walderwyss rechtsanwälte

Walder Wyss AG
Seefeldstrasse 123
Postfach
8034 Zürich
Schweiz

Telefon +41 58 658 58 58
Telefax +41 58 658 59 59
www.walderwyss.com

Executive Summary

an	Nationales Testinstitut für Cybersicherheit (NTC)
von	Michael Isler, Oliver Kunz, Gina Moll
Betreff	**Strafbarkeit von Ethical Hacking**
Datum	20. Juni 2023

Michael Isler
Partner
Dr. iur.
Rechtsanwalt
Direkt +41 58 658 55 15
michael.isler@walderwyss.com

Oliver Kunz
Partner
lic. iur., LL.M.
Rechtsanwalt
Direkt +41 58 658 56 41
oliver.kunz@walderwyss.com

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

1. Executive Summary

1.1. Sachverhalt und gutachterlicher Auftrag

1 Das Nationale Testinstitut für Cybersicherheit NTC testet im Rahmen von Schwachstellenanalysen digitale Produkte und vernetzte Infrastrukturen (Systeme) auf deren Cybersicherheit. Die Analysen erfolgen teilweise als Auftragsprojekte mit entsprechender Einwilligung der Systembetreiber, teilweise als sog. Initiativprojekte, d.h. aus eigener Initiative, ohne dass zwingend eine vorgängige Einwilligung vorliegt. Im Rahmen der Initiativprojekte untersucht das NTC jene digitalen Produkte und Infrastrukturen, die nicht oder nicht ausreichend geprüft werden. Damit bezweckt das NTC die Erhöhung der Cybersicherheit im Interesse der Systemnutzer und der Allgemeinheit.

2 Als öffentlich finanzierte Non-Profit Organisation verfolgt das NTC keine finanziellen Interessen oder Selbstprofilierungszwecke. Konkret fokussiert das NTC auf gesellschaftlich relevante Systeme (d.h. insbesondere weitverbreitete, kritische, alternativlose und behördliche Systeme), welche aufgrund von objektiven Anhaltspunkten als gefährdet erscheinen, z.B. weil Anhaltspunkte dafür bestehen, dass in einem Zielsystem Sicherheitslücken vorhanden sind.

3 Bei der Durchführung der Schwachstellenanalysen hält das NTC die Best-Practice Regeln des Nationalen Zentrums für Cybersicherheit (NCSC) ein.

4 Gestützt auf seine *Vulnerability Disclosure Policy* beabsichtigt das NTC, Erkenntnisse aus Initiativprojekten in angemessener Weise den Herstellern und Betreibern der Zielsysteme zu kommunizieren und in einem späteren Schritt in

geeigneter Form zu veröffentlichen, sodass Gesellschaft, Bevölkerung, Behörden und die Wissenschaft davon profitieren können.

5 Aufgrund der Ausgestaltung von Initiativprojekten als auftragslose Projekte stellen sich verschiedene Fragen in Bezug auf eine mögliche Strafbarkeit unter dem Schweizer (Cyber-)Strafrecht.

1.2. Strafbarkeit nach Art. 143bis StGB und Art. 144bis Abs. 1 StGB

6 Die Durchführung von Schwachstellenanalysen steht – sofern sie das (versuchte oder erfolgte) Eindringen in eine fremde Datenverarbeitungsanlage (Penetrationstests) beinhaltet – in potenziellem Konflikt mit dem Hacker-Tatbestand von Art. 143bis Abs. 1 StGB. Demgemäss wird bestraft, «wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt». Dabei ist es für die Tatbestandsmässigkeit unerheblich, mit welcher Motivation die Tathandlung verübt wird. Der Tatbestand will generell Datenverarbeitungssysteme vor unbefugten Zugriffen schützen. Das geschützte Rechtsgut ist hierbei der «Computerfrieden», also die Freiheit des Berechtigten, darüber zu entscheiden, wem er den Zugang zu seiner gesicherten Datenverarbeitungsanlage und den dort vorhandenen Daten gewährt.

7 Da bei Initiativprojekten unter anderem gezielt über Penetrationstests versucht wird, ohne Einwilligung der Träger des geschützten Rechtsguts und damit unbefugterweise allfällige Lücken im Sicherheitsdispositiv eines Zielsystems auszuforschen, besteht ein Strafbarkeitsrisiko. Strafbar ist auch bereits das versuchte Eindringen, sobald der Bereich der straflosen Vorbereitungshandlungen (etwa das Auskundschaften eines potenziellen Zielsystems durch *Portscans*) überschritten wird.

8 Die Publikation der Erkenntnisse von Initiativprojekten ist unter Art. 143bis Abs. 2 StGB (welcher das Zurverfügungstellen von Daten, die zur Tatbegehung nach Art. 143bis Abs. 1 StGB verwendet werden können, unter Strafe stellt) unproblematisch, sofern die veröffentlichte Sicherheitslücke vor der Publikation bereits vollständig behoben wurde. Ein zeitlich koordiniertes Vorgehen mit dem Betreiber des betroffenen Zielsystems kann also die Strafbarkeit nach Art. 143bis Abs. 2 StGB vollständig ausschliessen. Sofern jedoch die durch eine Sicherheitslücke geschaffene Vulnerabilität vor der Veröffentlichung der technischen Details noch nicht (oder nicht vollständig) geschlossen ist, kann das strafrechtliche Risiko nur über einen tieferen Detailierungsgrad der Publikation minimiert werden. In diesen Fällen sollten insbesondere keine konkreten Details zu einem möglichen *Exploit* publiziert werden und auch der technische Beschrieb der Sicherheitslücke sollte sich auf die Angaben beschränken, welche

nötig sind, damit betroffene Benutzer geeignete Schutzmassnahmen ergreifen können. Unter Art. 143bis Abs. 2 StGB strafrechtlich unproblematisch wäre in solchen Fällen auch die Meldung an eine Behörde, etwa das NCSC.

9 Mit Blick auf die mögliche Strafbarkeit für eine Datenbeschädigung gemäss Art. 144bis Ziff. 1 StGB sind im Rahmen der Schwachstellenanalysen temporäre Datenmanipulationen (etwa zum Zweck des Überwindens eines Sicherheitsdispositivs) nur mit möglichst geringer Eingriffsintensität und kurzer Dauer vorzunehmen, da ansonsten die Erheblichkeit des Veränderns der Daten im Sinne des Tatbestands zu bejahen wäre (so sind etwa temporär veränderte Passwörter o.dgl. umgehend zurückzusetzen). Ein zusätzliches strafrechtliches Risiko besteht auch in Bezug auf eine eventualvorsätzliche Begehung von Art. 144bis Ziff. 1 StGB, etwa dann, wenn durch eine technisch riskante Handlung in Kauf genommen wird, dass es zu einer Datenbeschädigung (z.B. vorübergehende oder anhaltende Unverfügbarkeit von Daten) kommen könnte. Eine Strafbarkeit nach Art. 144bis Ziff. 2 StGB (Verbreitung von Programmen zur Datenbeschädigung) kann im Rahmen von Initiativprojekten hingegen ausgeschlossen werden.

1.3. Rechtfertigender Notstand nach Art. 17 StGB

10 Ein Verhalten, das einen Straftatbestand erfüllt, kann unter besonderen Voraussetzungen ausnahmsweise nicht rechtswidrig und somit straffrei sein. Dies insbesondere dann, wenn sich der tatbestandsmässig Handelnde auf den strafrechtlichen Rechtfertigungsgrund des Notstands nach Art. 17 StGB berufen kann.

11 Ein solcher liegt vor, wenn die tatbestandsmässige Handlung begangen wurde, um ein eigenes oder das Rechtsgut eines Dritten aus einer unmittelbaren, nicht anders abwendbaren Gefahr zu retten. Das (grundsätzlich strafbare) Handeln ist ausnahmsweise rechtmässig, wenn der Notstandsberechtigte dadurch höherwertige Interessen wahrt.

12 Die konkreten Voraussetzungen des rechtfertigenden Notstands sind das Vorliegen einer (i) unmittelbaren Gefahr für ein Individualrechtsgut (z.B. das individuelle Freiheitsrecht des «Computerfriedens»), (ii) absolute Subsidiarität (d.h. die Handlung muss das mildestmögliche Mittel zur Gefahrenabwehr darstellen) sowie (iii) eine positive Interessenabwägung. In subjektiver Hinsicht ist vorausgesetzt, dass (iv) der Notstandsberechtigte die Notstandslage kennen muss und handelt, um das bedrohte Rechtsgut zu retten.

13 Erfolgt ein Penetrationstest zur Abwendung einer Gefahrenlage für die Integrität und Sicherheit des entsprechenden Systems (insbesondere, weil konkrete Anzeichen dafür bestehen, dass dieses von potenziellen Sicherheitslücken betroffen ist, welche auch böswillige Eingriffe ermöglichen),

ist das betroffene System jederzeit potenziell angreifbar. Unter diesen Voraussetzungen liegt die für eine Anrufung eines Notstands erforderliche unmittelbare Gefahr für ein Individualrechtsgut (nämlich den «Computerfrieden» der betroffenen Rechtsgutträger) grundsätzlich vor. Die Unmittelbarkeit der Gefahr ergibt sich bei gefährdeten Datenverarbeitungsanlagen/Systemen aus dem über längere Zeit andauernden gefahrdrohenden Zustand, der jederzeit in einen Schaden (z.B. böswilliger Hackerangriff, Datenbeschädigung, Datenverlust, etc.) umschlagen kann (sog. Dauergefahr).

14 Beim Notstand müssen die angewandten Mittel zur Abwendung der Gefahr geeignet sein, und es muss sich ausserdem um das mildeste, d.h. das die fremden Rechtsgüter am wenigsten beeinträchtigende Mittel handeln (absolute Subsidiarität).

15 Initiativprojekte sind dann mit dem Prinzip der absoluten Subsidiarität konform, wenn sich der Eingriff darauf beschränkt, die vorhandenen Sicherheitslücken aufzudecken, diese zu dokumentieren und hernach den Betreibern der Zielsysteme bekannt zu geben, damit diese den Gefahrenzustand beheben können. Zudem muss es unmöglich oder unzumutbar sein, das vorgängige Einverständnis aller potenzieller Rechtsgutträger einzuholen. Dies ist insbesondere dann der Fall, wenn Zielsysteme getestet werden, bei denen nicht alle potenziell betroffenen Rechtsgutträger abschliessend identifizierbar sind oder adäquat reagieren können und werden. Mitunter könnte die vorgängige Kontaktaufnahme (und die damit verbundene Offenlegung der Gefährdungslage) das Risiko gar erhöhen, dass die Sicherheitslücke ausgenutzt würde.

16 Unter den dargelegten Voraussetzungen fällt auch die Interessenabwägung bei Initiativprojekten positiv aus: Die Schwere des (kontrollierten) Zugriffs mit positiver Zweckorientierung (und ohne Schädigungswille) im Rahmen eines Initiativprojekts tritt im Verhältnis zum wesentlich höheren Grad der Gefahr für dasselbe Rechtsgut bei einem böswilligen Hackerangriff deutlich in den Hintergrund.

17 Relevant ist freilich, dass die Initiativprojekte ausschliesslich zum Zwecke der Behebung der Gefahr durchgeführt werden. Bei der Befolgung anderer Zwecke (z.B. Selbstprofilierung, Neugier oder gar die Erlangung von wirtschaftlichen Vorteilen) wird sich ein Hacker nicht auf den Rechtfertigungsgrund des Notstands berufen können. Insgesamt ergibt sich, dass der Rechtfertigungsgrund des Notstands nach Art. 17 StGB geeignet ist, das allfällige gemäss Art. 143^{bis} Abs. 1 StGB und Art. 144^{bis} Ziff. 1 StGB tatbestandsmässige Handeln im Rahmen der Durchführung von Initiativprojekten des NTC zu rechtfertigen.

1.4. Weitere strafrechtliche Risiken

18 In Bezug auf die übrigen Delikte des Cyberstrafrechts (insbesondere Art. 179^{novies} StGB [unbefugtes Beschaffen von Personendaten] und Art. 45c FMG i.V.m. Art. 53 FMG [Widerhandlung gegen das Fernmeldegesetz]) kann durch eine adäquate Ausgestaltung der Initiativprojekte und eine entsprechende Umsetzung der Schwachstellenanalysen bereits das tatbestandsmässige Handeln vermieden werden. Sollte der Tatbestand ausnahmsweise erfüllt sein, kommt unter gegebenen Voraussetzungen gleichermassen der Notstand als Rechtfertigungsgrund zum Tragen.