Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Berne, le 29 novembre 2023

La promotion du piratage éthique en Suisse

Rapport du Conseil fédéral en réponse au postulat 20.4594 du 17 décembre 2020

Table des matières

1 Introduction ... 3

1.1 Contexte ... 3
1.2 Mandat ... 4
1.3 Définition du piratage éthique ... 5

2 Instruments de promotion du piratage éthique ... 6

2.1 Programmes de promotion du piratage éthique ... 6
2.1.1 Tests de sécurité ... 6
2.1.2 Directives relatives au signalement et à la publication des vulnérabilités ... 7
2.1.3 Programmes de primes aux bogues ... 7

2.2 Divulgation coordonnée des vulnérabilités ... 8

3 Promotion du piratage éthique dans le contexte international ... 9

4 Promotion du piratage éthique en Suisse ... 10

4.1 Bases stratégiques et juridiques de la promotion du piratage éthique ... 10
4.2 Mise en œuvre de mesures à la Confédération ... 11
4.2.1 Signalement de vulnérabilités ... 11
4.2.2 Tests publics de sécurité ... 12
4.2.3 Organisation d'hackathons pour rechercher des vulnérabilités ... 12
4.2.4 Chasse aux bogues de la Confédération ... 13
4.2.5 Mise à disposition d'instruments et sensibilisation ... 13

4.3 Mise en œuvre dans l'économie ... 14
4.3.1 Mesures des entreprises ... 14
4.3.2 Mise en œuvre dans les entreprises proches de la Confédération ... 14
4.3.3 Offres de services en lien avec le piratage éthique ... 15

5 Conclusions ... 16

1 Introduction

La cybersécurité représente un défi majeur pour la sécurité de notre société. La numérisation a rendu l'économie, l'État et la population complètement dépendants du fonctionnement et de la sécurité des technologies de l'information et de la communication. Nombre de processus de la vie quotidienne ne seraient plus réalisables sans ces technologies, car celles-ci relient diverses applications en systèmes globaux multifonctionnels importants pour les utilisateurs. Ces vastes réseaux informatiques constituent donc la principale infrastructure de la numérisation.
La complexité est caractéristique de ces systèmes. En effet, l'association de différentes applications informatiques donne lieu à de nombreuses interfaces et interdépendances qui entravent une vue d'ensemble du système. De plus, les codes de programmation de ces systèmes comportent souvent plusieurs millions de lignes. Il n'est donc pas étonnant que des vulnérabilités y apparaissent régulièrement et menacent la sécurité des systèmes informatiques. Il s'agit généralement d'erreurs de programmation ou de configuration qui permettent d'accéder de façon non autorisée aux systèmes ou aux données qu'ils contiennent. De nombreux cyberattaquants exploitent ces vulnérabilités pour s'introduire dans les systèmes informatiques et compromettre la sécurité de ceux-ci.
En ce qui concerne la cybersécurité, il est décisif que tout soit entrepris pour réduire les risques pesant sur les systèmes informatiques en raison de vulnérabilités. La sécurité doit rester une priorité absolue dans le cadre du développement et de l'exploitation de matériel informatique et de logiciels. À cet égard, il est très important que les systèmes informatiques complexes soient analysés en permanence pour y détecter d'éventuelles vulnérabilités et les combler avant que les attaquants les exploitent.
L'une des tâches essentielles de la cybersécurité consiste à rechercher activement les vulnérabilités, à les décrire et à les évaluer de manière à pouvoir apprécier les dangers, d'une part, et à prendre des contre-mesures afin de combler ces failles de sécurité ou d'en réduire les risques, d'autre part. Or, compte tenu de la taille et de la complexité des systèmes informatiques, il s'agit là de tâches que les équipes de sécurité compétentes des fabricants et des utilisateurs ne sont plus en mesure d'assumer dans tous les cas avec une qualité suffisante. C'est pourquoi de nombreuses vulnérabilités échappent aux équipes de sécurité et peuvent être ensuite exploitées par des cyberattaquants.
De ce fait, le piratage éthique recèle un énorme potentiel d'amélioration de la cybersécurité. L'idée de base du piratage éthique est que les pirates recherchent activement des vulnérabilités dans les systèmes informatiques et les réseaux pour les signaler aux organisations et aux fabricants concernés plutôt que de lancer des cyberattaques. La promotion du piratage éthique vise à offrir aux pirates les meilleures incitations possible pour qu'ils utilisent leurs compétences dans l'esprit du piratage éthique et contribuent ainsi à la cybersécurité.

1.1 Contexte

La menace des cyberattaques est depuis des années l'un des principaux risques auxquels sont exposés les pouvoirs publics, les entreprises et les citoyens. En 2022, 34 000 incidents ont été annoncés au Centre national pour la cybersécurité (NCSC)[1]. Une large majorité de cyberattaques sont motivées par des raisons criminelles. L'éventail va des délits classiques commis à l'aide de moyens numériques («criminalité numérisée») aux délits qui visent Internet, des systèmes informatiques ou leurs données («cybercriminalité»). Les attaques au rançongiciel, au cours desquelles les pirates informatiques s'introduisent dans le système, chiffrent des données et bien souvent les dérobent, ont notamment connu une forte augmentation. Les auteurs de ces délits font ensuite chanter les victimes en leur proposant d'annuler le chiffrement contre une rançon et de renoncer à la publication des informations en cas de paiement.

[1] Rapport du NCSC «Sûreté de l'information: situation en Suisse et sur le plan international. Rapport semestriel 2022/2» du 11 mai 2023, p. 10 (consultable à l'adresse: https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/berichte/lageberichte/halbjahresbericht-2022-2.html)

Comme de très nombreuses attaques exploitent les points faibles des systèmes informatiques, la prévention et l'élimination des vulnérabilités sont d'une importance cruciale. La cyberstratégie nationale (CSN) adoptée en avril 2023 par le Conseil fédéral et les cantons le souligne: «Or, il est essentiel pour la cybersécurité de prévenir autant que possible l'apparition de ce genre de vulnérabilités, de les repérer à temps et d'y remédier rapidement.[2]» La promotion du piratage éthique est l'une des mesures les plus importantes à cet égard. L'objectif est d'exploiter le grand potentiel des pirates informatiques mus par des intentions éthiques en leur donnant des conditions-cadres propices à la recherche et au signalement des vulnérabilités de manière à détecter et à combler les failles plus tôt. Le respect du droit applicable est essentiel dans le cadre de la promotion du piratage éthique. Pour que le piratage soit considéré comme légal, les conditions posées par le droit pénal doivent notamment être remplies. L'art. 143bis du code pénal (CP) prévoit que quiconque s'introduit sans droit dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est punissable. Il convient à cet égard d'opérer une distinction avec le piratage réalisé à la demande ou avec l'accord de l'ayant droit du système concerné. Dans ce cas, il n'y a ni accès indu ni comportement illicite puisque le piratage fait suite à une demande, à une invitation ou à un appel d'offres.

1.2 Mandat

Le Conseil national a accepté le postulat suivant en date du 19 mars 2021 afin de mieux évaluer l'importance et le potentiel du piratage éthique en Suisse:

Postulat 20.4594 Bellaiche «Institutionnaliser le piratage éthique et améliorer la cybersécurité»
Le Conseil fédéral est chargé d'étudier dans quelle mesure le piratage éthique pourrait être institutionnalisé en tant que principe pour améliorer la cybersécurité et s'il pourrait être encouragé dans l'administration fédérale et les entreprises liées à la Confédération au moyen des mesures suivantes:

1. L'administration fédérale et les entreprises liées à la Confédération définissent des directives prévoyant des processus clairs pour détecter les failles de sécurité des systèmes informatiques et garantissant une divulgation coordonnée par le biais de tiers. Les directives doivent notamment préciser quels systèmes sont à vérifier, quels tests sont autorisés et à qui les failles doivent être signalées. Elles garantissent aux pirates qu'ils ne risquent aucune poursuite s'ils respectent les conditions prévues.
2. Les entreprises organisent des chasses aux bogues pour s'assurer de la robustesse de leurs systèmes. Les systèmes classifiés sont exceptés. Comme le succès de ces chasses dépend des primes offertes, les budgets des unités et entreprises concernées devront être adaptés.
3. Le NCSC soutient la démarche et accompagne sa mise en œuvre.

Pour remplir ce mandat d'examen, le rapport commence par présenter ce qu'il faut entendre par «piratage éthique». Puis, les divers instruments de promotion de ce dernier sont exposés. Le troisième chapitre met en lumière les instruments utilisés en faveur du piratage éthique dans le contexte international et quelles organisations internationales s'engagent à cet égard. Le quatrième chapitre est consacré au mandat d'examen proprement dit. Le piratage éthique joue un rôle toujours plus important en Suisse également. De nombreux pouvoirs publics et entreprises recourent déjà à des instruments de promotion du piratage éthique. Le présent rapport décrit comment cette promotion est conçue et dans quels domaines subsiste encore davantage de potentiel. Enfin, le rapport évalue le statu quo à titre de conclusion et il présente les mesures encore à prendre.

[2] Le Conseil fédéral suisse, CSN d'avril 2023, p. 19 (consultable à l'adresse: https://www.newsd.admin.ch/newsd/message/attachments/76794.pdf)

1.3 Définition du piratage éthique

Utilisé dans une acception très large, le terme de «piratage» intervient fréquemment comme un synonyme de cybercriminalité. Au sens propre cependant, «pirater» signifie s'introduire dans un système informatique[3]. Un pirate informatique est donc une personne qui, indépendamment de ses motifs, s'introduit activement dans des systèmes auxquels elle ne devrait pas avoir accès. À cette fin, les pirates recourent à diverses méthodes pour entrer dans les systèmes informatiques. Par exemple, ils peuvent hameçonner leurs victimes et les inciter à installer sur leurs systèmes des programmes qui permettent ensuite aux attaquants d'y accéder. Une méthode alternative consiste pour les pirates à exploiter les vulnérabilités des systèmes informatiques afin de s'y introduire directement. Souvent, les pirates utilisent une combinaison de plusieurs méthodes pour parvenir à leurs fins.
Dans les années 1990, les désignations de «black hat» (chapeau noir) et de «white hat» (chapeau blanc) sont apparues pour distinguer les pirates informatiques selon que leurs intentions sont éthiques ou non. Les chapeaux noirs ont des motifs non éthiques, souvent criminels, et utilisent leurs connaissances en programmation à des fins délictueuses. Ils correspondent aux bandits des anciens westerns, qui portaient des chapeaux noirs. À l'inverse, les chapeaux blancs appliquent leurs compétences en piratage au profit de la société. Tout comme les chapeaux noirs, ils tentent de s'introduire dans les systèmes informatiques ou à tout le moins d'identifier les possibilités d'y parvenir. Mais ils ne poursuivent pas des buts non éthiques ou criminels. Cela signifie qu'ils mettent leurs connaissances à la disposition des personnes concernées, contribuant ainsi à accroître aussi efficacement que possible la sécurité des exploitants de système et des autres personnes concernées.
La différenciation entre pirates éthiques et non éthiques repose principalement sur leur intention. Toutefois, il n'est pas toujours simple d'évaluer quelles intentions répondent au principe du piratage éthique. Il n'est pas rare que les actions de pirates informatiques donnent lieu à des discussions sur les limites entre piratage éthique et non éthique. En outre, cette discussion ne doit pas masquer le fait que s'introduire sans droit dans des systèmes appartenant à des tiers est illicite même s'il repose sur une intention éthique[4].
C'est pourquoi il est capital de définir des conditions-cadres aussi claires que possible selon lesquelles la pénétration de systèmes peut avoir lieu en toute légalité et au profit des personnes concernées. En plus de bénéficier de l'accord de l'ayant droit du système concerné, il est important de définir qui, comment et à quel moment les pirates éthiques doivent informer sur les vulnérabilités identifiées[5]. Si des conditions-cadres claires sont définies et respectées, on peut parler de piratage éthique.
Le piratage éthique repose donc globalement sur les mêmes méthodes que le piratage illicite. Des vulnérabilités techniques sont recherchées afin de pénétrer dans des systèmes informatiques. Les vulnérabilités peuvent se définir comme un comportement ou une série de conditions dans un système, un produit, un composant ou un service qui contrevient à une directive de sécurité implicite ou explicite. Une vulnérabilité peut se comprendre comme un point faible ou une menace susceptible d'impacter la sécurité ou d'entraîner des conséquences concernant la sécurité[6]. Des vulnérabilités peuvent se trouver dans certains éléments matériels ou logiciels ou découler de la connexion et de la configuration de ces produits.

---

3 Le législateur suisse qualifie de piratage l'action de celui qui s'introduit sans droit dans un système de traitement des données, cf. à cet égard message et projets législatifs concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF **1991** II 933 ss, 979.

4 Michael Isler, Oliver M. Kunz et Gina Moll sont d'un autre avis. Dans une expertise juridique réalisée à l'intention de l'Institut national de test pour la cybersécurité (NTC), ils expliquent que, dans la situation juridique actuelle, les pirates éthiques peuvent invoquer le motif justificatif relevant du droit pénal qu'est l'état de nécessité au sens de l'art. 17 CP à certaines conditions (cf. MICHAEL ISLER/OLIVER M. KUNZ/GINA MOLL, Rechtsgutachten: «Strafbarkeit von Ethical Hacking», walderwyss rechtsanwälte, 26 juin 2023, ch. marg. 209, p. 60, consultable à l'adresse: https://www.walderwyss.com/user_assets/news/230625-MASTERFILE-NTC-Gutachten.pdf).

5 Cf. ALANA MAURUSHAT, Ehtical Hacking, Ottawa 2019, deuxième chapitre SANDRO GERMANN ET DAVID WICKI-BIRCHLER, Hacking und Hacker im Schweizer Recht, in: Aktuelle Juristische Praxis (AJP), 1/2020, p. 86 (consultable à l'adresse: https://fh-hwz.ch/api/assets/31755dd2-fc53-47c2-914c-099ac3b1ede5).

6 Cf. norme ISO/IEC 29147:2018-10 (date de publication: octobre 2018), «Divulgation de vulnérabilités».

Comme les vulnérabilités ne sont souvent pas simples à déceler, il est très précieux que des pirates spécialisés les recherchent activement. Leur examen externe accroît les chances de découvrir les failles des systèmes avant que des pirates criminels ne puissent les exploiter.

2 Instruments de promotion du piratage éthique

Le piratage éthique apporte une précieuse contribution à la cybersécurité de l'économie et de la société. Leur travail est important pour la sécurité des entreprises et des pouvoirs publics. En outre, le piratage éthique est également judicieux du point de vue économique: un dommage potentiellement élevé peut être empêché lorsque des pirates décèlent des vulnérabilités, que ce soit sur mandat ou de leur propre initiative, et les communiquent aux personnes concernées. En termes économiques, les programmes où des pirates sont encouragés à rechercher des failles de sécurité et à les signaler sans être directement mandatés sont particulièrement intéressants. Dans le cadre de ces programmes, ils ne sont rémunérés que s'ils ont effectivement décelé une vulnérabilité.
D'un autre côté, le piratage éthique ne saurait être assimilé à de l'altruisme. Il est légitime que les pirates tentent de maximiser via des voies légales le bénéfice obtenu grâce à leurs capacités. C'est pourquoi il leur importe de savoir ce qu'ils peuvent attendre du signalement de vulnérabilités. À cet effet, il est utile de clarifier les conditions de recherche et de signalement des vulnérabilités et d'assurer une transparence quant aux rémunérations spécifiques aux diverses découvertes[7].
On peut donc qualifier le piratage éthique de modèle d'affaires. De très nombreux prestataires actifs dans le domaine de la sécurité informatique proposent le piratage éthique dans leur portefeuille de services. De plus, des pirates spécialisés dans la recherche rémunérée de vulnérabilités se sont d'ores et déjà établis comme indépendants dans ce domaine[8].
L'existence de conditions-cadres aussi claires que possible est capitale pour le bon fonctionnement du piratage éthique. Au final, ce sont les entreprises et les pouvoirs publics qui sont responsables de définir dans quelles circonstances et pour quels systèmes ou domaines ils autorisent des pirates à rechercher des vulnérabilités. Ce faisant, ils permettent aux pirates de rechercher activement des vulnérabilités sans risquer d'être inquiétés pour piratage illicite en raison d'une introduction sans droit dans des systèmes informatiques appartenant à autrui au sens de l'art. 143bis CP.
Les conditions-cadres sont définies dans des programmes de promotion du piratage éthique. Comme ces programmes sont très disparates quant aux rôles dévolus aux entreprises et aux organisations de même que s'agissant des incitations en faveur du piratage éthique, ils sont décrits brièvement ci-après. Le texte porte aussi à cet égard sur l'importance de la coordination entre les pirates et les personnes concernées ainsi que sur les rôles potentiels respectifs des acteurs étatiques.

2.1 Programmes de promotion du piratage éthique

Trois programmes d'utilisation du potentiel du piratage éthique sont décrits ci-après: la réalisation de tests de sécurité, l'édiction de directives relatives au signalement et à la publication des vulnérabilités et la mise en œuvre de programmes de primes aux bogues.

2.1.1 Tests de sécurité

Des tests de sécurité sont exécutés depuis de nombreuses années pour détecter précocement les vulnérabilités des systèmes informatiques. Les tests dits de pénétration sont la forme la plus répandue des tests de sécurité: les entreprises ou organisations mandatent des pirates pour qu'ils attaquent

[7] Omer Akgül et al., Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem, p. 1 ss (consultable à l'adresse: https://www.usenix.org/system/files/sec23fall-prepub-81-akgul.pdf)
[8] Cf. NZZ du 10 août 2022: «Xel» ist ein Schweizer Top-Hacker: Ein Besuch im Homeoffice (nzz.ch).

leurs systèmes et applications, et en identifient ainsi les failles éventuelles. Lors de tels tests, le mandant prescrit les modalités des tests et détermine quels systèmes y sont soumis. Les pirates recherchent des failles dans ce cadre bien établi. Contrairement à d'autres programmes de promotion du piratage éthique, les pirates et leurs mandants signent généralement une convention contractuelle, les pirates étant payés pour leurs activités et le temps investi indépendamment de savoir s'ils trouvent ou non une vulnérabilité. Les tests publics de sécurité («Public Security Tests») constituent une forme de test spéciale: les développeurs ou les exploitants d'un système ou d'une application en publient le code développé et appellent publiquement à le contrôler quant à sa vulnérabilité. De tels tests publics de sécurité présentent donc de nombreuses similitudes avec un programme public de primes aux bogues (cf. chap. 2.1.3), mais ils sont typiquement limités dans le temps et ne couvrent normalement qu'un système concret ou une application concrète.

2.1.2 Directives relatives au signalement et à la publication des vulnérabilités

Une forme très simple de promotion du piratage éthique consiste à définir et à publier des directives concernant le signalement et la publication des vulnérabilités décelées. Il importe aux pirates qui souhaitent rechercher et signaler des vulnérabilités d'avoir toute la certitude possible qu'ils ne seront pas inquiétés juridiquement par les organisations concernées. Il leur est donc très utile que les organisations fixent quel type de piratage éthique elles acceptent à quelles conditions et quelles modalités de signalement de leurs failles sont correctes. Tel est justement le but des directives relatives au signalement et à la publication des vulnérabilités.
Les organisations concernées doivent donner des indications sur la manière correcte de communiquer les vulnérabilités découvertes. La norme ISO 29147:2018, par exemple, décrit la forme que devraient prendre de telles directives[9]. Il faut au minimum clarifier comment les pirates peuvent contacter l'organisation. Il est en outre recommandable de renseigner sur la communication sécurisée des informations et d'indiquer à quel domaine de l'organisation se rapportent les directives (en particulier, si la recherche de vulnérabilités n'est en aucun cas souhaitée dans certains systèmes ou applications de l'organisation, il faut le faire savoir en toute transparence). Il est également conseillé, pour prévenir des conflits en lien avec la publication des vulnérabilités, que les directives précisent comment et dans quels délais l'organisation concernée publiera elle-même les vulnérabilités signalées ou qu'elles indiquent la procédure que cette organisation entend voir adopter par les pirates en matière de publication. Enfin, les directives devraient aussi comprendre une section dédiée à l'évaluation et peuvent aussi donner des indications quant à l'éventuelle rémunération pour l'annonce de vulnérabilités. Les programmes de primes aux bogues quant à eux incluent éventuellement des modalités de rémunérations.

2.1.3 Programmes de primes aux bogues

Dans ces programmes, les organisations prévoient des primes à verser pour la mise en évidence de failles de sécurité dans les systèmes désignés par les mandants et définissent quelles conditions s'appliquent à la recherche de vulnérabilités. Si le programme de primes aux bogues est ouvert, tous les pirates peuvent s'engager dans la recherche de vulnérabilités. Si le programme est fermé, seuls les pirates invités et choisis peuvent y participer.
Les premiers programmes de primes aux bogues ont été établis dès 1995 par la société Netscape Communications[10]. Au vu du succès qu'ils ont rencontré, de nombreuses entreprises y ont recours depuis lors.
Alors que beaucoup d'entreprises de taille importante mènent leurs propres programmes de primes aux bogues, d'autres entreprises recourent aux services de prestataires spécialisés qui proposent des

[9] Cf. norme ISO/IEC 29147:2018-10 (date de publication: octobre 2018), p. 35 ss.
[10] MATTHEW FINIFTER, DEVDATTA AKHAWE ET DAVID WAGNER, An Empirical Study of Vulnerability Rewards Programs, Proceedings of the 22nd USENIX Security Symposium, août 2013, p. 1 ss (consultable à l'adresse: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf)

plateformes de programmes de primes aux bogues. Ces plateformes facilitent le travail des entreprises qui, en mettant en ligne leurs propres programmes de primes aux bogues, souhaitent inviter directement des pirates et les rémunérer en cas de succès. De telles plateformes sont intéressantes pour les pirates, car elles leur permettent d'obtenir des mandats directement sans devoir consacrer du temps à clarifier si et dans quels cas les entreprises prévoient une rémunération.

2.2 Divulgation coordonnée des vulnérabilités

Les programmes de promotion du piratage éthique fournissent un bon cadre au signalement et à la divulgation des failles de sécurité. Mais ils ne sont de loin pas mis en œuvre partout et de nombreuses entreprises n'indiquent pas comment il faut gérer les vulnérabilités détectées dans leurs systèmes. De ce fait, il arrive souvent que des pirates trouvent des failles de sécurité sans que des programmes ou des directives ne prescrivent comment les faire connaître. Toutefois, dans ce cas également, le piratage éthique devrait respecter certains principes définis dans les processus de la divulgation coordonnée des vulnérabilités («Coordinated Vulnerability Disclosure»). La norme ISO/IEC 29147:2018-10 est déterminante en l'occurrence[11].

Le processus de divulgation coordonnée a été développé parce qu'il apparaît judicieux à première vue dans la plupart des cas de maximiser la transparence en matière de vulnérabilités, tous les intéressés potentiels étant ainsi immédiatement informés de la faille. Mais en pratique, une publication immédiate peut engendrer des risques sécuritaires importants. Les fabricants et les développeurs ont souvent besoin de temps pour éliminer une faille. Pendant ce temps, tous les utilisateurs qui continuent de recourir aux produits concernés par ignorance ou par manque d'alternative sont fortement menacés par la publication de la vulnérabilité.

L'objectif du processus de divulgation coordonnée est de garantir la plus grande transparence possible concernant les vulnérabilités, sans qu'aucun risque sécuritaire ne survienne. Le cœur du processus est que les fabricants soient les premiers informés si une faille de sécurité est décelée. Les pirates conviennent avec eux d'une période de blocage pendant laquelle ils ne diffuseront pas publiquement d'informations sur la vulnérabilité visée. Les fabricants ont ainsi le temps qu'il faut pour supprimer la faille avant qu'elle ne soit publiée.

Cette approche permet de garantir qu'aucune information sur les failles de sécurité ne soit publiée avant que des mesures visant à les éliminer n'aient été prises. Simultanément, l'accord sur un délai interdit aux fabricants d'ignorer la vulnérabilité visée.

Le principe de la divulgation coordonnée est certes simple, mais en pratique, la communication entre les découvreurs de la vulnérabilité et les fabricants du produit concerné est souvent compliquée. Pour prouver et documenter la présence d'une faille de sécurité, les pirates doivent l'exploiter eux-mêmes. De ce fait, ils s'introduisent très souvent dans des systèmes informatiques étrangers, ce qui peut constituer l'accès indu à un système informatique visé à l'art. 143bis CP, comme mentionné plus haut. Leur introduction dans des systèmes informatiques peut avoir lieu sans risque de poursuite pénale que s'il s'agit de leurs propres systèmes ou s'ils disposent de l'accord des personnes concernées. Cependant, les limites des actions auxquelles les personnes concernées consentent – par exemple dans leurs directives applicables au piratage éthique relatives à la notification et à la publication des vulnérabilités – ne sont pas toujours suffisamment claires. Cela peut donner lieu à des conflits entre les pirates et les organisations concernées. Ils surviennent souvent lorsqu'il s'agit de savoir comment et quand le public ou les tiers concernés doivent être informés de la faille découverte. En effet, les pirates souhaitent généralement maximiser la transparence alors que les entreprises craignent une atteinte à leur réputation en cas de publication.

Lors de conflits avec les entreprises concernées, les pirates risquent de se rendre punissables. C'est la raison pour laquelle nombre d'entre eux préfèrent travailler avec un organe de coordination. Le rôle de ce dernier consiste à établir des contacts entre les fabricants et les pirates en préservant

[11] Cf. norme ISO/IEC 29147:2018-10 (date de publication: octobre 2018), p. 14.

l'anonymat de ceux-ci lorsqu'ils le souhaitent. En outre, les coordinateurs peuvent s'avérer utiles dans la négociation sur l'agenda contraignant concernant la divulgation des failles de sécurité, ils peuvent assurer la vérification indépendante du signalement et de la documentation des vulnérabilités et ils peuvent aider les pirates à divulguer celles-ci correctement.[12]
Dans de nombreux pays, ce sont des organes publics qui assurent ce type de coordination. En Suisse, le NCSC peut s'en acquitter. Il est décrit de manière plus détaillée au chapitre 4.1.

3 Promotion du piratage éthique dans le contexte international

De nombreux États tentent de promouvoir le piratage éthique et ont développé leurs propres programmes à cet effet. Ces programmes, souvent décrits dans les stratégies nationales de cybersécurité, sont toutefois rarement réglementés par une législation propre.
Dans le contexte européen, la directive (UE) 2022/25555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2)[13] revêt en particulier une grande importance. Cette directive exige des États membres de l'UE qu'ils facilitent la coordination de la divulgation des vulnérabilités (art. 12) et qu'ils arrêtent les mesures à cet effet dans une stratégie nationale (art. 7, al. 2, let. c). Ils désigneront notamment l'un de leurs centres de réponse aux incidents de sécurité informatique comme service de coordination (art. 11, al. 5, let. c). Les centres de réponse aux incidents de sécurité informatique disposent des connaissances requises pour évaluer les vulnérabilités et ils peuvent contribuer, grâce à leur réseau, à en coordonner rapidement la publication.
Outre la promotion par l'État du piratage éthique, les activités des organisations internationales et des organisations non gouvernementales sont de grande importance. Citons en premier lieu les organismes de normalisation et de standardisation. Les normes 29147 et 30111 de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (IEC) constituent la base déterminante de la plupart des programmes de divulgation coordonnée des vulnérabilités et, partant, de la coopération entre pirates et entreprises concernées. Le National Institute of Standards and Technology (États-Unis) a lui aussi publié des normes de divulgation des vulnérabilités[14] qui concordent avec celles de l'ISO/IEC.
Internet Engineering Task Force (IETF) et Mitre Corporation sont aussi des organisations internationales non gouvernementales qui contribuent à promouvoir le piratage éthique. Internet Engineering Task Force a adopté la norme technique security.txt[15], qui améliore en les uniformisant les possibilités de contact et de signalement des incidents et des vulnérabilités aux entreprises et organisations concernées. L'application des normes permet la lecture des données de contact et de signalement tant aux machines qu'aux personnes, ce qui facilite la prise de contact avec les entreprises concernées. Mitre Corporation a développé avec son programme «Common Vulnerability and Exposures» une systématique permettant de catégoriser les vulnérabilités et de les identifier sans ambiguïté[16]. Cet outil permet aux pirates qui ont trouvé une vulnérabilité et souhaitent la divulguer de savoir aisément si elle est déjà connue ou non.
Outre ces normes techniques utiles au signalement et au traitement des failles de sécurité, un rapport de l'Organisation de coopération et de développement économiques (OCDE) montre comment les

12 Cf. norme ISO/IEC 29147:2018-10, p. 17.
13 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (consultable à l'adresse: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555&qid=1694072876640)
14 NIST Special Publication 800-216, Recommendations for Federal Vulnderability Disclosure Guidance, mai 2023 (consultable à l'adresse: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-216.pdf)
15 RFC 9116, A File Format to Aid in Security Vulnerability Disclosure, avril 2022 (consultable à l'adresse: https://www.rfc-editor.org/info/rfc9116)
16 Consultable à l'adresse: CVE - CVE (mitre.org)

gouvernements peuvent concevoir et déployer efficacement des programmes de divulgation coordonnée des vulnérabilités. Ce rapport propose de surcroît une «bonne pratique» à cet effet[17]. Par contre, le piratage éthique ne joue un rôle important ni dans le cadre des travaux du Conseil de l'Europe en lien avec la Convention sur la cybercriminalité[18] ni dans le cadre des négociations des Nations Unies concernant une convention internationale relative à la cybercriminalité[19]. Ces initiatives mettent au premier plan la coopération internationale ainsi qu'une harmonisation de la définition du piratage illégal et de la lutte contre celui-ci. C'est la raison pour laquelle des dispositions internationales contraignantes sur ce qui doit être considéré comme du piratage éthique ne devraient pas voir le jour dans un avenir proche.

4 Promotion du piratage éthique en Suisse

Ces dernières années, la promotion du piratage éthique a énormément gagné en importance pour la Suisse. Si les entreprises et les autorités qui s'intéressaient à la gestion des vulnérabilités n'étaient que peu nombreuses il y a encore quelques années, beaucoup de directives relatives au signalement des vulnérabilités ont aujourd'hui été publiées et des programmes de primes aux bogues sont mis en place. Les bases stratégiques et juridiques ainsi que l'état de la mise en œuvre des mesures de promotion du piratage éthique en Suisse sont décrits ci-après.

4.1 Bases stratégiques et juridiques de la promotion du piratage éthique

Les bases stratégiques et juridiques révèlent aussi comment la promotion du piratage éthique s'est établie en Suisse. Si les deux cyberstratégies nationales de 2012-2017 et 2018-2022 ne contiennent aucune mesure de gestion des vulnérabilités, la cyberstratégie actuelle définit, par sa mesure 5 «Identifier les vulnérabilités et y remédier», diverses étapes d'amélioration des conditions du piratage éthique. Cette mesure demande que soient établis des programmes de divulgation coordonnée des vulnérabilités. Il ne s'agit pas à cet égard de subventionner le piratage éthique, mais d'améliorer ses conditions-cadres et d'élaborer des outils. Concrètement, des directives doivent être définies et mises en œuvre, le NCSC assumant un rôle essentiel de coordination des processus de divulgation. Le piratage éthique doit être institutionnalisé par la réalisation de programmes dédiés (par ex. primes aux bogues) de manière que la sécurité juridique soit améliorée dans ce domaine[20].
Les bases juridiques suivent une évolution semblable. La révision de la loi sur la sécurité de l'information (LSI) adoptée le 29 septembre 2023[21], qui instaure une obligation de signaler les cyberattaques contre les infrastructures critiques, jette les bases légales de la coordination de la divulgation des vulnérabilités par le NCSC[22]. Le futur art. 73*b*, al. 3, LSI prévoit que si le NCSC prend connaissance d'une vulnérabilité, il en informe immédiatement le fabricant du matériel informatique ou du logiciel concerné et lui fixe un délai approprié pour l'éliminer. Le fabricant est alors tenu de prendre des mesures. S'il ne le fait pas, le NCSC est autorisé à publier la vulnérabilité en nommant le produit concerné. En outre, le projet prévoit de compléter la loi fédérale du 21 juin 2019 sur les marchés

17 OCDE, Encouraging vulnerability treatment: Overview for policy makers, documents de travail de l'OCDE sur l'économie numérique, nº 307, février 2021 (consultable à l'adresse: https://www.oecd-ilibrary.org/science-and-technology/encouraging-vulnerability-treatment_0e2615ba-en?mlang=fr)
18 Conseil de l'Europe, détails du traité nº 185, Convention sur la cybercriminalité (STE nº 185) (consultable à l'adresse: https://www.coe.int/fr/web/conventions/full-list?module=treaty-detail&treatynum=185)
19 Office des Nations Unies contre la drogue et le crime, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (les procès-verbaux de sessions et de consultations intersessions sont consultables à l'adresse: https://www.unodc.org/unodc/fr/cybercrime/ad_hoc_committee/home)
20 Rapport du Conseil fédéral suisse, CSN d'avril 2023, p. 20 (consultable à l'adresse: https://www.newsd.admin.ch/newsd/message/attachments/76794.pdf)
21 Loi fédérale sur la sécurité de l'information au sein de la Confédération (LSI; RS 128)
22 Cf. à cet égard également le communiqué du Conseil fédéral du 8 novembre 2023 (consultable à l'adresse: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-98497.html).

publics[23] de sorte que la non-observation du délai fixé par le NCSC pour éliminer les vulnérabilités puisse, lors d'une procédure de marché public, conduire à l'exclusion de la procédure ou à la révocation de l'adjudication et que le NCSC puisse publier la vulnérabilité à l'échéance du délai[24].
Ces dispositions de la LSI révisée constituent la base permettant au NCSC d'assumer un rôle actif dans la promotion du piratage éthique. La possibilité juridique de signaler une vulnérabilité au NCSC, qui dispose d'instruments pour imposer une réaction au fabricant, crée pour les pirates une incitation à communiquer les failles de sécurité. Cependant, la loi ne prévoit pas elle-même une rémunération pour de tels signalements et elle n'oblige pas les entreprises à coopérer avec eux.
Les systèmes de vote électronique représentent un cas spécial. L'art. 27*l*ter de l'ordonnance sur les droits politiques[25] prévoit que «les cantons encouragent notamment la participation du public et des milieux spécialisés à l'amélioration des systèmes de vote électronique». Cette disposition instaure la base juridique nécessaire à l'exécution de tests publics de sécurité et de programmes de primes aux bogues pour les systèmes de vote électronique.

4.2 Mise en œuvre de mesures à la Confédération

La Confédération met en œuvre diverses mesures visant à promouvoir le piratage éthique. Conformément aux bases juridiques, elle a positionné le NCSC comme service de contact pour le signalement des vulnérabilités de manière à promouvoir la divulgation coordonnée de celles-ci. À cet effet, le NCSC publie des directives sur le signalement. En outre, la Confédération a également réalisé certains tests publics de sécurité et elle met en œuvre un programme de primes aux bogues pour l'administration fédérale. Concernant cette dernière, le Conseil fédéral habilite, dans l'ordonnance sur la sécurité de l'information (art. 43, al. 1, let. c, OSI) qui entrera en vigueur le 1er janvier 2024, le NCSC (et donc le futur Office fédéral de la cybersécurité), d'entente avec les services compétents, à rechercher des vulnérabilités. Le NCSC est explicitement autorisé à charger des tiers de cette tâche.

4.2.1 Signalement de vulnérabilités

Le NCSC dispose depuis mars 2021 d'une directive sur le signalement de vulnérabilités[26]. La clarification des possibilités de contact et de signalement est l'élément clé de cette directive. Le NCSC met à disposition sur son site Internet un formulaire de notification des vulnérabilités. Il définit en outre dans ses directives et conditions-cadres relatives au signalement des vulnérabilités quelle procédure est exigée des pirates dans la gestion des failles et ce qu'ils peuvent attendre en retour du NCSC.
Les directives en question doivent être remplies pour que le NCSC puisse assumer un rôle de coordination et par exemple clarifier, entre les pirates qui souhaitent rester anonymes et les entreprises concernées, la marche à suivre concernant la publication des failles.
La première condition pour les pirates est de n'utiliser et de ne documenter la faille qu'à titre de preuve: ils ne tenteront pas d'obtenir des privilèges dans des systèmes étrangers. La directive établit également la procédure à suivre pour publier une vulnérabilité. Le NCSC s'oblige pour sa part à assurer la coordination et, si la vulnérabilité concerne un système de l'administration fédérale, à proposer une solution dans les 60 jours.
Par ailleurs, le NCSC a déployé la norme security.txt sur les sites Internet centraux de l'administration fédérale[27]. Cette norme Internet permet à une organisation ou à une entreprise de publier son contact

[23] LMP; RS **172.056.1**
[24] Message relatif à la modification de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), FF **2023** 84, 27
[25] RS **161.11**
[26] NCSC, Annonce d'une faille ou divulgation coordonnée d'une vulnérabilité (Coordinated Vulnerability Disclosure, CVD) (consultable à l'adresse: https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden.html)
[27] Consultable à l'adresse: https://www.ncsc.admin.ch/.well-known/security.txt

de sécurité et sa procédure de signalement de manière uniforme sur Internet, de sorte qu'on les trouve plus rapidement[28].
À la réception d'un signalement, le NCSC contrôle la vulnérabilité signalée et lui attribue un identificateur s'il s'agit d'une faille nouvellement décelée. À cet effet, le NCSC participe au réseau mondial du «Common Vulnerability and Exposures Programm». Ce programme repose sur une systématique selon laquelle les vulnérabilités sont numérotées pour être identifiées sans ambiguïté et intégrées dans le catalogue CVE. Depuis son adhésion au réseau CVE, le NCSC a attribué un numéro CVE à 41 vulnérabilités qu'il a ensuite publiées[29]. La plupart de ces failles ont été signalées au NCSC par des chercheurs dans le cadre de la procédure CVD.
Il est aussi possible de signaler les vulnérabilités à d'autres acteurs de l'administration fédérale que le NCSC. Fondamentalement, il faut toujours les signaler aux services concernés par la vulnérabilité en question. S'agissant de failles relevant de la loi sur la protection des données[30], leurs signalements peuvent être adressés au Préposé fédéral à la protection des données et à la transparence (PFPDT). Celui-ci a résumé dans une feuille d'information les dispositions liées au droit de la protection des données à respecter dans le cadre du piratage éthique[31]. Dans la feuille d'information, le PFPDT note aussi clairement que les failles ne doivent pas nécessairement lui être signalées et qu'une telle procédure n'est pas non plus spécifiquement prévue. Le PFPDT n'est pas censé assurer la coordination de la publication des failles. Mais en cas de signalement, il peut engager une enquête et coopérer avec le NCSC en vue d'une publication coordonnée.

4.2.2 Tests publics de sécurité

Les tests publics de sécurité sont surtout menés lorsqu'une transparence maximale en matière de sécurité doit être fournie dès le début d'un projet. Cette situation s'est présentée en 2021 lors de l'introduction d'un certificat COVID. Le NCSC a mené un test public de sécurité de l'ensemble des applications liées à l'émission et à la vérification de ce certificat. À cet effet, il a commencé par définir le cadre et les règles de ce test[32], puis il a publié le code source des applications développées pour que les chercheurs les testent et puissent signaler les failles au NCSC au moyen d'un formulaire de contact spécifique.
Les résultats ont été concluants. De nombreux chercheurs en cybersécurité et des pirates ont participé aux tests. Ils ont identifié 136 failles au total. Le NCSC a publié sur son site Internet toutes les vulnérabilités ainsi mises en évidence.
Vu le succès rencontré par ce test public de sécurité en lien avec le certificat COVID, le NCSC en a également organisé un pour le système de traçage de proximité de SwissCovid. Le 9 juin 2021, le NCSC mettait à la disposition du public le cadre et les règles du test ainsi que le code source de l'application complémentaire, afin que les chercheurs puissent la tester et lui en signaler les failles par un formulaire de contact spécifique. Ce test, lui aussi fructueux, a permis le lancement de l'application SwissCovid avec le système de traçage de proximité.

4.2.3 Organisation d'hackathons pour rechercher des vulnérabilités

Le Cyber Defence Campus (CYD Campus) d'armasuisse Science et technologies organise régulièrement des hackathons pour rechercher des vulnérabilités dans des systèmes sélectionnés particulièrement importants pour la sécurité de la Suisse. Issu de «hacking» et «marathon», le mot-valise «hackathon» désigne un événement lors duquel des solutions communes à un problème

[28] NCSC, Security.txt – Enregistrez un contact de sécurité sur votre site Internet (consultable à l'adresse: https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html)
[29] NCSC, Annonces reçues, vulnérabilités (consultable à l'adresse: https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/advisories.html)
[30] Loi fédérale sur la protection des données (LPD; RS **235.1**)
[31] PFPDT, White Hat Hacker: leur situation juridique, les risques qu'ils prennent et le rôle du PFPDT, 27 juin 2023 (consultable à l'adresse: https://www.edoeb.admin.ch/dam/edoeb/fr/Dokumente/datenschutz/MERKBLATT%20White%20Hat%20Hacker%20FR.pdf.download.pdf/MERKBLATT%20White%20Hat%20Hacker%20FR.pdf)
[32] NCSC, Cadre (scope) et règles (rules of engagement) du test public de sécurité (consultable à l'adresse: https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/covid-certificate-pst/scope_and_rules.html)

technique sont recherchées. Le CYD Campus a mis cet instrument en place depuis 2019 en vue de rechercher de manière ciblée des vulnérabilités dans des systèmes de contrôle industriels (Industrial Control Systems), des voitures, des infrastructures de recharge ou des systèmes de communication par satellite. Des spécialistes du campus, de l'armée, du NCSC, des hautes écoles et du secteur économique s'engagent à cette fin. L'événement permet de détecter des vulnérabilités critiques dans les systèmes[33].

4.2.4 Chasse aux bogues de la Confédération

Du 10 au 21 mai 2021, le NCSC a mené le premier programme de primes aux bogues pour l'administration fédérale, en collaboration avec la société Bug Bounty Switzerland SA, le Département fédéral des affaires étrangères (DFAE) et les Services du Parlement (SP)[34]. L'objectif de ce projet pilote était de clarifier si le lancement d'un tel programme serait réalisable pour les systèmes de l'administration fédérale et de déterminer ses avantages et inconvénients. Quinze pirates ont testé au total six systèmes informatiques du DFAE et des SP.
Dans ce cadre, le NCSC a mis à la disposition de ces pirates des directives qui définissaient des processus clairs de recherche, d'identification et de signalement des failles des systèmes. En outre, les systèmes à examiner concrètement ont été précisés. Pour le reste, les pirates impliqués étaient libres de choisir à quelles méthodes ils recouraient pour détecter les vulnérabilités des systèmes.
Au total, le projet pilote a permis d'identifier dix failles, dont une qualifiée de critique. La rémunération des pirates a atteint 9240 francs au final. Le nombre total de failles signalées était assez faible pour un premier test. Les systèmes testés disposaient en effet déjà d'un niveau élevé de maturité sécuritaire avant le test. Toutefois, le projet a montré que des vulnérabilités peuvent encore être trouvées même dans des systèmes qui ont fait l'objet de contrôles poussés.
En outre, ce projet pilote a montré que les programmes de primes aux bogues fonctionnent très bien pour l'administration publique et qu'ils génèrent une forte valeur ajoutée pour un coût financier relativement faible. Après ce projet pilote, diverses autres unités administratives ont manifesté leur intérêt à participer aux programmes de primes aux bogues auprès du NCSC. Vu les expériences positives réunies et le grand intérêt au sein de l'administration, le NCSC a décidé d'instaurer définitivement les programmes de primes aux bogues dans l'administration fédérale.
Depuis l'automne 2022, le NCSC publie les programmes de la Confédération sur la plateforme de Bug Bounty Switzerland SA[35]. Depuis l'été 2023, le programme de primes aux bogues du NCSC a été élargi et les pirates peuvent rechercher et signaler les failles de tous les systèmes exposés au public de l'administration fédérale centrale. Le NCSC rendra régulièrement compte du déroulement du programme, des failles détectées et des primes versées.

4.2.5 Mise à disposition d'instruments et sensibilisation

La Confédération ne recourt pas au potentiel du piratage éthique uniquement pour améliorer sa propre sécurité, elle encourage aussi son utilisation dans l'économie et la société. Le NCSC a publié sur son site Internet un guide qui aide les entreprises à définir des directives concernant la divulgation de vulnérabilités. Ce document met en lumière ce dont il faut tenir compte lorsque l'on publie des directives relatives au piratage éthique[36]. Ce guide explique l'utilité des directives dans le cadre du piratage éthique et montre comment mettre en pratique les exigences de la norme ISO/IEC 29147:2018-10.

---

33 Office fédéral de l'armement armasuisse, Approche collaborative pour l'élimination des failles de cybersécurité, 27 avril 2023 (consultable à l'adresse: https://www.ar.admin.ch/de/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.detail.news.html/ar-internet/news-2023/news-w-t/ics-hackathon.html)

34 Cf. communiqué Projet pilote de primes aux bogues mené avec succès au sein de l'administration fédérale, du 1er juillet 2021 (consultable à l'adresse: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-84304.html).

35 Cf. communiqué Programme de primes aux bogues pour le système central d'accès de la Confédération eIAM, 18 octobre 2022 (consultable à l'adresse: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-90725.html).

36 NCSC – gestion des vulnérabilités, Divulgation des vulnérabilités: guide à l'usage des organisations et des entreprises, 13 octobre 2022 (consultable à l'adresse: https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/infos-it-spezialisten/Vulnerability_Disclosure_Management-Leitfaden_V1-0-FR.pdf.download.pdf/Vulnerability_Disclosure_Management-Leitfaden_V1-0-FR.pdf)

Le NCSC renseigne aussi en détail sur les étapes nécessaires à la mise en œuvre du projet pilote de programme de primes aux bogues de l'administration fédérale, sur les coûts survenus et sur les effets déployés par le programme. Il montre ainsi aux entreprises intéressées que de tels programmes, réalisés à un coût relativement faible, peuvent déboucher rapidement sur des succès.
Enfin, le NCSC sensibilise aussi, en fonction des groupes cibles, à des mesures de promotion du piratage éthique facilement applicables. C'est ainsi qu'il a organisé au premier trimestre 2023 diverses manifestations sur la cybersécurité destinées aux communes suisses. Lors de ces manifestations, il a montré aux participants comment établir des possibilités de contact pour les pirates éthiques à l'aide de la norme security.txt. Depuis lors, le pourcentage des communes qui recourent à cette norme est passé de 11,5 % (état fin 2022) à 38 % (état septembre 2023). Ce succès montre que la sensibilisation à des mesures faciles à réaliser permet d'obtenir de bons résultats.

4.3 Mise en œuvre dans l'économie

Si le piratage éthique est appelé à contribuer à la sécurité de la Suisse, il ne suffit pas que la Confédération prenne des mesures. Il est déterminant que l'économie applique des mesures correspondantes. Nous présentons ci-après les mesures d'ores et déjà prises par des entreprises, en particulier les entreprises liées à la Confédération que cible le postulat. Pour terminer, nous présentons aussi le développement de l'offre de services dans le domaine du piratage éthique en Suisse.

4.3.1 Mesures des entreprises

Les entreprises ont reconnu le potentiel du piratage éthique et nombre d'entre elles y recourent depuis longtemps déjà. Il n'existe pas à ce jour d'analyse statistique complète sur le nombre d'entreprises qui utilisent des instruments de promotion du piratage éthique ni sur le type d'instruments qu'elles utilisent. Mais les expériences réunies par le NCSC et le fort développement de l'offre au cours des dernières années permettent de conclure que les tests de sécurité sont souvent utilisés, en particulier par les entreprises de taille importante[37]. Ces tests permettent d'exploiter le potentiel du piratage éthique de manière ciblée et clairement limitée dans le temps, ce qui améliore les possibilités de planification des entreprises. Les tests de sécurité font aujourd'hui partie du portefeuille des prestataires en cybersécurité. Ils peuvent être obtenus sans difficulté en fonction des besoins. Étonnamment, de nombreuses entreprises ne publient pas encore de directives sur le signalement et la diffusion des vulnérabilités, ce qui n'exige pourtant pas beaucoup de ressources. Les entreprises ne semblent pas avoir encore suffisamment pris conscience du fait qu'elles peuvent, avec de telles directives, clarifier simplement la situation concernant le piratage éthique. Le NCSC recommande donc à toutes les entreprises d'au moins désigner un contact pour les messages de sécurité. Des mesures simples comme celle-ci renforcent l'échange d'informations, qui est déterminant s'agissant de cybersécurité.

4.3.2 Mise en œuvre dans les entreprises proches de la Confédération

Certaines entreprises proches de la Confédération[38] sont pionnières dans la promotion du piratage éthique. Par exemple, Swisscom exploite depuis 2015 déjà un programme de primes aux bogues[39].

[37] Stefan Hunziker, Armand Portmann, Viviane Trachsel et Fernand Dubler, Cyber Risk Management in grösseren Schweizer Unternehmen, Lucerne 2022 (consultable à l'adresse: https://economiesuisse.ch/sites/default/files/articles/downloads/Cyber%20Risk%20Management%20Studie%202022.pdf)
[38] Sont comprises en l'occurrence les entreprises dont la Confédération est actionnaire majoritaire.
[39] Swisscom, Bug Bounty Programme (consultable à l'adresse: https://github.com/swisscom/bugbounty#5-bug-bounty-programme)

D'autres entreprises proches de la Confédération, comme la Poste[40] ou les CFF[41] disposent de programmes de primes aux bogues. Ces entreprises sont aussi exemplaires en ce qui concerne la publication de directives sur la divulgation coordonnée des vulnérabilités. La Poste[42], Swisscom[43] et les CFF[44] ont publié de telles directives.
Si les deux EPF n'ont pas publié de directives, elles proposent une adresse de contact pour signaler les vulnérabilités ou une possibilité de contact par security.txt. Les autres entreprises proches de la Confédération, comme la majorité écrasante des entreprises, n'ont pas établi de directives concernant la divulgation des failles ni défini un interlocuteur spécifique pour le signalement d'incidents sécuritaires et de vulnérabilités. Elles ne disposent pas davantage d'un programme de primes aux bogues.
La question est de savoir quelles mesures seraient susceptibles de les inciter à encourager davantage le piratage éthique. Il faut tout d'abord noter que, pour beaucoup d'entreprises dépourvues de connaissances techniques spécifiques, il n'était pas simple jusqu'ici d'identifier et de mettre en œuvre les bonnes mesures de promotion du piratage éthique. Mais cette situation s'est fondamentalement améliorée. L'élaboration de directives propres est grandement facilitée grâce aux exemples de directives relatives à la divulgation de vulnérabilités produits par le NCSC ou par d'autres organisations. Les offres de plateformes de primes aux bogues apparues en Suisse ces dernières années permettent aux entreprises de mener de tels programmes à moindre coût. Il y a donc lieu de penser que la promotion du piratage éthique se développera positivement en Suisse, que ce soit au niveau global, dans les administrations ou dans les entreprises proches de la Confédération.
Contrairement à ce qui prévaut pour les organisations de l'administration fédérale centrale, le Conseil fédéral ne peut pas décider pour les entreprises proches de la Confédération s'il leur faut prendre des mesures de promotion du piratage éthique. Il pourrait toutefois user de son influence par l'intermédiaire des représentants de l'État au sein des conseils d'administration ou lors de la définition des objectifs stratégiques s'il devait constater que ces entreprises ne prennent pas de telles mesures malgré les possibilités qui s'offrent à elles désormais. Le financement de programmes d'encouragement du piratage éthique, notamment le financement des rémunérations versées aux pirates, relève de la compétence des entreprises concernées.

4.3.3 Offres de services en lien avec le piratage éthique

L'offre de services liés aux programmes de primes aux bogues s'est fortement développée ces dernières années. Diverses entreprises proposent aujourd'hui des plateformes et des services pour des programmes de primes tant en Suisse qu'à l'étranger. Cette offre facilite la tâche des entreprises qui veulent mener de tels programmes. Nombre de ces programmes ne sont pas accessibles au public, ce qui empêche de constater la fréquence d'utilisation des programmes de primes aux bogues par les entreprises suisses. Il est certain que les conditions d'organisation de tels programmes sont considérablement simplifiées par les prestataires des plateformes suisses. Il y a donc lieu de supposer que cet instrument de promotion du piratage éthique par les entreprises continuera à se développer.
Outre les plateformes de primes aux bogues, le NTC, établi dans le canton de Zoug, fournit aussi une contribution à la promotion du piratage éthique en Suisse. Cet institut contrôle si les produits numériques comportent des failles. Il s'engage ainsi directement en faveur du piratage éthique en coopérant avec les producteurs, les exploitants des systèmes et le NCSC[45].

---

40 La Poste Suisse, Bug bounty Poste: sécuriser le Digital Trust (consultable à l'adresse: https://www.post.ch/fr/notre-profil/responsabilite/bug-bounty-poste)
41 CFF, Bug Bounty program (consultable à l'adresse: https://app.intigriti.com/programs/sbb/sbbglobal/detail)
42 La Poste Suisse, Vulnerability Disclosure Policy (VDP) (consultable à l'adresse: https://vdp.post.ch/p/Information-Security)
43 Swisscom, Bug Bounty Programme, Responsible Disclosure Policy (consultable à l'adresse: https://github.com/swisscom/bugbounty#3-responsible-disclosure-policy)
44 CFF, Vulnerability Disclosure Policy (consultable à l'adresse: https://company.sbb.ch/en/sbb-as-business-partner/services/vulnerability-disclosure-policy.html)
45 Institut national de test pour la cybersécurité, Mandat (consultable à l'adresse: https://fr.ntc.swiss/mandat)

5 Conclusions

Le rapport a montré que la promotion du piratage éthique a grandement progressé en Suisse au cours des dernières années. En instaurant l'obligation de signaler les cyberattaques contre les infrastructures critiques, le Parlement a créé les bases légales de la divulgation coordonnée des vulnérabilités. Un cadre a ainsi été donné à la procédure correcte de signalement des vulnérabilités à la Confédération. Simultanément, de nombreuses initiatives émanant de l'économie privée ont beaucoup fait avancer le piratage éthique en Suisse. Par exemple, les nouvelles plateformes dédiées aux programmes de primes aux bogues facilitent considérablement la réalisation de tels programmes par les entreprises intéressées. L'administration fédérale, qui a mis à exécution ces dernières années de nombreuses mesures visant à encourager le piratage éthique, joue un rôle pionnier en Suisse.
Le piratage éthique est ainsi devenu, au cours des dernières années, un facteur qui a amélioré durablement la cybersécurité dans notre pays et l'améliorera encore à l'avenir. Il représente aujourd'hui un élément clé dans la mise en œuvre de la mesure 5 de la cyberstratégie nationale, «Identifier les vulnérabilités et y remédier». Il y a lieu de penser que la tendance à l'utilisation accrue du piratage éthique s'amplifiera encore ces prochaines années. Plus le succès de ces programmes sera patent, plus les entreprises et les organisations seront nombreuses à utiliser les instruments disponibles.
La Confédération continuera de soutenir cette évolution: le NCSC et donc le futur Office fédéral de la cybersécurité jouera un rôle actif dans la coordination de la divulgation des vulnérabilités, l'administration elle-même continuera d'élargir l'application de mesures visant à promouvoir le piratage éthique et la Confédération encouragera le secteur de l'économie à réaliser de telles mesures en lui montrant le potentiel qu'elles recèlent.
Compte tenu de l'évolution positive, l'État n'a pas besoin d'intervenir directement en adoptant des mesures réglementaires pour promouvoir le piratage éthique, par exemple en obligeant les entreprises à mettre en œuvre des mesures à cette fin. De telles interventions pourraient au contraire s'avérer contreproductives si elles compliquaient les interactions entre pirates éthiques et entreprises par des exigences formelles. Les mesures mentionnées dans le présent rapport peuvent être mises en œuvre de manière à respecter le cadre du droit pénal. Il est notamment essentiel qu'elles reposent sur une demande ou au moins sur l'accord des propriétaires du système concerné. Comme nous l'avons vu, les mesures déjà en place ont encore du potentiel. Il n'est par conséquent pas nécessaire à l'heure actuelle de modifier le droit pénal pour renforcer davantage le piratage éthique. Mais il est clair que tous les acteurs impliqués doivent consentir à des efforts supplémentaires pour que le recours au piratage éthique continue d'améliorer la cybersécurité. Il est décisif que les failles signalées soient effectivement comblées. Malheureusement, les délais sont souvent trop longs jusqu'à ce qu'une faille connue soit supprimée chez le client final, même lorsque le fabricant met à disposition un correctif de sécurité[46]. Si une vulnérabilité n'est pas supprimée, il n'est pas vraiment utile que des pirates éthiques l'aient décelée et signalée correctement auparavant selon un processus de divulgation coordonnée. En outre, les pirates risquent de perdre leur motivation à rechercher et signaler des failles.
Par ailleurs, les échanges concernant les vulnérabilités peuvent être encore beaucoup améliorés. Lors de sa discussion sur l'instauration d'une obligation de signaler les cyberattaques contre les infrastructures critiques, le Parlement a aussi débattu de l'introduction d'une obligation générale de signaler les vulnérabilités. Il s'y est finalement refusé. L'un des arguments a été qu'il fallait d'abord encourager les échanges volontaires au sujet des vulnérabilités[47]. Ces échanges gagneront encore en importance avec la promotion du piratage éthique. Lorsque le piratage éthique permet de déceler dans une entreprise des vulnérabilités inconnues jusque-là, il peut être utile à toutes les autres entreprises concernées d'être informées sur ces failles. Le NCSC œuvrera avec les entreprises et les

[46] Cf. NCSC, communiqué Il est grand temps de combler les failles de sécurité de Microsoft Exchange Server, 16 février 2022 (consultable à l'adresse: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/schwachstelle-exchange-server.html).
[47] 22.073 | Loi sur la sécurité de l'information. Modification (Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques) | Objet | Le Parlement suisse

organisations, et plus particulièrement avec les exploitants d’infrastructures critiques, à intensifier ces échanges d’informations.
Pour terminer, nous constatons que l’évolution du piratage éthique en Suisse est de bon augure. Les conditions sont réunies pour que le potentiel important du piratage éthique soit mieux exploité à l’avenir. Si cet objectif est atteint, il est probable que la prévention contre les cyberattaques soit nettement améliorée et que les pouvoirs publics ainsi que les entreprises puissent nettement mieux se protéger qu’aujourd’hui.