de philosophie. En effet, il n'existe en droit pas de définition de l'éthique. La raison à cela peut s'expliquer, car elle correspond à « une discipline qui réfléchit sur les comportements humainement acceptables par la société à un moment donné de son histoire. Elle suit l'évolution des connaissances et des mentalités »[4] or même si le droit n'est pas immuable, il n'en demeure pas moins que si l'éthique est volatile, définir quelque chose qui est propre à chacun n'est pas possible dans un texte de loi (et pas souhaitable).
Par exemple, toute l'imprécision du terme peut être illustrée par un exemple : un gouvernement qui emploierait des logiciels de surveillance pour intercepter les communications en ligne, invoquant la sécurité nationale pour justifier une atteinte potentielle à la vie privée. D'un côté, cette action est vue comme nécessaire pour protéger la population contre des menaces comme le terrorisme. De l'autre, elle est perçue comme une violation des droits fondamentaux à la vie privée et à la liberté individuelle. Cet exemple soulève des questions sur la balance entre sécurité et vie privée. L'éthique dans ce cas varie selon que l'on privilégie la sécurité collective ou les droits individuels, illustrant ainsi le caractère flou et contextuel de l'éthique.

Contrairement à l'éthique, le droit exige une définition claire et précise pour garantir la sécurité juridique. Les lois sur la surveillance doivent spécifier clairement les conditions et limites de telles pratiques pour éviter

1 Même si la question de l'existence de potentiels collectifs en faisant des personnes morales peut se poser.
2 Site internet Info.gouv, « *Cybercriminalité* », publié le 12 mai 2023, modifié le 3 janvier 2025, https://www.info.gouv.fr/risques/cyber-criminalite
3 Formation ressources humaines, « *Qu'est-ce que l'éthique ?* », 2021, https://www.formation-ressources-humaines.com/quest-ce-que-lethique/#qu- entendez-vous-par-%C3%A9thique/. [En ligne; consulté le 26 avril 2024].
4 Muriel Levannier et Sylvie Ameline, « *La démarche éthique* »,DEAS Tout-en-un , Chapitre 11, 2021.

des interprétations abusives ou de violations des droits. La législation doit donc articuler précisément les circonstances, les méthodes de surveillance autorisées, et les protections contre les abus, reflétant un équilibre délibéré entre différents droits et valeurs éthiques.

Tandis que l'éthique peut comporter un degré de subjectivité et de flexibilité selon les circonstances, le droit doit fournir un cadre strict et clair pour réguler efficacement les pratiques controversées comme la surveillance gouvernementale.
Se pose alors la question de l'éthique professionnelle[5]. Cette dernière a pour objectif d'encadrer par des principes et de mettre en avant les valeurs d'une profession. Dès lors, est-ce qu'une éthique professionnelle peut s'appliquer à ces hackers étant donné qu'ils ne dépendent pas d'une entreprise et que ce métier est encore contesté aujourd'hui ? La possibilité qu'ils suivent un « code de déontologie » devient alors faible. En outre, étant donné la flexibilité possible d'un principe moral, décrit comme « éthique », un simple code serait trop peu contraignant, n'engageant en rien ceux qui le brisent à faire amende. Et même si un tel code existait, la question de l'existence d'une autorité permettant de vérifier la conformité des hackers vis-à-vis dudit code reste ouverte.

Le principe de bonne foi, l'éthique du droit ?

Il existe de nombreuses références à la bonne foi dans les textes de loi[6]. Elle peut se définir comme : « la croyance qu'a une personne de se trouver dans une situation conforme au droit, et la conscience d'agir sans léser les droits d'autrui »[7].
Cependant, la découverte d'une vulnérabilité critique, pouvant entraîner une fuite massive de données personnelles, par un hacker est un enjeu de sécurité majeur. Ainsi donc, empêcher une telle fuite semble correspondre à l'idée générale de l'éthique, et ce pour tout un chacun. Dans ce cas, la démarche du hacker, guidée par la bonne foi et l'intention claire d'assister l'entreprise dans la sécurisation de ses systèmes, n'entraîne aucun préjudice. Ce comportement exemplaire met en relief l'inutilité pour l'entreprise de poursuivre le hacker légalement, car il a agi sans intention de nuire et a contribué positivement à améliorer leur cybersécurité. Malgré cela, d'autres comportements peuvent être subjectivement jugés comme « éthique » sans pour autant correspondre au cadre légal actuel (exemple : protection de l'environnement en bloquant un site Internet, blocage d'accès à des sites pédopornographiques, etc.). Étant donné la complexité du droit (en particulier le droit français) même les professionnels ignorent parfois le cadre juridique de leur profession. Non pas de manière consciente, mais simplement due à la complexité des textes et à leur nombre.

La volatilité de ces concepts peut être illustrée l'exemple suivant : Andrew Auernheimer, surnommé « weev », a découvert une faille de sécurité chez AT\&T qui exposait les adresses email de nombreux abonnés iPad. Au lieu de rapporter directement cette vulnérabilité à AT\&T, il a partagé les données avec un journaliste, qui les a ensuite publiées. Cette action a mené à sa condamnation en vertu du Computer Fraud and Abuse Act (CFAA) aux États-Unis, car il a été jugé pour accès non autorisé et fraude en relation avec des données personnelles. La défense d'Auernheimer plaidait qu'il avait agi pour améliorer la cybersécurité en révélant une faille critique, mais la justice a retenu que la méthode de divulgation publique, sans précautions pour les utilisateurs concernés, ne reflétait pas une intention de sa bonne foi. Auernheimer a été perçu comme ayant compromis la sécurité des données, résultant en une condamnation à 41 mois de prison. Cette affaire souligne l'importance d'une divulgation responsable pour les hackers éthiques, qui doivent prendre en compte les implications légales et éthiques de leurs actions[8].

L'intentionnalité

Enfin, l'intentionnalité en droit pénal désigne l'état d'esprit d'une personne lorsqu'elle commet un acte, marqué par la conscience et la volonté de réaliser cet acte et d'en provoquer les conséquences. Ce concept est essentiel pour distinguer les infractions intentionnelles des infractions non intentionnelles. L'intentionnalité influence la qualification juridique des délits, la gradation des peines, et les exigences de preuve, nécessitant souvent l'utilisation de preuves circonstancielles pour démontrer l'état d'esprit de l'accusé. Ainsi, elle joue un rôle clé dans l'établissement de la culpabilité et la réponse judiciaire.

L'intention des hackers éthiques est généralement orientée vers des objectifs constructifs et sécuritaires. Elle est encadrée par des règles principalement éthiques qui visent à maximiser les bénéfices pour la cybersécurité tout en minimisant les risques de malentendus ou d'abus. Cette intention contraste nettement avec celle des cybercriminels, dont les actes visent à exploiter, nuire, ou bénéficier illégalement des faiblesses des systèmes informatiques. Cependant, l'intention n'est pas l'intentionnalité, dès lors que l'intentionnalité se réfère à l'obtention d'un certain

5 Site internet nicomal, « *Que signifie l'éthique professionnelle ?* », publié le 27 mai 2019, https://www.nicomak.eu/que-signifie-lethique-professionnelle/. [En ligne ; consulté le 26 avril 2024].
6 À l'article 1104 du Code civil par exemple.
7 Serge Braudo, « *Définition de Bonne foi* ». https://www.dictionnaire-juridique.com/definition/bonne-foi.php/. [En ligne ; consulté le 26-Avril-2024]. Wikipédia, « *Bonne foi* ». https://fr.wikipedia.org/wiki/Bonne_foi#France/. [En ligne ; consulté le 26-Avril-2024].
8 Third Circuit United States Court of Appeals. United States v. Auernheimer. https://casetext.com/case/united- states-v-auernheimer-3/case-summaries/. [En ligne; consulté le 28-Avril-2024]. 2014.

résultat factuel (à savoir tester une vulnérabilité dans le cas des hackers, ce qui revient à pénétrer frauduleusement un système automatisé de traitement des données ou STAD) alors l'intentionnalité de l'acte n'est plus à prouver. Ils commettent bel et bien une infraction au sens du Code pénal.

Il convient cependant de nuancer cela en pointant plusieurs choses : dans la majorité des cas, les hackers ont une conscience minimale d'enfreindre les lois, considérant que l'infraction n'intervient que s'il y a de « mauvaises intentions ». Cette conscience minimale ne dispense pas un professionnel de connaître les lois concernant sa pratique. De plus, comme vus précédemment, les concepts d'éthique et de morale n'ont que peu de poids, si ce n'est aucun, en matière de droit. Sachant que l'éthique et les codes moraux peuvent fluctuer dépendamment d'une situation géographique, temporelle ou de l'individu concerné.

La responsabilité et le préjudice

La responsabilité pénale des hackers sera ici questionnée, car ils enfreignent les articles 323-1 à 323-3 du Code pénal. Cependant, il est important d'introduire certaines notions de responsabilité civile. La responsabilité civile vise la responsabilité contractuelle et extracontractuelle (ou responsabilité délictuelle)[9] . La responsabilité civile se distingue de la responsabilité pénale : dans le premier cas, l'objectif est d'indemniser un dommage, tandis que dans le second, il s'agit de réprimer les comportements entraînant la violation d'une loi pénale (menant généralement à une amende ou à l'emprisonnement). Si l'infraction pénale peut entraîner la responsabilité individuelle sans même qu'il y ait dommage (elle vise la faute et l'imputation de cette faute), ce dernier est en revanche une condition nécessaire à la responsabilité civile. Le dommage résultant de la violation d'une loi pénale, par exemple un vol, peut aussi être actionné devant les tribunaux civils afin d'obtenir réparation.

Cependant, il est essentiel d'ajouter des nuances au sujet de la responsabilité en matière de cybersécurité, telles que soulignées par Me Marc-Antoine Ledieu dans son rappel des concepts juridiques de la responsabilité[10]. En effet, la responsabilité des hackers éthiques ou des pentesters dépend de leur cadre d'action. Par exemple, un pentester ou bug bounty opérant avec une autorisation peut être légalement protégé, mais cette responsabilité peut devenir délicate si les actions dépassent les limites de ce qui a été autorisé, transformant ainsi un test d'intrusion légitime en une activité potentiellement illégale.

De plus, dans des cas comme celui de WannaCry, la responsabilité peut être partagée entre plusieurs acteurs pour la diffusion des failles de sécurité[11] . Dans le cas de WannaCry (un ransomware), il est possible d'imaginer que la NSA, qui a manqué à la sécurisation de ses outils de piratage et n'a pas divulgué l'existence de cette faille connue à Microsoft, et Shadow Brokers, qui a publié ces outils, pourraient tous deux être considérés comme responsables des dommages au même titre que les auteurs du ransomware. Ce cas montre aussi l'importance du consentement en cybersécurité : la distinction entre un test d'intrusion et un acte de hacking repose sur une autorisation préalable. Toute intervention non autorisée peut être considérée comme illégale, même si l'intention du hacker n'était pas malveillante.
Cette situation met en lumière les défis juridiques liés aux attaques, où la responsabilité peut impliquer de multiples acteurs, des hackers aux agences gouvernementales, chacun jouant un rôle dans la chaîne des événements et contribuant aux conséquences globales de l'attaque.

La notion de préjudice possède également une importance cruciale : « Le préjudice est le dommage qui est causé à autrui d'une manière volontaire ou involontaire. Le préjudice peut être causé par le fait d'une personne, par le fait d'un animal ou d'une chose, ou encore par la survenance d'un événement naturel ; son existence comme son évaluation relèvent du pouvoir souverain d'appréciation des juges du fond »[12]. Si dans l'exemple précédent le préjudice est bien réel, tant pour les utilisateurs de Windows, la CIA que Microsoft, il est néanmoins plus difficile de localiser le préjudice si le hacker éthique fait preuve de bonne foi et que son intentionnalité n'est pas questionnable. En effet, s'il prévient seulement l'entreprise et l'ANSSI de la vulnérabilité et ne l'exploite pas pour avoir accès à des informations personnelles et/ou confidentielles, l'entreprise peut manquer de causes d'engagement de la responsabilité du hacker, le préjudice étant situé ailleurs. Il n'empêche que le hacker peut être poursuivi au pénal pour avoir enfreint le Code pénal et s'être introduit frauduleusement dans un STAD.

Il est possible de comparer cette situation au Code de la route. Afin d'obtenir le droit de conduire une voiture, il est nécessaire de passer le Code de la route et d'obtenir le permis de conduire. Ce Code est un ensemble de règles à respecter sous peine de pouvoir se faire condamner pour avoir commis une infraction. Ainsi, un automobiliste qui ne le respecterait pas pourrait tout de même être passible de condamnation.

9 Stéphanie Porchy-Simon, « *Manuel de droit des obligations 2025* », Dalloz, p. 357 & suiv.
10 Marc-Antoine Ledieu, « *test d'intrusion : droit et éthique* » – Cours ENIB Ecole Nationale d'Ingénieurs de Brest [23 janvier 2024]. https://technique- et- droit- du-numerique.fr/test- d- intrusion- droit- et- ethique- enib- ecole- nationale- d- ingenieurs- de-brest-23-janvier-2023/. [En ligne; consulté le 12-Novembre-2024].
11 Chris Graham, « *NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history* », The Telegraph, 13 mai 2017.
12 Serge Braudo, « *Définition de Préjudice* », https : / / www . dictionnaire - juridique . com / definition / prejudice.php/. [En ligne ; consulté le 26-Avril-2024].

Il existe néanmoins des exceptions à ce Code, dans le cas d'une urgence, certains véhicules telles les voitures de polices, de pompiers ou les ambulances peuvent ne pas le respecter. Les conducteurs de ces véhicules peuvent tout de même être tenus responsables si un accident se produit (la notion d'urgence n'effaçant pas la responsabilité du conducteur). Dans le cas des hackers, ne serait-il pas intéressant au titre de l'urgence à signaler une vulnérabilité de les exempter de respecter les articles 323-1 à 323-3 du Code pénal, sachant qu'ils mettraient néanmoins leur responsabilité en jeu ?

Afin de mieux appréhender le contexte, il est intéressant de se pencher sur deux notions plus techniques : la vulnérabilité et l'exploitation.

La fine ligne entre vulnérabilité et exploitation

Les experts en cybersécurité font une différence entre une vulnérabilité et une exploitation, à savoir : « dans le domaine de la sécurité informatique, une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient »[13]. Une exploitation en revanche désigne « un exploit informatique, aussi appelé code d'exploitation, est un code permettant à un cybercriminel ou à un malware d'exploiter une faille de sécurité présente dans un logiciel, une application ou un système informatique. […] Un exploit informatique n'est pas malveillant en tant que tel. Néanmoins, dans la plupart des cas, il est utilisé par les cybercriminels dans le but d'infecter un appareil ou de nuire à un système informatique »[14]. En somme l'exploitation d'une vulnérabilité est la phase suivant la découverte d'une vulnérabilité (dans le cas de cybercriminels).

Cependant, même si cette distinction est importante, il ne convient pas de faire la différentiation entre un cybercriminel et un hacker par l'exploitation ou non d'une vulnérabilité et donc de dépénaliser la recherche de vulnérabilité.
Dans le but de trouver une vulnérabilité, le hacker peut être amené à vérifier sa théorie quant à l'existence d'une faille en l'exploitant seulement si cette faille n'a jamais été découverte (une « Zero-day »). Ainsi on ne peut pas réellement différencier un cybercriminel d'un hacker en se basant seulement sur ce point. En effet, même si leurs finalités sont différentes à un moment donné, le hacker peut être amené au même titre que le cybercriminel à exploiter les vulnérabilités d'un STAD.

Dans le domaine de la sécurité informatique, une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système

Lorsque l'on parle de vulnérabilités, la majorité des professionnels se tournent vers une liste : les CVE (Common Vulnerabilities and Exposure)[15]. Cette liste, accessible au grand public, référence les différentes vulnérabilités en leur donnant un numéro, détaillant la vulnérabilité, les machines/protocoles/version sur lesquelles cette vulnérabilité a été trouvée. La base de données est gérée par l'ONG MITRE[16] et financée par des fonds gouvernementaux américains en partie. Cependant ce n'est pas le seul site référençant des vulnérabilités (en France il existe le CERT-Centre Gouvernemental de Veille, d'Alerte et de Réponse[17] par exemple). Pour rappel : « 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 € d'amende » (Art 323-1 du Code pénal).

Cependant il existe un cas où la question de l'introduction ou du maintien frauduleux dans un système de traitement automatisé ne se pose pas en théorie, mais qui en pratique peut être clairement associé à des activités de hacking. Par exemple, M.X est hacker. Pendant son temps libre, il consulte les dernières CVE. Dans ses recherches, il apprend qu'un service web spécifique est vulnérable. Il scanne alors les ports de l'entreprise qu'il investigue sur le moment et de là obtient l'information lui confirmant que ce service web est utilisé par cette entreprise. Un scan de ports consiste à envoyer des requêtes à tous les ports d'un serveur. Des informations sont alors transmises entre le client et le serveur (des requêtes).

Il s'agit donc de simplement vérifier la disponibilité du service. Il contacte alors l'entreprise pour leur faire part de ses découvertes et l'informer de la vulnérabilité. Dans cet exemple, M.X n'a jamais pénétré de façon frauduleuse dans le système de traitement automatisé de l'entreprise. Il ne devrait donc pas être inquiété

13 Wikipédia, « *Vulnérabilité (informatique)* », 2023, https : / / fr . wikipedia . org / wiki / Vuln % C3 % A9rabilit % C3 % A9 _ (informatique)/. [En ligne ; consulté le 26-Avril-2024].
14 Delphine Lacour, « *Qu'est-ce qu'un exploit et comment les éviter ?* », 2023, https://nordvpn.com/fr/blog/exploit-informatique/. [En ligne ; consulté le 26-Avril-2024].
15 Site internet CVE. https://www.cve.org/. [En ligne ; consulté le 26-Avril-2024].
16 Site internet MITRE. https://www.mitre.org/ [En ligne ; consulté le 02-Mai-2024].
17 Site internet CERT-FR. https://www.cert.ssi.gouv.fr/. [En ligne ; consulté le 02-Mai-2024].

pénalement. Cependant la question se pose quant à la possibilité pour un juge de distinguer un simple scan d'une pénétration frauduleuse en cas de poursuites.

La loi ne définit à aucun moment un STAD, ainsi, même si cela offre une certaine latitude afin de permettre au juge de condamner ou non l'auteur d'une infraction. Cela pose également un problème lorsqu'il s'agit de définir ce qui est considéré comme illégal ou non.

Le manichéisme de la cybersécurité et le statut des hackers

Les dernières directives de l'Union européennes permettent facilement de se rendre compte de l'importance de la cybersécurité, impliquant non seulement la sécurité des employés, mais aussi la sécurité nationale. Dans un secteur où, en France, les entreprises peinent à recruter, n'existerait-il pas une façon de transformer ces bénévoles en atouts ? Si aujourd'hui des entreprises comme Orange affirment que « La question n'est plus de savoir si l'on va se faire attaquer, mais plutôt quand » (en parlant de cyberattaques), n'est-il pas temps d'employer ces hackers en leur donnant un cadre ?

Une analogie bien connue revient régulièrement concernant les STADs : celle de la maison. Le système de traitement automatisé est une maison et toute intrusion reviendrait à pénétrer sur la propriété privée de quelqu'un. Cependant, si la fenêtre de la maison est ouverte, le signalement par un voisin est préférable au cambriolage. Bien sûr, il est nécessaire que ce « voisin » (en pratique le hacker) ne se comporte pas comme un cambrioleur, et partant du principe qu'une faille de sécurité sera très probablement exploitée si rien n'est fait. La pertinence d'un encadrement de ce type de situations se fait ressentir.

Une piste consiste à chercher un statut particulier pour les hackers. Le hacker ayant suivi les règles imposées pourrait bénéficier d'une exonération. Cependant, un statut est plus contraignant d'un point de vue administratif et légal, alors qu'un canal sécurisé afin de faire une déclaration de vulnérabilité auprès de l'ANSSI existe déjà. Cette déclaration, avec les différents logs, ainsi qu'une recherche afin de vérifier qu'aucune exfiltration de données n'a été effectuée, pourrait apporter une meilleure protection aux hackers. L'ANSSI ainsi impliquée, serait alors capable de réprimer les comportements jugés illégitimes des hackeurs ainsi que les protéger (étant en quelque sorte un arbitre). Il serait ainsi plus simple de condamner les soi-disant hackers dissidents. Cependant, l'ANSSI ne peut disposer de pouvoirs de sanction au sens du droit pénal.

Des inconvénients restent cependant liés à la pratique du hacking éthique. Les hackers ne sont pas toujours des professionnels entraînés. Leur statut n'existant pas, n'importe qui peut se déclarer « hacker » (même vous). Il existe donc plusieurs possibilités quant à ces personnes. D'un côté, certains professionnels ont suivi une formation et connaissent les conséquences de leurs actes. Ils savent donc normalement que s'ils découvrent une faille, la publier sans en avertir l'entreprise ou lui laisser le temps de la corriger équivaut à placer une cible sur ladite entreprise. D'un autre côté, il est aussi possible de trouver des novices, possiblement non informés des lois, des retombées et de la portée de leurs actions.

Ces novices, outre le fait d'être un potentiel danger pour les entreprises, peuvent aussi être un danger pour eux-mêmes. Leur méconnaissance peut les mener à enfreindre les lois dont ils n'ont pas conscience et à potentiellement être poursuivis en justice. Ils peuvent de plus entacher la réputation non seulement des entreprises, mais aussi des professionnels du milieu.

Cette atteinte à la réputation vise la diffamation, qui peut se définir par le fait d'affirmer « un fait qui porte atteinte à l'honneur ou à la considération d'une personne. Le fait en question doit être suffisamment précis pour pouvoir faire l'objet de preuve. [...] Il y a diffamation même si l'allégation est faite sous forme déguisée ou dubitative ou si elle est insinuée. [...] Il y a également diffamation si l'allégation vise une personne qui n'est pas désignée par son nom, mais qui est identifiable[18] . Dans notre cas, même si les faits sont avérés (la vulnérabilité existe), le fait de les publier directement peut porter atteinte à l'image publique de l'entreprise et à son intégrité (ou l'intégrité de ses données a minima). Il est donc possible d'alléguer que, bien que la faille soit avérée, l'entreprise peut porter plainte contre le hacker pour diffamation, dénigrement, ou atteinte à son image et à sa réputation.

Enfin, au regard du statut des hackers, son absence empêche de clairement définir le périmètre de la profession.
Pour rappel, un lanceur d'alerte se définit par « une personne physique qui signale ou divulgue, sans contrepartie financière directe et de bonne foi, des informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général [...] Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles mentionnées au I de l'article 8, le lanceur d'alerte doit en avoir eu personnellement connaissance »[19]. Dans le cas des hackers éthiques, les vulnérabilités peuvent dans la majorité des cas présenter un préjudice pour l'intérêt général étant

18 Article 29 de la loi du 29 juillet 1881 sur la liberté de la presse.
19 Loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte

donné que ces vulnérabilités mènent souvent à des vols de données personnelles. Or les vulnérabilités qu'un hacker découvre ne sont pas découvertes dans le cadre de leur activité professionnelle. Ainsi, lorsqu'ils découvrent une potentielle vulnérabilité, ils en ont donc personnellement connaissance. Dans ce cas, il serait juste de dire qu'ils peuvent prétendre au statut de lanceur d'alerte.

Mais, le statut de lanceur d'alerte n'excuse pas les crimes et délits commis pour obtenir des informations. Le hacker, même en lançant une alerte, peut toujours être condamné pour avoir enfreint le droit pénal en s'introduisant frauduleusement dans un système automatisé de traitement. Sans compter que la preuve de bonne foi d'un hacker repose sur le fait de prévenir l'entreprise concernée et/ou une agence gouvernementale (ANSSI ou CNIL). Ainsi cela empêche le hacker de lancer une alerte publique.
N'existe-t-il donc pas un autre statut qui pourrait protéger les hackers ? Étant donné qu'ils recherchent des vulnérabilités, ne peuvent-ils pas prétendre au statut de chercheur ?

À travers cette première partie, les définitions, motivations et implications éthiques et légales des actions des hackers éthiques ont été explorées. Il est apparu clairement que, malgré leur intention d'améliorer la sécurité des systèmes informatiques, les hackers éthiques naviguent dans un cadre légal complexe et souvent ambigu.

Mélanie
ROMANO

ETHICAL HACKING, PERSPECTIVE D'UN CISO

Laurent GUÉRIN, CISO CMA CGM

Depuis plusieurs années, les entreprises adoptent massivement et très rapidement le numérique. Face à cette numérisation croissante, le risque d'origine cyber s'est accru en parallèle et devient maintenant un des plus grands risques pour les sociétés, que ce soit en probabilité d'occurrence et en impact financier.

Face à cela, les organisations en charge de la protection des entreprises ont dû évoluer pour s'adapter. Souvent, il a fallu créer ces organisations depuis zéro et les faire grossir, même s'il reste encore beaucoup trop de sociétés qui en sont encore dépourvues. Cette évolution s'est souvent fait initialement par un accroissement de la taille des équipes. Cependant cette croissance atteint vite ses limites, ce pour plusieurs raisons, manque de personnel sur le marché, manque d'attractivité des sociétés (les salaires étant élevés, de nombreuses sociétés ne peuvent pas les proposer), problème de masse critique (maintenir des petites équipes est difficile), problème de compétences très spécifiques difficiles à trouver, problème de budget. Donc la sous-traitance est apparu comme la solution pour accompagner cette croissance. Elle permet aux entreprises d'accompagner la numérisation avec un coût sous contrôle, une charge et un niveau d'expertise ajustable.

Ainsi la plupart des sociétés délèguent massivement les activités de Pentest et de Red Team à des sociétés externes. La gestion de ces contrats est devenue un élément central dans les organisations Cyber. C'est aussi de plus en plus requis pour des questions de compliance. L'ethical hacking existe depuis longtemps, néanmoins depuis quelques années plusieurs choses ont changé, qui sont principalement le volume et la judiciarisation.

Le volume car conjointement la numérisation croissante de la société, la demande a explosé et l'offre a suivi. Le nombre de personnes travaillant dans le hack a cru énormément, et la communication faite autour du 'hacker' a créé beaucoup de vocations. Si cela a concerné principalement les pays occidentaux aux débuts, c'est désormais un mouvement mondial, et l'on voir apparaître des communautés très compétentes dans de nouveaux pays. Les bug bounty ont aussi massivement contribué à cette forte croissance, les revenus associés pouvant être conséquents par rapport à certains niveaux de vie.

Si ces évolutions ont permis d'absorber la charge de travail et de répondre aux besoins, elles ont également exacerbé la problématique des responsabilités. Les entreprises structurent la sous-traitance par le biais d'accord commerciaux, incluant des responsabilités juridiques contraignantes. C'est le second changement majeur dans ce secteur, maintenant, tout doit être borné et les responsabilités bien définies avant le démarrage des activités. Lancer une campagne de bug bounty ou autoriser une société externe à faire un pentest représente une prise de risque. Du fait de la complexité des SI, il n'est jamais certain à 100% qu'un pentest n'ai pas d'effet de bord négatif. C'est d'autant plus vrai pour une Red Team ou l'objectif est plus vaste. Il est donc impératif que la société cliente soit très claire sur ses attentes, qu'elle ait mis en place les politiques et l'organisation appropriées. C'est un sujet complexe particulièrement sur deux aspects, Red Team et Divulgation responsable (Vulnerability Disclosure).

Lors d'un gros exercice Red Team effectué par une société externe, le travail de préparation préalable est primordial et conséquent. Le principal élément de succès est de s'assurer d'impliquer le bon niveau de management. Un comité directeur composé des DSI/CIO, CISO, CSO, directeurs opérations doit valider les objectifs, la cible et des lignes rouges. Cela permet d'avoir des interfaces et des échanges très efficaces avec le sous-traitant. Le suivi de l'exercice doit être hebdomadaire au minimum. Des règles de délégation claires doivent permettre de prendre des décisions

très rapidement en cas de problème (impact sur la production, ou accès à des données sensibles). Seule une très bonne préparation permettra à l'exercice de se passer correctement tout en maîtrisant les risques associés.

A propos de la politique de Divulgation responsable c'est quelque chose de primordial à définir pour une société, mais souvent négligé. Bien que cela semble simple de prime abord, c'est assez complexe à mettre en place dans des sociétés industrielles.

Tout d'abord, la politique de divulgation doit être approuvée, publiée et accessible à tout le monde facilement. Cela implique en général d'avoir une équipe en charge de la gouvernance Cyber, un processus de validation et un soutient des équipes de la communication (publier une page cyber sur un site web corporate s'apparentant souvent à une mission impossible). Il est aussi recommandé d'avoir une approche « Groupe » dans le cas de nombreuses filiales. Il faut aussi bien réfléchir à deux éléments important. Le processus de déclaration et la rémunération associée. Publier une politique de divulgation implique d'avoir les processus pour y répondre. Comment se fait la déclaration, est-ce un email dédié ou un formulaire en ligne ? Est-ce que cela ouvre un ticket ? Qui reçoit l'information ? le CERT ? le CISO ? quel est l'engagement de délai réponse ? faut-il du 24/24 pour y répondre ? Il faut savoir que certaines personnes divulguant une vulnérabilité sont très pointilleuses sur les délais et sur les réponses et font planer la menace d'une divulgation publique si la société ne respecte pas les règles. Une fois l'accusé de réception fait, il convient d'analyser l'information reçue, pour valider sa véracité et son exploitabilité. Le monde de l'industrie n'a pas la même temporalité que celui des éditeurs logiciels, quand une société a de nombreux produits ou des produits très complexes (avions, raffineries, centrales…) et que la vulnérabilité concerne un système industriel ou embarqué, trouver la personne avec les compétences pour évaluer la pertinence de la vulnérabilité n'est pas toujours facile et peut prendre du temps. Si la vulnérabilité est avérée, le délai de correction est aussi problématique. Dans le cas de systèmes industriels ou embarqués, le délai des 90j est irréaliste. Une correction demande énormément d'analyse d'impact, de test, de validation, et même parfois de nouvelles certifications, ce qui peut prendre des mois voire plus. Nous sommes loin des délais de patchs pour les éditeurs logiciels.

Le sujet de la rémunération est aussi une vraie question qui peut faire débat. Lors d'un contrat de Bug Bounty, la rémunération s'entend et s'organise facilement. Mais pour une divulgation 'volontaire', c'est plus complexe. Il n'y a pas de structure contractuelle pour l'accompagner et le scope n'est pas défini. De plus l'estimation de la rémunération associée fait souvent débat (on connaît tous quelqu'un qui pense ne pas avoir été assez rémunéré pour une vulnérabilité). L'estimation des budgets annuels prévisionnels nécessaire se rajoute aussi a la complexité du sujet. Donc une approche non rémunérée est peut-être la solution la plus simple et la plus efficace. C'est même quelque part revenir à l'essence du hacker éthique que de travailler pour le bien commun.

Laurent
GUÉRIN

HACKING ÉTHIQUE : LE PIRATAGE LÉGAL ET RESPONSABLE

Christèle JACQ-ARNOULT, Stéphane SZYMANSKI, Damien HARDY

Le hacking éthique, aussi connu sous le nom de test d'intrusion éthique ou pentesting éthique, est une pratique qui vise à évaluer la sécurité des systèmes d'information (SI) en procédant à des attaques de manière légale et responsable. Partie intégrante de la protection numérique dans sa forme offensive, c'est une discipline incontournable des formations en cybersécurité.

La formation dispensée par les établissements publics

L'enseignement public mobilise une diversité de compétences et d'outils pédagogiques pour former les futurs hackers éthiques. L'enjeu est ici de répondre le plus concrètement possible à la demande croissante des organisations qui ont besoin de ces professionnels de la cybersécurité offensive pour se protéger des hackers malveillants.

L'approche pour former les hackers éthiques dans les établissements publics de formation s'articule autour de trois axes complémentaires.

Le premier axe s'appuie sur les connaissances et la pédagogie des enseignants

Les enseignants en informatique et en électronique apportent leurs connaissances des différentes typologies de réseaux, systèmes, matériels et applications numériques. Les futurs pentesters éthiques en auront besoin lorsqu'ils attaqueront les SI pour en tester la vulnérabilité et réduire la surface d'attaque. Ce socle de connaissances est en effet essentiel à la compréhension des spécificités techniques d'un système d'information et donc de ses failles potentielles.
Le pentester éthique va se demander « comment l'attaquant peut-il procéder pour pirater le SI ? » avant de se demander « comment peut-on sécuriser le SI ? ». Afin de répondre à cette question, les étudiants sont accompagnés par leurs professeurs pour mettre en pratique les apprentissages théoriques. Pour cela, ils ont notamment accès à des outils de simulation (ex. Cyber range, TryHackme, HackTheBox) ou à des challenges CTF (Capture The Flag).

Ces enseignements techniques sont complétés par des cours que leur dispensent les enseignants du cursus Droit de l'Université. L'objectif est de mettre en perspective les éléments connexes aux aspects purement techniques de la fonction. Grâce à cet éclairage, les futurs hackers éthiques pourront considérer les enjeux juridiques et mieux comprendre les implications légales, voire politiques de leurs actions. Nous pouvons citer par exemple les directives, réglementations, normes, textes de loi comme NIS2 (Network and Information Security), DORA (Digital Operational Resilience Act), DSA (Digital Service Act) ou encore LPM (Loi de Programmation Militaire) par exemple. Ils vont ainsi acquérir durant leur formation une meilleure compréhension du cadre légal relatif à la cybercriminalité. Cette acculturation leur sera utile dans leur mission, car ils pourront notamment être amenés à manipuler des données sensibles et/ou personnelles.
Ces enseignants possèdent un véritable savoir-faire dans la transmission des connaissances. C'est leur métier.

Le deuxième axe fait appel aux connaissances empiriques des professionnels métiers

Les formations mettent l'accent sur l'apprentissage pratique via des intervenants qualifiés qui sont proches du terrain. Il s'agit de personnes extérieures à l'université et aux écoles d'ingénieurs qui viennent donner des cours dans les établissements. Les étudiants acquièrent ainsi des compétences opérationnelles en profitant du retour d'expérience de professionnels en prise directe avec les problématiques « terrain » liées au métier de hacker éthique. Ces intervenants évoluent souvent dans des organisations dont c'est précisément le métier de mener des attaques responsables et légales pour hacker les SI et évaluer le niveau de criticité des failles que pourraient exploiter les cybercriminels. En plus de ces acteurs techniques, des juristes ou avocats spécialisés en cybersécurité, des experts en sciences cognitives ainsi que des étatiques comme la DGA MI (Direction Générale de l'Armement Maîtrise de l'Information) ou l'ANSSI (Agence Nationale de la Sécurité des Système d'Information) viennent partager leur expertise.

Les intervenants mettent régulièrement l'accent sur les « soft skills », ces compétences douces qui sont importantes pour le métier de hacker éthique. Il s'agit en effet d'être agile, persévérant, curieux, de toujours chercher à comprendre comment les choses fonctionnent, en quoi elles servent l'entreprise et quelles opportunités d'intrusion ou de déstabilisation elles peuvent présenter pour un attaquant. Évidemment, il faut avoir aussi beaucoup de rigueur pour ne pas causer de dégâts dans les systèmes informatiques qui sont hackés afin d'en détecter les failles de sécurité.

La collaboration dans les formations avec ces professionnels contribue assurément à la fluidité de la transition des étudiants vers le marché du travail.

L'approche pour former les hackers éthiques dans les établissements publics de formation s'articule autour de trois axes complémentaires.

Le troisième axe réside dans l'avantage de côtoyer au plus près les laboratoires de la recherche publique

Singularité de la formation publique, la proximité avec les laboratoires de recherche présente un avantage indéniable pour les étudiants. En effet, les chercheurs et les doctorants travaillent en avance de phase sur les problématiques et les innovations qui vont impacter de façon positive ou négative la protection des systèmes d'information et donc la pratique du métier de hacker éthique.

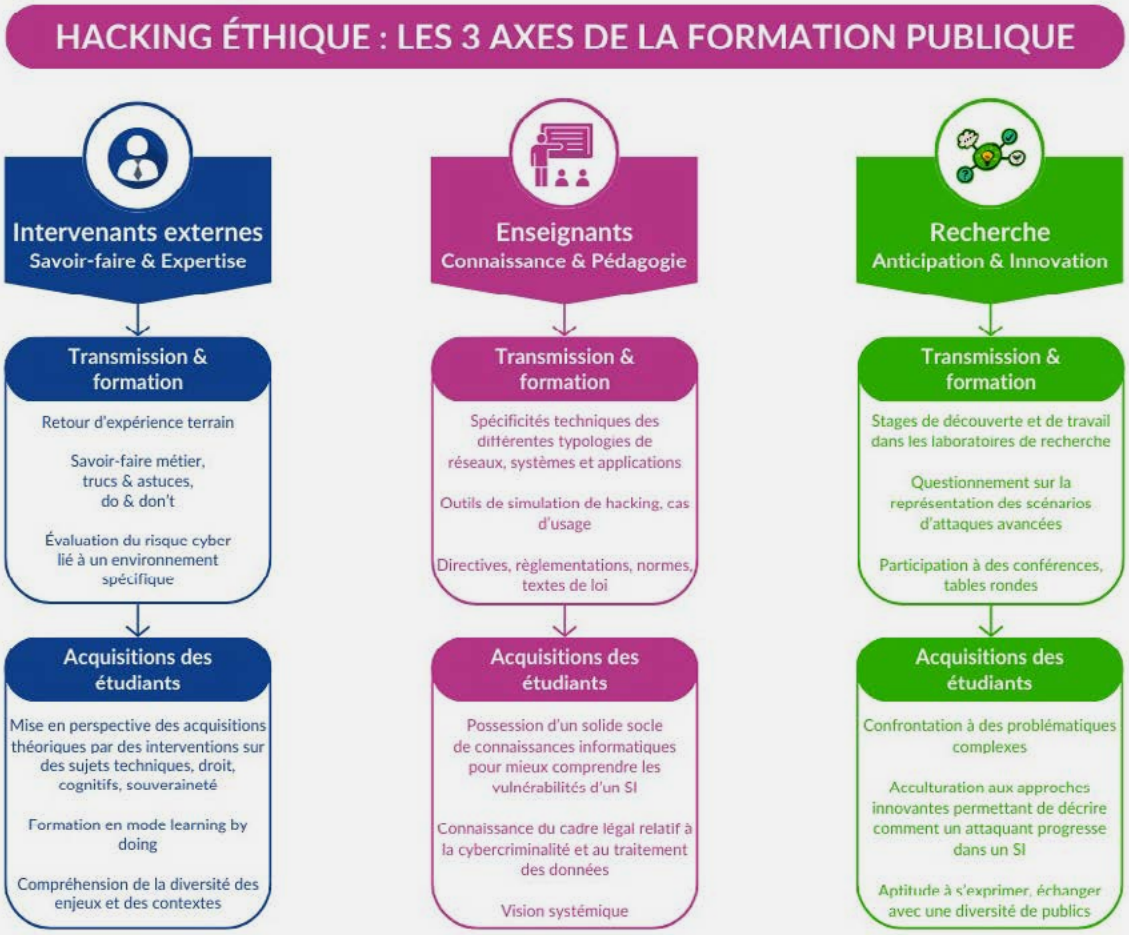
Prenons l'exemple de l'intelligence artificielle (IA). Les systèmes d'information embarquent tous de l'IA et sont donc à ce titre tous vulnérables à une forme d'extraction ou de falsification des données. Nos chercheurs travaillent à la modélisation de nouveaux concepts pour mieux comprendre et in fine outiller les professionnels de la cybersécurité -dont les pentesters éthiques font partie- de solutions qui leur permettront de garder une longueur d'avance sur les cybercriminels.

Cet apport universitaire peut prendre plusieurs formes. Les étudiants peuvent faire des stages dans les laboratoires de recherche. Ils peuvent également assister à des conférences de chercheurs comme cela leur a été proposé à l'occasion de l'école d'hiver de la recherche organisée par la CyberSchool (Consortium d'établissements publics) à Rennes en février dernier. Durant cet évènement, un sujet était par exemple consacré à la représentation des scénarios d'attaques avancées. Différentes approches et outils permettant de décrire comment un attaquant progresse dans un système d'information était présentés par Valerie Viet Triem Tong qui dirige les travaux de l'équipe PIRAT (Laboratoire Inria) sur le sujet.


Christèle JACQ-ARNOULT


Stéphane SZYMANSKI


Damien HARDY



En conclusion :

Grâce à la conjugaison de ces 3 axes, l'enseignement public se met en situation de proposer aux étudiants une vision systémique du métier de hacker éthique. Les formations qu'ils reçoivent les préparent ainsi à adresser les défis qu'ils auront à relever dans la légalité, avec professionnalisme, en citoyens responsables.

LE STATUT DE CHERCHEUR EN CYBERSÉCURITÉ

Mélanie Romano, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

Il est nécessaire d'approfondir l'analyse du statut des chercheurs et en particulier ceux impliqués dans la cybersécurité, au regard des conséquences de leurs recherches sur les vulnérabilités des systèmes informatiques.

Tout le monde ne peut prétendre au statut de chercheur ou d'enseignant-chercheur. D'après le Code de l'éducation (Article L952-6 du Code de l'éducation) : « Sauf dispositions contraires des statuts particuliers, et sauf lorsque le candidat est maître de conférences titulaire, la qualification des enseignants-chercheurs est reconnue par une instance nationale.

L'examen des questions individuelles relatives au recrutement, à l'affectation et à la carrière de ces personnels relève, dans chacun des organes compétents, des seuls représentants des enseignants-chercheurs et personnels assimilés d'un rang au moins égal à celui postulé par l'intéressé s'il s'agit de son recrutement et d'un rang au moins égal à celui détenu par l'intéressé s'il s'agit de son affectation ou du déroulement de sa carrière » (Article L952-6 de Code de l'éducation).

Ainsi, seules des personnes titulaires d'un diplôme délivré par une école doctorale et embauchées par des établissements de recherche peuvent prétendre à ce statut. Il est important de préciser que les parties suivantes ne traiteront que du statut d'enseignant-chercheur et de chercheur dans un cadre universitaire. En France, les missions d'un chercheur (et par extension d'un enseignant-chercheur) sont les suivantes (Article-L952-3 du Code de l'éducation) :

1. Recherche scientifique : Les chercheurs sont principalement chargés de conduire des recherches fondamentales ou appliquées. Ils doivent produire des connaissances nouvelles et contribuer à l'avancement de la science dans leurs domaines respectifs.

2. Publication et diffusion des connaissances : Ils doivent publier les résultats de leurs recherches dans des revues scientifiques reconnues et participer à des conférences, contribuant ainsi à la diffusion du savoir.

3. Encadrement et formation : Les chercheurs participent à la formation par la recherche. Cela inclut l'encadrement de doctorants, la direction de thèses, et l'enseignement dans des cursus universitaires ou spécialisés.

4. Valorisation de la recherche : Ils sont encouragés à valoriser leurs résultats de recherche, que ce soit par le transfert technologique vers le secteur industriel, par la création de start-ups, ou par des collaborations avec des entreprises.

5. Coopération internationale : Les chercheurs sont également impliqués dans des collaborations internationales, participant à des réseaux de recherche à l'échelle mondiale et contribuant à des projets internationaux.

6. Contribution à la vie institutionnelle : Ils prennent part aux activités et à l'organisation des institutions de recherche, incluant les comités de pilotage et les instances de gouvernance.

Les chercheurs en France jouissent d'une liberté quasi entière dans le cadre de leurs recherches.
La loi prévoit que « les enseignants-chercheurs, les enseignants et les chercheurs jouissent d'une pleine indépendance et d'une entière liberté d'expression dans l'exercice de leurs fonctions d'enseignement et de leurs activités de recherche, sous les réserves que leur imposent, conformément aux traditions universitaires et aux dispositions du présent code, les principes de tolérance et d'objectivité. Les libertés académiques

sont le gage de l'excellence de l'enseignement supérieur et de la recherche français. Elles s'exercent conformément au principe à caractère constitutionnel d'indépendance des enseignants-chercheurs » (Article L952-2)[20].

Mais que se passe-t-il si l'on prend l'exemple d'un chercheur en cybersécurité spécialisé dans la découverte de vulnérabilités ? Par son statut, il jouit d'une pleine indépendance sur les sujets qu'il choisit de traiter. Il n'est donc pas tenu de notifier une entreprise s'il décide de rechercher des vulnérabilités sur son système de traitement automatisé. S'il trouve une vulnérabilité, dans le but d'apporter une preuve de sa présence et de la possibilité de l'exploitation de ladite vulnérabilité, il est très probable que le chercheur exploite la vulnérabilité. Par la suite, conformément à ses missions de chercheur, il publiera probablement en exposant la vulnérabilité à la communauté scientifique. Cependant ces démarches peuvent soulever plusieurs questions : le chercheur, étant donné son statut particulier, a-t-il le droit de ne pas respecter les articles 323-1 à 323-3 du Code pénal ? Dans quelles mesures une publication engage-t-elle la responsabilité du chercheur ?

Code pénal vs Code de l'éducation

Si en vertu de la liberté de la recherche, un chercheur en cybersécurité décide d'enfreindre l'article 323-1 du Code pénal, il est alors important de considérer plusieurs points afin de savoir dans quelle mesure ou s'il est condamnable. Dans un premier temps, le chercheur est tenu de faire preuve d'objectivité, d'impartialité et de neutralité. Il est aussi à noter que les conflits d'intérêts nuisent à cette objectivité, en ce qu'ils constituent une situation d'interférence entre intérêts publics et/ou privés de nature à impacter cette objectivité, impartialité et neutralité[21].

Alors si le chercheur réunit tous ces points, a-t-il le droit de déroger au Code pénal en vertu du Code de l'éducation ?

En France, le principe de spécialité législative peut s'appliquer, sauf dans ce cas précis : aucun code ne peut déroger à la loi pénale. Le principe de spécialité législative signifie que lorsque deux codes ou lois contiennent des dispositions spécifiques à une situation donnée, c'est la norme la plus spécialisée qui prévaut dans ce contexte précis. Le Code pénal régit les infractions et les peines en général, tandis que le Code de l'éducation contient des dispositions spécifiques relatives au système éducatif. Bien que le Code de l'éducation prévoie le cas des chercheurs, il n'autorise pas à déroger au Code pénal. Il est cependant possible aux chercheurs de s'associer aux entreprises en leur faisant signer des contrats autorisant leurs recherches. Cependant, ils donnent un droit de regard à l'entreprise sur leurs publications a minima, ce qui pose des questions d'entrave à leur pleine et entière liberté d'expression. Il est donc d'autant plus crucial de créer une dérogation ou un statut particulier pour les hackers qui engloberait aussi les chercheurs.

S'agissant de la liberté de publication, l'une des missions d'un chercheur repose sur son habilité à publier et diffuser son travail. Peut-on réellement empêcher les chercheurs en vulnérabilités de publier leurs découvertes ?

Par souci de sécurité pour l'entreprise et sa réputation, et pour la sécurité du chercheur (et afin de se prémunir contre de potentielles poursuites en diffamation) il est normal que le chercheur ne fasse pas mention du nom de l'entreprise dans son article. En effet, citer une entreprise peut entraîner un préjudice et dans ce cas elle peut tenter d'engager des poursuites à l'encontre du chercheur pour dommages et intérêts. De plus, il a noté que la majorité des vulnérabilités sont caractérisées par des noms techniques (version de logiciels, protocoles, etc.). Le chercheur peut donc expliquer ses trouvailles sans avoir besoin de citer de nom d'entreprise.
Il peut cependant être intéressant, même si non obligatoire, de contacter l'entreprise pour lui faire part de la présence de vulnérabilités. Il est de même possible au chercheur de contacter en parallèle les organismes gouvernementaux tels l'ANSSI ou la CNIL. S'il s'agit d'un système critique au sein de l'entreprise, il semble logique de faire appel au bon sens du chercheur pour rendre publiques le moins d'informations possible sur la ou les entreprises potentiellement affectées et la façon d'exploiter cette faille. Il est néanmoins important de noter que rien n'obligeant les chercheurs à alerter les entreprises ou à attendre avant de publier leurs découvertes, il semblerait intéressant de proposer à minima un « code de bonne conduite » de règles à appliquer dans un ordre précis afin de protéger, entreprises, chercheurs, instituts de recherche et clients des entreprises.

Mais une dernière difficulté réside dans la publication de logiciel de hacking. Afin de faire valider ses recherches et publications par la communauté scientifique, les chercheurs se doivent de fournir dans leurs publications assez d'éléments pour permettre

20 La liberté scientifique, Université de Tours. [consulté le 17 février 2025] https://www.univ-tours.fr/liberte-scientifique.
21 Loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique.

aux autres membres de la communauté de reproduire leur expérience afin d'en valider les résultats. Or dans le cadre de recherches de vulnérabilités cela peut s'avérer un challenge, car donner tous les outils et méthodes, ainsi qu'une marche à suivre explicite peut s'avérer contre-productif, voire répréhensible (article 323-3-1 du Code pénal, ci-après). En effet, si même quelqu'un n'ayant jamais touché à un ustensile de cuisine de sa vie peut cuisiner avec une recette assez détaillée et claire, alors un apprenti cybercriminel peut lui aussi prétendre exploiter les vulnérabilités que les chercheurs trouvent. Le juste milieu peut donc être difficile à trouver, même pour des professionnels, afin de révéler ce qu'il faut pour permettre aux autres chercheurs de reproduire leur expérience, sans trop en dévoiler.

Dans le cas où une publication scientifique entraînerait une attaque, est-il possible que les chercheurs puissent être accusés de complicité ? La complicité se définit comme telle : « Est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation. Est également complice la personne qui par don, promesse, menace, ordre, abus d'autorité ou de pouvoir aura provoqué à une infraction ou donnée des instructions pour la commettre » (Article 121-7 du Code pénal). Dans notre cas, le chercheur, s'il a suivi les principes de tolérance et d'objectivité, ne devrait pas pouvoir être attaqué sous cet angle. N'ayant en effet, pas sciemment contribué à la cyberattaque. Le chercheur publie à visée académique et non criminelle.

D'après le 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 » (Article-323-3-1 du Code pénal). Or les chercheurs rentrent clairement dans la catégorie de la publication avec un motif légitime de recherche. Ils sont donc autorisés à mettre à disposition des équipements, instruments ou programmes informatiques permettant de trouver des vulnérabilités ou exploits. Il n'en demeure pas moins que mettre à disposition certains logiciels, équipements ou instruments pourrait avoir des répercussions certaines. La mise à disposition reste donc entièrement à la discrétion du chercheur.

Mélanie
ROMANO

LA PROTECTION DES ENFANTS EST-T-ELLE INCLUE PARMI LES OBJECTIFS DE L'ÉTHIQUE « HACKING » ? De l'empowerment à la sécurité by design

Stefania ATTOLINI, Docteur en Droit

Le Parlement européen a clairement inscrit les enfants parmi les personnes ayant accès à l'internet, en leur garantissant « à l'utilisation d'outils, de services et de contenus numériques pluralistes et sûrs» pour assurer la jouissance des droits civils et politiques et d'autres droits de l'homme, y compris la participation à la vie culturelle, sociale et démocratique. En effet, le Réseau offre de larges possibilités, surtout pour les plus jeunes, de faire entendre leur voix et d'exprimer leurs opinions, en créant une inclusion toujours plus grande des mineurs comme citoyens actifs dans la nouvelle société numérique. D'autre part, on parle désormais de «natifs numériques» -actuellement, pour la plupart encore mineurs- se référant justement à la génération de sujets nés dans un monde où être connecté à Internet n'est pas du tout un luxe mais une nécessité et qui interagissent, dès leur plus jeune âge, grâce à différents outils numériques dans la vie quotidienne[22].

Dans un monde où la technologie est omniprésente, surtout après la pandémie de Covid-19 et le confinement, de plus en plus de mineurs utilisent l'Internet quotidiennement. Il est donc devenu impératif de protéger les enfants en ligne[23] et de les sensibiliser sur l'importance de la sécurité en ligne, ainsi que de leur apprendre à utiliser la technologie de manière éthique.

Ceci est en effet l'approche promue par l'Union européenne et par ses Institutions, et confirmée récemment quand elles se sont engagées à respecter, entre autres, les principes proclamés dans la Déclaration européenne sur les droits et principes numériques pour la décennie numérique[24], parmi lesquels il est prescrit que les enfants et les jeunes soient protégés en ligne et formés à cet environnement[25].

Les enfants sont réellement exposés à un large éventail de risques en ligne, allant de la cyberintimidation à l'exploitation sexuelle. Pour répondre à ces défis, l'Union européenne s'est engagée à renforcer la protection des enfants dans le domaine numérique et plus en général à promouvoir une approche holistique de la protection de l'enfance, intégrant des aspects

22 Guidelines for Empowering and Protecting Child and Adolescent Rights on the Internet in Central America and the Dominican Republic" del 2018, *«[R]ecent generations were born into a world where Internet access is no longer considered a privilege, but rather, according to the United Nations (UN), a human right. […]»*

23 La présidente de la Commission européenne Ursula Von der Leyen, dans son discours *« Assurer le leadership de la décennie numérique », prononcé à Sines, le 1er juin 2021, a énoncé l'importance d'une « transition numérique centrée sur l'humain. Il s'agit de savoir qui nous voulons être en tant qu'Européens. Afin de mieux appréhender cette question, nous formulerons un ensemble de principes numériques. Par l'exemple, l'accès de tous à l'internet ; un espace en ligne sécurisé ; le droit d'acquérir des compétences numériques ; des algorithmes respectueux des personnes ; la protection des enfants en ligne. Ces principes importants viendront compléter les droits légaux qui protègent déjà les Européens en ligne, tels que la protection des données à caractère personnel ou la liberté d'expression ».*

24 Déclaration européenne sur les droits et principes numériques pour la décennie numérique, du 26.01.2022, COM(2022) 28 final. Il s'agit d'un acte non contraignant, conclu par les Institutions afin de *« promouvoir une voie européenne de la transformation numérique, centrée sur les citoyens, qui repose sur les valeurs européennes et les droits fondamentaux de l'UE, qui réaffirme les droits de l'homme universels et qui profite à tous les citoyens et entreprises, et à la société dans son ensemble ».*

25 Ce principe énonce que *« Les enfants et les jeunes devraient être formés à l'environnement en ligne afin d'y faire des choix sûrs, en connaissance de cause, et d'y exprimer leur créativité. Des contenus adaptés à chaque âge devraient améliorer l'expérience, le bien-être et la participation des enfants dans cet environnement. Les enfants ont le droit d'être protégés contre toute forme de criminalité, commise ou facilitée par les technologies numériques. Nous nous engageons à: – promouvoir un environnement numérique positif, adapté à l'âge et sûr pour les enfants et les jeunes; – offrir à tous les enfants la possibilité d'acquérir les aptitudes et les compétences nécessaires pour naviguer activement et en toute sécurité dans l'environnement en ligne et pour y faire des choix en connaissance de cause; – protéger tous les enfants contre les contenus nuisibles et illicites, l'exploitation, la manipulation et les abus en ligne, et à empêcher l'utilisation de l'espace numérique pour commettre ou faciliter des actes criminels ».*

juridiques, technologiques, éducatifs et sociaux[26].

Une approche innovante pour parvenir à une protection effective passerait par l'introduction de la protection des mineurs parmi les objectifs, les concepts et les techniques du « *hacking éthique* »[27].
Le hacking éthique, consiste à utiliser les compétences en informatique de manière légale et éthique pour identifier les failles de sécurité dans les systèmes informatiques et les réseaux. Contrairement au hacking malveillant, qui vise à causer des dommages ou à violer la loi pour d'intérêts propres au hacker, le hacking éthique est une pratique légale et bénéfique qui vise à renforcer la sécurité des systèmes informatiques, avec la permission du propriétaire du système.

Outre les compétences techniques, le hacking éthique repose sur des valeurs éthiques solides. Les hackers éthiques doivent respecter la vie privée des autres, obtenir le consentement approprié avant de tester un système et utiliser leurs compétences uniquement à des fins légales et éthiques. Cette pratique joue un rôle crucial dans la protection des données et de la vie privée en ligne : en identifiant et en corrigeant les vulnérabilités dans les systèmes informatiques, les hackers éthiques contribuent à rendre l'internet plus sûr pour les internautes, notamment les plus jeunes utilisateurs. Ceux-ci doivent faire face à plusieurs menaces outre que les contenus illicites et inadaptés, comme par exemple le harcèlement, la discrimination et la restriction d'accès à des services, la surveillance en ligne, les atteintes à la vie privée et à la liberté d'expression et d'information et le manque de transparence des finalités de collecte des données personnelles.

Pour cette raison, les mesures de prévention et d'intervention pour la protection des mineurs doivent aussi tenir compte de l'empreinte numérique (ledit digital footprint), ce qui peut dans le long terme engendrer des effets négatifs sur le développement de l'enfant et par rapport à sa participation future à la société numérique.

La sécurité des technologies et des services fournis par l'Internet est à la base de l'inclusivité des citoyens, en garantissant à ce que la vie démocratique, les services publics et les services de santé et de soins soient accessibles en ligne à tous réellement et sans risques, en offrant des services et des outils inclusifs, efficaces et personnalisés répondant à des normes élevées en matière de sécurité et de respect de la vie privée[28].

Des instances proviennent de diverses parties prenantes de la cybersécurité, concernant l'exigence de proclamation d'un code de bonnes pratiques couvrant le hacking éthique, surtout à la lumière des tendances récentes qui voient le hacking éthique au service de l'État[29] et des intérêts publics, parmi lesquels la protection des enfants en ligne revête un rôle primaire.

Idéalement, ces codes devraient donc promouvoir un niveau élevé de protection des enfants, en prévoyant qu'une attention particulière soit prêtée aux menaces spécifiques.

Stefania
ATTOLINI

26 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Stratégie de l'UE sur les droits de l'enfant, du 24.03.2021, COM(2021) 142 final.
27 Cette approche pourrait être complétée par des initiatives de promotion de l'éducation des enfants au hacking éthique, en apprenant les bases de la programmation et de la sécurité informatique : en éduquant les enfants sur les principes de base du hacking éthique et en leur fournissant les ressources nécessaires pour développer leurs compétences, nous pouvons les aider à devenir des citoyens numériques responsables et à contribuer à un monde en ligne plus sûr et plus sécurisé.
28 Décision du Parlement européen et du Conseil du 15.09.2021 COM(2021) 574 final, établissant le programme d'action à l'horizon 2030, La voie à suivre pour la décennie numérique, adoptée sur la base de l'article 173, paragraphe 3, du TFUE, énonce que « *sans préjudice de l'objectif consistant à doter l'ensemble de la population de l'Union européenne de compétences numériques de base, conformément au plan d'action relatif au socle européen des droits sociaux et au plan d'action en matière d'éducation numérique, le programme «La voie à suivre pour la décennie numérique» fixe à 80 % la proportion de personnes âgées de 16 à 74 ans qui devront posséder au moins des compétences numériques élémentaires en 2030* ».
29 En janvier 2024, un programme public réservé aux «*bug bounties*» a ainsi été lancé par l'État afin de traquer les éventuelles failles de sécurité dans l'application «*France Identité*» (créée en 2022)

02

LE CADRE JURIDIQUE DU HACKING ÉTHIQUE EN FRANCE

- Approche juridique de la notion de hacking éthique
- Renforcer le statut des lanceurs d'alerte numérique "hackers éthiques" en droit français
- L'importance du contrat dans le cadre du pentest
- Le statut juridique du lanceur d'alerte « numérique »

APPROCHE JURIDIQUE DE LA NOTION DE HACKING ÉTHIQUE

ASC Eve TOURNY, DC DIRISI/DIV NUMO/SD CYBER

Le juriste aime à débuter un travail de recherche par une définition des termes de son sujet. En droit français, le hacking a fait l'objet de la loi relative à la fraude informatique du 5 janvier 1988[30] qui est venue insérer les articles 323-1 et suivants dans le code pénal[31]. Le hacking ou piratage en droit est donc un comportement infractionnel, pris en compte, défini et puni.

La dimension éthique n'est pas prise en compte par ce texte. Cette absence est récurrente et renvoi en droit pénal à la question de l'élément moral de l'infraction tel qu'il est défini à l'article 121-3 du Code pénal[32]. L'élément intentionnel, élément constitutif de l'infraction à l'instar de l'élément légal et de l'élément matériel, tel qu'il est défini par la doctrine, consiste dans la conscience et la volonté d'accomplir l'acte interdit dans la loi. La conscience est présumée sur le fondement de l'adage selon lequel « nul n'est censé ignorer la loi ». La volonté d'accomplir l'acte elle est présumée avec la matérialité des faits[33].

La loi sur la république numérique est venue modifier cette situation en créant le statut de hacker blanc. Cette loi a inséré un article dans le code de la défense prévoyant que « pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale[34] n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données ». L'alinéa deux prévoit que « l'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée »[35].

Le hacker éthique se voit donc offrir un statut protecteur mais un statut relatif. Dans l'hypothèse où l'ANSSI ne reconnaît pas le caractère de bonne foi alors le dispositif prévu par l'article L.2321-4 du Code de la défense précité ne s'applique plus et le hacker ne bénéficie plus d'aucune protection. Or, le concept de bonne foi en droit est sujet à interprétation car il n'est pas défini par la loi.

Il existe une notion connexe est celle du pentest ou test d'intrusion. Dans cette situation, le hacker est protégé par un contrat qui le lie au propriétaire du système de traitement automatisé de données dans lequel il va tenter de s'introduire sans avoir les accès. Le statut de pentester n'est pas exempt d'insécurité mais le contrat amoindri les risques en encadrant les relations et l'activité du pentesteur.
Ce rapide examen montre donc que le régime juridique du hacker éthique présente de fortes lacunes.

La Belgique s'est dotée récemment d'une loi sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constaté au sein d'une entité juridique du secteur privé[36]. Cette loi a un champ d'application matériel plus large puisque sont visés tous les lanceurs d'alerte. Mais le hacker éthique est considéré comme une catégorie de lanceur d'alerte. L'article 2 vise le hacking en prévoyant

30 Loi n°88-15 disponible sur le site Légifrance - Publications officielles - Journal officiel - JORF n° 0004 du 06/01/1988 (accès protégé) (legifrance.gouv.fr)
31 Chapitre III. Des atteintes aux systèmes de traitement automatisé de données (article 323-1 à 323-8).
32 Art. 121-3 du code pénal « *Il n'y a point de crime ou de délit sans intention de le commettre.*
Toutefois, lorsque la loi le prévoit, il y a délit en cas de mise en danger délibérée de la personne d'autrui.
Il y a également délit, lorsque la loi le prévoit, en cas de faute d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement, s'il est établi que l'auteur des faits n'a pas accompli les diligences normales compte tenu, le cas échéant, de la nature de ses missions ou de ses fonctions, de ses compétences ainsi que du pouvoir et des moyens dont il disposait.
Dans le cas prévu par l'alinéa qui précède, les personnes physiques qui n'ont pas causé directement le dommage, mais qui ont créé ou contribué à créer la situation qui a permis la réalisation du dommage ou qui n'ont pas pris les mesures permettant de l'éviter, sont responsables pénalement s'il est établi qu'elles ont, soit violé de façon manifestement délibérée une obligation particulière de prudence ou de sécurité prévue par la loi ou le règlement, soit commis une faute caractérisée et qui exposait autrui à un risque d'une particulière gravité qu'elles ne pouvaient ignorer ».
Il n'y a point de contravention en cas de force majeure.
33 Cf. Cass. Crim. 28 février 2018
34 Article 40 alinéa 2 du Code de procédure pénale *« toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs »*
35 Art. L. 2321-4 du Code de la défense.
36 Loi du 28 novembre 2022 disponible sur Loi du 28/11/2022 sur la protection des personnes qui signalent des violations au droit de l'union ou au droit national constatees au sein d'une entite juridique du secteur prive (openjustice.be)

que « la présente loi établit des normes minimales communes pour la protection des personnes signalant les violations suivantes : les violations qui concernent les domaines suivants : (…) j/ protection de la vie privée et des données à caractère personnel et sécurité des réseaux et des systèmes d'information ».

L'article 8 de ce texte prévoit les conditions pour que les auteurs de signalement, donc les hackers éthiques, bénéficient de la protection[37].

La Belgique a donc mis en place un régime juridique qui prend en compte le hacking éthique, même s'il n'est pas exempt de failles. Ainsi, selon l'article 6 la loi belge s'applique « aux auteurs de signalement travaillant dans le secteur privé qui ont obtenu des informations sur des violations dans un contexte professionnel ». Interprété a contrario cela signifie qu'une personne isolée qui pratique le hacking éthique ne bénéficiera pas de la protection mise en place par cette loi.

L'appréhension du hacking éthique par le droit reste parcellaire.

La différence entre le « bon hacker » et le « mauvais hacker » se heurte à la pratique car il s'agit de démontrer l'intentionnalité d'une action.

Le pentest comme le bug bounty sont encadrés non seulement par la loi mais également par un contrat qui lie l'expert en cybersécurité à la cible. Les bonnes volontés existent. Le besoin également surtout pour les petites, moyennes entreprises et celles de taille intermédiaire.

Dans le cas du hacking éthique, et parce que le droit n'offrira qu'une réponse partielle, il semble nécessaire d'introduire un tiers de confiance chargé non seulement d'établir un pont entre les citoyens éclairés désirant mettre leurs compétences à disposition et entreprises, mais également d'encadrer les usages et partager les bonnes pratiques.

Eve
TOURNY

37 Art. 8.1er. Les auteurs de signalement bénéficient de la protection en vertu des chapitres 6 et 7 pour autant que : 1° ils aient eu des motifs raisonnables de croire que les informations signalées sur les violations étaient véridiques au moment du signalement et que ces informations entraient dans le champ d'application de la présente loi; et 2° ils aient effectué un signalement soit interne conformément à l'article 12, soit externe conformément à l'article 15, ou aient fait une divulgation publique conformément à l'article 19.Le premier critère est apprécié au regard d'une personne placée dans une situation similaire et disposant de connaissances comparables.
L'auteur de signalement ne perd pas le bénéfice de la protection au seul motif que le signalement effectué de bonne foi s'est avéré inexact ou infondé.
§ 2. Les entités juridiques du secteur privé, les autorités compétentes et le coordinateur fédéral acceptent les signalements anonymes de violations et en assurent le suivi.
Par dérogation à l'alinéa 1er, les entités juridiques du secteur privé qui comptent moins de 250 travailleurs ne sont pas tenues d'accepter les signalements anonymes.
§ 3. Les personnes qui ont signalé ou divulgué publiquement des informations sur des violations de manière anonyme, mais qui sont identifiées par la suite et font l'objet de représailles, bénéficient de la protection en vertu des chapitres 6 et 7, pour autant qu'elles répondent aux conditions visées au paragraphe 1er.
§ 4. Les personnes qui signalent auprès des institutions, organes ou organismes de l'Union compétents des violations relevant du champ d'application de la présente loi bénéficient de la protection en vertu de la présente loi dans les mêmes conditions que les personnes qui effectuent un signalement externe.
§ 5. Les personnes qui signalent auprès des autorités judiciaires des violations relevant du champ d'application de la présente loi dans le cadre de l'article 30 du Code d'instruction criminelle bénéficient de la protection en vertu de la présente loi dans les mêmes conditions que les personnes qui effectuent un signalement externe, sans préjudice du régime de protection des témoins menacés visé aux articles 102 et suivants du Code précité et dans la mesure où ces mesures de protection leur sont plus favorables.

RENFORCER LE STATUT DES LANCEURS D'ALERTE NUMÉRIQUE "HACKERS ÉTHIQUES" EN DROIT FRANÇAIS

Fabien LEMARCHAND, Président de Hack4Values

Introduction

L'évolution rapide du paysage numérique mondial a entraîné une augmentation spectaculaire des cyberattaques, engendrant des dommages considérables tant pour les entreprises que pour les services publics. Ces attaques, souvent sophistiquées, ont des répercussions profondes sur la confidentialité des données, la sécurité financière et même la stabilité des infrastructures essentielles. Dans ce contexte, l'importance croissante des hackers éthiques, également connus sous le nom de «hackers bienveillants», dans la protection des systèmes informatiques est indéniable. Le hacker éthique prévient le risque d' attaques cyber en découvrant en amont les faiblesses de sécurité d'un système informatique. Cependant, malgré leur rôle crucial, ces acteurs sont souvent confrontés à un vide juridique et à des défis en matière de reconnaissance officielle de leur travail. Cet article examine la nécessité pressante de renforcer le statut des hackers éthiques en droit français, en mettant en lumière leur contribution essentielle à la cybersécurité et en proposant des mesures concrètes pour assurer leur protection juridique.

Le cadre juridique actuel

Actuellement, le cadre juridique français aborde la question du hacking dans l'article 323-1 du code pénal, qui réprime le piratage informatique. Cependant, une distinction est clairement établie entre les hackers malveillants et les hackers éthiques. En effet, l'article L-2321-4 du code de la défense, issu de la loi pour une République numérique de 2016, offre une protection limitée aux hackers éthiques agissant de bonne foi et l'intrusion doit notamment être proportionnée et se borner à prouver la faille sans aller plus loin.

Cependant, cette disposition est limitée par le fait que les hackers éthiques ne peuvent informer seulement l'Autorité nationale de sécurité des systèmes d'information (ANSSI) de l'existence d'une vulnérabilité dans un système informatique, et non en parallèle directement le responsable du système informatique concerné par la vulnérabilité de sécurité découverte. Cette restriction pose des défis significatifs pour la cybersécurité, notamment en ce qui concerne la rapidité et l'efficacité de la réponse aux failles de sécurité.
Aujourd'hui, une grande partie des hackers éthiques n'informent ni le responsable du système informatique par risque de sanction pénale, ni l'ANSSI par peur d'inefficacité et de confiance sur le traitement de la vulnérabilité en question. Pour le reste des hackers éthiques, ils informent directement le responsable du système informatique en prenant de potentiels risques pénaux.

Renforcer le statut des hackers éthiques

Afin de combler cette lacune réglementaire et de promouvoir davantage l'engagement des hackers éthiques, il est impératif de renforcer leur statut en droit français. Cette démarche repose sur deux principaux piliers :

1. Encadrement juridique complet : Il est essentiel d'élaborer un cadre juridique exhaustif qui définit clairement le rôle, les droits et les responsabilités des hackers éthiques. Ce cadre devrait inclure des dispositions protégeant ces acteurs contre les poursuites judiciaires lorsqu'ils agissent de manière éthique et dans l'intérêt public et devrait autoriser les hackers éthiques à informer directement les responsables des systèmes informatiques en plus de l'ANSSI. De plus, il devrait établir des mécanismes permettant aux entreprises et aux organisations de coopérer en toute confiance avec les hackers éthiques pour identifier et corriger les failles de sécurité.

2. Élaboration d'un code de conduite national : La mise en place d'un code de conduite spécifique pour les hackers éthiques permettrait de définir des normes éthiques et opérationnelles claires pour leur activité. Ce code devrait aborder des aspects tels que les règles de fonctionnement et de conduite. En instaurant des lignes directrices communes, ce code favoriserait la transparence et la cohérence dans les pratiques des hackers éthiques, renforçant ainsi la confiance des entreprises et des organisations à leur égard.

3. Amélioration de la réactivité : Autoriser les hackers éthiques à informer directement les responsables des systèmes informatiques permettrait une réaction plus rapide face aux failles de sécurité. En évitant les retards potentiels liés à la transmission de l'information par l'intermédiaire de l'ANSSI, les responsables des systèmes informatiques pourraient prendre des mesures immédiates pour corriger les vulnérabilités et renforcer la sécurité de leurs systèmes.

4. Renforcement de la confiance : En permettant aux hackers éthiques de communiquer directement avec les responsables des systèmes informatiques, la confiance entre les différentes parties impliquées dans la gestion des failles de sécurité serait renforcée. Les responsables des systèmes informatiques seraient plus enclins à collaborer avec les hackers éthiques s'ils peuvent échanger des informations de manière transparente et directe, ce qui conduirait à une meilleure protection des données et à une cybersécurité renforcée.

5. Optimisation des ressources : Autoriser les hackers éthiques à informer directement les responsables des systèmes informatiques permettrait d'optimiser l'utilisation des ressources, en évitant la surcharge potentielle de l'ANSSI. En encourageant une répartition plus équilibrée des responsabilités dans la gestion des failles de sécurité, cette approche contribuerait à une réponse plus efficace et efficiente aux cybermenaces.

6. Encouragement de la collaboration : En reconnaissant le rôle des hackers éthiques en tant que partenaires dans la lutte contre les cybermenaces, cette proposition encouragerait la collaboration entre les différentes parties prenantes, y compris les responsables des systèmes informatiques, les hackers éthiques et les autorités compétentes. Cette collaboration renforcée favoriserait l'échange d'expertise et de meilleures pratiques, conduisant à une cybersécurité plus robuste et à une protection accrue des données sensibles.

Conclusion

Face à la multiplication des cybermenaces et à la complexité croissante des systèmes informatiques, la contribution des hackers éthiques à la cybersécurité est plus précieuse que jamais. Pour tirer pleinement parti de leur expertise et de leur engagement, il est impératif de leur accorder une reconnaissance juridique adéquate et de leur offrir un cadre réglementaire clair et protecteur. En renforçant le statut des hackers éthiques en droit français, nous pouvons non seulement renforcer la sécurité de nos systèmes informatiques, mais aussi promouvoir une culture de responsabilité et de coopération dans le domaine de la cybersécurité.

Fabien
LEMARCHAND

L'IMPORTANCE DU CONTRAT DANS LE CADRE DU PENTEST

Jules COOPER, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

Un pentester est une personne qui agit dans un cadre professionnel et fermé, qui est engagée par une entreprise pour réaliser des audits de sécurité sur des entreprises autres que la sienne.

Dans cette définition, il existe plusieurs sous-domaines ou spécialisations de pentester, comme les red teams, qui, à la différence d'un pentester classique, opèrent sur une durée de plusieurs mois, les spécialistes hardware, participant à des activités de reverse engineering et de reconnaissance de faille matérielle, et enfin les spécialistes software, spécialité la plus courante qui prennent part à des audits de failles sur site Internet et applications.

En regroupant l'ensemble des actions effectuées par un pentester pour réaliser son audit, une liste de compétences ressort contenant : la reconnaissance du système dans lequel il va opérer, la recherche de ports ouverts et des différents services accessibles sans utiliser de vulnérabilité. Puis, il va user de différentes méthodes pour chercher des vulnérabilités. En conséquence, il peut décider d'exploiter ou non ce qu'il trouve. Toutes les informations que le pentester aura trouvées lors de sa recherche seront détaillées dans son rapport pour que le client en prenne connaissance. La question du cadre juridique peut se poser, puisqu'a priori, ces actions ont des similitudes avec celles des hackers. Ce cadre, comme il sera étudié dans les parties qui suivent, est très contraignant.

La loi vis-à-vis des activités du pentester

En se référant strictement à ce que dit la loi, beaucoup d'infractions au droit pénal peuvent être constatées. 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 € d'amende ». Fondamentalement un pentester est forcé d'accéder et de se maintenir dans le système et ici peut se poser la question de l'action frauduleuse. Usuellement quelque chose de frauduleux a pour but de tromper dans l'attente d'obtenir un avantage illégitime. Juridiquement cet attribut est étendu dans ce cas à un accès sans autorisation et en connaissance de cause. Un exemple concret pourrait être un pentester qui accède à l'aide d'une faille à une boite mail du client. Le pentester a bien accédé ici au système de traitement automatisé de données (ci-après « STAD »).

Le métier de pentester est donc, par nature, un métier réalisant des tâches qui peuvent être considérées comme illégales[38]. Une subtilité qui peut être amenée ici est celle de la requête du client de l'audit. En effet, pour pouvoir appliquer les articles du Code pénal, trois grands principes doivent être prouvés, la matérialité, l'intentionnalité et l'absence de consentement.

L'infraction est déterminée par la matérialité et l'intentionnalité des infractions commises par un pentester, pour analyser ensuite la responsabilité. Ici, l'exemple de l'article 323-1 alinéa premier du Code pénal est pris à titre illustratif, mais il est possible de l'appliquer également aux autres articles du Code pénal sur l'atteinte aux STAD.

En droit, la matérialité de l'infraction de l'article 323-1 du Code pénal prévoit un accès ou un maintien dans un STAD, sans autorisation. Elle ne suppose pas, en l'espèce, une altération du fonctionnement au STAD ou une altération des données, étant donné que ce sont des circonstances aggravantes spécifiquement visées. Cependant, la demande d'audit du client et la volonté de création d'un contrat traduisent une autorisation du client de s'introduire dans le système. Cela exclut

38 Voir notamment les articles 323-1 à 323-8 du Code pénal.

donc l'intrusion de manière frauduleuse[39]. L'élément matériel ne semble pas caractérisé dans ce cas précis. Cependant, il faudra apporter une nuance dans le cas où un pentester sortirait du périmètre de l'accord.

Bien que l'élément matériel ne soit pas caractérisé, il est utile de démontrer l'intentionnalité, l'étude de celle-ci restant intéressante. En droit, l'élément moral ou l'intentionnalité est important. Selon l'article 121-3 du Code pénal : « il n'y a pas de crime ou de délit sans intention de le commettre ». Donc l'auteur du délit doit avoir agi volontairement et en connaissance de cause (ce qui se distingue du mobile de l'infraction). Or ici le pentester, qui a des connaissances en informatique, a cherché à s'introduire dans le système et il sait que cet acte est illégal et interdit. Donc même avec l'accord entre les deux parties, l'élément moral est caractérisé. Comme l'élément de matérialité ne peut être démontré, l'infraction ne peut, en principe, être caractérisée tant que le pentester reste dans les limites de l'audit et en accord avec ce qui a été défini par le client. Pourtant, le cadre juridique du pentest reste relativement confus et doit faire l'objet d'une analyse plus approfondie.

> « Il n'y a pas de crime ou de délit sans intention de le commettre »

Les contrats du pentester

Le contrat de prestation de services informatique : quels risques juridiques ?

Le pentester, engagé par une entreprise, par un contrat préalablement établi, va être positionné sur des missions. Missions qui sont créées par le client et qui sont elles aussi contrôlées par des contrats. Un contrat appelé contrat de prestation de services informatique[40], qui est une sous-catégorie de contrat commercial, se définit par un prestataire informatique (société ou individu spécialisés) qui s'engage à fournir un service informatique, moyennant rémunération, et selon les conditions indiquées par le contrat. Ce dernier constitue une sorte de « forfait » (afin de tester un certain périmètre), et vise des moyens humains que le prestataire met en place. Tout comme le précise l'article 1101 du Code civil, il a la propriété de pouvoir créer, modifier, transmettre ou éteindre des obligations. Le contrat est également signé par les deux parties, l'entreprise engageant les pentesters et celle demandant l'audit (client).

Avant la mission : l'importance de la définition du périmètre

Dans la majorité des cas, le contrat de prestation, qui précise la durée du contrat et le coût de l'expertise, est rédigé par la société prestataire de l'entreprise qui demande l'audit de sécurité et fournit le cahier des charges. L'entreprise demandeuse peut, ensuite, apporter des modifications au contrat avant de décider de l'accepter ou non. Ce contrat reste très global et ne contient que très peu d'informations, les principales étant : la durée fixe de l'audit, le coût de la prestation, la destruction de tout ce qui a été trouvé après un certain temps, l'interdiction de publier publiquement les vulnérabilités trouvées (clauses de non-divulgations), et le périmètre d'action auquel le pentester sera restreint. Cette information est pertinente, car elle soulève des questions sur les limites potentielles des ressources allouées aux clients. Cela est particulièrement vrai lorsque les serveurs ne sont pas hébergés en interne, c'est-à-dire on premise. De nombreux clients disposent de leur propre infrastructure, mais certains clients utilisent des serveurs dédiés fournis par des prestataires cloud, ce qui élimine le risque de débordement théorique sur des serveurs partagés. Même en cas de bonne foi pour trouver une vulnérabilité de son hébergeur, le client ne peut pas choisir d'étendre le périmètre jusqu'à l'hébergeur. En dehors de cette spécification, le client est libre d'inclure ce qu'il souhaite dans le périmètre d'action.

En supplément du contrat de prestation, des modifications et ajouts peuvent être apportés. Il est courant de voir les pentesters, en contact avec le client, échanger à ce sujet par mail. Ces mails agissent alors comme trace pouvant être apportée lors d'un procès, mais leur valeur reste relative par rapport à celle d'un contrat (la valeur juridique d'emails professionnels a déjà été reconnue). Le recours aux échanges par mail créé une difficulté supplémentaire au métier en cas de litige. En effet, il est déjà complexe d'apporter un jugement concernant la profession de pentester, non définie en droit.

Pendant la mission : que se passe-t-il en cas de problème ?

Pendant la mission, deux scénarios d'erreur peuvent être imaginés : le premier lorsque le pentester est resté dans les limites et le périmètre du contrat, et le second, lorsqu'il en est sorti. Ils peuvent tous deux requérir l'intervention du service informatique (SI), pour réparer la panne. À la différence des bug bounty hunter, le service informatique reste en contact constant avec le pentester, leur permettant dès lors des réparations plus rapides lorsque des dégâts sont causés.

Pour ce premier cas, les pentesters sont protégés par les contrats en termes de responsabilité civile. Aucune

39 Fabrice Mattatia, « *Faut-il dépénaliser les hackers blancs ?* »,: Revue de science criminelle et de droit pénal comparé, 2015.
40 Philippe Le Tourneau, Contrat du numérique, « *des notions de contrat informatiques et électroniques* » p.81 et suivantes, et « *la fourniture de contenus ou de services numériques* » p. 368 et suivantes.

répercussion ne peut a priori être observée à leurs égards, à condition que ceux-ci ne commettent pas de faute lourde.

Dans le second cas, la responsabilité pénale entre en jeu et les contrats ne protègent plus l'individu. Ses actions sont dès lors illégales puisqu'elles vont à l'encontre d'articles du Code pénal, notamment l'article 323-1 précédemment cité. Le pentester pourra donc voir sa responsabilité civile engagée potentiellement (mais pas forcément délictuelle) et pénale.

Que se passe-t-il en cas de rupture de contrat ?

Dans le cas d'une faute grave qui forcerait le client à mettre fin au contrat, il s'agit ici de résiliation unilatérale, c'est-à-dire qu'une des deux parties met fin au contrat en raison de la violation d'une clauses du contrat. Dans ce cas si le client décide de se retourner contre l'entreprise en raison de la faute commise, les responsabilités du pentester et de l'entreprise pourront être engagées.

De plus la notion de bon sens est mise en avant. Le contenu des contrats reste très global, il permet aux pentesters d'agir assez librement. Il y existe un flou inhérent à la prestation, dans lequel le pentester peut faire des actions qui constituent un manquement au contrat de prestation de services, mais qui reste dans l'intérêt du client. Ceci introduit la deuxième ambiguïté concernant ce type de contrats de prestation, ils peuvent être amenés à changer de manière indirecte, par exemple avec des mails ou des discussions orales avec client. Leur périmètre peut être modifié : élargis ou certaines actions peuvent être conseillées par le client. Chacun de ces points peut poser des problèmes, car ils peuvent ne pas laisser de trace et comporter des coquilles et des erreurs juridiques.

Les responsabilités dans le cadre d'un audit

Dans le cadre du pentest, les articles du Code pénal précédemment cités peuvent amener à engager la responsabilité pénale du pentester ou de l'employeur en cas de condamnation, c'est-à-dire, dans le cas où le pentester causerait un dommage en sortant du périmètre de l'audit. Lorsque l'existence d'une infraction est constatée, il existe des cas d'irresponsabilité pénale, par exemple, lorsqu'un acte est autorisé par des dispositions législatives (article 122-4 du Code pénal). Cependant, les dispositions pénales en droit français sont impératives et ne peuvent normalement pas être écartées par un accord entre particuliers[41]. Ainsi, les contrats de mission de pentest ne peuvent normalement pas exclure la responsabilité des prestataires[42]. Cette précision apportée, le cas de la responsabilité de l'employeur et du pentester mérite une analyse au regard des liens juridiques entre les deux protagonistes et les risques encourus.

La responsabilité de l'employeur

Deux responsabilités peuvent être engagées : civile qui permet de réparer un préjudice pour des dommages causés à un tiers, et pénale, qui oblige l'auteur ou le complice d'une infraction délictueuse à répondre de ses actes devant la société[43]. Du point de vue de la responsabilité civile, il est nécessaire de distinguer la responsabilité contractuelle (article 1231-1 du Code civil) de la responsabilité délictuelle (article 1240 du Code civil).

Dans le cadre de la responsabilité contractuelle, la responsabilité « du débiteur » (ici l'entreprise ou le chef d'entreprise) peut être engagée en cas de non-respect du contrat. Ici l'inexécution de l'obligation étant le non-respect du contrat de mission émit, par exemple en dépassant le périmètre établi. Il reste alors à prouver que le résultat du non-respect du contrat a causé un dommage au client, et que les deux ont un lien, à savoir que c'est à cause du pentester qui est sorti du contrat que les dommages ont eu lieu. En outre, il est nécessaire de déterminer si les pentesters ont une obligation de moyen ou de résultat. L'obligation de moyens oblige l'entreprise à mettre en place tous les moyens nécessaires à la réalisation de la prestation, mais elle ne pénalise pas l'absence de résultat. Ici, ces contrats de prestation de services ne mettent en place que cette obligation, et non celle de résultat. L'obligation de moyens est essentielle et permet au pentester et à l'entreprise de ne pas être assujetti à des poursuites légales dans les cas où aucune faille ne soit trouvée dans la durée imposée.

Dans le cadre de la responsabilité délictuelle (et de manière simplifiée), en dehors d'un contrat, doivent être démontrés la faute, le dommage et le lien de causalité. Si toutes ces conditions sont réunies alors l'entreprise du pentester ou l'entreprise du client pourra être poursuivie pour les actions effectuées par ce dernier. Il faudra ainsi dédommager l'entreprise, et réparer les dégâts subis par cette dernière. Pour illustrer ce point, un pentester peut effectuer un audit sur les boites mail d'un client et s'intéresser au site web de réponse automatique de donnée, qui dès lors est en dehors du périmètre d'action. Dans le cas où la plateforme de réponse automatique cesse de fonctionner, reste à prouver que le pentester était en faute (dans notre cas oui puisqu'il agit hors du périmètre du contrat). D'autre part que les dommages observés consistent en l'arrêt

41 Voir notamment les articles 6 et 1162 du Code civil, ainsi que l'article 111-4 du Code pénal.
42 Marc-Antoine LEDIEU, « *Le pentest, le contrat et la responsabilité* » Cours CNAM droit de la cyber-sécurité, 2024. https://technique- et- droit- du- numerique.fr/le- pentest- le- contrat- et- la- responsabilite- le- cnam- droit- de- la- cyber- securite- 22- avril-2024/. [En ligne; consulté le 28-Avril-2024].
43 Bercy Infos, « *Chef d'entreprise, dans quels cas votre responsabilité civile ou pénal peut-elle être engagée* », 2022. https://www. economie.gouv.fr/entreprises/responsabilite-civile-penale-chef-entreprise. [En ligne; consulté le 10 mai 2024]..

du fonctionnement des réponses automatiques. Le pentester ayant effectué une action dessus, le lien est alors établi. Ses actions peuvent donc engager sa responsabilité délictuelle. Cet exemple simplifié essaie donc de démontrer la possibilité d'établir la responsabilité délictuelle d'un pentester.

Du point de vue de la responsabilité pénale, les individus sont responsables de leur propre fait (article 121-1 du Code pénal). Il est possible d'engager la responsabilité de l'entreprise (article 121-2 du Code pénal) et celle du chef d'entreprise en cas d'infraction pénale dans le cadre d'un audit. Cependant, une exception à l'engagement de la responsabilité du chef d'entreprise doit être présentée. La délégation de pouvoir peut permettre de ne pas engager la responsabilité du chef d'entreprise si certaines conditions sont remplies : si le chef d'entreprise exerce une subordination sur son salarié, qui l'a accepté, tout en disposant des moyens nécessaires. Il est donc facile d'imaginer que dans le cas du pentester, celui-ci agit en tant que délégué, conformément à l'autorisation de son entreprise avec laquelle il a signé un contrat de travail. Si la tâche donnée au pentester est assez précise, par exemple d'aller utiliser une attaque spécifique pour tester un aspect particulier, et que cette dernière vient à fausser le fonctionnement du STAD, le pentester ne verrait alors pas sa responsabilité engagée, et seul le chef d'entreprise pourrait être poursuivi.

L'entreprise et le chef d'entreprise peuvent donc être à la fois responsables pénalement et civilement des actions du pentester.

La responsabilité de l'employé

Même si la responsabilité pénale de l'employeur peut être engagée, elle ne justifie nullement que le pentester ayant commis la faute puisse être excusé (article 121-2 du Code pénal).

La seule utilité qu'aurait un pentester à être sous contrat de travail avec une entreprise serait la sécurité d'emploi, il n'a pas besoin de chercher les clients, c'est à l'entreprise de le faire. Le pentester employé est stable financièrement grâce à son salaire mensuel que l'entreprise ait trouvé des clients ou non. En principe, d'après le Code civil, un salarié ne peut être déclaré civilement responsable des dommages causés à son employeur à l'occasion du travail. La responsabilité civile du pentester est engagée, et il peut être amené à dédommager l'entreprise cliente, et réparer les dégâts réalisés. Les exceptions qui peuvent amener à engager sa responsabilité civile sont les fautes lourdes, pouvant venir d'une intention de nuire à l'employeur. Des exemples de fautes lourdes seraient une dégradation volontaire d'un outil de l'entreprise, ou encore la divulgation d'information obtenue dans le cadre de son audit.

Enfin une dernière précision peut être apportée. Le contrat de travail n'a pas de définition dans le Code du travail, mais il en existe une proposée par la jurisprudence face à ce vide juridique : « La convention par laquelle une personne s'engage à exécuter au profit d'une autre personne et sous sa subordination, un travail moyennant une rémunération appelée salaire[44]» . Le lien de subordination est défini par la Cour de cassation[45] comme « l'exécution d'un travail sous l'autorité d'un employeur qui a le pouvoir d'en donner des ordres et des directives, d'en contrôler les manquements et de sanctionner les manquements de son subordonné »[46]. Cette définition est fondée sur l'existence d'un rapport de pouvoir. Elle implique un contrôle de l'activité du salarié, qui peut se qualifier de différentes manières comme avec des vérifications des systèmes, de comptages ou autre. En cas d'observation d'un manquement et selon la gravité de celui-ci, l'employeur peut se retourner contre le salarié, pour le sanctionner, voire de le licencier dans les cas de fautes lourdes et graves.

L'absence de formation juridique et ses risques

À la suite des échanges organisés avec des pentesters, un manque de formation juridique des professionnels est regretté. Ce manque peut s'expliquer par l'absence de loi les concernant. En dehors de la loi Godfrain[47] qui dicte que toutes les actions effectuées par les pentesters sont illégales, aucune loi ne concerne directement le pentester en entreprise.

Il est aussi ressorti de certains échanges que le manque de précision dans les contrats et la loi conduit à des points relevant de la libre interprétation de chacun. Par exemple un pentester peut décider de s'arrêter dès qu'il a trouvé une vulnérabilité et de ne pas aller au-delà. De même, un autre pentester peut se dire qu'il est engagé pour trouver des vulnérabilités et celles qui en découlent, et décidera donc d'aller plus loin. Même si dans le dernier cas, le contrat peut tomber, puisque le pentester a agi en dehors du périmètre préalablement établi.
Il est assez courant qu'au-delà des contrats préalablement définis, le client et le pentester décident d'augmenter le périmètre d'action ou de faire tout autre changement au contrat. Ces changements ne font pas toujours l'objet de nouveaux contrats et peuvent être écrits par mails, qui constituent une trace écrite ayant

44 Véronique Roy, « *Droit du travail en 28 fiches* », Dunod 2024.
45 Cour de Cassation, Chambre sociale, du 13 novembre 1996, 94-13.187, Publié au bulletin.
46 Site internet Ministère du Travail, « *Contrat de travail : les principales caractéristiques* » 2024. https://travail-emploi.gouv.fr/droit-du- travail/la-vie-du-contrat-de-travail/article/contrat-de-travail-les-principales-caracteristiques. [En ligne; consulté le 26 avril 2024].
47 Loi no 88-19 du 5 janvier 1988 relative à la fraude informatique.

une force juridique relative. Ils peuvent poser donc des problèmes de justifications quand le client se retourne vers le pentester ou lorsque la direction de l'entreprise n'a pas été prévenue en cas de changements de la feuille de route.

Dans cette situation, la notion de bonne foi de la part du pentester est essentielle et a juger au cas par cas. En effet, dès lors qu'un doute est émis et que le client a été préalablement mis au courant de la situation par le pentester, alors la notion de bonne foi, de ce dernier, peut être appliquée.

Jules
COOPER

LE STATUT JURIDIQUE DU LANCEUR D'ALERTE « NUMÉRIQUE »

Titouan LE BLÉ, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

En restant dans le cadre de leur mission, les experts en cybersécurité peuvent identifier des problèmes importants qui, si corrigés, éviteraient aux entreprises des dizaines de milliers d'euros de pertes de chiffre d'affaires[48] ou la mise en danger de leurs clients[49] ou des biens de ces derniers.

Ces vulnérabilités, même signalées à leur hiérarchie, peuvent ne pas être résolues. En effet, comme l'ont souligné de nombreux professionnels lors de nos interviews, les entreprises tierces peuvent choisir de ne pas donner suite aux recommandations, car les signaux d'alerte ne sont pas toujours suffisamment pris au sérieux. C'est dans ce contexte que nous avons choisi d'étudier la législation relative aux lanceurs d'alerte.
Le statut de lanceur d'alerte pourrait offrir une protection plus robuste aux pentesters, leur permettant de signaler des failles de sécurité ou des pratiques contestables sans crainte de représailles. Cependant, ce statut n'est pas exempt de critiques. Certains affirment qu'il n'est pas suffisamment adapté aux spécificités du domaine de la cybersécurité et qu'il ne répond pas pleinement aux besoins de protection des pentesters.

La directive européenne sur la protection des personnes qui signalent des violations du droit de l'Union, adoptée en 2019, vise à instaurer un cadre juridique harmonisé pour la protection des lanceurs d'alerte au sein de l'Union européenne. Sa mise en œuvre par les États membres est obligatoire, et ces derniers peuvent aller au-delà des exigences minimales. En France, par exemple, la loi dite « Sapin 2 », qui désigne la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique[50], proposait alors un cadre robuste, mais incomplet, pour les lanceurs d'alerte. Cette dernière fut révisée dans la loi n° 2022-401 du 21 mars 2022 à la suite du rapport de juillet 2021 sur l'évaluation de son impact.
Cette nouvelle loi précise la définition de lanceur d'alerte et élargit son champ d'action dans sa réécriture de l'article 6-I de la loi n° 2016-1691 : *« Un lanceur d'alerte est une personne physique qui signale ou divulgue, sans contrepartie financière directe et de bonne foi, des informations portant sur un crime, un délit, une menace ou un préjudice pour l'intérêt général, une violation ou une tentative de dissimulation d'une violation d'un engagement international régulièrement ratifiée ou approuvée par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, du droit de l'Union européenne, de la loi ou du règlement. Lorsque les informations n'ont pas été obtenues dans le cadre des activités professionnelles mentionnées au I de l'article 8, le lanceur d'alerte doit en avoir eu personnellement connaissance. ».*

Une législation relative aux lanceurs d'alerte incomplète

Les personnes pratiquant le métier de pentester rentrent théoriquement dans la définition encadrant les lanceurs d'alerte. Par exemple, un pentester qui, au cours d'un audit du système d'information d'une entreprise, découvrirait un manquement caractérisé au Règlement général sur la protection des données (ci-après « RGPD ») commis par cette dernière serait en droit de signaler cette violation. Bien qu'un pentester ne soit pas tenu de se former au RGPD, l'audit de système automatisé de traitement des données peut faire partie de ses missions. Une faille présente, comme la possibilité d'accéder, par l'exploitation d'une vulnérabilité, à une base de données contenant des informations d'utilisateurs, sera alors flagrante même sans avoir connaissance de la loi.

Même s'il existe d'autres infractions comme le financement du terrorisme ou l'évasion fiscale que

48 Étude IFOP réalisée pour Kaspersky et Euler Hermes. « *Les PME face aux enjeux de sécurité informatique* », 2018. https: //www.allianz- trade.fr/content/dam/onemarketing/aztrade/allianz- trade_fr/news/131218/etude- IFOP- PME- enjeux- cybersecurite.pdf. [En ligne ; consulté le 28-Avril-2024].
49 Site internet France 3, Aline Métais « *Ce que l'on sait sur la cyberattaque qui perturbe l'activité à l'hôpital de Cannes* » 2024. https://france3- regions.francetvinfo.fr/provence- alpes- cote- d- azur/alpes- maritimes/cannes/une- cyberattaque- paralyse- l- hopital- de-cannes-2956256.html. [En ligne; consulté le 28 avril 2024].
50 Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

le pentester serait obligé de signaler, être témoin de ces infractions impliquerait que le pentester prenne connaissance du contenu des fichiers auxquels il pourrait avoir accès au cours de ses missions, là où des infractions au RGPD par exemple, nécessitent de n'avoir que des connaissances de la structure du système d'information.

Afin de bénéficier des protections qui leur sont accordées, les lanceurs d'alerte doivent impérativement utiliser une procédure de signalement régie par la loi de 2022[51]. Plusieurs types de procédures de signalement sont mis à la disposition des lanceurs d'alerte. Depuis la modification de la loi « Sapin 2 » en 2022, les lanceurs d'alerte bénéficient de choix quant à la procédure de signalement qui correspond le mieux à leur situation et à la nature des informations à divulguer. La procédure de signalement interne n'étant plus obligatoire. Elle demeure néanmoins une option valable, notamment si le problème peut être résolu rapidement en interne. Le signalement interne peut également être combiné à un signalement externe, qui peut toutefois être effectué de manière indépendante. Cette pluralité de choix vise à encourager les lanceurs d'alerte à signaler les manquements graves en toute confiance.

La procédure de signalement est non commutable. Le dispositif lanceur d'alerte ne prévoit pas de dispense de signalement d'un crime ou d'un délit porté à la connaissance d'un officier public ou d'un fonctionnaire[52]. L'obligation de signalement au procureur de la République doit se faire en priorité, avant même tout signalement, qu'il soit interne ou externe. À titre d'exemple, si un pentester embauché comme fonctionnaire au sein d'une institution comme un ministère était témoin d'un délit ou d'un crime pareil à ceux des atteintes aux systèmes de traitement automatisé de données, il devrait en informer en priorité le procureur puis sa hiérarchie. Il pourrait ensuite choisir d'effectuer une procédure de signalement interne ou externe afin d'obtenir le statut de lanceur d'alerte.

Au regard des signalements en interne, toute entreprise comptant plus de cinquante employés est tenue d'établir un système de collecte et de traitement des signalements, qu'elle doit clairement communiquer à ses employés. Ce dispositif doit se conformer aux exigences énoncées dans le décret n°2022-1284 du 3 octobre 2022. Elles comprennent, notamment, des obligations de conservation des informations et de l'anonymat des lanceurs d'alerte pendant le recueil et le traitement des signalements. La procédure ainsi que les obligations auxquelles l'entreprise doit s'astreindre doivent être clairement présentées et accessibles via un ou plusieurs canaux propres aux employés. Le lanceur d'alerte doit être informé de la réception de son signalement dans un délai de sept jours ouvrables, et des mesures prises pour y remédier dans un délai n'excédant pas trois mois[53]. La procédure doit être rendue publique par l'entreprise, notamment via des notifications, affichages ou publications, y compris sur son site Internet, pour une accessibilité permanente aux lanceurs d'alerte. Enfin, des informations claires sur les procédures de signalement externe doivent être mises à disposition. Si l'entreprise compte moins de cinquante employés, les signalements internes peuvent être adressés à un supérieur hiérarchique ou directement à l'employeur[54]. La majorité des entreprises spécialisées dans l'audit des systèmes d'information d'entreprises comptant moins de cinquante employés, les pentesters tendent à rester dans le cadre de leur contrat et gardent pour eux les délits potentiels commis par l'entreprise contractante dont ils seraient témoins. Cela est dû, d'après un professionnel interrogé[55], à une méconnaissance de leurs droits et des canaux de communication, résultant en un non-respect de la loi relative aux lanceurs d'alerte dans les petites entreprises.

Les signalements externes, quant à eux, s'effectuent auprès d'autorités compétentes. Différentes organisations, associations, institutions ou organes étatiques se partagent les signalements en fonction de leur pôle de compétence. Par exemple, les signalements effectués quant à la sécurité d'un système d'information doivent être communiqués auprès de l'ANSSI[56]. Des guides sont disponibles sur les sites de ces différentes entités afin d'aiguiller les lanceurs d'alerte. Les signalements externes doivent préciser si un signalement préalable a déjà été transmis, qu'il ait été interne ou non. En outre, les modalités de recueil et de traitement du signalement ainsi que la réponse qui y est apportée.

Le dernier mode de signalement à la disposition des lanceurs d'alertes est la divulgation publique. Ce mode de signalement, consistant à publier les informations dont il dispose par des moyens de communication tels que des médias ou un réseau social, est inusité

51 Site internet gouv.fr, « *Signalement par un lanceur d'alerte : adresser une alerte à l'ANSSI* », 2023. https://cyber.gouv.fr/signalement-par- un-lanceur-dalerte-adresser-une-alerte-lanssi. [En ligne; consulté le 28 avril 2024].
52 Article 40 du Code de procédure pénale.
53 Françoise Berton. « *La protection des lanceurs d'alerte.* », 2023, https://www.berton-associes.fr/blog/droit-europeen/ protection-lanceur-alerte/. [En ligne; consulté le 20 avril 2024] ; Yann-Maël Larher, « Recueil et traitement des signalements des lanceurs d'alerte : quelles sont les autorités compétentes? », Village Justice, 2024, https://www.village- justice.com/articles/recueil- traitement- des- signalements- des- lanceurs- alerte- quelles- sont- les,49518.html. [En ligne; consulté le 20 avril 2024].
54 ite internet, Direction de l'information légale et administrative, « *Lanceurs d'alerte en entreprise* », 2022. https://www.service-public.fr/ particuliers/vosdroits/F32031. [En ligne ; consulté le 20 avril 2024].
55 Entretien privé dans le cadre des travaux de recherche.
56 Site internet, gouv.fr. « *Signalement par un lanceur d'alerte : adresser une alerte à l'ANSSI* », 2023. https://cyber.gouv.fr/signalement-par- un-lanceur-dalerte-adresser-une-alerte-lanssi. [En ligne; consulté le 28 avril 2024].

par les lanceurs d'alertes, du fait des restrictions qui l'entourent. En effet, il ne peut être utilisé que dans trois cas définis à l'article 8-III de la loi du 21 mars 2022 : en cas d'absence de mesures dans un délai de 6 mois après le signalement, en cas de danger grave et imminent, et si le signalement entraîne des risques pour sa personne (en résumé). Enfin, il est important de préciser que les points deux et trois ne s'appliquent pas si la divulgation publique met à mal les intérêts de la défense ou la sécurité nationale.

Néanmoins, même si les lanceurs d'alerte préfèrent souvent éviter les canaux de divulgation traditionnels, l'anonymat et la liberté d'expression qu'offre Internet leur procurent de puissants outils pour alerter sur des agissements répréhensibles. En effet, les modes de gouvernance propres à Internet, décentralisés et moins contrôlables par les États, permettent aux lanceurs d'alerte numériques de diffuser des informations sensibles à une échelle mondiale et de contourner les restrictions imposées par les autorités locales. Cette situation est particulièrement propice aux pentesters et aux hackers éthiques qui, en publiant des rapports détaillés sur des vulnérabilités critiques, contribuent à améliorer la sécurité informatique de tous en obligeant les entreprises ne voulant pas remédier aux failles de sécurité dont elles ont été notifiées et en prévenant l'utilisation de vulnérabilités qui seraient présentes dans de nombreuses infrastructures. Cependant, il est important de souligner que la divulgation de failles de sécurité, si elle n'est pas accompagnée d'une coordination avec les acteurs concernés, peut s'avérer illégale et avoir des conséquences néfastes.

Une protection renforcée

Les lanceurs d'alerte qui signalent ou divulguent des informations sensibles bénéficient d'une protection renforcée contre plusieurs formes de représailles, à condition de respecter les conditions définies aux articles 6 et 8 de la loi de 2022.

• **Contre la divulgation d'informations personnelles** : L'anonymat du lanceur d'alerte est crucialement garanti tout au long des processus de recueil et de traitement des signalements, comme le soulignent explicitement les différents articles de la loi précédemment cités. Cette protection s'applique, quel que soit le canal de signalement choisi par le lanceur d'alerte, du moment que la procédure est valable. Cette mesure essentielle vise à prévenir toute forme de représailles et à préserver la vie personnelle, professionnelle et relationnelle du lanceur d'alerte.

• **Contre les représailles et leur garantissant une immunité civile et pénale :** L'article 10-1-I de la loi du 21 mars 2022 dispose que le lanceur d'alerte n'est pas civilement responsable des dommages causés par ses révélations s'il avait des raisons valables de croire que le signalement ou la divulgation publique était nécessaire pour protéger l'intérêt général. Pour ce qui est des responsabilités pénales des lanceurs d'alerte, l'article 122-9 du Code pénal explicite : « N'est pas pénalement responsable la personne qui porte atteinte à un secret protégé par la loi, dès lors que cette divulgation est nécessaire et proportionnée à la sauvegarde des intérêts en cause, qu'elle intervient dans le respect des conditions de signalement définies par la loi ». Une extension de cet article prévoit même la suppression des répercussions pénales pour la soustraction, le détournement ou le recel de documents obtenus licitement et qui sont par la suite divulguées dans les conditions mentionnées dans le précédent alinéa. Enfin, les mesures de représailles pouvant être émises par l'entreprise employant le lanceur d'alerte, comme des procédures-bâillons visant à faire se rétracter le lanceur d'alerte en lui faisant peur, comme en le menaçant d'un procès ou en l'attaquant en justice de manière excessive, sont prohibées. La protection apportée par cet article 10-1-I de la loi du 21 mars 2022 est telle qu'il est précisé que « Tout acte ou décision pris en méconnaissance du présent II est nul de plein droit. ». En cas de recours contre une mesure de représailles présumée, la charge de la preuve incombe à l'employeur ou à l'entité responsable. Ils doivent démontrer, preuves à l'appui, que la sanction est justifiée par des motifs ne relevant en aucun cas du signalement effectué. Par ailleurs, il est important de souligner qu'entraver la transmission d'un signalement par un lanceur d'alerte constitue une infraction pénale. Les pentesters, comme tout individu, encourent des risques de représailles. Cependant, ces risques peuvent être encore plus importants pour eux, ainsi que pour les hackers éthiques, comme démontré précédemment, car ils utilisent des méthodes non conventionnelles pour divulguer leurs informations.

• **Valable également pour les proches :** Le lanceur d'alerte n'est pas le seul à bénéficier d'une protection renforcée. En effet, les facilitateurs, qui peuvent être des proches, des collègues ou des associations à but non lucratif, qui l'aideraient dans ses démarches de signalement ou de divulgation, pourraient être sujets aux mêmes représailles que le lanceur d'alerte. Ces protections accordées aux proches des lanceurs d'alerte n'étaient pas à l'origine dans la loi Sapin 2, elles furent ajoutées lors de sa révision en 2022, toujours dans l'optique de favoriser les signalements et d'en augmenter le nombre. Cette protection renforcée est particulièrement importante pour les pentesters et les hackers éthiques. En effet, la découverte et le signalement de vulnérabilités, peu importe leur criticité, impliquent souvent une collaboration étroite entre plusieurs individus. Il est donc crucial que l'ensemble des personnes impliquées dans ce processus puissent bénéficier d'une protection juridique adéquate, afin de les inciter à agir sans crainte de représailles.

Cette protection semble, pour l'heure, insuffisante. Toute personne physique peut agir en tant que lanceur d'alerte du moment qu'elle respecte les conditions de l'article 6-I de la loi n° 2016-1691. Un pentester devra donc faire part à sa hiérarchie ou à l'ANSSI des infractions dont il a été témoin directement ou non dans le cadre de son travail. Aucune rémunération directe, ne doit être acceptée pour qu'il effectue le signalement, impliquant que ce dernier doit être effectué de son plein gré et de bonne foi, bien que ce point soit difficile à prouver. Le pentester pourrait signaler des infractions de certaines entreprises l'ayant embauché, pour des bénéfices ultérieurs provenant d'autres entreprises concurrentes, caractérisant un conflit d'intérêts quasiment indétectable si bien réalisé. Une distinction existe cependant, entre les pentesters, les bounty-hunters et les hackers éthiques, distingués par leur contrat ou l'absence de ce dernier. Celle-ci réside dans l'origine de la connaissance des faits signalés. Les lanceurs d'alerte qui n'étaient pas sous contrat avec l'entreprise sont dits externes à celle-ci et doivent avoir personnellement constaté les manquements qu'ils dénoncent, tandis que les lanceurs d'alerte sous contrats avec l'entreprise sont dits internes et peuvent en plus, signaler des faits qui leur ont été rapportés par des collègues. Cette notion est primordiale dans le domaine de la cyberdéfense, car elle différencie les experts en cybersécurité du fait des risques qu'ils prennent afin de divulguer l'infraction dont ils ont été témoins.

Selon l'article 8-I-A de la loi du 21 mars 2022, les faits rapportés doivent être : « des informations mentionnées au I de l'article 6 et portant sur des faits qui se sont produits ou sont très susceptibles de se produire dans l'entité concernée ». Cet article vise à garantir que les signalements effectués par les lanceurs d'alerte portent sur des faits réels et sérieux, justifiant une action et relevant du champ d'application de la loi. Ramené au cas des pentesters ou hackers éthiques, rapporter des vulnérabilités ou manquements dont la criticité ne serait que peu importante, comme des vulnérabilités dont l'exploitation nécessiterait qu'un attaquant réside sur le même réseau local que la victime ou ne fournisse qu'un accès très limité, n'accorderait pas à l'émetteur du signalement le statut de lanceur d'alerte. Et ce, même si l'exploitation de cette vulnérabilité, bien que peu probable, caractériserait un délit commis par l'entreprise. En principe, un pentester n'a pas intérêt à signaler publiquement ou à l'ANSSI une vulnérabilité détectée dans le cadre de sa mission. Un signalement à sa hiérarchie puis à l'entreprise concernée est généralement suffisant. Toutefois, si le pentester intervient régulièrement pour l'entreprise et constate qu'une vulnérabilité présentant un caractère délictuel n'est pas corrigée malgré les signalements, il peut envisager de saisir l'ANSSI.

Les lanceurs d'alerte numérique, oubliés des réformes

En 2023 furent déposés plusieurs amendements, notamment portés par Mme Nathalie Delattre, Sénatrice de la Gironde[57]. Ces derniers avaient pour but de modifier l'article L.2321-4 du Code de la défense afin d'améliorer la protection d'une partie des lanceurs d'alerte nommés lanceurs d'alerte numériques. Il n'y a aucune différence de forme entre les lanceurs d'alerte et les lanceurs d'alerte numériques. Cette appellation désigne simplement tous les lanceurs d'alerte pour lesquels l'infraction divulguée repose sur une, ou plusieurs failles de cybersécurité. Les lanceurs d'alerte numérique font face à de nombreuses difficultés qui mettent en péril le signalement de failles importantes de sécurité qui pourraient avoir un impact sur l'intérêt général, comme d'importantes failles dans la sécurisation de bases de données contenant des informations bancaires et/ou personnelles pouvant mener, par exemple, à des usurpations d'identité ou des vols.

La loi offre une protection quasi totale aux lanceurs d'alerte, à condition qu'ils respectent tous les conditions établies, ce qui peut déjà s'avérer difficile en théorie et qui l'est d'autant plus en pratique, le lanceur d'alerte devant prouver qu'il respecte ces conditions. Cependant, malgré l'existence de ce cadre juridique protecteur, plusieurs obstacles demeurent. D'une part, la méconnaissance de la loi par les professionnels de la cybersécurité limite son application effective, et ce, même si l'entreprise a obligation d'informer ses employées de leurs droits. D'autre part, même lorsqu'ils en ont connaissance, les lanceurs d'alerte hésitent à l'utiliser par crainte de représailles ou de nuire à leur réputation ou à celle de leur entreprise. Ces obstacles sont particulièrement prégnants dans le secteur de la cybersécurité. S'il signale une telle faille, le lanceur d'alerte risque de voir son identité révélée, ce qui pourrait nuire à sa réputation ou celle de son entreprise dont il dépend et diminuer ses chances de réembauche dans une autre entreprise du secteur. Les entreprises clientes pourraient craindre que leurs propres manquements ne soient signalés aux autorités, ce qui les dissuaderait de faire appel aux services de l'entreprise de cybersécurité en question, ce qui aurait également un effet néfaste sur la situation du lanceur d'alerte.

Les vulnérabilités critiques peuvent avoir des

57 Proposition de loi, Protection des lanceurs d'alerte, (1ère lecture), Amendement n°22 rect. 19 janvier 2022 Texte de la commission N° 300 (2021-2022) sur la proposition de loi, adoptée par l'Assemblée nationale, après engagement de la procédure accélérée, visant à améliorer la protection des lanceurs d'alerte visant à améliorer la protection des lanceurs d'alerte.

répercussions sur l'ensemble du système, par l'obtention de privilège administrateur par exemple. Ce n'est pas tant la précision des informations découvertes par les experts en cybersécurité, comme des fichiers contenant des données personnelles de clients ou des données internes à l'entreprise que celle-ci ne voudrait pas voir fuiter, mais l'assurance que, si une information sensible existe, alors elle sera obtenue en utilisant cette vulnérabilité qui devrait permettre aux lanceurs d'alerte d'obtenir ce statut.
Conséquemment, l'obtention d'informations sensibles pouvant faire l'objet d'un signalement pose un défi particulier dans le cadre des activités de pentest et d'audit. En effet, les contrats encadrant ces prestations définissent souvent précisément les cibles autorisées aux tests. Cette distinction permet de différencier les informations obtenues dans le respect du contrat de celles acquises en dehors de son périmètre.

Les informations collectées conformément aux termes du contrat peuvent être signalées sans entrave à la fois à l'entreprise cliente et à l'ANSSI, conformément à l'amendement proposé. Dans ce cas, le lanceur d'alerte bénéficie d'une protection étendue pour les actions entreprises en vue de prouver la véracité de ces informations, y compris celles pouvant constituer des infractions pénales. En revanche, les informations acquises en dehors du cadre contractuel ne peuvent être signalées par le lanceur d'alerte sans s'exposer à des sanctions pénales.

La protection offerte par l'article 122-9 du Code pénal, évoquée précédemment, est à nuancer. Elle ne couvre que les infractions commises strictement dans le but d'obtenir des preuves pour des informations obtenues licitement. Ainsi, un pentester découvrant une infraction après avoir outrepassé les limites de son contrat pourrait être tenu pénalement responsable de son intrusion et de son maintien dans le système compromis. Il lui est, néanmoins, toujours possible de signaler le délit en interne à sa hiérarchie ou en externe à l'autorité compétente, mais en assumant les conséquences probables. Ces mêmes restrictions s'appliquent également aux contrats dans le cadre du bug-bounty.

Les préoccupations liées à l'obtention d'informations sensibles s'étendent également aux hackers éthiques, dont le nombre augmente chaque année[58], qu'ils soient experts ou non, qui effectuent des recherches de vulnérabilité sur leur temps libre en dehors de tout cadre contractuel. Il est important de souligner que ces pratiques, bien qu'animées par de nobles intentions, sont illégales et sévèrement sanctionnées, en France, par les articles 323-1 à 323-3 du Code pénal. En effet, l'intrusion non autorisée dans un système d'information, qu'il soit d'entreprise ou d'institution étatique, par exemple, expose son auteur à des amendes pouvant atteindre plusieurs centaines de milliers d'euros ainsi qu'à des peines de prison. Ces sanctions s'aggravent en cas de maintien dans le système compromis ou de vol de documents internes. Malgré ce cadre juridique contraignant, ces personnes, si tentées qu'elles puissent prouver leur bonne foi, pourraient jouer un rôle crucial dans le renforcement de la cybersécurité. Leur expertise et leur capacité à identifier des failles de sécurité permettent de prévenir de nombreuses attaques qui pourraient mettre en péril l'intérêt général.

La divulgation de failles de sécurité, même effectuée de bonne foi, comporte un risque d'exploitation par des acteurs malveillants.

La publication d'informations détaillées sur des vulnérabilités spécifiques peut alerter des cybercriminels opportunistes qui pourraient mener des attaques ciblées sur les systèmes affectés.
Ce risque est particulièrement élevé lorsque les failles concernent des opérateurs d'importance vitale (Loi de Programmation Militaire (« LPM ») de 2013), une administration, une entreprise publique ou privée dont l'État a jugé le fonctionnement indispensable à la vie de la nation) tels que des systèmes de défense ou des réseaux électriques. En effet, l'exploitation de telles failles pourrait avoir des conséquences graves sur la sécurité nationale, le bon fonctionnement de la société, ou encore l'image et la crédibilité des organisations concernées.

Face à ce dilemme, il est crucial de trouver un équilibre entre transparence et protection des intérêts légitimes. La divulgation des failles de sécurité est essentielle pour sensibiliser les acteurs concernés et leur permettre de prendre les mesures correctives nécessaires. Cependant, cette divulgation doit être effectuée de manière responsable, en tenant compte des risques d'exploitation et en protégeant les informations sensibles.

La non-reconnaissance des signalements de failles de sécurité par les autorités compétentes ou la hiérarchie, en raison du caractère illicite de l'obtention des informations, peut avoir des conséquences dramatiques pour les lanceurs d'alerte et leurs facilitateurs. En effet, dans ce cas, non seulement le lanceur d'alerte perd son statut protecteur et s'expose à des représailles de la part de l'entité concernée, mais ses facilitateurs, qui bénéficient normalement d'une partie des protections accordées aux lanceurs d'alerte,

58 Maryse Gros, « *+63% de hackers éthiques en 2020, selon HackerOne* », 11 mars 2021, site internet Le monde informatique. https://www.lemondeinformatique.fr/actualites/lire-63-de-hackers-ethiques-en-2020-selon-hackerone-82251.html. [En ligne; consulté le 20 avril 2024].

perdent également ces protections et peuvent être sujets à des représailles, voire à des sanctions pénales pour complicité ou association de malfaiteurs (Articles 323-4 à 323-8 du Code pénal).

Pour un pentester ou un hacker éthique, qui disposent déjà de moyens plus sûrs de divulguer la vulnérabilité, sans passer par les canaux officiels, qui les forceraient à s'impliquer bien davantage qu'un simple poste anonyme sur les réseaux sociaux. Les autorités compétentes ou l'entreprise victime de la vulnérabilité pourraient obtenir des informations à la suite d'un dépôt de plainte ou d'un procès, puisque le divulgateur ne serait plus protégé par le statut de lanceur d'alerte, ce qui mettrait en péril leur vie personnelle et professionnelle.

L'article L2321-4 du Code de la défense : un article salvateur, mais incomplet

Le Code de la défense, texte qui régit la défense nationale, précise dans son article L2321-4 :
« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du Code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.
L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.
L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

Cet article, bien que peu utilisé en pratique, est la porte d'entrée vers une amélioration des protections visant les lanceurs d'alerte numérique. L'article L2321-4 du Code de la défense dispense déjà aux lanceurs d'alerte numérique, qui sont fonctionnaires, officiers publics ou représentants d'une autorité constituée, dans l'exercice de leur fonction, de rapporter les délits ou crimes dont ils seraient témoins au procureur de la République, si et seulement si ce signalement est une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données[59]. La dispense de signalement à l'autorité judiciaire prévue par l'article 40 du Code de procédure pénale n'impose pas, contrairement à la loi sur les lanceurs d'alerte, la conservation de l'anonymat du lanceur d'alerte.

De plus, cet article place la vulnérabilité au centre du signalement et non plus les infractions commises, ou potentielles, en lien avec cette vulnérabilité. Cette méthodologie est beaucoup plus cohérente avec le domaine de la cybersécurité et le fonctionnement des systèmes d'information. Cela élimine nombre des obstacles vus précédemment imposés par la loi sur les lanceurs d'alertes.

Cependant, cet article possède certaines limites. L'article L2321-4 ne couvre pas l'ensemble des aspects essentiels à la protection des lanceurs d'alerte numériques. En particulier, il omet de prendre en compte les délits liés au fonctionnement des systèmes d'information, tels qu'entraver le bon fonctionnement d'un système d'information ou encore introduire des données nuisibles dans un système d'information amené par les articles 323-2 à 323-8 précédemment discutés. Seul l'article 323-1 relatif à l'intrusion et au maintien dans un système de traitement automatisé des données semble être couvert.

En l'état, l'article L2321-4 du Code de la défense semble protéger le lanceur d'alerte, bien qu'on ne puisse pas considérer cela comme une protection convenable, tant elle l'oblige à prendre des risques sans être certain d'être protégé par la suite par l'ANSSI. Cette protection n'est que minime et intervient à un stade parallèle de la procédure pénale. Il est toujours possible de poursuivre le lanceur d'alerte pour intrusion dans un STAD (articles 323-1 du Code pénal). Dans ce type de situation, il est facilement envisageable d'imaginer qu'un lanceur d'alerte ait été détecté par les moyens de sécurité d'une entreprise (exemple : EDR, SOC, SIEM, etc.)[60]. Mais en informant l'ANSSI, le lanceur d'alerte pourra bénéficier de l'intervention de cette dernière en cas de signalement au procureur, qui abandonnera les poursuites s'il est avéré que le lanceur d'alerte n'a pas enfreint les autres articles du Code pénal.

De l'autre côté du spectre, la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 porte diverses dispositions intéressant la défense. Elle ajoute, entre autres, l'article L2321-4-1 au Code de la défense précisant la marche à suivre, pour les éditeurs de logiciel seulement, si une vulnérabilité venait à apparaître. Aucune mention n'est faite dans l'article de la provenance potentielle de l'information sur la vulnérabilité. Si la loi ne mentionne pas explicitement les pentesters, elle établit tout de même un cadre pertinent pour leur activité. En effet, en imposant aux éditeurs de logiciels de mettre en place une procédure de gestion des vulnérabilités, la loi encourage indirectement le recours aux pentesters.

59 Eric A. Caprioli, « *Les lanceurs d'alertes dans la Loi pour une République numérique* » Site usine digitale, 2016. https://www.usine-digitale.fr/ article/les-lanceurs-d-alertes-dans-la-loi-pour-une-republique-numerique.N469128. [En ligne ; consulté le 26 avril 2024].
60 *Ibid.*

Cet ajout permet à l'ANSSI de s'assurer que les vulnérabilités découvertes, susceptibles d'affecter significativement un de leurs produits, font bien l'objet d'une enquête en interne et que des solutions sont mises en place. Cet article permettra également à l'ANSSI de déterminer plus facilement la bonne foi des hackers éthiques ayant révélé indirectement (par des traces laissées lors de leur passage, par exemple) la vulnérabilité à l'entreprise et ayant effectué un signalement, dans le même temps, à l'ANSSI seule. Cet article donne plus de pouvoir à l'ANSSI, mais ne renforce que de peu la protection des lanceurs d'alerte numériques.

Des améliorations envisageables

Parmi les propositions faites, mais non retenues, la sénatrice Mme Nathalie Delattre, propose notamment de modifier l'article L2321-4 du Code de la défense afin de préciser et élargir l'éventail d'action des lanceurs d'alerte numérique[61]. Ces derniers devront effectuer leur signalement simultanément à l'ANSSI et au responsable du système de traitement automatisé de données en cause[62]. Le durcissement de ce point, bien qu'il puisse sembler contraignant pour les lanceurs d'alerte, permettrait de simplifier la preuve de bonne foi. Elle propose également d'ajouter des exceptions à l'article 323-1 du Code pénal rédigé comme suit :
« Toute personne de bonne foi qui a tenté de commettre ou commis ce délit est exemptée de poursuites si : 1° Elle a respecté les règles de fonctionnement et de conduite des lanceurs d'alerte numérique ; 2° Elle a transmis à l'Agence nationale de sécurité des systèmes d'information et au responsable du système de traitement automatisé de données en cause une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données ; 3° Elle n'a pas agi au-delà de ce qui est nécessaire et proportionné afin de vérifier l'existence de ladite vulnérabilité».

Bien que cet ajout permettrait de formaliser les dispositions implicites de l'article du Code de la défense, leur limitation au seul article 323-1 du Code pénal ne les rend pas aptes à résoudre le problème soulevé précédemment concernant la négligence des délits définis dans les articles du Code pénal relatifs aux STAD, pourtant fréquemment commis lors d'intrusions et de maintien dans des systèmes d'information.

La difficulté de cette proposition d'article vise l'encadrement de la conduite du lanceur d'alerte et la proportionnalité de son action. Ces deux paramètres ne font pas l'unanimité dans la communauté cyber, et restent difficilement compréhensibles. La notion d'action proportionnée est également centrale aux améliorations à apporter à l'article L2321-4 du Code de la défense. En effet, cette mesure simplifierait également la preuve de bonne foi. Des discussions plus poussées doivent être envisagées sur le sujet.
Une piste d'amélioration de ces propositions serait d'élargir les modifications apportées, aux articles 323-2 et 323-3 seuls.

L'instauration d'une obligation de documentation précise pour les lanceurs d'alerte numériques, contenant des logs détaillés des actions réalisées avant le signalement de la vulnérabilité découverte, constituerait un progrès majeur pour renforcer la transparence et la bonne foi de leurs signalements. Si la mesure proposée semble s'inscrire dans le prolongement des preuves déjà requises pour démontrer l'existence d'une vulnérabilité, il est important d'aller au-delà de la simple preuve de la faille. L'exigence de documenter les actions menées au sein du système d'information permettrait d'éclairer l'intention derrière les actions des lanceurs d'alerte, en particulier des hackers éthiques. L'obligation de documentation précise pour les lanceurs d'alerte numériques permettrait d'harmoniser les pratiques existantes et de renforcer la protection de ces acteurs essentiels à la cybersécurité. Cette mesure contribuerait à instaurer un climat de confiance entre les lanceurs d'alerte, les entreprises et les autorités, favorisant ainsi la découverte et la correction des failles de sécurité de manière responsable et efficace.

Le statut de lanceur d'alerte offre donc, en théorie, un cadre juridique protecteur aux pentesters, bounty hunters et hackers éthiques qui souhaitent signaler des infractions, soit dans le but de signaler une vulnérabilité présente sur de nombreuses machines, et donc avec un fort impact pour l'intérêt général, soit dans le but d'obliger une entreprise à corriger une vulnérabilité dont elle aurait été mise au courant auparavant. Les manquements au RGPD, par exemple, découverts par ces experts dans l'exercice de leurs missions, ou non, constituent des exemples parfaits d'informations relevant du champ d'application de ce statut.

Cependant, les obstacles vus précédemment freinent l'utilisation de ce statut par les experts en cybersécurité, à savoir la méconnaissance des droits et des procédures de signalement, couplée à la communication insuffisante des entreprises sur ces sujets et les restrictions implicites au signalement de vulnérabilités liées à la solution partielle présentée par

61 Proposition de loi, Protection des lanceurs d'alerte, (1ère lecture), Amendement n°22 rect. 19 janvier 2022 Texte de la commission N° 300 (2021-2022) sur la proposition de loi, adoptée par l'Assemblée nationale, après engagement de la procédure accélérée, visant à améliorer la protection des lanceurs d'alerte visant à améliorer la protection des lanceurs d'alerte.
62 Eric A. Caprioli, « Les lanceurs d'alertes dans la Loi pour une République numérique » Site usine digitale, 2016. https://www.usine-digitale.fr/ article/les-lanceurs-d-alertes-dans-la-loi-pour-une-republique-numerique.N469128. [En ligne ; consulté le 26 avril 2024]..

l'article L2321-4 du Code de la défense.

Si le statut d'hacker éthique et celui de lanceur d'alerte partagent des objectifs communs de lutte contre les cybermenaces et de protection de la sécurité informatique, leur compatibilité juridique reste discutable. En l'état actuel du droit, les risques encourus par les hackers éthiques lors de leurs signalements sont disproportionnés par rapport aux bénéfices potentiels. De plus, la distinction entre les hackers éthiques et les hackers malveillants («black hats») n'est pas toujours claire dans le regard de la loi. Ce flou juridique expose les hackers éthiques à des risques de poursuites pénales, même lorsqu'ils agissent de bonne foi et signalent une vulnérabilité à l'ANSSI.

Sans d'importantes modifications de la loi ou sans une clarification du statut de hacker éthique, il est peu probable que ces experts puissent s'intégrer pleinement dans le paysage de la cybersécurité. De plus, même avec les modifications proposées, ce statut ne représente pas et ne doit pas représenter une échappatoire aux problématiques présentées précédemment.

Titouan
LE BLÉ


03

LE CADRE JURIDIQUE DU HACKING ÉTHIQUE À L'ÉTRANGER

- Étude comparée du droit des hackers « éthiques »
- Hacking éthique aux États-Unis : entre risque judiciaire permanent et émergence d'un statut protecteur

ÉTUDE COMPARÉE DU DROIT DES HACKERS « ÉTHIQUES » : ALLEMAGNE, BELGIQUE ET FRANCE

Elyes HAKMOUNI, Groupe de recherche de Master 1 Cybersécurité, ISTIC/Cyberschool

L'Allemagne, la Belgique et la France ont été sélectionnées pour leur approche proactive et leur cadre législatif élaboré concernant la cybersécurité. De plus, en tant que membres influents de l'Union européenne, leurs législations ont un impact significatif sur les politiques de sécurité informatique et de protection des données au sein de l'Union européenne.

Allemagne

S'agissant de l'Allemagne, le cadre juridique qui régit le hacking éthique souligne la nécessité d'obtenir un consentement explicite préalable de la part du propriétaire du système informatique testé. Le Code pénal allemand (Strafgesetzbuch - StGB) contient plusieurs dispositions pertinentes :

- Article 202a StGB aborde spécifiquement l'acquisition illégale de données, précisant que les actions sont sanctionnées si elles impliquent un accès aux données sans autorisation, notamment si cet accès implique de contourner les mesures de sécurité mises en place pour protéger les données.
- Article 202c StGB concerne la préparation d'activités d'espionnage ou d'interception de données, ce qui pourrait inclure certains outils ou méthodes utilisés dans le hacking sans autorisation appropriée.
- Article 303b StGB couvre le sabotage informatique, qui comprend tout dommage aux données ou toute interférence avec les systèmes informatiques qui entraînent des perturbations des opérations ou de l'intégrité des données.

De plus, le hacking éthique, même avec de bonnes intentions, reste une zone juridique grise. La loi ne fait pas de distinction explicite entre le piratage malveillant et le hacking éthique si cela implique des actions non autorisées. Par conséquent, tout test de pénétration ou évaluation de sécurité doit être explicitement autorisé par le propriétaire du système pour éviter d'éventuels problèmes juridiques. Cela reflète une forte emphase sur le respect de la vie privée et de l'intégrité des données et des systèmes.

En outre, dans le contexte de tests de pénétration légaux, le respect des réglementations sur la protection des données reste primordial. Cela est conforme aux directives établies par l'Office fédéral allemand de la sécurité de l'information (BSI), qui souligne l'importance cruciale de maintenir des pratiques robustes de protection des données lors de telles activités[63].

Belgique

S'agissant de la Belgique, la réglementation encadrant le hacking éthique est clairement définie pour maintenir un équilibre entre la sécurité informatique et la légalité des tests de pénétration.

63 Guidelines by the Federal Office for Information Security (BSI). https://iclg.com/practice-areas/cybersecurity-laws- and-regulations/germany. ICLG.

La loi du 28 novembre 2000 relative à la criminalité informatique joue un rôle central dans ce cadre légal. Cette loi a établi les règles concernant l'accès non autorisé et d'autres infractions informatiques. Elle dispose que tout hacker éthique doit obtenir un consentement explicite et documenté avant de réaliser des tests de pénétration sur des systèmes informatiques. Cette exigence vise à protéger à la fois les entités testées et les professionnels de la sécurité en s'assurant que toutes les parties comprennent et approuvent la portée et les objectifs des tests[64].

En outre, la politique de divulgation coordonnée du Centre pour la Cybersécurité Belgique (CCB) a été publiée pour renforcer la collaboration entre les découvreurs de vulnérabilités et les entités affectées. Cette politique encadre le processus de divulgation pour s'assurer qu'il est effectué de manière éthique et constructive. Elle encourage une approche où la sécurité est améliorée grâce à une coopération proactive, en évitant des divulgations qui pourraient autrement causer des dommages ou être exploitées de manière malveillante[65].

Ces dispositions illustrent l'engagement de la Belgique à vouloir créer un environnement sûr et réglementé pour les activités de hacking éthique, tout en soutenant une culture de la sécurité par la transparence et la collaboration. Ces mesures sont essentielles pour maintenir la confiance entre les secteurs public et privé et pour garantir que les pratiques de sécurité informatique contribuent positivement à la protection des infrastructures critiques.

France

Enfin, s'agissant de la France, la législation encadrant le hacking éthique est centrée sur la prévention des accès non autorisés à des systèmes informatiques et la protection des données, tout en proposant un cadre pour les activités de sécurité informatique légales.

Pour rappel, les articles du Code pénal 323-1 et suivants disposent que l'accès ou le maintien frauduleux dans un système de traitement automatisé de données est puni par la loi. Cette disposition vise à décourager les accès non autorisés aux systèmes informatiques en imposant des sanctions strictes. Bien que cette loi ne cible pas spécifiquement les hackers éthiques qui agissent avec un consentement valide, ceux-ci doivent être extrêmement prudents. Toute action sans consentement explicite du propriétaire du système pourrait être considérée comme illégale, exposant ainsi le hacker à des poursuites pénales. En outre, la loi du 7 octobre 2016 renforce la sécurité informatique en obligeant les hackers éthiques à signaler les vulnérabilités découvertes à l'Autorité Nationale de Sécurité des Systèmes d'Information (ANSSI) sans les divulguer publiquement. Cette mesure vise à protéger les systèmes informatiques en garantissant que les failles de sécurité soient traitées de manière responsable. Cependant, malgré ce cadre de signalement, les hackers éthiques ne sont pas entièrement à l'abri de poursuites judiciaires. Si l'entreprise concernée choisit de poursuivre en justice pour intrusion non autorisée, le hacker éthique peut encore faire face à des répercussions légales. Ces mesures illustrent l'approche équilibrée de la France, cherchant à promouvoir la cybersécurité tout en protégeant les droits et les responsabilités des parties impliquées dans les activités de hacking éthique.

Elyes
HAKMOUNI

64 La loi du 28 novembre 2000 relative à la criminalité informatique. https://etaamb.openjustice.be/ fr/loi-du-28-novembre-2000_n2001009035.html. Moniteur Belge. 2000
65 Politique de divulgation coordonnée du CCB. https://ccb.belgium.be/fr/politique-de-divulgation-coordonnee.

HACKING ÉTHIQUE AUX ÉTATS-UNIS : ENTRE RISQUE JUDICIAIRE PERMANENT ET ÉMERGENCE D'UN STATUT PROTECTEUR

Kamel EL HILALI, Docteur en Droit, Chercheur Associé, Information Society Project, Yale Law School

Contrairement aux apparences, les Etats-Unis ne sont pas un eldorado pour les hackers éthiques (white hats).

Le droit fédéral et la mosaïque de lois adoptées par les Etats fédérés ont longtemps assimilé la recherche en cybersécurité conduite de bonne foi et à des fins d'intérêt général (recherche universitaire ou publique, amélioration des systèmes d'information) au piratage motivé par le profit, le vol, ou la destruction de données. Les hackers éthiques étaient donc placés en fait et en droit dans une forme de marginalité avec des conséquences parfois tragiques. En 2011, le Department of Justice (DOJ) poursuit Aaron Swartz, un chercheur en cybersécurité spécialisé dans la neutralité du net, pour avoir téléchargé depuis le MIT des millions d'articles universitaires stockées sur la base de données JSTOR en violation du *Computer Fraud and Abuse Act* (1986, codif. 18 U.S.C. § 1030), une loi fédérale sanctionnant le piratage. En 2013, un mois avant le début de son procès, Swartz se suicide après l'échec des négociations avec les procureurs en vue d'éviter à l'accusé un procès et une peine d'emprisonnement de 35 ans. Cette affaire illustre les rapports complexes qu'entretiennent les États-Unis avec leurs chercheurs en cybersécurité. Ces derniers peuvent contribuer à renforcer la sécurité des systèmes d'information, l'activité des entreprises, et la vie privée des individus mais la nature duale de leurs activités les place en permanence aux confins de la légalité et dans une situation d'incertitude juridique permanente.

Le droit positif est relativement hostile aux hackers éthiques qui encourent des poursuites au civil et/ou au pénal en vertu de plusieurs lois fédérales et des Etats fédérés. Premièrement, au plan civil, les hackers éthiques peuvent recevoir des mises en demeure provenant des entreprises ciblées leur intimant l'ordre de cesser et de se désister (cease and desist) de leurs activités. La valeur de ces courriers est contestable et ne préjuge pas d'éventuelles poursuites judiciaires mais elle provoque un effet dissuasif certain. De même, les hackers éthiques peuvent être poursuivis au civil motif d'une méconnaissance du droit des contrats. En effet, les conditions d'utilisation (terms of service, terms of use, end user license agreement) des logiciels ou des terminaux (ordinateurs, téléphones) ou les accords de confidentialité (non-disclosure agreement) délimitent le champ des utilisations acceptées par le fabricant ou le fournisseur de service numérique. A cet égard, la multiplication des bug bounties ou des vulnerability disclosure programs organisés par les grandes entreprises ne sont pas sans risque pour les hackers pourtant invités à y participer.

En l'absence d'engagement préalable de l'entreprise de ne pas poursuivre les hackers (un programme qualifié de safe harbor), ces derniers risquent un procès au civil afin d'obtenir des dommages-intérêts dès lors que leurs techniques ne seraient pas approuvées par l'entreprise. Deuxièmement, le hacking même éthique est passible de sanctions civiles et pénales en cas de violation de l'*Electronic Communications Privacy Act* (ECPA, 1986, codif. 18 U.S.C. §§2510–2523), du secret des affaires, et du contrôle des exportations. L'ECPA interdit l'interception des communications électroniques en transit (cela concerne le network packet inspection, les données wifi et les métadonnées) sur le réseau sans le consentement d'une partie.

Le droit de la propriété intellectuelle (Copyright law) constitue l'une des sources les plus importantes du risque judiciaire pour les hackers éthiques. En effet, l'absence d'autorisation explicite du propriétaire des droits d'auteur expose le hacker aux poursuites. Ainsi, la copie, la création de dérivés, la distribution, et dans certains cas la simple consultation de logiciels peuvent constituer une violation du copyright, même en cas d'achat dudit programme. La sanction relève du droit pénal lorsque l'infraction est intentionnelle et poursuit un but financier. Elle est civile quelque soit le but poursuivi. Toutefois, le droit américain consacre un moyen de défense important, la *fair use doctrine* (17 U.S.C. §107). Ce moyen peut profiter aux hackers éthiques, y compris aux chercheurs en cybersécurité. Les juges doivent déterminer au terme d'une analyse *in concreto*, au cas par cas, si l'utilisation faite bénéficie à l'intérêt général (public good) à partir de cinq facteurs : la nature du travail protégé, le but poursuivi, le type d'utilisation, la proportionnalité, et les conséquences sur le marché. Ainsi, par exemple, un universitaire spécialisé en cybersécurité ou un white hat qui effectue des tests à des fins non lucratives, en transformant l'œuvre originale sans en faire un produit ou service concurrent sur le marché, et qui publie uniquement les parties de code strictement nécessaires à sa démonstration pourrait invoquer utilement la *fair use doctrine* devant les tribunaux et échapper aux sanctions.

Le droit de la propriété intellectuelle (Copyright law) constitue l'une des sources les plus importantes du risque judiciaire pour les hackers éthiques.

Le second texte du droit de la propriété intellectuelle qui porte atteinte à la recherche en cybersécurité est la section 1201 du *Digital Millenium Copyright Act* (DMCA, 1998, codif. 17 U.S. Code §1201) qui punit le contournement des mesures techniques protégeant l'accès aux œuvres protégées sans l'autorisation de l'auteur, quand bien même l'accès à l'œuvre elle-même est juridiquement autorisée. Ce contournement peut prendre la forme, par exemple, d'un déchiffrement ou de la désactivation de certains paramètres comme les CAPTCHAs. La sanction sera pénale en cas d'atteinte volontaire commise dans le but d'obtenir un gain financier ou un avantage commercial. Ce régime juridique est plus strict car le *fair use* ne peut faire échec à la responsabilité des auteurs de l'infraction. Toutefois, la §1201 prévoit deux types d'exception à son application. D'une part, les exceptions permanentes dont celle relative à la recherche sur le chiffrement (§1201(g)) ou aux tests de sécurité (§1201(j)(4)) afin d'identifier et de corriger les vulnérabilités des systèmes. Cependant, ces tests doivent être effectués avec l'autorisation du propriétaire du terminal, du réseau ou du service concerné. Cette disposition a permis au secteur privé de proposer une offre de tests d'intrusion (pen test) aux fournisseurs de services numériques. D'autre part, des exceptions temporaires, mais plus larges que les permanentes, ont été consacrées en 2018 en faveur de la recherche en cybersécurité. Ainsi, le contournement de mesures techniques de sécurité effectuée de bonne foi et avec l'autorisation de leur propriétaire sur des appareils acquis légalement permet d'échapper à la mise en jeu de la responsabilité civile et pénale. La condition de bonne foi s'analyse au regard du contexte de l'opération menée. Celle-ci doit en effet être conduite dans un environnement de nature à éviter tout dommage causé aux individus. Les informations obtenues à partir de cette opération doivent servir à améliorer la sécurité des appareils ou des programmes testés ou des personnes. Par ailleurs, les informations obtenues ne doivent pas aboutir à des violations du droit d'auteur.

Enfin, le risque de poursuites le plus important a trait au *Computer Fraud and Abuse Act* (18 U.S. Code § 1030). Cette loi fédérale relative au piratage informatique sanctionne quiconque « accède intentionnellement à un ordinateur sans autorisation ou outrepasse l'accès qui lui est autorisé, et obtient ainsi (…) des informations » depuis tout ordinateur (ou appareil connecté, comme un téléphone). Les pratiques illégales recouvrent, notamment et outre l'accès non autorisé, le phishing, l'attaque par déni de service, l'infection par malware, le vol de données, le pen test non sollicité, la possession de matériel permettant de commettre des actes relevant de la cybercriminalité, et toute activité qui menace la sécurité, la confidentialité ou l'intégrité des systèmes d'information. Cette loi a une portée extraterritoriale depuis l'adoption de l'*USA Patriot Act* (2001). Les sanctions encourues sont de nature civiles et pénales et peuvent atteindre 10 à 20 ans de prison.

L'interprétation extensive de cette loi a provoqué la mobilisation des universitaires et d'associations spécialisées comme l'Electronic Frontier Foundation (EFF). En effet, le Congrès n'a pas défini les termes de la loi, de sorte que le fait d'« outrepasser l'accès autorisé » a fait l'objet d'une interprétation large conduisant à criminaliser des actions aussi banales que les achats en ligne ou le visionnage de compétitions sportives depuis un ordinateur professionnel. Les tribunaux se sont divisés sur la portée de cette disposition et ont tantôt retenu que la création de faux profils sur les réseaux sociaux comme l'accès non autorisé aux bases de données du gouvernement fédéral constituait un crime en vertu du CFAA, tantôt que la simple violation d'une obligation contractuelle ne suffisait pas à caractériser un crime au sens de la loi. La Cour suprême dans une décision *Van Buren v. U.S.* (140 S.

Ct. 2667 (2020)), a mis un terme à cette divergence jurisprudentielle en retenant la seconde option. La Cour adopte une interprétation étroite de la §1030(a)(2) pour décider qu'un individu « outrepasse l'accès autorisé » lorsqu'il accède légalement à un ordinateur mais qu'il obtient des informations qui sont hors de sa portée. Ce faisant, les juges ont écarté la lecture extensive du gouvernement fédéral qui aurait conduit à sanctionner pénalement des activités banales et à admettre que la responsabilité pénale puisse être établie sur la base d'une évaluation arbitraire des faits.

En mai 2022, et de façon remarquée, le Department of Justice a annoncé une nouvelle politique d'interprétation et d'application du CFAA (Justice Manual (J.M.) §9-48.000 (Revised CFAA Guidelines)) dans un sens plus favorable aux hackers éthiques. En effet, le DOJ a annoncé qu'il ne poursuivrait plus les personnes qui effectuent des « « recherche[s] de bonne foi en matière de sécurité » [expression qui désigne] l'accès à un ordinateur uniquement à des fins de test, d'enquête et/ou de correction de bonne foi d'une faille ou d'une vulnérabilité de sécurité, lorsque cette activité est menée de manière à éviter tout préjudice aux particuliers ou au public et que les informations tirées de cette activité sont utilisées principalement pour promouvoir la sécurité ou la sûreté de la catégorie d'appareils, de machines ou de services en ligne à laquelle appartient l'ordinateur accédé, ou de ceux qui utilisent ces appareils, ces machines ou ces services en ligne ». Depuis cette annonce, les white hats ne sont plus poursuivis dès lors que leurs activités respectent ce cadre.

Cette évolution est positive dans la mesure où le gouvernement fédéral reconnaît l'apport des chercheurs à la cybersécurité et la protection des données. Toutefois, cette décision demeure fragile pour plusieurs raisons. D'abord, elle ne change pas le texte du CFAA et ne lie pas les juges. Ensuite, elle peut être modifiée par une administration moins favorable aux hackers éthiques. Enfin, elle ne suspend pas le risque de poursuite sur les autres fondements, en particulier le DMCA ou les lois adoptée par les Etats (v. par ex. California Penal Code 502(c)).

Les hackers éthiques bénéficient donc depuis 2022 d'un cadre juridique un peu plus favorable à leurs activités. Il demeure toutefois important que le Congrès consacre un véritable statut protecteur pour les hackers éthiques afin de reconnaître pleinement leur contribution à la cybersécurité, la protection des données et la sécurité nationale dans un contexte marqué par la recrudescence de la cybercriminalité, le détournement des plateformes numériques et l'émergence du piratage propulsé par l'intelligence artificielle.

Kamel
EL HILALI

PERSPECTIVES

- Proposition d'amélioration du cadre juridique des hackers éthiques
- Conclusion

PROPOSITION D'AMÉLIORATION DU CADRE JURIDIQUE DES HACKERS ÉTHIQUES

Cyberschool

Responsabilités partagées et code de conduite

En France, les hackers éthiques, pentesters et hunters opèrent dans un cadre légal qui ne leur fournit que peu de protection contre les poursuites judiciaires. Selon le Code pénal français, tout accès non autorisé à un système de traitement automatisé de données peut entraîner des sanctions sévères, y compris des peines d'emprisonnement et des amendes substantielles. Il est donc nécessaire de réfléchir à une forme de légitimation de leur profession.

Dilemme éthique et responsabilité

Les hackers éthiques, pentesters et hunters ne sont pas à l'abri des poursuites pour des actions qui peuvent être interprétées comme malveillantes ou allant au-delà du consentement explicite accordé par le propriétaire du système. Cela crée un dilemme qualifié d' « éthique » significatif, car même des actions bien intentionnées peuvent être perçues comme des infractions si elles ne sont pas adéquatement documentées et autorisées.

Proposition de Code de Conduite

Il est suggéré que les hackers éthiques adoptent un code de conduite clair, incluant la conservation détaillée des logs de leurs actions pour démontrer leur conformité et leur bonne foi. Ces logs devraient inclure des détails précis sur chaque étape du test de pénétration, les méthodes utilisées et les résultats obtenus, ce qui assurerait une transparence et pourrait servir de preuve en cas de litiges ou d'audits juridiques. La proposition de ce Code de conduite est pertinente, car elle constitue un moyen efficace pour guider les pratiques des hackers éthiques, garantissant ainsi une approche standardisée et reconnue pour la gestion des activités de cybersécurité, sans entraîner une loi contraignante qui irait dans un sens contraire à celui de la profession.

Des organisations professionnelles telles que l'Association for Computing Machinery (ACM) recommandent que les hackers éthiques évaluent de manière approfondie les impacts de leurs actions et communiquent ouvertement leurs méthodes et découvertes, tout en respectant la confidentialité contractuelle[66]. Cette recommandation souligne l'importance de la transparence et de la communication responsable dans les activités de hacking éthique, contribuant à une meilleure compréhension et acceptation des procédures par toutes les parties prenantes.

La documentation rigoureuse et la divulgation responsable sont également renforcées par le RGPD, qui exige que toute violation de données personnelles soit signalée aux autorités compétentes dans les 72 heures suivant la découverte de la faille et les personnes concernées (articles 33 et 34 du RGPD). Cette exigence met en lumière l'importance d'une gestion sécurisée et conforme des informations sensibles, rendant ainsi la documentation détaillée et la divulgation transparente non seulement utiles, mais essentielles pour respecter les lois en vigueur.

Ces mesures visent à équilibrer la nécessité de découvrir et de signaler les vulnérabilités de sécurité avec la nécessité de respecter les lois et règlements en vigueur. En proposant un code de conduite, l'objectif est de fournir aux hackers éthiques un cadre clair (mais non contraignant) qui guiderait leurs actions et renforcerait la légitimité de leur travail. Cela permettrait non seulement de contribuer positivement à la cybersécurité, mais aussi de minimiser les risques juridiques pour les praticiens, en leur fournissant des lignes directrices claires pour naviguer dans le paysage complexe de la légalité et de la sécurité informatique.

Discussion sur un statut réglementé pour les hackers éthiques

La discussion sur l'établissement d'un statut spécifique pour les hackers éthiques en France est un sujet complexe qui mélange des considérations légales, éthiques et pratiques. L'idée serait de créer un cadre réglementé, potentiellement sous l'égide de l'Agence

66 Association for Computing Machinery. "ACM Code of Ethics and Professional Conduct". https://www.acm.org/code-of- ethics.

nationale de la sécurité des systèmes d'information (ANSSI), qui encadrerait les actions des hackers éthiques à travers des protocoles stricts, incluant la nécessité de conserver des logs détaillés pour chaque action. Ce statut viserait à légitimer et à sécuriser les pratiques de hacking éthique tout en s'assurant de leur conformité avec les lois en vigueur.

Nécessité de logs détaillés

La conservation de logs pour chaque action est cruciale. Un log est « un fichier contenant des métadonnées pouvant servir à contextualiser un événement qui s'est produit à un moment donné »[67]. Ces logs serviraient non seulement à prouver la bonne foi des hackers éthiques en cas de litige, mais aussi à tracer de manière précise et détaillée les tests effectués. Cela inclurait les méthodes utilisées, les cibles testées, et les résultats obtenus. Cette documentation rigoureuse pourrait protéger les hackers contre des accusations injustifiées et faciliter l'audit et la revue des actions par des tiers autorisés.

Sanctions en cas de non-respect

Le non-respect des statuts et des obligations pourrait entraîner des sanctions sévères. Si un hacker éthique ne suit pas les procédures établies, ne respecte pas les contrats, ou dépasse les limites autorisées par la loi, il pourrait faire face à des poursuites judiciaires. Ces sanctions pourraient inclure des peines d'emprisonnement et des amendes substantielles, conformément au Code pénal français.

Bien que l'ANSSI n'ait pas actuellement de pouvoirs de sanction directe, la création d'un cadre réglementé implique la délégation de certaines responsabilités « punitives » aux autorités judiciaires. Ainsi, les infractions constatées par l'ANSSI pourraient être transmises aux autorités compétentes. Ces mesures strictes sont essentielles pour dissuader les comportements irresponsables et garantir que le hacking éthique reste une pratique bénéfique pour la sécurité informatique globale.

Évaluation des Bénéfices et des Limites d'un Statut Réglementé pour les Hackers Éthiques

Avantages d'un statut réglementé pour les hackers éthiques

L'instauration d'un statut réglementé pour les hackers éthiques offre plusieurs avantages significatifs. Premièrement, la clarification des activités légales par un cadre clairement défini aiderait à distinguer les activités légitimes de hacking éthique des actions illégales. Cette clarification contribuerait à une meilleure compréhension et acceptation de ces pratiques au sein du système juridique et des entreprises, facilitant ainsi leur intégration dans les stratégies de sécurité informatique des organisations. Pour maximiser ces avantages, il est proposé de définir explicitement dans la législation ce qui constitue une activité éthique de hacking, distinguant les différentes formes d'interventions et précisant les conditions sous lesquelles ces activités peuvent être menées. Cela réduirait l'ambiguïté légale et diminuerait les risques de litiges injustifiés.

D'autre part, avec des règles claires, les hackers éthiques bénéficieraient d'une protection légale lorsqu'ils dévoilent des vulnérabilités de manière responsable, réduisant ainsi le risque de litiges. Cette protection serait essentielle pour encourager les professionnels à signaler les vulnérabilités sans crainte de répercussions négatives. Pour renforcer cette protection, il serait judicieux d'instaurer un système de permis ou de certification pour les hackers éthiques qui démontrent leur conformité avec les normes éthiques et légales établies.

Un système de permis ou de certification offrirait plusieurs avantages. Premièrement, il formaliserait le statut des hackers éthiques, leur donnant un cadre légal reconnu qui légitime leurs actions lorsqu'elles sont menées dans le respect des règles établies. Un tel système pourrait être géré par une autorité compétente, telle qu'une agence gouvernementale ou une organisation internationale dédiée à la cybersécurité, qui délivrerait des certifications après une évaluation rigoureuse des compétences techniques et des connaissances juridiques du candidat.

Les hackers éthiques certifiés pourraient ainsi bénéficier d'une protection légale accrue contre les poursuites en cas de divulgation responsable de vulnérabilités. Par exemple, si un hacker éthique certifié découvre une faille de sécurité et la signale de manière appropriée à l'entité concernée, la certification pourrait agir comme une preuve de bonne foi et de respect des procédures, minimisant le risque de représailles juridiques. Ce type de protection encouragerait plus de professionnels à entrer dans le domaine du hacking éthique, sachant qu'ils sont soutenus par un cadre juridique solide. De plus, un système de certification permettrait aux entreprises et aux organisations de faire confiance aux hackers éthiques qui leur signalent une vulnérabilité ou pour tester la sécurité de leurs systèmes.

Enfin, un tel système renforcerait la confiance du public dans les pratiques de hacking éthique. Les utilisateurs finaux et les consommateurs pourraient avoir l'assurance que les vulnérabilités découvertes et divulguées par des hackers certifiés sont gérées

67 Arfan Sharif. « *Qu'est-ce qu'un Log ?* », 23 février 2023, https://www.crowdstrike.fr/cybersecurity-101/observability/log-file/. [En ligne ; consulté le 9-Juillet-2024].

de manière responsable, avec un souci constant de protéger les données sensibles et de minimiser les risques.

Inconvénients d'un statut réglementé pour les hackers éthiques

Cependant, l'adoption d'un cadre réglementé présente également des inconvénients. Un cadre trop strict pourrait limiter la capacité des hackers éthiques à découvrir efficacement les vulnérabilités, notamment en imposant des méthodes ou des processus qui ne correspondent pas à la pratique ou aux technologies visées. Pour atténuer cet inconvénient, il est suggéré d'établir un cadre réglementaire qui spécifie clairement les activités autorisées tout en laissant une marge de manœuvre suffisante pour l'adaptation aux nouvelles technologies et méthodes. Ce cadre inclurait des lignes directrices adaptatives, régulièrement mises à jour en consultation avec les professionnels de la cybersécurité et des représentants de l'industrie, pour s'assurer qu'elles restent pertinentes et pratiques.

De plus, un tel cadre peut encourager une vision trop binaire des actions, où toute activité non explicitement autorisée pourrait être considérée comme malveillante. Pour contrer ce manichéisme, il est crucial de promouvoir une compréhension plus nuancée des scénarios de sécurité informatique réels, en mettant en place des programmes de formation et de sensibilisation soutenus par l'État pour éduquer à la fois les hackers éthiques et le grand public sur l'importance et les limites du hacking éthique. Ces programmes aideraient à améliorer la compréhension publique et professionnelle de ce que signifie être un hacker éthique, clarifiant les rôles et les attentes, et augmentant ainsi la reconnaissance sociale de leur contribution à la sécurité numérique.

CONCLUSION

Par Brunessen BERTRAND

Le hacking éthique, dans sa forme contemporaine, illustre à la fois les promesses et les tensions qui structurent l'espace numérique et les enjeux de sa régulation. Cet ouvrage cherche à clarifier la pluralité des aspects d'une pratique technique qui tend à s'institutionnaliser, à se professionnaliser, et, dans le même temps, à revendiquer une légitimité fondée sur l'éthique. Une légitimité fragile, contestée parfois, mais qui s'inscrit dans les réflexions sur la gouvernance de la cybersécurité.
Les ambiguïtés juridiques qui entourent cette pratique et les efforts émergents pour établir une déontologie montrent que le hacking éthique soulève des questions fondamentales : qui a le droit d'examiner, de tester, de corriger les systèmes numériques ? Quels contre-pouvoirs devons-nous autoriser, ou même encourager, face à des architectures techniques de plus en plus opaques, centralisées, et vulnérables ?

Trois observations peuvent être formulées à titre de conclusion.

Le premier enseignement de cet ouvrage est que l'intention déclarée d'agir pour le bien ne constitue pas, en soi, une justification suffisante. Dans un espace aussi sensible que celui du numérique, l'éthique ne peut être réduite à une posture subjective ou à une revendication morale. Elle doit s'incarner dans des pratiques méthodiques, transparentes, encadrées par des principes clairs. Certes, le hacking éthique cherche à divulguer des vulnérabilités avant qu'elles ne soient exploitées à des fins malveillantes. Mais cette intention doit être accompagnée. Sans cadre structurant, l'éthique peut devenir un prétexte à la transgression, voire à la manipulation des justifications. Il est donc essentiel que le hacker éthique accepte de se soumettre à des principes déontologiques et de responsabilité. Cette exigence implique de penser cette activité dans sa singularité, par exemple à travers des formations intégrant les dimensions éthiques. Le hacking éthique ne peut sans doute pas se structurer de façon spontanée à partir de trajectoires individuelles. Il doit devenir une culture professionnelle partagée, nourrie par la transparence des pratiques, et le dialogue avec les autres corps de métier concernés.

La deuxième observation est celle d'un décalage entre les réalités du hacking éthique et le cadre juridique. La majorité des systèmes juridiques nationaux conservent une approche binaire du piratage : il est soit licite et autorisé dans le cadre d'un mandat contractuel, soit il constitue une infraction pénale. Cette lecture ignore la diversité des situations, la complexité des motivations, et surtout l'existence de zones grises, dans lesquelles de nombreux acteurs opèrent. Certes, des avancées notables existent : les politiques de divulgation coordonnée (responsible disclosure), les programmes de bug bounty encadrés, ou encore la reconnaissance partielle du statut de lanceur d'alerte dans certains pays. Mais ces dispositifs restent fragmentaires et peu harmonisés, et ancrés dans une logique d'application territoriale du droit.

La troisième observation porte sur le degré pertinent de régulation. La voie est étroite, dès lors qu'il ne s'agit ni de définir un encadrement trop strict de ces pratiques, ni de donner un blanc-seing aux intrusions dans les systèmes d'information. L'enjeu est de trouver un équilibre pour définir un cadre souple qui garantisse une sécurité juridique fondé sur des principes déontologiques agiles qui laisse peut être la place à des formes d'autorégulation à travers des chartes, labels, comités d'éthique, expérimentation encadrée.

Plus fondamentalement, le développement du hacking éthique interroge la manière dont nos sociétés veulent penser et gouverner l'espace numérique. C'est pourquoi la reconnaissance du hacking éthique ne doit pas être réduit à un enjeu technique ou juridique, mais doit s'inscrire dans une vision de la protection des sociétés dans un cadre démocratique. Il s'agit de construire un numérique robuste, pensé de façon collective et démocratique à partir de réalités mouvantes et parfois complexes.

Brunessen
BERTRAND

NOTES

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org
02 23 06 10 30 | contact@pole-excellence-cyber.org