walderwyss avocats

Walder Wyss SA
123, Seefeldstrasse
Case postale
8034 Zurich
Suisse

Téléphone +41 58 658 58 58
Fax +41 58 658 59 59
www.walderwyss.com

Résumé analytique

à	Institut national de test pour la cybersécurité (NTC)
de	Michael Isler, Oliver Kunz, Gina Moll
Concerne	**Punissabilité du hacking éthique**
Date	le 26 juin 2023

Michael Isler
Associé
Dr. iur.
Avocat
Direct +41 58 658 55 15
michael.isler@walderwyss.com

Oliver Kunz
Associé
lic. iur., LL.M.
Avocat
Direct +41 58 658 56 41
oliver.kunz@walderwyss.com

Gina Moll
Associate
M.A. HSG in Law, LL.M.
Avocate
Direct +41 58 658 51 56
gina.moll@walderwyss.com

1. Résumé analytique

1.1. Faits et mandat d'expertise

1 L'Institut national de test pour la cybersécurité NTC teste la cybersécurité des produits numériques et des infrastructures en réseau (systèmes) dans le cadre d'analyses des vulnérabilités. Les analyses sont effectuées soit sur mandat avec le consentement des exploitants de systèmes, soit sous la forme de projets d'initiative, c'est-à-dire de la propre initiative du NTC, sans qu'il y ait obligatoirement consentement préalable. Dans le cadre des projets d'initiative, le NTC examine les produits et les infrastructures numériques qui ne sont pas testés ou qui le sont de manière insuffisante. Le NTC vise ainsi à renforcer la cybersécurité dans l'intérêt des utilisateurs des systèmes et de la collectivité.

2 En tant qu'organisation à but non lucratif financée par des fonds publics, le NTC ne poursuit pas d'intérêts financiers ni d'objectifs d'autopromotion. Concrètement, le NTC se concentre sur les systèmes importants pour la société (à savoir, en particulier, les systèmes largement répandus, critiques, sans alternative et les systèmes administratifs) qui semblent menacés sur la base d'indices objectifs, par exemple parce qu'il existe des indices laissant supposer que des failles de sécurité existent dans un système cible.

3 Lors de l'analyse des vulnérabilités, le NTC applique les règles de «best practice» du Centre national pour la cybersécurité (NCSC).

4 Sur la base de sa *Vulnerability Disclosure Policy,* le NTC entend communiquer de manière adéquate les résultats des projets d'initiative aux fabricants et aux exploitants des systèmes cibles, et les publier ultérieurement sous une forme

appropriée, afin que la société, la population, les autorités et les milieux scientifiques puissent en bénéficier.

5 Étant donné que les projets d'initiative sont des projets sans mandat, plusieurs questions se posent quant à une éventuelle punissabilité à l'aune du droit pénal suisse, notamment en matière de cybercriminalité.

1.2. Punissabilité selon les art. 143 bis CP et 144 bis al. 1 CP

6 La réalisation d'analyses des vulnérabilités - dans la mesure où elle implique l'intrusion (tentée ou réalisée) dans un système informatique de tiers (tests de pénétration) - peut entrer en conflit avec l'infraction de piratage de l'art. 143bis al. 1 CP. Est ainsi puni celui qui «s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part». Peu importe à cet égard pour quels motifs l'acte a été commis. L'infraction vise de manière générale à protéger les systèmes informatiques contre les accès non autorisés. Le bien juridique protégé ici est la «paix informatique», c'est-à-dire la liberté de l'ayant droit de décider à qui il donne accès à son système informatique sécurisé et aux données qu'il contient.

7 Comme les projets d'initiative tentent, notamment par le biais de tests de pénétration, de rechercher d'éventuelles failles dans le dispositif de sécurité d'un système cible sans le consentement des détenteurs du bien juridique protégé, et donc sans autorisation, un risque de punissabilité existe. La tentative d'intrusion est également punissable dès que le domaine des actes préparatoires non punissables (p. ex. la recherche d'un système cible potentiel par *portscans*) est outrepassé.

8 La publication des résultats de projets d'initiative n'est pas problématique au sens de l'art. 143bis al. 2 CP (qui réprime la mise à disposition de données pouvant servir à commettre une infraction au sens de l'art. 143bis al. 1 CP), pour autant que la faille de sécurité publiée ait déjà été entièrement corrigée avant la publication. Une démarche coordonnée dans le temps avec l'exploitant du système cible concerné peut donc exclure complètement la punissabilité au sens de l'art. 143bis al. 2 CP. Toutefois, si la vulnérabilité créée par une faille de sécurité n'est pas encore (ou pas entièrement) corrigée avant la publication des détails techniques, le risque au regard du droit pénal ne peut être réduit que par un degré de précision moindre de la publication. Dans ces cas, il ne faudrait en particulier pas publier de détails concrets sur un éventuel *exploit* et la description technique de la faille de sécurité devrait se limiter aux indications nécessaires pour que les utilisateurs concernés puissent prendre des mesures de protection appropriées. Selon l'art. 143bis al. 2 CP, le signalement à une autorité, par exemple au NCSC, ne poserait pas de problème sur le plan pénal.

9 Eu égard à l'éventuelle punissabilité d'une détérioration de données au sens de l'art. 144bis ch. 1 CP dans le cadre des analyses de vulnérabilité, les manipulations temporaires de données (par exemple dans le but de déjouer un dispositif de sécurité) ne doivent être effectuées qu'avec une intensité d'intervention aussi faible que possible et pour une courte durée, faute de quoi l'importance de la modification des données au sens de cette infraction devrait être admise (par exemple, les mots de passe temporairement modifiés, etc., doivent être immédiatement réinitialisés). Un risque de punissabilité supplémentaire existe également en cas de commission par dol éventuel de l'infraction réprimée par l'art. 144 ^{bis} ch. 1 CP, si, par une action techniquement risquée, l'auteur accepte qu'il puisse y avoir une détérioration des données (par ex. indisponibilité temporaire ou durable de données). Une punissabilité au sens de l'art. 144bis ch. 2 CP (diffusion de programmes visant la détérioration de données) peut en revanche être exclue dans le cadre de projets d'initiative.

1.3. État de nécessité licite selon l'art. 17 CP

10 Un comportement qui réalise les éléments constitutifs d'une infraction peut exceptionnellement, à des conditions particulières, être licite et, partant, non punissable. Tel est notamment le cas lorsque l'auteur de l'infraction peut se prévaloir du motif justificatif pénal de l'état de nécessité au sens de l'art. 17 CP.

11 Un tel motif justificatif existe lorsque l'acte constitutif de l'infraction a été commis pour préserver un bien juridique propre ou celui d'un tiers d'un danger imminent et impossible à détourner. L'acte (en principe punissable) est exceptionnellement licite si l'auteur invoquant l'état de nécessité sauvegarde ainsi des intérêts prépondérants.

12 Les conditions concrètes de l'état de nécessité licite sont (i) l'existence d'un danger imminent pour un bien juridique individuel (p. ex. la liberté individuelle de la «paix informatique»), (ii) la subsidiarité absolue (c'est-à-dire que l'acte doit constituer le moyen le moins dommageable de prévenir le danger) et (iii) une pesée positive des intérêts en présence. Du point de vue subjectif, il faut que (iv) l'auteur invoquant l'état de nécessité ait connaissance du danger et agisse pour préserver le bien juridique menacé.

13 Si un test de pénétration est effectué pour écarter un danger pour l'intégrité et la sécurité du système concerné (en particulier parce qu'il existe des indices concrets que celui-ci comporte des failles de sécurité potentielles qui permettent également des interventions malveillantes), le système concerné peut donc être attaqué à tout moment. Dans ces conditions, le danger imminent pour un bien juridique individuel (à savoir la «paix informatique» des titulaires du bien juridique concernés) requis pour invoquer l'état de nécessité est en principe donné. Dans le cas d'installations ou de systèmes de traitement

de données menacés, le caractère imminent du danger résulte de l'état de danger qui persiste sur une longue période et qui peut, à tout moment, se transformer en dommage (p. ex. attaque de piratage malveillante, détérioration de données, perte de données, etc.) («danger permanent»).

14 En cas d'état de nécessité, les moyens utilisés doivent être propres à écarter le danger et il doit en outre s'agir du moyen le plus doux, c'est-à-dire celui qui porte le moins atteinte aux biens juridiques appartenant à autrui (subsidiarité absolue).

15 Les projets d'initiative sont conformes au principe de subsidiarité absolue lorsque l'intervention se limite à déceler les failles de sécurité existantes, à les documenter et à les communiquer ensuite aux exploitants des systèmes cibles afin qu'ils puissent remédier à l'état de danger. En outre, il doit être impossible ou déraisonnable d'obtenir le consentement préalable de tous les titulaires du bien juridique concernés. C'est notamment le cas lorsque des systèmes cibles sont testés, pour lesquels tous les titulaires du bien juridique concernés ne peuvent pas être identifiés de manière exhaustive ou ne peuvent, et ne seront pas en mesure, de réagir de manière adéquate. Dans certains cas, la prise de contact préalable (et la divulgation de la situation de danger qui en découle) pourrait même augmenter le risque que la faille de sécurité soit exploitée.

16 Au vu des conditions exposées ci-dessus, la pesée des intérêts pour les projets d'initiative s'avère également positive: la gravité de l'accès (contrôlé) à des fins positives (et sans volonté de nuire) dans le cadre d'un projet d'initiative passe clairement au second plan par rapport au degré nettement plus élevé de danger pour ce même bien juridique en cas d'attaque de piratage malveillant.

17 Il est toutefois important que les projets d'initiative soient réalisés exclusivement dans le but de remédier au danger. Lorsqu'un hacker poursuit d'autres buts (p. ex. l'autopromotion, la curiosité, voire l'obtention d'avantages économiques), il ne pourra pas se prévaloir du motif justificatif de l'état de nécessité. Dans l'ensemble, il apparaît que le motif justificatif de l'état de nécessité au sens de l'art. 17 CP est propre à justifier les actes potentiellement réprimés par les art. 143bis al. 1 CP et 144bis ch. 1 CP dans le cadre de la réalisation de projets d'initiative du NTC.

1.4. Autres risques de droit pénal

18 En ce qui concerne les autres infractions du droit de la cybercriminalité (en particulier l'art. 179^{novies} CP [soustraction de données personnelles] et l'art. 45c LTC en relation avec l'art. 53 LTC [infraction à la loi sur les télécommunications]), une conception adéquate des projets d'initiative et une mise en œuvre appropriée des analyses des vulnérabilités permettent déjà d'éviter la commission d'actes constitutifs d'une infraction de ce type. Si les

éléments constitutifs de l'infraction devaient exceptionnellement être réalisés, l'état de nécessité pourra également être invoqué comme motif justificatif, à certaines conditions.