walderwyss attorneys at law

Walder Wyss Ltd.
Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

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

Executive Summary

Michael Isler
Partner
Dr. iur.
Attorney at Law
Direct +41 58 658 55 15
michael.isler@walderwyss.com

Oliver Kunz
Partner
lic. iur., LL.M.
Attorney at Law
Direct +41 58 658 56 41
oliver.kunz@walderwyss.com

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

to	National Test Institute for Cybersecurity (NTC)
from	Michael Isler, Oliver Kunz, Gina Moll
re	**Criminal liability of “ethical hacking”**
Date	26 June 2023

1. Executive Summary

1.1. Facts and subject of the commissioned expert opinion

1 The National Test Institute for Cybersecurity NTC uses vulnerability analyses to test digital products and networked infrastructures (systems) for their cybersecurity. Some of the analyses are carried out as commissioned projects with the prior consent of system operators and some projects are not commissioned, i.e. they are carried out on the NTC's own initiative, without necessarily obtaining prior consent ("initiative projects"). As part of its initiative projects, the NTC examines digital products and infrastructures that are not, or not adequately, assessed. In doing so, the NTC aims to increase cybersecurity in the interest of system users and the general public.

2 As a publicly-funded non-profit organisation, the NTC does not pursue any financial interests and does not seek to promote itself. Specifically, the NTC focuses on socially relevant systems (i.e., particularly on systems that are widespread, critical, official and to which there are no alternatives) which appear to be at risk based on objective signs, e.g., because there are signs that a target system has security gaps.

3 In carrying out vulnerability analyses, the NTC complies with the best practice rules laid down by the National Cyber Security Centre (NCSC).

4 Based on its *Vulnerability Disclosure Policy*, the NTC intends to appropriately communicate findings arrived at from its initiative projects to manufacturers and operators of target systems and subsequently publish them in an

appropriate manner so that wider society, the population, public authorities and academia can benefit.

5 The way initiative projects are structured as uncommissioned projects raises a number of questions with regard to possible criminal liability under Swiss (cyber-)criminal law.

1.2. Criminal liability pursuant to Article CrimC 143bis and CrimC Article 144bis(1)

6 The performance of vulnerability analyses – insofar as they involve the (attempted or actual) gaining of access to a third-party data-processing system (penetration tests) – may constitute a hacking offence pursuant to CrimC Article 143bis(1). Accordingly, "any person who obtains unauthorised access by means of data transmission equipment to a data processing system that has been specially secured to prevent their access" is liable to prosecution. The statutory definition of the offence is met regardless of the motivation for carrying out the act. This offence generally seeks to protect data processing systems against unauthorised access. The protected legal interest in this case is "computer freedom", i.e. the freedom of the rightful owner to decide to whom they grant access to their secured data-processing system and the data stored thereon.

7 Since, in the case of initiative projects, attempts are made, *inter alia* by way of penetration tests, to investigate any issues in the security structure of a target system without the consent of the holders of the protected legal interest and thus without authorisation, there is a risk of criminal liability. The attempt to gain access is also punishable as soon as the act goes beyond any preparatory acts that are not punishable (such as exploring a potential target system by way of port scans).

8 The publication of the findings of initiative projects does not pose an issue pursuant to CrimC Article 143bis(2) (which punishes the provision of data that can be used to commit an offence under CrimC Article 143bis(1)) if the published security gap has already been fully eliminated prior to publication. A coordinated approach with the operator of the target system in question in terms of timing can therefore completely rule out any criminal liability under CrimC Article 143bis(2). However, if the vulnerability created by a security gap has not yet been (or not fully) eliminated prior to publication of the technical details, the risk of criminal liability can only be minimised by a lower degree of detail in the publication. In such cases, in particular, no specific details of a possible exploit should be published and the technical description of the security gap should be limited to the information necessary to enable affected users to take appropriate protective measures. Under CrimC Article 143bis(2),

filing a report with an authority such as the NCSC would also not pose an issue in terms of criminal law in such cases.

9 In light of the possible criminal liability for damage to data under CrimC Article 144bis(1), when carrying out vulnerability analyses, any temporary data manipulation (for example, in order to overcome a security mechanism) should only be carried out with the minimum possible intensity of interference and for a short period of time since this act might otherwise amount to a relevant alteration of data for purposes of this criminal offence (for example, temporarily modified passwords or similar must be reset immediately). An additional risk of criminal liability also exists in connection with the reckless (*dolus eventualis*) commission of CrimC Articles 144bis(1), for example, if a technically risky act is carried out in the acceptance that damage to data may occur (for example, the temporary or persistent unavailability of data). However, criminal liability under CrimC Article 144bis(2) (disseminating programs used for causing damage to data) can be ruled out in the context of initiative projects.

1.3. Legitimate act in a situation of necessity pursuant to CrimC Article 17

10 In exceptional circumstances, conduct that falls within the definition of an offence might not be illegal and thus might not be punished. This is particularly the case if the perpetrator can invoke the criminal law justification of a "situation of necessity" pursuant to CrimC Article 17.

11 This is the case when the act that falls within the definition of an offence was carried out in order to save the perpetrator's own legal interest or that of a third party from immediate danger that is not otherwise avertable. Conduct (that is generally punishable) is lawful in exceptional cases if the person relying on this justification thereby protects interests of a higher value.

12 The specific prerequisites for a justification of "situation of necessity" are the existence of (i) an immediate threat to an individual legal interest (e.g. the individual freedom of "computer freedom"), (ii) absolute subsidiarity (i.e. the act must be the mildest possible means of averting the threat), and (iii) a positive weighing-up of interests. Subjectively, the prerequisite is that (iv) the person relying on the justification must be aware of the threat and must act in order to save the threatened legal interest.

13 If a penetration test is carried out to avert a threat to the integrity and security of the corresponding system (particularly because there are specific signs that it is affected by potential security gaps which also make malicious access possible), the system in question can be potentially attacked at any time. In those circumstances, there is an immediate threat to individual rights (namely the "computer freedom" of the persons entitled to the legally-protected

interest) which is required in order to rely on the justification of "situation of necessity". The immediacy of the threat in the case of threatened data-processing systems arises from the long-term threat which may result in damage at any time (e.g. malicious hacker attack, damage to data, data loss, etc.) (known as a perpetual threat).

14 In the event of a "situation of necessity", the means employed must be appropriate to avert the threat and they must also be the least restrictive, i.e. the means least detrimental to other people's legal interests (absolute subsidiarity).

15 Initiative projects are compatible with the principle of absolute subsidiarity if the interference is limited to identifying the existing security gaps, documenting them and subsequently making them known to the operators of the target systems to allow them to remedy the threat. In addition, it must be impossible or unreasonable to obtain the prior consent of all potential persons entitled to the legally-protected interest. This is particularly the case if target systems are tested, in relation to which it is not possible to identify all persons entitled to the legally-protected interest who may potentially be affected, or where such persons cannot or will not react in an adequate way. In some cases, prior contact (and the associated disclosure of the threat) could even increase the threat that the security gap would be exploited.

16 In view of the above, the weighing-up of interests in the case of initiative projects also leads to a positive result. The seriousness of (controlled) access with a positive purpose (and without any intent to cause damage) in the context of an initiative project falls significantly short of the substantially higher degree of threat to the same legal interest in the event of a malicious hacker attack.

17 It is, of course, significant that the initiative projects must be carried out solely for the purpose of remedying the threat. When pursuing other purposes (e.g. self-promotion, curiosity, let alone obtaining economic advantages), a hacker will not be able to invoke the justification of a "situation of necessity". The overall conclusion is that the justification of a "situation of necessity" pursuant to CrimC Article 17 is suitable to justify any actions that constitute an offence pursuant to CrimC Article 143bis(1) and CrimC Article 144bis(1) in the course of implementing NTC initiative projects.

1.4. Other criminal risks

18 In relation to the other offences under cyber criminal law (in particular, CrimC Article 179^{novies} [obtaining personal data without authorisation] and Article 45c in conjunction with Article 53 of the Swiss Telecommunications Act [infringement of the Telecommunications Act]), the commission of a criminal

act can be prevented by structuring the initiative projects in an adequate manner and implementing the vulnerability analyses accordingly. If, in exceptional cases, action taken by the NTC meets the criteria of the offence then, under certain conditions, a "situation of necessity" may constitute grounds for justification.