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

Rechtsgutachten

an Nationales Testinstitut für Cybersicherheit (NTC)

von Michael Isler, Oliver Kunz und Gina Moll

Betreff **Strafbarkeit von *Ethical Hacking***

Datum 26. 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

Inhaltsverzeichnis

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. 143bis Abs. 1 StGB und Art. 144bis 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.

2. Gutachterlicher Auftrag

19 Das Nationale Testinstitut für Cybersicherheit NTC ist ein privatrechtlicher Non-Profit Verein unter öffentlich-rechtlicher Trägerschaft mit Sitz in Zug. Es führt zum einen Prüfaufträge von Betreibern kritischer Infrastrukturen und Behörden aus. Daneben testet es unter Anwendung festgelegter Kriterien aus eigener Initiative (unaufgefordert) digitale Produkte und vernetzte Infrastrukturen (sog. Schwachstellenanalysen). Die Erkenntnisse von solchen (unaufgeforderten) Schwachstellenanalysen werden den betroffenen Herstellern, Betreibern oder Anbietern mitgeteilt und nach Ablauf einer angemessenen Karenzfrist in angemessener Weise veröffentlicht.

20 Vor diesem Hintergrund hat das NTC Walder Wyss beauftragt, die Zulässigkeit und Risiken solcher Schwachstellenanalysen und der anschliessenden Veröffentlichung gewisser Erkenntnisse unter dem Blickwinkel des schweizerischen Strafrechts einzuschätzen.

21 Das vorliegende Gutachten ist in sechs Teile gegliedert. Kapitel 2 umschreibt den gutachterlichen Auftrag und Kapitel 3 die relevanten Begrifflichkeiten. In Kapitel 4 wird die Tätigkeit und Arbeitsmethodologie des NTC, insbesondere in Bezug auf Initiativprojekte, umschrieben. Die rechtliche Beurteilung folgt in Kapitel 5, wobei einerseits die Tatbestandsmässigkeit nach den einschlägigen Normen des Schweizer (Cyber-)Strafrechts beurteilt wird und andererseits die Rechtfertigung über den Notstand nach Art. 17 StGB abgehandelt wird. Eine Zusammenfassung der Resultate findet sich im Fazit in Kapitel 6 sowie dem Executive Summary in Kapitel 1.

3. Begrifflichkeiten

3.1. Hacking

22 Im Rahmen dieses Gutachtens wird der Begriff *Hacking* für sämtliche Handlungen verwendet, mit denen über eine Netzwerkverbindung von aussen in eine für die eindringende Person nicht freigeschaltete oder frei zugängliche fremde Datenverarbeitungsanlage eingedrungen wird, unabhängig von der zugrundeliegenden Motivation.

3.2. Ethical Hacking

23 Beim *Ethical Hacking* oder *White Hat Hacking* werden mittels oben beschriebener Vorgehensweise Sicherheitslücken aufgespürt mit dem alleinigen Ziel, dass diese geschlossen werden können. Auf diese Weise soll präventiv zum Schutz

vor Cyberattacken beigetragen werden.[1] Zum *Ethical Hacking* gehört die ausführliche Dokumentation des Vorgehens sowie die Kommunikation der Erkenntnisse an die Betreiber, sodass diese allfällig entdeckte Sicherheitslücken beheben können. Wenn die latente Gefahr eines Angriffs gebannt ist, erfolgt in einem zweiten Schritt regelmässig auch eine geeignete Publikation der Erkenntnisse, wodurch andere Betreiber sowie Benutzer für das Thema Informations- und Cybersicherheit sensibilisiert werden. Ein entsprechender öffentlicher Diskurs und das Teilen von Informationen über die Funktionsweisen moderner *Exploits* soll langfristig zur strukturellen Verbesserung von Software- und Hardwaresicherheit beitragen.

3.3. Auftragsprojekte und Initiativprojekte

24 Häufig handeln *Ethical Hacker* im Auftrag des Systembetreibers oder -benutzers (Auftragsprojekte).[2] Es sind jedoch auch auftragslose Formen (Initiativprojekte) verbreitet.

25 Initiativprojekte erfolgen meistens dann, wenn der Hersteller oder Betreiber keine ausreichenden Garantien liefert, dass seine Systeme oder Komponenten gegen unbefugtes Eindringen geschützt sind. Das ist z.B. der Fall, wenn keine unabhängigen Sicherheitsüberprüfungen stattfinden oder die veröffentlichten Resultate nicht vertrauenswürdig sind und niemand bereit ist, für die Allgemeinheit in eine Überprüfung zu investieren und einen entsprechenden Auftrag zu erteilen.

26 Daneben gibt es auch Hacker, die (ohne Beachtung der Grundsätze von *Ethical Hacking*) zur Selbstprofilierung oder mit Bereicherungsabsicht handeln, beispielsweise indem sie für ihre auftragslose Tätigkeit im Nachhinein eine Entschädigung verlangen und die Publikation der Erkenntnisse als Drohmittel einsetzen. Entsprechendes Vorgehen wird im Rahmen dieses Gutachtens nicht unter den Begriff Initiativprojekte subsumiert.

3.4. Daten und Datenverarbeitungsanlage im (Cyber-)Strafrecht

27 Das sogenannte Cyberstrafrecht umfasst als (untechnischer) Sammelbegriff eine Reihe von Tatbeständen des Schweizerischen Strafgesetzbuches (StGB)[3], welche die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie den «Frieden» von Datenverarbeitungsanlagen schützen wollen.

28 Aus den Gesetzesmaterialien zum Cyberstrafrecht ergibt sich, dass der Gesetzgeber sich in diesem Bereich bewusst für die Begriffsbestimmung

---

1 Vgl. auch GERMANN/WICKI-BIRCHLER, Hacking, S. 86.

2 Ibid.

3 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0.

Datenverarbeitungsanlage entschieden hatte, um den fremdsprachigen Begriff *Computer* zu meiden und die beiden Begriffe als Synonyme erachtet.[4] Auf eine Legaldefinition der Begriffe *Daten* und *Datenverarbeitungsanlage* im Strafgesetzbuch wurde allerdings verzichtet. In der Botschaft 1991 findet sich die folgende Definition:[5]

> *«In einem weiteren Sinne verstanden sind **Daten** alle Informationen über einen Sachverhalt in Form von Buchstaben, Zahlen, Zeichen, Zeichnungen u.a., die zur weiteren Verwendung vermittelt, verarbeitet oder aufbewahrt werden. Es können dies Briefe, Telegramme oder Buchhaltungsbelege, aber auch mündliche Mitteilungen sein. Im vorliegenden Zusammenhang kommen als Daten aber nur jene Informationen in Frage, die von einer **Datenverarbeitungsanlage**, einem Computer, verarbeitet, gespeichert und weitergegeben werden. Es sind mithin Informationen, die von einer solchen Anlage mittels der zu ihrem Betriebe gehörenden Programme in nicht direkt visuell erkennbarer, üblicherweise codierter Form entgegengenommen, automatisiert bearbeitet und wieder abgegeben werden. Die heute üblichen Datenverarbeitungsanlagen funktionieren auf der Basis der Elektronik, d.h. die Informationen werden in codierter Form auf magnetisierbare Medien wie Magnetspeicher oder -bänder, Disketten u.ä. übertragen. Man spricht denn auch häufig von elektronischer Datenverarbeitung (EDV). Es ist jedoch ohne weiteres möglich, dass in Zukunft für die Datenverarbeitung auch andere Medien (z.B. solche auf biologischer Basis) verwendet werden können. In der Fachsprache wird heute denn auch oft verallgemeinernd von Datenverarbeitung (oder automatisierter Datenverarbeitung) gesprochen. Der vorliegende Entwurf trägt den möglichen künftigen Entwicklungen in der Computertechnik dadurch Rechnung, dass er regelmässig von elektronisch oder in vergleichbarer Weise gespeicherten Daten oder von elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgängen spricht.»*

[4] Botschaft 1991, 986 f.

[5] Botschaft 1991, 986 f. [Hervorhebungen hinzugefügt].

4. NTC-Framework für Initiativprojekte

4.1. Prozess zur Durchführung von Initiativprojekten

29 Das vorliegende Gutachten widmet sich insbesondere der rechtlichen Beurteilung von Initiativprojekten, wie sie beispielsweise vom NTC durchgeführt werden. Das NTC agiert dabei innerhalb eines vordefinierten Rasters, welches den Prozess zur Auswahl und Durchführung von Initiativprojekten klar definiert und leitet.

30 Bei der Identifikation und Priorisierung möglicher Zielsysteme orientiert sich das NTC an den folgenden Grundsätzen:

(a) Das NTC bezweckt einzig die Erhöhung der Cybersicherheit im Interesse betroffener Systemberechtigter/-nutzer und der Allgemeinheit, insbesondere verfolgt es keine finanziellen Interessen oder Selbstprofilierungszwecke;

(b) Das NTC testet mittels Initiativprojekten Zielsysteme, für die es aus unterschiedlichen Gründen keine Auftraggeber gibt, die mit anderen Worten ansonsten nicht getestet werden;

(c) Zum optimalen Einsatz der beschränkten Ressourcen werden gesellschaftlich relevante Systeme oder Komponenten getestet. Bei der Identifizierung gesellschaftlich relevanter Systeme wendet das NTC die folgenden Aufgreifkriterien an:

(i) **Weitverbreitete Systeme**

Weitverbreitete Systeme oder Komponenten mit einer hohen Anzahl an betroffenen Personen und Unternehmen im Falle einer Kompromittierung (z.B. *Smart Meters* zur Stromverbrauchsmessung, Überwachungskamerasysteme, etc.).

(ii) **Kritische Systeme**

Kritische Infrastrukturen, Systeme oder Komponenten, bei denen im Falle einer Kompromittierung ein erheblicher Schaden für einen relevanten Teil der Gesellschaft droht (z.B. Kommunikationsinfrastruktur von Notrufzentralen).

(iii) **Alternativlose Systeme**

Alternativlose Systeme oder Komponenten, bei denen ein *de-facto* Zwang zur Nutzung besteht. Dies kann beispielsweise aufgrund von gesetzlichen Vorgaben oder einer monopolartigen Stellung des Herstellers der Fall sein (z.B. Zertifikatsapps während einer Pandemie).

(iv) **Behördliche Systeme**

Systeme, welche für Behörden (Bund, Kantone oder Gemeinden) und somit für die Gesellschaft betrieben werden (z.B. Geburtenregister, BAG-Meldeformular für infektiöse Krankheiten, etc.).

(d) Wird ein Zielsystem anhand der obigen Aufgreifkriterien als gesellschaftlich relevant erachtet, entscheidet das NTC anhand des Eingriffskriteriums der potenziellen Gefährdung des Zielsystems, ob das entsprechende System im Rahmen eines Initiativprojekts getestet werden soll. Eine potenzielle Gefährdung wird angenommen, wenn Anhaltspunkte dafür bestehen, dass in einem Zielsystem Sicherheitslücken vorhanden sind. Eine entsprechende Einschätzung gewinnt das NTC aus verschiedenen Vorabklärungen sowie Berichten und Meldungen anderer Stellen (siehe dazu im Detail Rz 162 ff.).

(e) Das NTC hält bei der Durchführung der Schwachstellenanalysen die Best-Practice Regeln des Nationalen Zentrums für Cybersicherheit (NCSC) ein.[6] Insbesondere verzichten die Analysten des NTC darauf, Schwachstellen über das für einen *Proof of Concept* Notwendige hinaus auszunutzen, indem sie etwa Daten herunterladen, ändern oder löschen. Sie verzichten sodann auf den Einsatz von Methoden wie *Brute-Forcing* oder *Social-Engineering*, installieren keine *Malware* oder Viren und führen keine *Denial of Service*-Angriffe durch.

4.2. Vulnerability Disclosure Policy

31 Das NTC beabsichtigt, Erkenntnisse aus Initiativprojekten in angemessener Weise zu kommunizieren und zu veröffentlichen.

32 Mit der Kommunikation an den Hersteller bzw. Betreiber eines Zielsystems wird darauf hingewirkt, dass die entdeckten Sicherheitslücken schnellstmöglich und adäquat behoben werden.

33 Mit der Veröffentlichung wird weiter das Ziel verfolgt, über eine breit angelegte Diskussion von Schwachstellen und *Exploits* langfristig zur strukturellen Verbesserung der Software- und Hardwaresicherheit beizutragen. Der Austausch zwischen den Sicherheitsanalysten und das Teilen von Erkenntnissen kann dazu beitragen, potenzielle angreifbare Komponenten schneller zu identifizieren und

[6] Nationales Zentrum für Cybersicherheit (NCSC): Rahmenbedingungen und Regeln, <www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html> (zuletzt besucht am 25. Juni 2023).

Fehlerquellen zu korrigieren,[7] sowie die Funktionsweisen von modernen *Exploits* frühzeitig zu durchschauen. Bei *Patches*, welche nicht automatisch eingespielt werden, kann eine Veröffentlichung sodann auch wichtig sein, um die Öffentlichkeit und potenziell betroffene Nutzer auf eine Schwachstelle aufmerksam zu machen.

34 Bei der Kommunikation und Veröffentlichung von Erkenntnissen aus unaufgeforderten Schwachstellenanalysen wird grob zwischen vier Arten unterschieden:

(a) *No Disclosure*: Die Resultate werden weder veröffentlicht noch den Betreibern des Zielsystems kommuniziert.

(b) *Private Disclosure*: Die Resultate werden lediglich den Betreibern des Zielsystems kommuniziert.

(c) *Full Disclosure*: Die vollständigen technischen Details der Sicherheitslücke werden veröffentlicht, sobald sie entdeckt werden. Das bedeutet, dass alle Einzelheiten (manchmal auch der *Exploit-Code*) öffentlich zur Verfügung stehen, oft bevor ein *Patch* verfügbar ist.

(d) *Coordinated Disclosure*: Eine erste Meldung erfolgt lediglich an die Betreiber, die vollständigen technischen Details der Sicherheitslücke werden veröffentlicht, sobald ein *Patch* verfügbar ist (manchmal mit einer Verzögerung, um mehr Zeit für die Installation der *Patches* zuzulassen).

35 Die Kommunikation an die betroffenen Betreiber sowie die Veröffentlichung der Erkenntnisse von Initiativprojekten des NTC erfolgt nach den in dessen *Vulnerability Disclosure Policy*[8] festgelegten Kriterien.

36 Das NTC führt in aller Regel eine Veröffentlichung im Sinne eines *Coordinated Disclosure* durch. Für die zeitliche Komponente greift der NTC auf die branchenweite Best-Practice Regelung «90+30-Tage» zurück (vgl. dazu unten Rz 93). Das bedeutet, dass ein Hersteller 90 Tage Zeit hat, nachdem er über eine Sicherheitslücke informiert wurde, um den Nutzern einen *Patch* zur Verfügung zu stellen. Wenn er innerhalb von 90 Tagen einen *Patch* zur Verfügung stellt, werden 30 Tage nach der Bereitstellung des *Patches* für die Nutzer die Erkenntnisse über die Sicherheitslücke veröffentlicht. In Koordination mit dem Hersteller kann im Einzelfall ein längerer oder kürzerer Zeitraum vereinbart werden.

---

7 Dieses Bedürfnis wird auch in der Botschaft zur Änderung des Informationssicherheitsgesetzes (Botschaft 2023, S. 27), genannt in Bezug auf das vorgesehene Recht zur Veröffentlichung von Schwachstellen durch das NCSC: «Die rasche Veröffentlichung einer Schwachstelle mit Nennung der betroffenen Hard- oder Software kann notwendig sein, um weitere Cyberangriffe zu verhindern».

8 Nationales Testinstitut für Cybersicherheit (NTC): Vulnerability Disclosure Policy, <https://www.ntc.swiss/ueber-uns/rechtsdokumente> (zuletzt besucht am 16. Juni 2023).

37 Stellt ein Hersteller innert der 90 Tagen keinen *Patch* zur Verfügung resp. reagiert der Hersteller nicht auf eine Kontaktaufnahme durch das NTC, entscheidet das NTC basierend auf den Grundsätzen seiner *Vulnerability Disclosure Policy*, ob das NTC die Erkenntnisse aus der Schwachstellenanalyse direkt publiziert oder diese an eine öffentliche Stelle meldet. Bei direkter Veröffentlichung wird der Detailierungsgrad der technischen Details in angemessenem Umfang reduziert.

5. Rechtliche Beurteilung

5.1. Rechtlicher Rahmen in der Schweiz

38 *Ethical Hacking* ist in der Schweiz ein Begriff; in der nationalen Cyberstrategie vom April 2023 wird es zum Ziel erklärt, *Ethical Hacking* in der Schweiz zu institutionalisieren, zu fördern und die Rechtssicherheit für *Ethical Hacker* zu verbessern.[9] Bislang ist *Ethical Hacking* in der Schweiz jedoch nicht spezialgesetzlich geregelt. Für die strafrechtliche Beurteilung ist deshalb auf die allgemeinen Bestimmungen des Strafgesetzbuchs zurückzugreifen.

39 In einzelnen Ländern gibt es mittlerweile rechtliche Rahmenbedingungen für *Ethical Hacking*. So hat etwa das *Center for Cyber Security* in Belgien im Frühjahr 2023 einen entsprechenden nationalen *Safe Harbor Framework* erlassen. Darin wird Personen, die Schwachstellen ohne betrügerische oder böswillige Absicht untersuchen und melden, Straffreiheit garantiert, wenn sie gewisse Kriterien einhalten.[10]

5.2. Strafbarkeit nach Art. 143bis StGB

40 Möglichen weiteren Cyberdelikten vorgelagert ist regelmässig ein unbefugtes Eindringen in ein Datenverarbeitungssystem i.S.v. Art. 143bis StGB:

> ***143bis Unbefugtes Eindringen in ein Datenverarbeitungssystem***
>
> *[1] Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*

---

9 Vgl. Nationales Zentrum für Cybersicherheit (NCSC), Nationale Cyberstrategie (NCS) vom April 2023, S. 20, <https://www.newsd.admin.ch/newsd/message/attachments/76793.pdf> (zuletzt besucht am 25. Juni 2023).

10 Vgl. für detaillierte Informationen: Centre for Cyber Security Belgium (CCB): Vulnerability Reporting to the CCB, <ccb.belgium.be/en/vulnerability-reporting-ccb> (zuletzt besucht am 25. Juni 2023).

> [2] *Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*

5.2.1. Entstehung und Normzweck

41 In Art. 143bis StGB wird (in Ergänzung von Art. 143 StGB, der die Datenbeschaffung strafrechtlich verfolgt; vgl. dazu unten Rz 127 ff.) das eigentliche *Hacking*, sprich das *Eindringen* in eine fremde Datenverarbeitungsanlage strafrechtlich erfasst. Der Tatbestand wurde 1995 in das Strafgesetzbuch eingeführt und zuletzt im Rahmen der Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität (CCC)[11] per 1. Januar 2012 revidiert.[12] Der heute gültige Wortlaut stimmt weitgehend mit Art. 2 CCC überein, wobei sich die Schweiz mittels Erklärung nach Art. 40 CCC vorbehalten hat, für die Strafbarkeit das Überwinden einer Zugangssicherung vorauszusetzen.[13]

42 Art. 143bis Abs. 1 StGB schützt die Freiheit des Berechtigten, darüber zu entscheiden, wem er den Zugang zu seiner gesicherten Datenverarbeitungsanlage und den dort vorhandenen Daten gewährt. So ist etwa der Anspruch des Betreibers einer Datenverarbeitungsanlage darauf geschützt, dass sein System als technische Anlage, aber auch die damit abgewickelte Datenverarbeitung und Datenübermittlung ungestört von Eingriffen Unberechtigter betrieben werden kann.[14] Das geschützte Individualrechtsgut ist – analog zum Hausfriedensbruch nach Art. 186 StGB – der «Computerfrieden».[15]

43 Mit Art. 143bis Abs. 2 StGB sind seit der Revision von 2010 überdies ausgewählte Vorbereitungs- bzw. Beihilfehandlungen zum *Hacking* strafrechtlich erfasst, namentlich das Bereitstellen von Hilfsmitteln zur Ausübung der Haupttat. Die Einführung von Art. 143bis Abs. 2 StGB wurde mit der Ratifizierung der CCC erforderlich. Art. 143bis Abs. 2 StGB nimmt dabei die Verbote nach Art. 6 CCC auf, wobei die Schweiz dahingehend eine Einschränkung angebracht hat, als nur das Inverkehrbringen bzw. Zugänglichmachen (und nicht auch der Besitz,

---

11 Übereinkommen des Europarats über die Fälschung von Arzneimitteln und Medizinprodukten und über ähnliche die öffentliche Gesundheit gefährdende Straftaten (Medicrime-Konvention), abgeschlossen in Moskau am 28. Oktober 2011, SR 0.812.41.

12 Botschaft 2010, 4697 ff.

13 Botschaft 2010, 4703.

14 Vgl. auch BGer, Urteil 6B_456/2007 vom 18. März 2008, E. 4.2: «Art. 143bis StGB schützt den Anspruch des Betreibers einer Datenverarbeitungsanlage darauf, dass sein System als technische Anlage, aber auch die damit abgewickelte Datenverarbeitung und Datenübermittlung ungestört von Eingriffen Unberechtigter betrieben werden kann».

15 BGE 130 III 28, E. 4.2; BGer, Urteil 6B_456/2007 vom 18. März 2008, E. 4.1 f.; Wirtschaftsstrafrecht-Graf, S. 1034.

das Einführen und die Herstellung von entsprechenden Mitteln zur Tatbegehung in der Schweiz) strafbar sind.[16]

5.2.2. Tatbestand von Art. 143bis Abs. 1 StGB

5.2.2.1. Objektiver Tatbestand

(a) Fremdes Datenverarbeitungssystem

44 Tatobjekt von Art. 143bis Abs. 1 StGB ist eine *fremde* Datenverarbeitungsanlage. Die Fremdheit orientiert sich dabei nicht primär an den Eigentumsverhältnissen, sondern ist über die Benutzungsberechtigung gegeben.[17] Auch der unautorisierte Zugriff eines Providers in ein von ihm dem Benutzer zur Verfügung gestellten Sub-System kann folglich ein Eingriff in ein *fremdes* System sein.[18]

45 Beim Ermitteln von Schwachstellen ausgewählter Systeme im Rahmen von Initiativprojekten wird die Fremdheit des Systems regelmässig zu bejahen sein. Anders kann es allenfalls sein, wenn Schwachstellenanalysen auf Offline-Kopien oder an Hardware ausgeführt werden (wobei in solchen Fällen zumeist auch kein Zugriff auf dem Weg einer Datenübertragungseinrichtung vorliegt, vgl. dazu Rz 51).

(b) Besondere Sicherung gegen fremden Zugriff

46 Wie bereits erwähnt, erfasst Art. 2 CCC von seinem Wortlaut her jedes Eindringen in ein fremdes Computersystem oder einen Teil davon. Allerdings ist gemäss der Erklärung der Schweiz nach Art. 40 i.V.m. 2 CCC sowie nach Art. 143bis Abs. 1 StGB zusätzlich erforderlich, dass das Datenverarbeitungssystem «gegen [s]einen Zugriff besonders gesichert» ist.

47 Die Anforderungen an eine besondere Sicherung sind nicht hoch anzusetzen; es genügt, wenn sich die Zugangssicherung lediglich an einem (trivialen) Mindeststandard orientiert,[19] auch wenn dieser keine optimale Schutzwirkung erzeugt resp. keinen spezifischen Schutz gegen den konkret eingetretenen Angriff bietet.[20]

48 Art. 143bis Abs. 1 StGB bezieht sich einzig auf das Eindringen *auf dem Wege der Datenübertragungseinrichtung*, weshalb sich der (elektronische bzw. technische) Schutz explizit gegen derartige Zugriffe richten muss. Dabei reicht ein

---

16 Botschaft 2010, 4710; Wirtschaftsstrafrecht-GRAF, S. 1034.

17 Vgl. STRATENWERTH/BOMMER, BT I, S. 352 f.

18 Vgl. SCHMID, Computer, S. 167 N 20 mit Verweis auf S. 116 ff. N 28 ff.; Wirtschaftsstrafrecht-GRAF, S. 1035; auch Appellationsgericht Basel-Stadt, Urteil AG.2021.594 vom 2. November 2021, E. 3.

19 So wäre beispielsweise ein trivialer individueller Passwortschutz i.S.v. «1234» bereits ausreichend.

20 Vgl. etwa Obergericht Bern, Urteil 2007/187 vom 13. November 2007, E. 2b (in: forumpoenale 2008 Nr. 50, 224 ff.); Wirtschaftsstrafrecht-GRAF, S. 1030; BSK StGB-WEISSENBERGER, Art. 143 N 19.

einfacher Passwortschutz oder eine handelsübliche, vorinstallierte Schutzvorrichtung gegen fremden Zugriff (*Firewall*) bereits aus. Einer weitergehenden Verschlüsselung der Daten bedarf es nicht.[21]

Eine besondere Sicherung ist beispielsweise nicht anzunehmen bei *Amazon S3-Buckets*, die falsch konfiguriert sind, sodass die enthaltenen Daten versehentlich öffentlich zugänglich sind. Bei *Amazon S3-Buckets* handelt es sich um Cloud-Container für die Datenspeicherung. *Amazon S3-Buckets* sind mit einer Reihe von Berechtigungs- und Zugriffskontrollmechanismen ausgestattet, dabei kann es bei falsch konfigurierten *Amazon S3-Buckets* vorkommen, dass gewisse Daten öffentlich abrufbar sind. Offene *Buckets* können über unterschiedliche Abrufhandlungen identifiziert werden.[22] Dabei wird in kein besonders geschütztes System eingegriffen, da die Daten resp. das System, auf dem sie gespeichert sind, (versehentlicherweise) öffentlich zugänglich gehalten werden.

Auch Zutrittsberechtigungen, welche sich noch in der generischen Originalkonfiguration befinden, also nicht individualisiert wurden, gelten nicht als besondere Sicherung: Im Jahr 2001 ermöglichte es eine solche generische Originalkonfiguration einem Hacker nach einem erfolgreichen *Portscan*, auf die nicht passwortgeschützte Datenbank des WEF zuzugreifen. Das Verfahren gegen den Hacker wurde vom Untersuchungsrichteramt Bern im Oktober 2002 eingestellt, da das Tatbestandselement der besonderen Sicherung nicht erfüllt war.[23]

49 Gegenstand der Schwachstellenanalysen im Rahmen von Initiativprojekten ist gerade das Aufdecken von allfälligen Lücken im implementierten Sicherheitsdispositiv eines Zielsystems. Da die Anforderungen an die besondere Sicherung äussert gering sind, wird auch dieses Tatbestandsmerkmal bei den in Initiativprojekten getesteten Systemen regelmässig gegeben sein.

---

21 Wirtschaftsstrafrecht-GRAF, S. 1035.

22 Siehe etwa Hacktricks Boitatech: AWS-S3, <hacktricks.boitatech.com.br/pentesting/pentesting-web/buckets/aws-s3> (zuletzt besucht am 25. Juni 2023); Blog Yes We Hack: Abusing S3 Bucket Permissions, <blog.yeswehack.com/yeswerhackers/abusing-s3-bucket-permissions/> (zuletzt besucht am 25. Juni 2023).

23 Zum Ganzen: DOLDER/WÜEST, IT-Recht, S. 433 ff.

(c) Tathandlung: Unbefugtes Eindringen auf dem Wege von Datenübertragungseinrichtungen

(i) Eindringen auf dem Wege von Datenübertragungseinrichtungen

50 Tatbestandsmässig ist das *Eindringen* in das fremde Datenverarbeitungssystem. Damit ist gemeint, dass ein Täter «sich Zugang dazu verschafft, d.h. sich in die Lage bringt, von darin befindlichen Daten Kenntnis zu nehmen, ohne dass ihm eine entsprechende Befugnis zusteht.»[24] In der Lehre ist umstritten, ob das Delikt bereits mit dem Überwinden der ersten[25] oder erst der letzten[26] Zugangsschranke zum ungehinderten Zugriff auf die geschützten Daten vollendet ist. Einigkeit herrscht dahingegen, dass es für die Vollendung irrelevant ist, ob sich der Täter, der sich innerhalb des Datenverarbeitungssystems bewegt, tatsächlich Kenntnis oder unmittelbaren Zugriff auf die dort vorhandenen Daten verschafft hat.[27]

51 Das Eindringen muss auf dem Wege von Datenübertragungseinrichtungen erfolgen, woraus hervorgeht, dass sich der Täter entweder über eine drahtgebundene Linie oder über drahtlose Kanäle der Datenfernübermittlung Eintritt in ein System verschafft.[28]

52 Solange die Tathandlung über einen Datenübermittlungskanal erfolgt,[29] erfasst Art. 143bis Abs. 1 StGB jede erdenkliche Handlung, mit welcher die vorhandene Zugangssicherung ausgeschaltet oder umgangen wird. Beispielweise kann unter Einsetzung technischer Mittel «gewaltsam» eingedrungen werden, etwa beim *Brute-Forcing* zum Ausfindigmachen des Passworts. Auch das Überwinden der Zugangsbeschränkung durch Täuschung oder List ist bereits tatbestandsmässig. Dies geschieht beispielsweise über den Weg des *Social-Engineering*, indem Zugangsdaten beim Datenberechtigten erhältlich gemacht werden, oder wenn eine *Malware* erst durch Zutun des Benutzers in das System eingespeist wird. Diese letzten Varianten instrumentalisieren den Benutzer, welcher als Tatmittler zur Umgehung der Zugangssicherung dient.[30]

53 Nicht erfasst wäre demgegenüber das Ausbauen einer Festplatte eines passwortgeschützten Computers, um sodann von einem anderen System auf die

---

24 DONATSCH et al., StGB, Art. 143 N 3.

25 So etwa SCHMID, Computer, S. 167 f. N 21 und BSK StGB-WEISSENBERGER PHILIPPE, Art. 143bis N 21.

26 So Wirtschaftsstrafrecht-GRAF, S. 1035.

27 SCHMID, Computer, S. 167 f. N 22; Wirtschaftsstrafrecht-GRAF, S. 1035; auch BGE 130 III 28, E. 4.2 wobei eine zivilrechtliche Betrachtungsweise angewendet wird und kein Unterschied gemacht wird zwischen Bereichen innerhalb eines Systems.

28 DONATSCH et al., StGB, Art. 143 N 5.

29 Umstritten ist beispielsweise die Frage, ob nicht schon die Verbindung zwischen der Tastatur eines Terminals und der Zentraleinheit eines Computers eine derartige Einrichtung ist, vgl. STRATENWERTH/BOMMER, BT I, S. 354.

30 Wirtschaftsstrafrecht-GRAF, S. 1036 f.

Daten auf dieser Festplatte zuzugreifen.[31] Ebenfalls nicht erfasst ist das Erforschen von Schwachstellen eines Systems über die Analyse des (allenfalls bekannten) Quellcodes. Solche Analysen können vollständig offline und ohne vorgängigen Kontakt mit dem System erfolgen und setzen typischerweise kein *Eindringen* in das fremde System voraus.

So etwa bei der Analyse der Schweizer Messenger Applikation Threema durch eine ETH-Forschungsgruppe:[32]

Threema, eine Schweizer Alternative zu WhatsApp, Signal, u.Ä., gilt als besonders sicher und wird deshalb seit 2019 beispielsweise auch von der Schweizer Bundesverwaltung genutzt. Ein Forscherteam des Informatik-Departements der ETH Zürich untersuchte Threema und insbesondere die verwendete Verschlüsselung auf Schwachstellen. Dabei identifizierte das Forscherteam anhand ihrer Analyse der Kommunikationsprotokolle sieben Schwachstellen. Die Forschenden fanden dabei insbesondere Probleme im Zusammenhang mit der Authentifizierung und der Verschlüsselung, die es potenziellen Angreifern ermöglichen könnten, Metadaten von Nachrichten zu erhalten, die Zustellung zu verhindern, Konten zu klonen, etc.

Die gesamte Analyse fand ohne ein effektives Eindringen in eine fremde Datenverarbeitungsanlage und nur anhand einer Analyse des Quellcodes bzw. der Kommunikationsprotokolle statt.

(ii) Straflose Vorbereitungshandlungen

54 Vor dem effektiven Eindringen in eine Datenverarbeitungsanlage gibt es eine Reihe von Handlungen, über die ein System ausgekundschaftet werden kann, ohne dass bereits der *Point-of-no-return* nach der Schwellentheorie[33] für einen strafbaren Versuch einer Handlung nach Art. 143bis Abs. 1 StGB überschritten ist.

55 Bei den sogenannten straflosen Vorbereitungshandlungen handelt es sich um Handlungen, die (selbst wenn sie im Vorfeld einer Deliktsbegehung vorgenommen werden) straffrei sind.

56 Im Bereich von Art. 143bis Abs. 1 StGB gilt dies in erster Linie für das Generieren und Abfangen von Datenübermittlungen während des Transports, beispielsweise aktiv über *Portscans* oder passiv über Signalanalysen.[34]

---

31 Vgl. auch Online Kommentar StGB-KOST, Art. 143bis.

32 PATERSON/SCARLATA/TUONG TRUONG, Threema; vgl. auch MÄDER, Verschlüsselung.

33 Vgl. statt vieler: BGE 83 IV 142, E. 1a.

34 Vgl. auch Wirtschaftsstrafrecht-GRAF, S. 1036.

Beim *Portscanning* wird untersucht, welche Ports in einem Zielsystem geöffnet sind und Daten empfangen bzw. senden können. Im selben Prozess können auch Pakete an bestimmte Ports gesendet werden und anhand der Analyse der erhaltenen Antworten (beispielsweise Versionsnummer des Dienstes, Liste der angebotenen Funktionen oder Konfigurationsparameter, etc.) etwaige Schwachstellen ermittelt werden. Vor dem *Portscanning* erfolgt meist ein Netzwerk-Scan, womit eine Liste aktiver Hosts ermittelt wird und diese ihren IP-Adressen zugeordnet werden. Port- und Netzwerk-Scans dienen dazu, die Organisation zwischen IP-Adressen, Hosts und Ports zu identifizieren, um offene oder unsichere Server resp. deren Angriffsflächen zu erkennen. Port- und Netzwerk-Scans können beispielsweise aufzeigen, ob Zugangssicherungen, wie etwa Firewalls, zwischen den Servern und den einzelnen Benutzergeräten, vorhanden sind.

In Bezug auf Art. 143bis StGB Abs. 1 StGB bleibt das *Portscanning* straffrei, da damit lediglich eine Kommunikation mit dem betroffenen System hergestellt, aber nicht in das fragliche System eingedrungen wird.

Noch weniger invasiv als ein *Portscan* ist die Signalanalyse. Dabei werden ohne eine Kommunikation mit dem System die von einer Datenverarbeitungsanlage ausgehenden Signale mit den geeigneten Mitteln aufgezeichnet und ausgewertet. Auf diese Weise können beispielsweise schwache Verschlüsselungen von WLAN-Netzwerken festgestellt werden.

57 Durch die soeben diskutierten Handlungen können im Rahmen von Initiativprojekten im Vorfeld zu einem effektiven Penetrationstest bereits wesentliche Informationen über mögliche Schwachstellen von zu testenden Systemen gewonnen werden. Diese Handlungen bleiben straflos. Sie können jedoch insbesondere für die Beurteilung eines potenziellen Zielsystems von Bedeutung sein, insbesondere kann sich daraus eine Indikation über die potenzielle Gefahr ergeben, welcher ein Zielsystem ausgesetzt ist (vgl. dazu weiter unten Rz 162 ff.).

(iii) Unbefugt: Fehlende Einwilligung als Tatbestandsmerkmal

58 Die Tatbestandmässigkeit fällt dahin, wenn aufgrund der Einwilligung des Berechtigten das Eindringen nicht *unbefugterweise* erfolgt. Die Einwilligung hat somit tatbestandsausschliessenden und nicht bloss rechtfertigenden Charakter.[35]

59 Im Bereich des Cyberstrafrechts ist eine solche Einwilligung etwa im Bereich von *Bug Bounty*-Programmen gegeben. *Bug Bounty*-Programme werden von Unternehmen oder Organisationen ausgeschrieben, wobei für das Entdecken von Schwachstellen in Software, Anwendungen oder Webdiensten meistens

[35] SCHMID, Computer, S. 172 N 33 mit Verweis auf S. 134 N 84.

Prämien in Geld- oder Sachpreisen ausgelobt werden. Ein solches Programm wird in der Schweiz von einer Vielzahl Unternehmen als Teil ihrer Sicherheitsstrategie geführt, darunter auch die Schweizerische Post. Die Post gibt den Teilnehmern des *Bug Bounty*-Programms einen Verhaltenskodex[36] vor, unter dessen Einhaltung sie die Systeme der Post hacken dürfen, wobei sich die Post verpflichtet keine straf- oder zivilrechtlichen Schritte einzuleiten. Eine solches Framework wird oft als *Safe Harbor* bezeichnet.[37] Damit kann von einer impliziten Einwilligung[38] der Post zum allfälligen Eindringen in ihre Datenverarbeitungsanlagen ausgegangen werden, jedenfalls wenn der Verhaltenskodex seitens der *Hacker* eingehalten wird. Das objektive Tatbestandselement des *unbefugten* Eindringens entfällt damit und Art. 143bis Abs. 1 StGB ist nicht erfüllt.

60 Aufgrund des fehlenden externen Auftragsgebers existiert bei Initiativprojekten häufig keine solche Einwilligung. Das Eindringen erfolgt somit *unbefugterweise*.

61 Auch eine nachträgliche Billigung durch eine betroffene Person kann für die Analysten bei Initiativprojekten nur bedingt Abhilfe schaffen: Das Schweizer Strafrecht kennt grundsätzlich keine nachträgliche Genehmigung. Weil die Willenswidrigkeit zum Tatbestand gehört, hat eine Einwilligung vor der Tat zu erfolgen. Eine nachträgliche Billigung der Verletzung hemmt die Strafbarkeit somit nicht.[39] Im Resultat würde eine nachträgliche Billigung in Bezug auf Art. 143bis Abs. 1 StGB jedoch immerhin einem Verzicht auf einen Strafantrag gleichkommen.

62 Diese Lösung ist für die Analysten bei Initiativprojekten nicht zufriedenstellend, da bei einem Verzicht auf den Strafantrag letztlich nicht die Strafbarkeit an sich entfällt, sondern lediglich ein strafrechtlich unzulässiges Verhalten nicht verfolgt wird. Bis zu einem Verzicht bzw. zum Ablauf der Strafantragsfrist von drei Monaten (vgl. Art. 31 StGB; ab Kenntnisnahme der antragsberechtigten Person über die Tat und den Täter) befindet sich eine betroffene Person daher in einem unerwünschten Schwebezustand. Ausserdem kann es gerade bei Tathandlungen nach Art. 143bis Abs. 1 StGB schwierig sein, den Kreis der Strafantragsberechtigten abschliessend festzustellen. So dürfte etwa bei einem unbefugten Zugriff auf eine mandantenfähige Cloud-Anwendung sowohl dem Betreiber wie auch den Nutzern, in deren zugriffsgeschützten Bereich eingedrungen wurde, das Antragsrecht je einzeln zustehen (dazu unten Rz 181 ff.).

---

36 Ein darauf basiertes Beispiel einer *Legal Safe Harbor* Formulierung für *Bug-Bounty* Programme findet sich in: NAFZGER SANDRO, Safe Harbor.

37 Vgl. Schweizerische Post: Swiss Post bug bounty programme, Securing digital trust <www.post.ch/en/about-us/responsibility/swiss-post-bug-bounty?shortcut=bug-bounty> (zuletzt besucht am 25. Juni 2023).

38 Eine Einwilligung kann auch durch konkludentes Handeln abgegeben werde (vgl. Handkommentar StGB-WOHLERS, Vorbemerkungen zu den Art. 14 ff. N 4).

39 Handkommentar StGB-WOHLERS, Vorbemerkungen zu den Art. 14 ff. N 4; so auch BSK StGB-NIGGLI/GÖHLICH, Vor Art. 14 N 19.

63 Auch das Konzept einer mutmasslichen Einwilligung bietet dafür keine Lösung. Eine mutmassliche Einwilligung kann nämlich nur ausnahmsweise unterstellt werden, wo eine Einwilligung zum Zeitpunkt des Eingriffs faktisch nicht eingeholt werden kann, etwa weil die (bekannten) Träger des individuellen Rechtsguts schwer oder nicht erreichbar sind und ein Handlungszwang bzw. eine erhebliche Gefahr bei Aufschub der Handlung besteht.[40]

64 Bei einem Initiativprojekt ist es schwierig, wenn nicht gar unmöglich, im Vorfeld alle potenziell betroffenen Träger von individuellen Rechtsgütern zu identifizieren. Somit könnte nicht für jeden Rechtsgutträger eine mutmassliche Einwilligung antizipiert werden. Auch kann nicht in allen Fällen ohne weiteres angenommen werden, dass die betroffene(n) Person(en) einem Eingriff im Rahmen eines Initiativprojekts aufgrund dessen Zwecks zur Verbesserung der Cyber-Resilienz des Zielsystems zustimmen würde(n), zumal auch Eingriffe im Rahmen von Initiativprojekten für ein Zielsystem nicht nur positive Folgen (insbesondere auf Reputationsseite) haben können. Gibt es Anhaltspunkte für einen entgegengesetzten Willen der Betroffenen, so scheidet eine mutmassliche Einwilligung in jedem Fall aus.[41]

65 Ein Ausschluss der objektiven Strafbarkeit über die mutmassliche Einwilligung ist nach dem Gesagten nur in Ausnahmefällen anzunehmen. *Hacks* im Rahmen von Initiativprojekten geschehen somit i.d.R. *unbefugterweise* und erfüllen das entsprechende Tatbestandsmerkmal nach Art. 143bis Abs. 1 StGB.

5.2.2.2. Subjektiver Tatbestand

66 Art. 143bis Abs. 1 StGB erfordert (Eventual-)Vorsatz. Ein solcher ist nicht gegeben, wenn jemand beispielsweise ungewollt oder irrtümlich in eine Datenverarbeitungsanlage eindringt, selbst wenn er anschliessend vorsätzlich darin verbleibt, zumal das Verbleiben für sich nicht tatbestandsmässig ist.[42]

67 Beim gezielten Versuch, über unterschiedliche Handlungen im Rahmen von Penetrationstest in ein System einzudringen, ist in der Regel ein direkter Vorsatz anzunehmen. Der subjektive Tatbestand von Art. 143bis Abs. 1 StGB ist unweigerlich erfüllt.

68 Unter Schweizer Recht ist unerheblich, mit welcher Motivation in eine fremde Datenverarbeitungsanlage eingedrungen wird.[43] Art. 2 CCC hätte einen entsprechenden Vorbehalt in Bezug auf die subjektive Komponente zugelassen, wobei es den Vertragsparteien vorbehalten blieb «als Voraussetzung vor[zu]sehen,

---

40 BGE 99 IV 208, E. 4; BGE 100 IV 155, E. 4; DONATSCH/TAG, Strafrecht I, S. 268; Handkommentar StGB-WOHLERS, Vorbemerkungen zu den Art. 14 ff. N 10; STRATENWERTH, AT I, S. 236.

41 STRATENWERTH, AT I, S. 237.

42 Wirtschaftsstrafrecht-GRAF, S. 1038.

43 Vgl. SCHMID, Computer, S. 169 N 26.

dass die Straftat […] in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht […], begangen worden sein muss.»[44] Davon hat der Schweizer Gesetzgeber keinen Gebrauch gemacht.[45] Dies erklärt sich vor dem Hintergrund, dass die damals bereits geltende (ursprüngliche) Fassung von Art. 143bis StGB explizit das Eindringen «ohne Bereicherungsabsicht» (in Abgrenzung zu Art. 143 StGB) unter Strafe stellte und beispielsweise auch den bloss aus Neugier handelnden Täter erfassen wollte.[46]

69 Somit handelt sowohl der Analyst im Rahmen von Initiativprojekten als auch ein böswilliger Hacker (welcher allenfalls über eine Tatbegehung nach Art. 143bis Abs. 1 StGB hinaus noch weitere Delikte wie etwa die Datenbeschaffung beabsichtigt) mit Vorsatz, wenn er mit Willen und im Wissen um die Erfüllung des objektiven Tatbestands in eine fremde Datenverarbeitungsanlage eindringt.

5.2.2.3. Zwischenfazit

70 Die Analysten, welche Initiativprojekte durchführen, laufen bei ihrer Tätigkeit regelmässig Gefahr, tatbestandsmässig i.S.v. Art. 143bis Abs. 1 StGB zu handeln. Selbst wenn bei Schwachstellenanalysen das Überwinden der Zugangsschranken zuletzt nicht gelingt, kann zuvor bereits ein strafbarer Versuch nach Art. 143bis Abs. 1 StGB i.V.m. Art. 22 Abs. 1 StGB vorliegen. Die in Rz 54 ff. diskutierten (Vorbereitungs-)Handlungen bleiben straflos.

---

44 Art. 2 CCC.

45 Vgl. Botschaft 2010, 4703; von einem solchen Vorbehalt haben nur wenige Länder Gebrauch gemacht, namentlich die USA, Belgien, Andorra, Chile und die Türkei (vgl. Council of Europe, Treaty Office: Reservations and Declarations for Treaty No. 185 – Convention on Cybercrime, verfügbar unter: <www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0> [zuletzt besucht am 25. Juni 2023]).

46 Vgl. Botschaft 2010, 4703 f. mit Verweis auf den ursprünglichen Willen des Gesetzgebers.

5.2.3. Tatbestand von Art. 143bis Abs. 2 StGB

71 Art. 143bis Abs. 2 StGB stellt das Inverkehrbringen von Passwörtern, Programmen oder anderen Daten, die ein unbefugtes Eindringen in ein Datenverarbeitungssystem ermöglichen, unter Strafe. Somit kriminalisiert diese Bestimmung gewisse Vorbereitungshandlungen zum eigentlichen *Hacking* nach Art. 143bis Abs. 1 StGB, eine effektive Begehung einer Tat nach Art. 143bis Abs. 1 StGB ist hingegen nicht vorausgesetzt.[47] Bezüglich des Besitzes, Einführens und Herstellens von entsprechenden Daten hat die Schweiz zu Art. 6 CCC einen einschränkenden Vorbehalt angebracht.[48]

72 Art. 143bis Abs. 2 StGB ist ein abstraktes Gefährdungsdelikt und wird – im Gegensatz zu Abs. 1 – von Amtes wegen verfolgt.[49]

73 Gemäss der Botschaft ist die Durchführung von Sicherheitstest an Computersystemen, sog. *Vulnerability Assessments* (vorliegend auch als *Schwachstellenanalysen* bezeichnet), sowie die Entwicklung und Zurverfügungstellung neuer Programme zu diesem Zweck nicht strafbar. Diese Straflosigkeit knüpft die Botschaft daran an, dass solche Analysen bei eigenen Systemen oder im Auftrag Dritter durchgeführt werden.[50] Somit gilt keine generelle Straffreiheit im Bereich von Schwachstellenanalysen.

74 Für Analysten bedeutet dies, dass sie mit der Publikation von gewonnen Erkenntnissen aus Initiativprojekten je nach den Umständen das Risiko einer Tatbegehung nach Art. 143bis Abs. 2 StGB auf sich nehmen.

75 Unter welchen Voraussetzungen dies der Fall ist, wird nachfolgend untersucht.

5.2.3.1. Objektiver Tatbestand

(a) Passwörter, Programme oder anderen Daten, die zur Begehung von Straftaten gemäss Art. 143bis Abs. 1 StGB verwendet werden können und sollen

76 Als Tatobjekt gemäss Art. 143bis Abs. 2 StGB kommen Passwörter, Programme (wie beispielsweise Scripts, Codeteile oder Viren) oder andere Daten in Frage, welche objektiv geeignet sind, um damit eine Tathandlung nach Art. 143bis Abs. 1 StGB zu begehen. Mit anderen Worten müssen die entsprechenden Daten einen wesentlichen, kausalen Tatbeitrag zum Eindringen in eine fremde, besonders gesicherte Datenverarbeitungsanlage leisten können.[51] Ein

---

47 BALTISSER, Datenbeschädigung, S. 183.

48 Botschaft 2010, 4710; vgl. auch BALTISSER, Datenbeschädigung, S. 186.

49 BSK StGB-WEISSENBERGER, Art. 143bis N 7 und 46.

50 Vgl. Botschaft 2012, 4710; auch BSK StGB-WEISSENBERGER, Art. 143bis N 43 und DONATSCH, Strafrecht III, S. 208.

51 BSK StGB-WEISSENBERGER, Art. 143bis N 36.

tatsächlicher Einsatz der Daten für eine Handlung nach Abs. 1 ist für die Strafbarkeit nach Abs. 2 nicht erforderlich.[52]

77 Die Geeignetheit ist beispielsweise bei Passwörtern und anderen Zugangsinformationen für einen Server oder einen E-Mail-Account zu bejahen. Auch zu bejahen ist sie bei Verschlüsselungs- bzw. Entschlüsselungssoftware sowie generell bei Daten (beispielsweise in Form von Programmen wie *Malware* oder Anleitungen), mittels welchen eine Vielzahl von Systemen «geknackt» werden könnte, die mit demselben Schutz ausgestattet sind.[53] Eine bloss generische Anleitung zum Erforschen und Beschaffen von Zugangsdaten wäre hingegen nicht geeignet.[54]

78 Eine generelle oder gar konkrete Eignung der Daten ist allerdings noch nicht ausreichend. Es braucht zusätzlich einen objektiv illegalen Verwendungszweck. Dieses Erfordernis lässt sich der Formulierung entnehmen, dass «der Täter weiss oder annehmen muss, dass sie [die Daten] zur Begehung einer strafbaren Handlung gemäss Abs. 1 verwendet werden sollen». Daten oder Programme besitzen per se keinen Zweck, vielmehr wird ihr Verwendungszweck durch die sie nutzenden Personen vorgegeben. Somit kann über einen möglichen delikti-schen Verwendungszweck nur unter Berücksichtigung des Wissens und Willens der betreffenden Personen geurteilt werden.[55]

79 Da die im Rahmen von Initiativprojekten zu publizierenden Daten aus durchgeführten Schwachstellenanalysen und somit regelmässig aus *Hacks* im Sinne von Abs. 1 stammen, ist ein möglicher Verwendungszweck für eben solche Handlungen potenziell gegeben. Selbst wenn die Publikation der Daten Gegenteiliges bewirken soll, nämlich den Schutz vor und die frühzeitige Erkennung möglicher Sicherheitslücken.

80 Beim Kriterium der Eignung ist eine genauere Abgrenzung vorzunehmen:

81 Soweit ersichtlich hat sich das Bundesgericht bislang noch nicht mit dem Kriterium der Eignung nach Art. 143bis Abs. 2 StGB auseinandergesetzt.

In BGE 129 IV 230 setzte sich das Bundesgericht hingegen in Zusammenhang mit Art. 144bis Ziff. 2 StGB[56] unter anderem mit der Frage auseinander, ob eine bruchstückartige Anleitung zur Herstellung von *Malware* den genannten Tatbestand erfüllt. Im Entscheid ging es um die Weitergabe von CD-ROM

52 Ibid., Art. 143bis N 40.

53 Vgl. BSK StGB-Weissenberger, Art. 143bis N 36; auch Botschaft 2010, 4709.

54 Wirtschaftsstrafrecht-Graf, S. 1038.

55 BSK StGB-Weissenberger, Art. 143bis N 37.

56 Gemäss Art. 144bis Ziff. 2 StGB macht sich strafbar, «wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken [Datenbeschädigung] verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt.».

Exemplaren, welche zwar keinen lauffähigen Computervirus, jedoch Anleitungen zur Herstellung von datenschädigenden Programmen beinhalteten. Das Bundesgericht kam entgegen der Auffassung des Beschwerdeführers zum Schluss, dass eine Anleitung nicht alle zur Herstellung eines datenschädigenden Programms nötigen Schritte abzudecken braucht.[57] Es genügt, gemäss Bundesgericht, wenn Informationen zu wesentlichen Herstellungsvorgängen abgegeben werden und dadurch die Herstellung von datenschädigenden Programmen «wesentlich erleichtert wird».[58] Das Bundesgericht leitet dies nicht zuletzt aus den Sprachversionen des Wortlauts von Art. 144bis Ziff. 2 ab, die darauf hindeuten würden, dass das Geben jeglicher (also auch unvollständiger) Angaben, die zur Herstellung von datenschädigenden Programmen nützlich sind, genügt. Somit kommt das Bundesgericht zum Schluss, dass selbst «bruchstückhafte spezifische Anleitungen zur Herstellung von datenschädigenden Programmen von Art. 144bis Ziff. 2 StGB erfasst sind.»[59]

82 Obschon der Wortlaut der Bestimmungen in Art. 144bis Ziff. 2 StGB und Art. 143bis Abs. 2 StGB weitgehend übereinstimmt, ist beachtlich, dass in Art. 144bis Ziff. 2 StGB explizit auch das Geben einer «Anleitung zur Herstellung» von entsprechenden Programmen als Tatvariante genannt wird und sich das Bundesgericht in seinem Urteil explizit darauf bezieht. In Art. 143bis Abs. 2 StGB ist diese Tatvariante nicht genannt. Es ist daher in Bezug auf Art. 143bis Abs. 2 StGB eine weniger weitgreifende Auslegung angemessen.

83 Selbst in Bezug auf den weiterreichenden Wortlaut von Art. 144bis Ziff. 2 StGB wird die Auslegung in BGE 129 IV 230 teilweise als zu umfassend kritisiert.[60] Beide Tatbestände sollten nicht auf Lebenssachverhalte ausgeweitet werden, bei denen es für die Verletzung des Rechtsguts (Integrität resp. Verfügungsfreiheit über die Datenverarbeitungsanlage oder Daten) in entscheidendem Mass darauf ankommt, dass ein Adressat der zugänglich gemachten Informationen über weit überdurchschnittliche Informatikkenntnisse verfügt und eine hohe kriminelle Energie an den Tag legt, um aus den verfügbaren (fragmentierten) Informationen oder Daten ein lauffähiges *Malware*-Programm herzustellen oder in eine fremde Datenverarbeitungsanlage einzudringen.[61]

84 Entscheidend für die Eignung ist nach dem Gesagten insbesondere der Detaillierungsgrad der Publikation. Wird in der Publikation der Prozess zur Überwindung der Sicherung eines Systems anhand der identifizierten Sicherheitslücken im

---

57 BGE 129 IV 230, E. 4.1 f.

58 Ibid, E. 4.1.

59 Ibid, E. 4.2.

60 Vgl. DOLDER/WÜEST, IT-Recht, S. 464 f.; siehe auch BALTISSER, Datenbeschädigung, S. 108, gemäss welcher zu fordern sein wird, dass es sich um Anleitungen zur Herstellung lauffähiger Programme und damit im Minimum um Quelltext handelt, was etwa bei der Abgabe von wenigen Codefragmenten nicht der Fall wäre.

61 Vgl. DOLDER/WÜEST, IT-Recht, S. 464 f.

Sinne einer detaillierten «Anleitung» wiedergegeben, so ist die Eignung grundsätzlich zu bejahen. Bleibt es bei einer generischen Widergabe des Vorgehens oder einem Umschreiben der gewonnenen Erkenntnisse, wobei ein Nachahmer selbst noch erheblichen Mehraufwand für eine Tat nach Art. 143bis Abs. 1 StGB betreiben müsste, so wäre die Eignung zu verneinen.

85 Der Detailierungsgrad einer Publikation im Bereich des *Vulnerability Disclosure* variiert zwischen:[62]

(i) Full Details of Vulnerability + Full Exploit,

(ii) Full Details of Vulnerability + Proof of Concept,

(iii) Full Details of Vulnerability + no Exploit,

(iv) Partial Details of Vulnerability + no Exploit,

(v) Metadata only, no Details of Vulnerability or Exploit.

86 Die Abstufung ist dabei graduell.

87 *Full Exploit* meint das Bereitstellen eines kompletten Programms, Codes, Scripts, oder Plugins für ein *Hacking Tool*, wobei dieses direkt für einen entsprechenden (schädigenden) *Hack* auf eine Datenverarbeitungsanlage einsetzbar ist, ohne dass für einen Dritten ein erheblicher Eigenaufwand notwendig wäre.

88 Die Eignung im Sinne von Art. 143bis Abs. 2 StGB wäre somit bei einer *Full Exploit*-Publikation zu bejahen. Bei der Publikation von Initiativprojekten sollte daher auf eine Veröffentlichung eines *Full Exploits* verzichtet werden.

89 Gleiches gilt für eine Veröffentlichung im Sinne eines *Proof of Concept*. Dort wird anhand einer identifizierten Sicherheitslücke ein *Exploit* technisch dargelegt, allerdings wird er in der Regel auf eine für das Zielsystem unschädliche Funktion reduziert. Die publizierten Daten reichen dabei aber bereits für das schlichte Eindringen in eine Datenverarbeitungsanlage nach Art. 143bis Abs. 1 StGB. Eine Eignung nach Art. 143bis Abs. 2 StGB wäre somit bereits bei einer *Proof of Concept*-Publikation zu bejahen, auch wenn für ein umfassendes Ausnutzen der Sicherheitslücke (beispielsweise im Sinne einer konkreten Instrumentalisierung zum Zweck der unbefugten Datenbeschaffung) bei einer *Proof of Concept*-Publikation ein gewisser Zusatzaufwand nötig wäre.

90 *Full* oder *Partial Details of Vulnerability* bezieht sich sodann auf eine (mehr oder weniger) detaillierte wörtliche Umschreibung der Sicherheitslücke, ein eigentlicher Fehlerbericht, ohne Zurverfügungstellung eines *Exploits* oder Teilen davon. Die Entwicklung eines vollständigen und zuverlässigen *Exploit-Codes* basierend auf einer solchen Information setzt regelmässig qualifizierte technische

---

[62] Google Project Zero: Day 2 Keynote, Project Zero's Disclosure Philosophy, verfügbar unter: https://www.youtube.com/watch?v=9x0ix6Zz4Iw&t=1155s (Min. 19, Sek. 18) (zuletzt besucht 25. Juni 2023).

Fähigkeiten voraus. Potenzielle Angreifer, welche über die Ressourcen und technischen Fähigkeiten verfügen, einen solchen Fehlerbericht in einen zuverlässigen *Exploit-Code* zu wandeln, wären in der Regel unabhängig in der Lage, einen ähnlichen *Exploit* zu erstellen, was mit einem vergleichbaren Aufwand verbunden wäre. Die Eignung im Sinne von Art. 143bis Abs. 2 StGB wäre somit bei einer Publikation mit lediglich *Full* oder *Partial Details of Vulnerability* zu verneinen.

91 Die Eignung ist in jedem Fall auch dann ausgeschlossen, wenn eine aufgedeckte Sicherheitslücke bis zur Publikation der entsprechenden Daten bereits vollständig behoben wurde. Selbst eine detaillierte Publikation wäre nach der Behebung der Sicherheitslücken kein taugliches Mittel für eine Begehung der entsprechenden Handlung nach Art. 143bis Abs. 1 und somit nicht geeignet im Sinne von Abs. 2. Der Tatbestand wäre nicht erfüllt.

92 Um das strafrechtliche Risiko zu minimieren, sollte die Vorlaufzeit zwischen der Erstinformation des betroffenen Zielsystems und der Publikation daher unbedingt so festgesetzt werden, dass eine technische Umsetzung der Behebung der entdeckten Sicherheitslücken (über die Freigabe eines entsprechenden *Patchs*) zeitlich möglich ist.

93 Dem wird in der Branche standardmässig über eine «90+30»-Lösung beim *Vulnerability Disclosure* Rechnung getragen.[63] Demnach wird eine Sicherheitslücke mit einer detaillierten technischen Beschreibung des Problems vorab einzig dem betroffenen Betreiber kommuniziert. Vor jeglicher Veröffentlichung wird dem Betreiber eine Frist von 90 Tagen zur Behebung des Problems belassen. Stellt der Betreiber den Nutzern innert dieser 90 Tagen einen *Patch* zur Verfügung, mit dem die Sicherheitslücke behoben wird, so werden 30 Tage nach Bereitstellung des *Patchs* für die Benutzer die technischen Details über die entsprechende Sicherheitslücke veröffentlicht.[64]

94 Bei der Umsetzung von Initiativprojekten kann dieser Branchenstandard übernommen werden. Da eine Eignung im Sinne von Art. 143bis Abs. 2 StGB im

---

63 Vgl. etwa: CERT-EU: Coordinated Vulnerability Disclosure Policy, <cert.europa.eu/coordinated-vulnerability-disclosure-policy>; European Union Agency for Cybersecurity: Coordinated Vulnerability Disclosure Policies in the EU, April 2022 <https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu>; Google: Google Project Zero Vulnerability Disclosure, <googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html>; UN Office of Information and Communications Technology: United Nations Responsible Disclosure & Reporter Acknowledgment Policy, <unite.un.org/content/united-nations-responsible-disclosure-reporter-acknowledgment-policy>; US Department of Homeland Security: Vulnerability Disclosure Program Policy and Rules of Engagement, <https://www.dhs.gov/publication/vulnerability-disclosure-program-policy-and-rules-engagement>; Open Web Application Security Project (OWASP): Vulnerability Disclosure Cheat Sheet, <cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html> (alle zuletzt besucht am 25. Juni 2023).

64 Vgl. statt vieler Google: Google Project Zero Vulnerability Disclosure, <googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html> (zuletzt besucht am 25. Juni 2023).

Voraus jedenfalls dann entfällt, wenn eine Sicherheitslücke vor der Publikation vollständig behoben wurde, kann die zeitliche Koordination einer Publikation mit den Betreibern des betroffenen Zielsystems für die Analysten insbesondere bei herkömmlichen, zentralisierten Systemen Sicherheit schaffen. Vor diesem Hintergrund ist es sinnvoll, eine gewisse Flexibilität vorzusehen, welche den Betreibern bei Bedarf eine verlängerte Frist für die Behebung komplexerer Fehler einräumt und die Publikation in entsprechender Weise zurückbehalten wird.

95 Die Eignung gemäss Art. 143bis Abs. 2 StGB bleibt demgegenüber grundsätzlich dann bestehen, wenn eine entdeckte Lücke bei der Publikation der technischen Details (noch) nicht (vollständig resp. überall) geschlossen ist. In der Praxis kann dies etwa bei aufgedeckten Sicherheitslücken in verteilten Systemen (z.B. *Client-based* Systemen) der Fall sein, wenn aufgrund der Grosszahl an Nutzern unmöglich abschliessend sichergestellt werden kann, ob ein verfügbarer *Patch* flächendeckend eingespielt wurde. Problematisch ist jedoch auch der Fall, wenn sich ein Betreiber nach erfolgter Information weigert, ein entsprechendes Problem zu beheben. Solche Fälle dürften die Ausnahme bleiben, zumal Hersteller und Betreiber von Zielsystemen daran interessiert sind, eine entdeckte Sicherheitslücke zu schliessen. Gemäss Angaben von *Google Project Zero* liegt der Prozentsatz der bislang entdeckten Sicherheitslücken, welche innert der 90 Tage Frist behoben wurden, bei 96.1%. Nach einer Verlängerung der Behebungsfrist auf individueller Basis wurden gar 97.2% aller entdeckten Sicherheitslücken behoben.[65]

96 Für die strafrechtliche Beurteilung nach Art. 143bis Abs. 2 StGB ist es letztlich nicht entscheidend, ob der Betreiber des Zielsystems einer Veröffentlichung zustimmt oder nicht. Geschützt ist die Integrität des Systems und nicht das (Reputations-) Interesse des Betreibers. Ein Bericht über eine bereits geschlossene Sicherheitslücke verletzt deshalb Art. 143bis Abs. 2 StGB nicht bereits deshalb, weil der Betreiber keine Veröffentlichung wünscht.

97 In den Fällen, in denen eine Sicherheitslücke (noch) nicht (vollständig) geschlossen wurde, kann das strafrechtliche Risikos dadurch minimiert werden, dass bei der Publikation ein tieferer Detailierungsgrad gewählt wird (vgl. Rz 84 ff.). So wird in diesen Fällen davon abgeraten, konkrete Daten zum *Exploit* zu publizieren und im technischen Beschrieb der Sicherheitslücke sollte auf relevante Details für die Umsetzung resp. den Aufbau eines konkreten *Exploits* verzichtet werden. Die Publikation ist im Wesentlichen auf die Information zu beschränken, welche nötig sind, damit sich betroffene Nutzer adäquat vor einem Ausnutzen der festgestellten Sicherheitslücke schützen können.

---

[65] Ibid.

98 Unter Art. 143bis Abs. 2 StGB strafrechtlich unproblematisch wäre es in solchen Fällen auch, wenn nicht die Öffentlichkeit, sondern eine Behörde oder öffentliche Stelle informiert wird. Die Veröffentlichung der Resultate wäre alsdann nicht mehr im Machtbereich des Analysten. Über eine Meldung an das NCSC beispielsweise wäre ein alternativer Zugang zur Öffentlichkeit resp. die Möglichkeit einer Veröffentlichung der Erkenntnisse gesichert. Eine entsprechende Möglichkeit zur Veröffentlichung von Informationen aus Meldungen durch das NCSC ist neu in E-Art. 73c des Bundesgesetzes über die Informationssicherheit beim Bund (ISG) vorgesehen.[66] Der Entwurf sieht vor, dass das NCSC Informationen zu Schwachstellen unter Angabe der betroffenen Hard- oder Software veröffentlichen kann, selbst wenn keine Einwilligung der Hersteller vorliegt und diese die Schwachstelle nicht innert einer angemessenen Frist behoben haben.

99 Bei mangelnder Kooperation eines betroffenen Herstellers oder Betreibers kann die Meldung an das NCSC für das NTC somit eine sinnvolle Alternative zur direkten Veröffentlichung der eigens gewonnen Erkenntnisse von Initiativprojekten sein. Eine solche Meldung kann die gleiche oder eine ähnliche Wirkung haben und allenfalls die Behebung der Sicherheitslücken erreichen.

100 Zu beachten ist allerdings, dass laut Botschaft in Bezug auf eine allfällige Strafbarkeit nach Art. 143bis Abs. 1 StGB für Meldungen von Schwachstellen an das NCSC kein *Legal Safe Harbor* eingeführt werden soll.[67]

101 Die in der *Google Project Zero Vulnerability Disclosure Policy* propagierte Lösung, bei Weigerung des Betreibers einen *Patch* herauszugeben, die identifizierte Sicherheitslücke nicht mehr als sicherheitsrelevant einzustufen und ohne Einschränkung zu veröffentlichen,[68] hätte unter dem schweizerischen Strafrecht keinen Bestand. Insbesondere dann nicht, wenn der Analyst um die Sicherheitsrelevanz des entdeckten Problems weiss und somit vorsätzlich technische Daten, welche im Sinne von Art. 143bis Abs. 1 StGB verwendet werden können, uneingeschränkt veröffentlicht.

102 Die für die Würdigung von Initiativprojekten unter Art. 143bis Abs. 2 StGB entscheidenden Kriterien sind somit der Detaillierungsgrad der Publikation sowie die Vorlaufzeit der Information an die Betreiber des betroffenen Zielsystems

---

66 Der entsprechende Gesetzesentwurf wurde mit der Botschaft zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen) vom 2. Dezember 2022 dem Parlament vorgelegt (Botschaft 2023).

67 Botschaft 2023, S. 26; die Mitarbeitenden des NCSC wären gemäss E-Art. 73d Abs. 3 von ihrer Anzeigepflicht nach Art. 22a Abs. 1 Bundespersonalgesetz vom 24. März 2000, SR 172.220.1, befreit (vgl. Botschaft 2023, S. 8).

68 Google: Google Project Zero Vulnerability Disclosure, <googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html>, (zuletzt besucht am 25. Juni 2023).

vor der Veröffentlichung der entsprechenden Erkenntnisse resp. die Behebung der Sicherheitslücke vor erfolgter Veröffentlichung.[69]

(b) Inverkehrbringen oder Zugänglichmachen

103 Unter Inverkehrbringen oder Zugänglichmachen kann jede Weitergabe entsprechender Daten an einen (unberechtigten) Dritten subsumiert werden, wenn zu erwarten ist, dass dieser dadurch tatsächlich in die Lage versetzt wird, die Daten zu gebrauchen. Das Inverkehrbringen oder Zugänglichmachen der Daten kann durch die Übermittlung von Passwörtern Dritter auf einem Blatt Papier oder durch mündliche Mitteilung tatbestandsmässiger Informationen bzw. Daten, oder aber durch deren Verbreitung im Internet oder über elektronische Mitteilungen erfolgen.[70]

104 Durch die Veröffentlichung von Erkenntnissen aus Initiativprojekten im Internet oder anderen öffentlichkeitswirksamen Kanälen ist dieses Tatbestandsmerkmal unweigerlich erfüllt. Hingegen wäre dieses Tatbestandsmerkmal nicht erfüllt, wenn die Erkenntnisse aus einem Initiativprojekt einzig an eine Behörde, wie etwa NCSC, kommuniziert würden.

5.2.3.2. Subjektiver Tatbestand

105 Die Strafbarkeit nach Art. 143bis Abs. 2 StGB setzt Vorsatz oder Eventualvorsatz voraus. Die Formulierung, wonach der Täter «wissen oder annehmen muss», dass die Daten zur Begehung einer strafbaren Handlung verwendet werden, bedeutet keine Strafbarkeit für eine fahrlässige Begehung, sondern soll lediglich verdeutlichen, dass es ausreicht, wenn dem Täter die Umstände bekannt sind, welche einen deliktischen Gebrauch (nach Abs. 1) der in Verkehr gebrachten Daten nahelegen, er mit anderen Worten eventualvorsätzlich handelt.[71]

106 Der Vorsatz muss sich auf alle Merkmale des Tatbestandes beziehen, also insbesondere auf die oben beschriebene Eignung zur Begehung einer Tathandlung nach Art. 143bis Abs. 1 StGB, auf das in Verkehr bringen oder das Zugänglichmachen der Daten sowie auf die dadurch geschaffene Gefahr, dass ein Dritter diese zur Begehung einer Tathandlung nach Art. 143bis Abs. 1 StGB (Nachfolgehandlung) verwenden könnte. In Bezug auf letztere Voraussetzung ist Eventualvorsatz dann zu bejahen, wenn jemand den Verwendungszweck hätte annehmen sollen, selbst wenn er ihn nicht als sicher betrachtete.[72]

---

69 So auch das Nationale Zentrum für Cybersicherheit: Rahmenbedingungen und Regeln <www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html> (zuletzt besucht am 25. Juni 2023).

70 BSK StGB-Weissenberger, Art. 143bis N 38 mit Verweis auf BSK StGB-Weissenberger, Art. 144bis N 60 ff.

71 Wirtschaftsstrafrecht-Graf, S. 1039.

72 BSK StGB-Weissenberger, Art. 143bis N 43 f.

Im oben bereits thematisierten Entscheid BGE 129 IV 230[73] zu Art. 144bis Ziff. 2 StGB setzt sich das Bundesgericht in den nicht publizierten Erwägungen mit dem dort ebenfalls erforderlichen Eventualvorsatz hinsichtlich der Nachfolgehandlung auseinander:

Das Bundesgericht erläutert mit Verweis auf die Botschaft, dass die Formulierung «weiss oder annehmen muss» dem Hehlerei Tatbestand entnommen wurde. In Anlehnung an die sich daraus entwickelte Rechtsprechung erwägt das Bundesgericht, dass Eventualvorsatz dann vorliegt, wenn sich die «nahe liegende Möglichkeit» einer (bei Art. 144bis Ziff. 2 StGB datenschädigenden, bei Art. 143bis Abs. 2 StGB zum Zweck des Eindringens in eine Datenverarbeitungsanlage) Verwendung der Programme, Viren, Daten, etc. aufdrängt. Bei der Beurteilung verlangt das Bundesgericht eine anhand der konkreten Umstände des Einzelfalls erfolgende sorgfältige Prüfung, massgeblich sind namentlich die Gestaltung der Informationen, die Umstände ihrer Abgabe und der Kreis der Abnehmer.[74]

Im konkreten Fall pries der Beschwerdeführer die CD-ROMs mit den Herstellungsanleitungen für Computerviren im Internet direkt als «Sammlung von Untergrundinformationen» in interessierten Kreisen an und vertrieb diese für einen Verdienst und ohne jegliche Kontrolle über den Gebrauch. Das Bundesgericht schloss mit der Vorinstanz, dass er unter diesen Umständen mit einem Missbrauch habe rechnen müssen oder diesen in Kauf genommen habe, selbst wenn er diesen weder gewünscht noch beabsichtigt habe.[75]

107 Die Botschaft zu Art. 143bis Abs. 2 StGB beschreibt eine Strafbarkeit für das «vorsätzliche Verbreiten von Programmen und anderen Daten sowie das **unverantwortliche Verbreiten** solcher Datensätze, wenn deren sensitiver Inhalt, der Adressatenkreis oder andere Umstände den deliktischen Einsatz der Tools als naheliegend erscheinen lässt. Ein **verantwortungsloses Streuen** von Hacking-Werkzeugen in einem deliktsbereiten Umfeld soll nicht straffrei bleiben.»[76]

108 Vom Zweck, verantwortungsloses Streuen von *Hacker*-Materialien zu pönalisieren, ist die Publikation von Ergebnissen aus Initiativprojekten offenkundig nicht erfasst. Ganz im Gegenteil bezwecken die Publikationen eine Erhöhung der Cybersicherheit und können Bewusstsein für die aufgedeckten oder ähnliche Sicherheitslücken schaffen.

109 Auch wird es bei den Publikationen im Rahmen von Initiativprojekten regelmässig am (Eventual-)Vorsatz in Bezug auf die Eignung zur Begehung einer

[73] Urteil des BGer 6S_499/2002 vom 6. August 2003.
[74] Urteil des BGer 6S_499/2002 vom 6. August 2003, E. 5.3.2.
[75] Urteil des BGer 6S_499/2002 vom 6. August 2003, E. 5.3.3.
[76] Botschaft 2010, 4709 f. [Hervorhebungen hinzugefügt].

Tathandlung nach Art. 143bis Abs. 1 StGB fehlen, da die Erkenntnisse aus den Initiativprojekten wie oben bereits diskutiert mit einer Vorlaufzeit an die Verantwortlichen der betroffenen Systeme kommuniziert werden, sodass bei Publikation grundsätzlich davon ausgegangen werden kann, dass entsprechende Sicherheitslücken bis dahin geschlossen wurden. Dies gilt sicherlich dann, wenn für eine entdeckte Sicherheitslücke ein entsprechender *Patch* verfügbar ist.

110 Der Detailierungsgrad, welcher das NTC für seine zukünftigen Publikationen andenkt, ist zuletzt auch nicht derart ausgestaltet, dass die publizierten Daten ein *Eindringen* nach Art. 143bis Abs. 1 StGB direkt ermöglichen. Vielmehr müssten die publizierten Daten dafür zweckentfremdet bzw. teilweise *reverse-engineered* werden, was gegen einen Eventualvorsatz in Bezug auf mögliche Nachfolgehandlungen spricht. Hier ist beachtlich, dass bei der von der bundesgerichtlichen Rechtsprechung geforderten Einzelfallbeurteilung die individuellen (Informatik-)Kenntnisse der veröffentlichenden Person berücksichtigt werden. Im Resultat handelt ein Spezialist, welcher aufgrund seiner eigenen professionellen Informatikkenntnisse eine mögliche Nachfolgehandlung durch einen Dritten mit ebensolchen professionellen Informatikkenntnissen lückenlos voraussehen kann, bei der Veröffentlichung solcher Daten schneller eventualvorsätzlich als ein Durchschnittsmensch, dem eine solche Beurteilung nicht möglich ist.[77]

5.2.4. Würdigung: Tatbestandsmässiges Verhalten i.S.v. Art 143bis StGB?

111 Bei Penetrationstests im Rahmen von Initiativprojekten ist die Gefahr imminent, nach Art. 143bis Abs. 1 StGB tatbestandsmässig zu handeln. Dies insbesondere, wenn das Eindringen in die Datenverarbeitungsanlage gelingt. Auch ein Versuch ist strafbar, wenn die Schranke der straflosen Vorbereitungshandlungen überschritten wird.

112 In Bezug auf Art. 143bis Abs. 2 StGB ist auch die Publikation von Erkenntnissen aus einem Initiativprojekt relevant. Entscheidend für den Ausschluss der Strafbarkeit ist hier einerseits der Detailierungsgrad, mit welchem die Erkenntnisse durchgeführter Schwachstellenanalysen bzw. der *Exploit* beschrieben werden, sowie der zeitliche Vorlauf der Information an die Betroffenen bzw. dass die Sicherheitslücke vor Veröffentlichung behoben wurde. Würdigt man die hinter der Veröffentlichung von Erkenntnissen aus Initiativprojekten stehende Motivation unter dem Normzweck von Art. 143bis Abs. 2 StGB so ist regelmässig auch die Erfüllung des subjektiven Tatbestands zu verneinen.

5.3. Strafbarkeit nach Art. 144bis StGB

Art. 144bis: Datenbeschädigung

[77] Vgl. DOLDER/WÜEST, IT-Recht, S. 465.

> *[1] Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*
>
> *Hat der Täter einen grossen Schaden verursacht, so kann auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.*
>
> *[2] Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*
>
> *Handelt der Täter gewerbsmässig, so kann auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren erkannt werden.*

113 Art. 144bis StGB regelt die Strafbarkeit von Handlungen in Zusammenhang mit der Beschädigung von Daten (Abs. 1) und der Herstellung von datenschädigenden Programmen (Abs. 2). Er schützt «die ungestörte Verfügungsmacht über Daten und insbesondere das Interesse des Verfügungs- oder Nutzungsberechtigten, Daten ungestört verwenden zu können.»[78]

114 Nach Art. 144bis Ziff. 1 StGB wird auf Antrag bestraft, wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht. Bezüglich des Datenbegriffs kann auf die Definition gemäss Rz 27 verwiesen werden, wobei diese im Unterschied zu Art. 143bis StGB für eine Tathandlung nach Art. 144bis Ziff. 1 StGB nicht besonders gegen fremden Zugriff gesichert sein müssen.[79] Ungeschriebenes Tatbestandselement ist ausserdem eine gewisse Erheblichkeit der Verletzungswirkung.[80] Dabei muss ein Eingriff einerseits dauerhaft sein; dies ist zu bejahen, wenn er durch die berechtigte Person nicht oder nur mit einigem Aufwand rückgängig gemacht werden kann. Andererseits muss er für die betroffene Person hinreichend erheblich sein.[81] Dies erfordert jeweils eine Einzelfallbeurteilung und Bagatellfälle würden über die Rechtsmissbräuchlichkeit des Strafantrags ausgeschlossen.[82]

---

78 Baltisser, Datenbeschädigung, S. 67.

79 BSK StGB-Weissenberger, Art. 144bis N 10; Praxiskommentar StGB-Trechsel/Crameri, Art. 144bis N 2; Schmid, Computer, S. 188 f. N 21.

80 BSK StGB-Weissenberger, Art. 144bis N 18; a.A. Baltisser, Datenbeschädigung, S. 83 f.

81 BSK StGB-Weissenberger, Art. 144bis N 26.

82 Vgl. BGE 120 IV 319, E. 2d.

115 Die Aufzählung der Tathandlungen ist abschliessend,[83] und soll alle Formen der Beschädigung, Veränderung und Entziehung von Daten erfassen, welche dazu führen, dass diese der berechtigten Person (mindestens vorübergehend) gar nicht mehr oder nicht in der gewünschten Form zur Verfügung stehen.[84] Eine u.U. notwendige Beteiligung der Datenberechtigten, etwa durch Öffnen eines E-Mails, welches einen Computervirus enthält, ist für die Tatbestandserfüllung wie schon bei Art. 143bis Abs. 1 StGB ohne Belang.[85]

116 Dabei umfasst *Verändern* jede Datenmanipulation inhaltlicher oder formeller Natur unabhängig von deren Auswirkungen auf den Gebrauchswert der Daten:[86] Beispielsweise Teillöschungen, Hinzufügen von Daten in Software, inhaltliche oder formale Anpassungen z.B. in deren Darstellung, Verknüpfungen mit anderen Daten, Verändern oder Ersetzen von Codes, Passwörtern oder Verschlüsselungen, auch Beseitigen, Ausschalten oder Durchbrechen einer elektronischen Zugangs- oder Kopiersperre oder das Einschleusen von Computerviren.[87] Andererseits stellt das Hinzufügen von Daten auf einem Datenspeicher keine Veränderung im Sinne von Art. 144bis Abs. 1 StGB dar, solange dadurch der Bedeutungsgehalt der bereits gespeicherter Daten nicht abgeändert wird.[88]

117 *Löschen* bedeutet irreversibles Unkenntlichmachen einer Speicherung (durch Überschreiben, Neuformatierung, Installation eines datenzerstörenden Programms [Virus], etc.) unabhängig davon, ob die Speicherung auf einem anderen Datenträger noch vorhanden ist oder allenfalls mit besonderem Aufwand (Beizug von Spezialisten oder geeigneter Software) wiederhergestellt werden kann.[89] Wenn die Daten dem Berechtigten jedoch auf einem sofort greifbaren Doppel etwa in der Form eines Back-ups zur Verfügung stehen, wird eine Tatbestandmässigkeit mangels Erheblichkeit verneint.[90]

118 Zuletzt bedeutet *Unbrauchbarmachen* eine Beeinträchtigung der Gebrauchsfähigkeit, sodass die Daten ihren Zweck nicht mehr erfüllen können. Gemäss Botschaft ist zudem auch der Fall der Datenunterdrückung und Datenentziehung erfasst, in denen die Daten zwar unverändert vorhanden, jedoch dem Berechtigten (zumindest vorübergehend) zur unbeeinträchtigten Verwendung entzogen sind.[91] Darunter fallen insbesondere das Ändern von Passwörtern, Codes

---

83 SCHMID, Computer, S. 190 N 24.
84 BSK StGB-WEISSENBERGER, Art. 144bis N 17.
85 Ibid., Art. 144bis N 32.
86 Zum Ganzen: Ibid., Art. 144bis N 21 ff.
87 SCHMID, Computer, S. 190 N 26; BSK StGB-WEISSENBERGER, Art. 144bis N 22.
88 BSK StGB-WEISSENBERGER, Art. 144bis N 23 und 25.
89 Ibid., Art. 144bis N 28; SCHMID, Computer, S. 190 N 27.
90 SCHMID, Computer, S. 190 N 27.
91 Botschaft 1991, 1014.

oder anderen Zugangsdaten sowie das Einfügen von Zugriffsschranken.[92] Weitere Beispiele für die Datenunterdrückung sind die inhaltliche Umgestaltung, die Löschung oder Veränderung eines Dateinamens oder einer Serveradresse, der Einsatz von Computerviren, die einer berechtigten Person den Zugriff auf Daten verunmöglichen, sowie *Denial of Service*-Angriffe und vergleichbare Angriffe, die fremde Datenverarbeitungsanlagen zum Erliegen bringen.[93] Bei der Entziehung der Zugriffsmöglichkeit reicht bereits eine vorübergehende (kurze) Unzugänglichkeit der Daten für eine erhebliche Verletzung.[94] Nicht erfasst sind demgegenüber Behinderungen der Zugriffsmöglichkeit, welche nur zu kurzen Unannehmlichkeiten jedoch zu keinerlei Beeinträchtigungen führen.[95]

119 Bei Initiativprojekten geht es primär darum, Schwachstellen innerhalb eines Zielsystems ausfindig zu machen. Das dauerhafte Verändern, Löschen oder Unbrauchbarmachen von Daten innerhalb des Systems ist nicht vorgesehen, zumal es nicht Teil der Schwachstellenanalyse ist. Dennoch besteht auch im Rahmen von Initiativprojekten (je nach Ausgestaltung der Penetrationstests) ein nicht unerhebliches Risiko, Tathandlungen nach Art. 144bis Abs. 1 StGB zu begehen. Einige Handlungen, wie etwa das Manipulieren von Logdaten (beispielsweise um ein erfolgtes Eindringen unkenntlich zu machen) würden den Tatbestand aufgrund der fehlenden Erheblichkeit nicht erfüllen. In anderen Fällen wäre der Tatbestand jedoch erfüllt, etwa wenn während eines laufenden Penetrationstests über eine erhebliche Dauer die Berechtigten nicht auf gewisse Daten zugreifen könnten, oder zur Penetration einer Sicherheitslücke erhebliche Veränderungen an Daten vorgenommen würden (beispielsweise Änderung von Passwörtern, o.Ä.).

120 In subjektiver Hinsicht verlangt Art. 144bis Abs. 1 StGB (Eventual-)Vorsatz. Die fahrlässige Begehung ist nicht strafbar.[96] Wie zuvor erwähnt, beabsichtigen die Analysten bei Initiativprojekten eine Datenbeschädigung i.S.v. Art. 144bis Abs. 1 StGB nicht als Selbstzweck, hingegen kann bei einer (temporären) Datenveränderung in Ausführung eines Penetrationstests dennoch ein direkter Vorsatz für die tatbestandsmässige Handlung nach Art. 144bis Abs. 1 StGB vorliegen.

121 Sodann wäre auch bei fehlendem direktem Vorsatz die Erfüllung des subjektiven Tatbestands nicht kategorisch ausgeschlossen, denn selbst wenn der Analyst bei einem Initiativprojekt die Datenbeschädigung nicht direkt beabsichtigt, handelt er allenfalls mit Eventualvorsatz, wenn er die Tatbestandsmässigkeit (hier die Datenbeschädigung) ernsthaft für möglich hält, sich aber mit ihr

92 Botschaft 1991, 1014; vgl. BSK StGB-Weissenberger, Art. 144bis N 34.

93 BSK StGB-Weissenberger, Art. 144bis N 35; Schmid, Computer, S. 191 N 30.

94 BSK StGB-Weissenberger, Art. 144bis N 36.

95 Praxiskommentar StGB-Trechsel/Crameri, Art. 144bis N 7.

96 Vgl. Baltisser, Datenbeschädigung, S. 95; Im Vorfeld wurde die Aufnahme der Strafbarkeit einer fahrlässigen Datenbeschädigung diskutiert, jedoch verworfen, vgl. Schmid, Computer, S. 195 N 42.

abfindet bzw. diese in Kauf nimmt. In einer solchen Konstellation wäre daher der subjektive Tatbestand von Art. 144bis Abs. 1 StGB auch erfüllt.

122 Die Abgrenzung zwischen Eventualvorsatz und bewusster Fahrlässigkeit kann im Einzelfall schwierig sein, da sowohl der eventualvorsätzlich als auch der (bewusst) fahrlässig handelnde Täter um die Möglichkeit des Erfolgseintritts bzw. um das Risiko der Tatbestandsverwirklichung Bescheid wissen. Der Unterschied liegt bei der Willenskomponente. Bewusst fahrlässig handelt, wer (aus pflichtwidriger Unvorsichtigkeit) darauf vertraut, dass der von ihm zwar als möglich vorausgesehene Erfolg nicht eintreten wird. Demgegenüber nimmt der eventualvorsätzlich handelnde Täter den Eintritt des als möglich erkannten Erfolgs ernst, er rechnet mit dem Erfolg und findet sich mit diesem ab.[97]

123 Ob jemand die Tatbestandsverwirklichung im Sinne des Eventualvorsatzes in Kauf genommen hat, ist aufgrund der Umstände zu entscheiden. Dazu gehören etwa die Grösse des dem Täter bekannten Risikos der Tatbestandsverwirklichung, die Schwere der Sorgfaltspflichtverletzung, die Beweggründe des Täters und die Art der Tathandlung. Je grösser die Wahrscheinlichkeit der Tatbestandsverwirklichung ist und je schwerer die Sorgfaltspflichtverletzung wiegt, desto näher liegt die Schlussfolgerung, der Täter habe die Tatbestandsverwirklichung in Kauf genommen.[98]

124 Diese Abgrenzungsfrage wurde in Bezug auf eine Datenbeschädigung nach Art. 144bis Ziff. 1 StGB im Rahmen von *Hacks* oder Penetrationstests soweit ersichtlich bislang nicht höchstrichterlich beurteilt. Anhand der oben definierten Kriterien der Rechtsprechung ist insbesondere dann von einer eventualvorsätzlichen Handlung auszugehen, wenn der Analyst Befehle tätigt, deren Funktion – wie er weiss – direkt auf eine Datenbeschädigung im Sinne von Art. 144bis Ziff. 1 StGB (Beeinträchtigung der Verfügbarkeit, Beschädigung, Veränderung, Verlust, etc. der Daten) gerichtet ist. Dies selbst dann, wenn er eine Datenbeschädigung beispielsweise im Rahmen eines Penetrationstests nicht direkt beabsichtigt. Das Fachwissen und die damit einhergehende erhöhte Kompetenz der Analysten, die technischen Folgen ihres Handelns abzuschätzen, werden bei dieser Beurteilung berücksichtigt.

125 Art. 144bis Abs. 2 StGB, welcher das Inverkehrbringen von datenschädigenden Programmen (*Malware*) unter Strafe stellt, ist vorliegend nicht weiter von Belang, da im Rahmen von Initiativprojekten weder solche Programme verwendet resp. erstellt noch publiziert und somit in Verkehr gebracht werden. Der

---

97 Statt vieler: BGE 133 IV 9, E. 4.1; vgl. sodann für detaillierte Ausführungen zum Eventualvorsatz BSK StGB-NIGGLI/MAEDER, Art. 12 N 48 ff.

98 Vgl. Urteil des BGer 6B_131/2021 vom 11. August 2021, E. 3.2 mit weiteren Hinweisen.

objektive Tatbestand von Art. 144bis Abs. 2 StGB wird somit im Rahmen von Initiativprojekten nicht erfüllt.

126 Bei der Durchführung von Initiativprojekten ist stets die Gefahr einer Datenbeschädigung i.S.v. Art. 144bis Ziff. 1 StGB im Auge zu behalten. Im Rahmen von Penetrationstest sind temporäre Datenmanipulationen (etwa zum Zweck des Überwindens eines Sicherheitsdispositivs) nur mit möglichst geringer Eingriffsintensität und kurzer Dauer vorzunehmen, da ansonsten die Erheblichkeit der Handlung im Sinne des Tatbestands grundsätzlich auch bei einer zum Zweck der Schwachstellenanalyse erfolgenden Datenbeschädigung zu bejahen wäre. Ein zusätzliches strafrechtliches Risiko besteht auch in Bezug auf eine eventualvorsätzliche Begehung. Dies etwa dann, wenn durch eine technisch riskante Handlung in Kauf genommen wird, dass es zu einer Datenschädigung (z.B. vorübergehende oder anhaltende Unverfügbarkeit von Daten) kommen könnte. Eine Strafbarkeit nach Art. 144bis Abs. 2 StGB kann im Rahmen von Initiativprojekten hingegen ausgeschlossen werden.

5.4. Strafbarkeit nach Art. 143 StGB

> ***Art. 143 StGB: Unbefugte Datenbeschaffung***
>
> *[1] Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.*
>
> *[2] Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.*

127 Bei Penetrationstests ist es teilweise erforderlich, dass auch Daten wie beispielweise Passwörter oder andere Zugangsdaten erlangt und verwendet werden.

128 Selbst wenn die Datenbeschaffung beim Durchführen von Initiativprojekten nicht im Zentrum steht, besteht somit die latente Gefahr, durch die vorzunehmenden Handlungen den objektiven Tatbestand von Art. 143 StGB zu erfüllen, wenn fremde, elektronisch gespeicherte Daten, welche gegen unbefugten Zugriff besonders geschützt sind, für die Tätigkeit im Rahmen der Initiativprojekte beschafft oder verwendet werden. Eine unbefugte Datenbeschaffung kann im Gegensatz zum klassischen Diebstahl auch bereits durch das Kopieren oder gar nur die optische Wahrnehmung von Daten erfolgen und erfordert nicht zwingend den Entzug der Verfügungsmöglichkeit des Berechtigten.[99]

129 Entscheidendes Abgrenzungs- und die Strafbarkeit ausschliessendes Kriterium bei der Tätigkeit im Rahmen von Initiativprojekten ist der subjektive Tatbestand von Art. 143 StGB und dort insbesondere die fehlende Bereicherungsabsicht:

130 Nach Art. 143 StGB macht sich nur strafbar, wer vorsätzlich handelt[100] und zugleich beabsichtigt, sich oder einen anderen mit der Erfüllung des objektiven Tatbestands (Beschaffung von Daten, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind) unrechtmässig zu bereichern.

131 Die Bereicherungsabsicht meint das Abzielen auf eine wirtschaftliche (geldwerte) Besserstellung im Sinne des strafrechtlichen Vermögensbegriffs.[101] Ein rein ideeller Vorteil oder Nutzen fällt nicht darunter.[102]

---

99 BSK StGB-Weissenberger, Art. 143 N 2.

100 Vgl. Art. 12 Abs. 1 StGB.

101 BGE 91 IV 130, E. 2.a; auch Urteil des BGer 6B_446/2011 vom 27. Juli 2012, E. 5.4.1; Urteil des BGer 6S.414/2004 vom 28. Februar 2005, E. 2.3.

102 BSK StGB-Niggli/Riedo, Vor Art. 137 N 78.

132 Dass die Bereicherung eingetreten ist, ist nicht erforderlich – entscheidend ist das Vorliegen einer entsprechenden Absicht.[103]

133 Bei Art. 143 StGB kann der Täter eine Bereicherung durch die Daten selbst anstreben, etwa wenn diese einen Verkehrswert haben oder er für deren Beschaffung bezahlt wird. Oder aber es geht ihm um einen mittelbaren Vermögensvorteil, beispielsweise indem er die Daten veräussert oder sie zum Zweck weiterer Vermögensdelikte (z.B. Erpressung) verwenden möchte. Auch in dieser zweiten Konstellation kommt den Daten nach herrschender Lehre ein vermögensrelevanter Gebrauchswert zu.[104]

Im Rahmen der Durchführung von Initiativprojekten ist aufgrund des oben beschriebenen Zwecks eine entsprechende Bereicherungsabsicht zu verneinen. Durch das Beschaffen von allfälligen Daten im Sinne von Art. 143 StGB im Verlauf oder zum Zweck der Durchführung von Schwachstellenanalysen verfolgen die Analysten bei Initiativprojekten weder mittelbar noch unmittelbar die Erlangung eines Vermögensvorteils im Sinne des Strafrechts. Trotz der weiten Auslegung der Bereicherungsabsicht würde es zu weit greifen, eine nebst dem gemeinnützigen Hauptzweck von Initiativprojekten unweigerliche Suche nach Reputation für die eigene Organisation und die damit allenfalls verbundene mittelfristig günstigen finanziellen Auswirkungen (beispielsweise in Form von allfälligen Unterstützungszahlungen aus öffentlicher Hand) darunter zu subsumieren.

---

[103] ACKERMANN et al., Strafrecht, S. 95.

[104] BSK StGB-WEISSENBERGER, Art. 143 N 29; vgl. zum Gebrauchswert insb. BGE 111 IV 74 = Praxis 1985 Nr. 133; sodann BSK StGB-NIGGLI/RIEDO, Vor Art. 137 N 79 ff. zur Auseinandersetzung in der Lehre über die Möglichkeit der mittelbaren Bereicherung.

5.5. Erfordernis der Rechtswidrigkeit: Rechtfertigungsgründe

134 Analysten werden im Rahmen von Initiativprojekten grundsätzlich tatbestandsmässig nach Art. 143bis Abs. 1 StGB handeln. Je nach Ausgestaltung resp. Erfordernis der Schwachstellenanalyse ist auch eine Tatbegehung nach Art. 144bis Abs. 1 StGB möglich oder zur Durchführung eines konkreten Penetrationstests gar erforderlich.

135 Ein Verhalten, das einen Straftatbestand erfüllt, kann unter besonderen Voraussetzungen ausnahmsweise nicht rechtswidrig und somit nicht strafbar sein. Diese besonderen Voraussetzungen sind in sogenannten Rechtfertigungsgründen verortet. Diese sind zum Teil im StGB selbst geregelt (Nothilfe, Notstand, etc.), ergeben sich teilweise aber auch aus der sonstigen Rechtsordnung (vgl. Art. 14 StGB), oder begründen sich gar ohne gesetzliche Grundlage etwa aus dem Gewohnheitsrecht.[105]

136 Wie nachfolgend aufgezeigt wird, sind im Bereich von Initiativprojekten mehrere Rechtfertigungsgründe denkbar, vorrangig kommt der rechtfertigende Notstand nach Art. 17 StGB zum Tragen.

5.5.1. Notstand (Art. 17 StGB)

137 Zweck von Initiativprojekten ist es, über die Durchführung von Schwachstellenanalysen Erkenntnisse über Sicherheitslücken in als gesellschaftlich relevant erachteten Systemen zu gewinnen und durch die Information der Betreiber sowie der Öffentlichkeit zur Schliessung solcher Lücken im Konkreten und einer Erhöhung der Cybersicherheit im Allgemeinen beizutragen.

138 Zur strafrechtlichen Rechtfertigung des (allenfalls) tatbestandsmässigen Verhaltens nach Art 143bis Abs. 1 und Art. 144bis Abs. 1 StGB bei der Durchführung von Initiativprojekten kann unter gewissen Voraussetzungen der Notstand nach Art. 17 StGB angerufen werden.

139 Ein rechtfertigender Notstand nach Art. 17 StGB liegt vor, wenn die strafbare Handlung begangen wurde, um ein eigenes oder das Rechtsgut einer anderen Person aus einer unmittelbaren, nicht anders abwendbaren Gefahr zu retten. Das (grundsätzlich strafbare) Handeln ist ausnahmsweise rechtmässig, wenn der Notstandsberechtigte dadurch höherwertige Interessen wahrt.[106] Dabei spielt es keine Rolle, von wo die Gefahr ausgeht. Auch ist nicht entscheidend, ob in die Rechtsgüter eines unbeteiligten Dritten zum Schutz eines fremden

---

[105] Handkommentar StGB-WOHLERS, Vorbemerkungen zu den Art. 14 ff. N 1; BSK StGB-NIGGLI/GÖHLICH, Art. 17 N 19; StGB Annotierter Kommentar-MAUSBACH/STRAUB, Art. 17 N 10.

[106] Statt vieler: Urteil des BGer 6B_1356/2016 vom 5. Januar 2018, E. 3.1.2.

Rechtsguts eingegriffen wird, oder ob die Gefahr für das Rechtsgut vom Dritten selbst ausgeht.[107]

140 Die konkreten Voraussetzungen sind das Vorliegen einer (a) unmittelbaren Gefahr für ein Individualrechtsgut (Notstandslage), (b) absolute Subsidiarität sowie (c) eine positive Interessenabwägung. In subjektiver Hinsicht ist vorausgesetzt, dass (d) der Notstandsberechtigte die Notstandslage kennen muss und handelt, um das bedrohte Rechtsgut zu retten.[108]

141 Zu den einzelnen Voraussetzungen im Konkreten:

(a) Unmittelbare Gefahr für ein Individualrechtsgut

142 Ob eine Gefahr vorliegt, ist *ex ante* zu bestimmen. Dabei ist zu beurteilen, ob sich die Gefahr konkret in einer Rechtsgutsverletzung niederschlagen könnte. Es ist allerdings nicht auf die subjektive Einschätzung des Täters abzustellen (vgl. jedoch Rz 166 f. für die bloss vermeintlich bestehende Gefahr). Beurteilt wird die Gefahr anhand des *ex-ante* Urteils eines verständigen Drittens aus der Perspektive des Täters. Eine Gefahr im Sinne des Art. 17 StGB liegt vor, wenn eine gewisse Wahrscheinlichkeit der Rechtsgutsverletzung besteht. Eine überwiegende Wahrscheinlichkeit (>50%) ist hingegen nicht vorausgesetzt, auch ist nicht vorausgesetzt, dass sich die Gefahr auch tatsächlich materialisiert abzugrenzen sind lediglich die völlig abstrakten Risiken.[109]

143 Notstand kann nur zum Schutz von Individualrechtsgütern (darunter versteht man die absoluten Rechte des Einzelnen wie etwa Leben, Gesundheit, Freiheit, Ehre, Eigentum, etc. sowie das relative Recht auf Vermögen) in Anspruch genommen werden; nach bundesgerichtlicher Rechtsprechung sind kollektive Rechtsgüter (wie etwa die öffentliche Sicherheit, die öffentlichen Gesundheit, der öffentliche Frieden, die Funktionalität des Staates bzw. dessen Existenz, die Integrität der Rechtspflege, etc.) als solche nicht notstandsfähig,[110] obschon nicht ausgeschlossen ist, dass eine unmittelbare Gefahr für Individualrechtsgüter zugleich auch eine Gefährdung von Rechtsgütern der Allgemeinheit beinhaltet.[111]

144 In Datenverarbeitungssystemen mit bislang nicht aufgedeckten Sicherheitslücken besteht eine latente Gefahr (böswilliger) Angriffe über ebendiese zuvor unentdeckten Sicherheitslücken. Die Gefahr für die Integrität und Sicherheit der

---

107 Handkommentar StGB-WOHLERS, Art. 17 N 4.

108 Ibid., Art. 17 N 10.

109 BSK StGB-NIGGLI/GÖHLICH, Art. 17 N 10 f.

110 BGE 147 IV 297, E. 2.1; Die Geltendmachung von Kollektivrechtsgütern oder staatlichen Interessen hätte – wenn überhaupt – über Art. 14 StGB zu erfolgen.

111 Praxiskommentar StGB-TRECHSEL/GETH, Art. 17 N 4; StGB Annotierter Kommentar-MAUSBACH/STRAUB, Art. 17 N 4.

entsprechenden Systeme und somit auch für Individualrechtsgüter (nämlich den «Computerfrieden» der Berechtigten) ist deshalb zu bejahen.

145 Mit Initiativprojekten werden auf längere Dauer auch weitere (Kollektiv-) Rechtsgüter geschützt; zu denken ist etwa an den Schutz der allgemeinen Gesundheit und Sicherheit, indem Sicherheitslücken zentraler (Datenverarbeitungs-) Infrastrukturen präventiv festgestellt und kommuniziert werden, damit diese Sicherheitslücken vor möglichen Angriffen oder Zusammenbrüchen behoben werden können.

Die unmittelbare Gefahr für Individualrechtsgüter kann an einem fiktiven Beispiel wie folgt dargestellt werden:

Im Rahmen eines Initiativprojekts wird ein *Smart Meter* Modell eines Herstellers einer Schwachstellenanalyse unterzogen. *Smart Meter* sind in der Schweiz weit verbreitet und werden von der Schweizer Energiestrategie vorgeschrieben.

Das Modell des Herstellers «MeasureMe», hat ein sehr attraktives Preis-Leistungs-Verhältnis und wird deshalb in der Schweiz durch die Verteilnetzbetreiber und Installateure in vielen Haushalten verbaut. Diese *Smart Meter* sind mit dem Internet und der «MM Cloud» des Herstellers «MeasureMe» verbunden. Der zuständige Verteilnetzbetreiber kann zu Wartungszwecken und für die Abrechnung aus der Ferne auf die *Smart Meter* zugreifen.

Beim besagten Hersteller kam es in der Vergangenheit zu einigen Zwischenfällen, bei denen Produkte von «MeasureMe» gehackt wurden und auch sonst ist sein Umgang mit Cybersicherheit intransparent. Er liefert insbesondere keine belastbaren Informationen wie Security-Whitepapers, Berichte von Penetrationstests, etc.

Die Analysten des Initiativprojekts beschaffen einige *Smart Meter* und unterziehen diese einem Penetrationstest (wobei nicht in eine *fremde* Datenverarbeitungsanlage eingedrungen wird). Es wird insbesondere ein Penetrationstest der Netzwerkschnittstelle durchgeführt, darüber gelingt den Analysten das Eindringen auf den *Smart Meter*. Dies erhärtet den Verdacht, dass das Produkt von «MeasureMe» erhebliche Sicherheitslücken aufweist und davon eine entsprechende Gefahr für die Sicherheit des Systems ausgeht.

Gestützt auf diese Kenntnis, unterziehen die Analysten auch die «MM Cloud» des Herstellers einem Penetrationstest.

Den Analysten gelingt auch das Eindringen in die «MM Cloud» des Herstellers. Potenziell könnten darauf die verarbeiteten Kundeninformationen eingesehen und heruntergeladen werden.

Die Analysten teilen die aus dem Initiativprojekt gewonnenen Erkenntnisse dem Hersteller mit, welcher die Sicherheitslücken nach kurzer Zeit über geeignete Massnahmen schliessen kann.

Die bis vor dem Initiativprojekt unentdeckten Sicherheitslücken begründeten eine dauernde Gefahr für die Integrität und Sicherheit des Systems, wobei diese Sicherheitslücken jederzeit für (böswillige) Angriffe auf die «MM Cloud» hätten ausgenutzt werden können.

Die Individualrechtsgüter, auf deren Schutz das durchgeführte Initiativprojekt abzielt, sind einerseits die Freiheit des Herstellers, darüber zu entscheiden, wem er den Zugang zu seiner gesicherten Datenverarbeitungsanlage (der «MM Cloud») und den dort vorhandenen Daten gewährt. Gleiches gilt für den zuständigen Verteilnetzbetreiber, und zwar für den Bereich der Datenverarbeitungsanlage, über welchen er gemäss Vereinbarung mit dem Hersteller verfügungsberechtigt ist. Soweit der Verteilnetzbetreiber ausserdem an den dort vorhandenen Daten berechtigt ist (für die Auslesung beispielsweise), so ist auch sein ungestörter Zugang zu diesen Daten ein zu schützendes Individualrechtsgut. Zuletzt sind je nach Auslegung und Identifizierungsmöglichkeiten auch individuelle Rechtsgüter der von den Daten betroffenen Personen (also der in den Haushalten lebenden Personen) betroffen.

146 Weiter muss es sich um eine *unmittelbare* Gefahr handeln. Die Gefahr muss entweder gegenwärtig sein oder die erst zu einem späteren Zeitpunkt drohende Gefahr muss nur gegenwärtig sicher abgewehrt werden können. Es muss «*un danger qui n'est ni passé ni future, c'est-à-dire un danger actuel mais aussi concret*»[112] sein. Die Unmittelbarkeit einer Gefahr kann auch dann gegeben sein, wenn ein potenzieller Schadenseintritt zwar nicht unmittelbar droht, die Abwehr aber später nicht mehr oder nur unter viel höheren Risiken möglich wäre. Beim Kriterium der Unmittelbarkeit tritt das Element der zeitlichen Entfernung des Schadenseintritts entsprechend in den Hintergrund.

147 Eine Unmittelbarkeit ist insbesondere auch bei einer sogenannten Dauergefahr gegeben.[113] Die Dauergefahr beschreibt einen «gefahrdrohenden Zustand, der über längere Zeit andauert und jederzeit in einen Schaden umschlagen kann, mag auch die Möglichkeit offen bleiben, dass der Schaden noch eine lange Zeit auf sich warten lässt.»[114]

Diesen Zustand hat das Bundesgerichts in BGE 147 IV 297 im Bereich des Klima-Aktivismus verneint. Entgegen dem vorgebrachten Argument der Verteidigung hat das Bundesgericht das Vorliegen einer Dauergefahr verneint, da

[112] BGE 122 IV 1, E. 3a; BSK StGB-Niggli/Göhlich, Art. 17 N 14.
[113] Vgl. BGE 147 IV 297, E. 2.3.4.
[114] Payer, Klimawandel, S. 25.

die durch die globale Erderwärmung ausgehende erhöhte Gefahr von Naturkatastrophen – im Unterschied zur ursprünglichen Form der Dauergefahr bei Situationen häuslicher Gewalt – jeden wahllos, an jedem Ort und jeder Zeit treffen könnte und sich insbesondere kein konkret bedrohtes Rechtsgut identifizieren lässt.[115]

148 Entscheidendes Kriterium für das Vorliegen einer Dauergefahr ist die Identifikation eines *konkret bedrohten* Rechtsguts.

149 Ein solches lässt sich vorliegend einfach identifizieren: Offene Sicherheitslücken machen die betroffenen Zielsysteme angreifbar. Solche Lücken können durch Angreifer jederzeit ausgenutzt werden. Dabei beschränkt sich die Gefahr nicht auf Eingriffe i.S.v. Art. 143bis Abs. 1 StGB, es muss vielmehr mit weiteren Handlungen insbesondere Datenbeschädigung und -beschaffung, sowie Folgedelikten und -schäden gerechnet werden. Solange solche Lücken nicht aufgedeckt werden, sind Angriffe auf die betroffenen Systeme (mit weit schwerwiegenderen Folgen) jederzeit möglich. Wenn in einem Datenverarbeitungssystem bislang unentdeckte Sicherheitslücken vorhanden sind, so besteht eine konkrete und unmittelbare Gefahr, dass ebendiese Lücken in einem (böswilligen) Angriff ausgenutzt werden könnten. Die Gefahr ist nicht wahllos, zufällig oder willkürlich, sondern betrifft das konkrete System und somit lässt sich ohne Mühe ein resp. mehrere konkret bedrohte Individualrechtsgüter identifizieren. Mit dem Aufdecken der Sicherheitslücken und der entsprechenden Kommunikation an die Verantwortlichen Hersteller oder Betreiber kann dieser Zustand behoben werden.

(b) Absolute Subsidiarität

150 Der Rechtfertigungsgrund des Notstands ist subsidiär, was bedeutet, dass eine «Normverletzung im Interesse übergeordneter Rechtsgüter nur dann Straflosigkeit nach sich zieht, wenn der Schutz des betreffenden Rechtsguts nicht anders als durch eine Normverletzung möglich ist.»[116] Die angewandten Mittel müssen zur Abwendung der Gefahr geeignet sein und es muss sich ausserdem um das mildeste Mittel, d.h. dass die fremden Rechtsgüter am wenigsten beeinträchtigende, handeln.[117] Die vorzunehmende Notstandshandlung muss mit anderen Worten alternativlos sein.[118]

151 Die Notstandssituation im Bereich der Cybersicherheit unterscheidet sich von den in der Rechtsprechung bereits beurteilten Fällen des Notstands merklich.

---

115 BGE 147 IV 297, E. 2.5; vgl. CAPRARA, Klimaaktivisten, S. 140.

116 Kantonsgericht Graubünden, Urteil vom 3. Juli 1991 (in: PKG 1991 S. 148 ff., S. 149 N 42).

117 BGE 98 IV 5.

118 StGB Annotierter Kommentar-MAUSBACH/STRAUB, Art. 17 N 9; Handkommentar StGB-WOHLERS, Art. 17 N 6; im Unterschied zur (nicht subsidiären) Notwehr ist beim Notstand beispielsweise auch das Ausweichen vor der drohenden Gefahr eine relevante Verhaltensoption (vgl. BGE 94 IV 68, E. 2).

Die Unmittelbarkeit der Gefahr im vorliegenden Fall ergibt sich anders als in den klassischen Fällen des Notstands nicht über die zeitliche Nähe des Gefahreneintritts, sondern über die andauernde Möglichkeit des jederzeitigen (jedoch zeitlich nicht klar prognostizierbaren) Eindringens. Dies ist auch beim Kriterium der Subsidiarität entsprechend zu berücksichtigen, wenn es darum geht, Alternativen zur Gefahrenabwehr zu beurteilen.

152 Die Durchführung von Schwachstellenanalysen im Rahmen von Initiativprojekten ermöglicht es, das Ausmass der Gefahr effektiv festzustellen. Über die Information an die Betreiber des betroffenen Zielsystems wird die Möglichkeit eröffnet, die festgestellten Sicherheitslücken schnellstmöglich zu schliessen und somit die latente Gefahr von Cyberangriffen langfristig abzuwenden.

153 Da bei Initiativprojekten oftmals Systeme mit einer hohen Benutzerzahl getestet werden und kein Auftraggeber vorhanden ist, stellt insbesondere das Vorwarnen oder Einholen des Einverständnisses keine geeignete Alternative für die Abwehr der Gefahr dar. Eine Vorabinformation an alle potenziell betroffenen Rechtsgutträger bzw. das Einholen einer Einwilligung ist für die Analysten im Rahmen eines Initiativprojekts nicht zumutbar. Der vorgängige Kontakt mit den (teilweise zahlreichen und nicht abschliessend identifizierbaren) betroffenen Rechtsgutträgern würde einen effizienten Prüfablauf faktisch verunmöglichen. Auch ist aufgrund der Dauergefahr ein möglichst rasches Vorgehen gefragt.

154 Andererseits ist auch nicht garantiert, dass die Betreiber oder sonstige Berechtigte der betroffenen Systeme im Voraus nach einer entsprechenden Warnung in Bezug auf die mögliche Gefahr von Sicherheitslücken Massnahmen zur ganzheitlichen Beurteilung und Behebung der Gefahr ergreifen würden oder könnten. Vielmehr ist wahrscheinlich, dass erst nach dem Aufzeigen des Ausmasses der Gefahr durch die Mitteilung der Erkenntnisse aus einem Initiativprojekt an die verantwortlichen Personen entsprechende Schritte vorgenommen würden.

155 Hinzu kommt die latente Gefahr, dass eine Vorwarnung vor einer konkreten Eingrenzung des Problems nicht ernst genommen oder verworfen würde oder aber, dass zu unspezifische Massnahmen ergriffen würden, welche die effektiv vorliegende (aber noch nicht vollständig identifizierte) Sicherheitslücke letztlich nicht (oder nicht vollständig) beheben. Im schlimmsten Fall könnte gerade die Vorwarnung erst recht dazu führen, dass die Sicherheitslücke ausgenutzt wird, etwa aufgrund eines Leaks der entsprechenden Information.

156 Initiativprojekte sind somit grundsätzlich mit dem Prinzip der absoluten Subsidiarität konform. Es ist indes bei deren Durchführung insbesondere auch dem Kriterium der Erforderlichkeit Rechnung zu tragen. Der Eingriff sollte das mildeste Mittel zur Gefahrenabwehr begründen. Im Bereich von Initiativprojekten drängt sich daher die Frage auf, wie weit die Schwachstellenanalysen gehen dürfen,

also wie viel Aktivität in Penetration des fremden Datenverarbeitungssystems erforderlich ist.

157 Allermindestens muss es im Rahmen von Initiativprojekten möglich sein, die Sicherheitslücken so weit zu erkunden, als man anhand der gewonnenen Erkenntnisse das Ausmass der Gefahr darlegen kann. Somit haben alle Massnahmen, welche für ein *Proof of Concept* nötig sind, noch als erforderlich im Sinne der absoluten Subsidiarität zu gelten.

158 Bereits nicht mehr im Bereich des Erforderlichen wäre es indes, Daten herunterzuladen, zu ändern, zu löschen oder in anderer Weise unbrauchbar zu machen, sofern diese Daten nicht zum Zweck der Schwachstellenanalyse selbst verwendet werden.[119] Ganz allgemein gilt es, Manipulationen im fremden System möglichst zu unterlassen.

Die Grenze des Erforderlichen ist fliessend und kann anhand eines fiktiven Beispiels wie folgt skizziert werden:

Ein Analyst identifiziert bei einem Penetrationstest einer Webanwendung eine *Cross-Site-Scripting (XSS)*-Schwachstelle.

Ein *Ethical Hacker* resp. Analyst, der im Rahmen eines Initiativprojekts agiert, achtet auf Subsidiarität bzw. Erforderlichkeit und wird die Sicherheitslücke nur ausnutzen, um beispielsweise ein harmloses Popup-Fenster erscheinen zu lassen. Dies reicht aus, um die Existenz der Sicherheitslücke nachzuweisen (*Proof of Concept*). Darauf aufbauend kann das Ausmass für weitere mögliche Angriffe abgeschätzt werden.

Dagegen würde ein unethisch handelnder Hacker, der z.B. mit Bereicherungsabsicht oder Profilierungsabsicht agiert, einen Angriff allenfalls im Sinne eines *Full Exploit* weiterführen, indem er statt eines harmlosen Pop-up-Fensters seinen Zugang ausnutzt, um beispielsweise Kreditkarteninformationen von Nutzern zu entwenden.

(c) Interessenabwägung

159 Grundsätzlich soll es die Ausnahme bleiben, eine strafbare Handlung nur deshalb nicht zu bestrafen, weil sie in einem anderen (Dritt-)Interesse liegt. Der Rechtfertigungsgrund des Notstands setzt deshalb ein deutliches Überwiegen der verfolgten Interessen des Täters voraus.[120] Bei der Interessenabwägung sind insbesondere die Schwere des Eingriffs sowie das Ausmass der drohenden Gefahr für das geschützte und für das beeinträchtigte Rechtsgut zu

[119] Nationales Zentrum für Cybersicherheit (NCSC): Rahmenbedingungen und Regeln, <www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html> (zuletzt besucht am 25. Juni 2023).

[120] BGE 122 IV 1, E. 2b; BGE 116 IV 364, E. 1a.

berücksichtigen.[121] Bedeutend ist bei der Interessenabwägung ausserdem, ob die Notstandshandlung unmittelbar in die Rechtssphäre eines Unbeteiligten eingreift (Aggressivnotstand) oder einzig in das Rechtsgut dessen, aus dessen Sphäre die Gefahr resultiert (Defensivnotstand). Beim Defensivnotstand ist der Schutz höherwertiger Interessen grundsätzlich erst zu verneinen, wenn der Schaden, welcher durch die Notstandshandlung entstanden ist, ausser Verhältnis steht zu dem anderenfalls drohenden Schaden. Anders ist es beim Aggressivnotstand, bei dem die notwendige Aufgabe fremder Individualrechtsgüter nur dann als gerechtfertigt ansehen werden kann, wenn damit ein ungleich höheres Rechtsgut geschützt oder eine signifikant schwerere Verletzung oder Gefährdung abgewendet würde.[122]

160 Bei Initiativprojekten ist die Situation deshalb besonders, weil das zu schützende Rechtsgut mit dem tangierten Rechtsgut übereinstimmt. Es wird letztlich in den «Computerfrieden» der am Zielsystem Berechtigten eingegriffen, um ebendieses präventiv vor (böswillig motivierten) zukünftigen Eingriffen zu schützen. Sekundär wirkt sich dies natürlich auch auf den Schutz unbeteiligter oder lediglich indirekt beteiligter Drittinteressen (z.B. weiterer Benutzer der getesteten Systeme oder der Betreiber und Nutzer anderer Systeme mit den gleichen oder sehr ähnlichen Sicherheitslücken) aus.

161 Es handelt sich folglich insofern um einen Defensivnotstand, als dass die latente Gefahr von Hackerangriffen aus der Sphäre des Zielsystems selbst resp. dessen potenziellen Sicherheitslücken hervorgeht bzw. erhöht wird. Der drohende Schaden bei einem unkontrollierten, böswilligen Hackerangriff würde den aufgrund der Schwachstellenanalysen ggf. entstehenden «Schaden» deutlich übersteigen. Die Schwere des (kontrollierten) Eingriffs mit positiver Zweckorientierung (und ohne Schädigungswillen) im Rahmen eines Initiativprojekts tritt gegenüber dem erhöhten Grad der Gefahr für dasselbe Rechtsgut bei einem böswilligen Hackerangriff somit deutlich in den Hintergrund. Die geforderte Interessenabwägung hat daher positiv auszufallen.

(d) Kenntnis der Notstandslage / Handeln zum Zweck der Behebung der Notlage

162 Wer den Notstand anruft, muss in Kenntnis der rechtfertigenden Sachlage und zum Zweck der Behebung des Notstands handeln.[123]

163 Bei Initiativprojekten ist es oft so, dass das effektive Ausmass der Gefahr für die Sicherheit des Systems erst nach erfolgten Schwachstellenanalysen bekannt wird. Hingegen können über straflose Vorbereitungshandlungen (wie etwa

[121] BGE 106 IV 65; vgl. auch BSK StGB-Niggli/Göhlich, Art. 17 N 22; StGB Annotierter Kommentar-Mausbach/Straub, Art. 17 N 12.

[122] Handkommentar StGB-Wohlers, Art. 17 N 7.

[123] Vgl. Stratenwerth, AT I, S. 246.

Portscanning, etc.) einigermassen belastbare Einschätzungen darüber gewonnen werden, ob ein System Sicherheitslücken aufweist. Es sind daneben insbesondere sogenannte *Code Smells*[124], d.h. oberflächliche Hinweise auf tieferliegende Probleme im System, die es Analysten erlauben, vor dem effektiven Eindringen in eine Datenverarbeitungsanlage bereits vorzeitige Schlüsse über das Vorhandensein von allfälligen Sicherheitslücken zu ziehen. Obschon das vollständige Ausmass des Notstands offenkundig vor Eindringen in das Zielsystem nicht bekannt ist, kann dieser doch sinnvoll antizipiert werden.

164 Bei den Initiativprojekten des NTC wird über verschiedene Massnahmen eine solche Vorabeinschätzung getroffen, darunter etwa:

(a) Nationales Schwachstellen-Monitoring: dabei sollen zukünftig potenzielle Zielsysteme, welche die Aufgreifkriterien für ein Initiativprojekt des NTC erfüllen (vgl. Rz 4.1(c)), regelmässig über *Portscans* und Signalanalysen gescannt werden;[125]

(b) Begründete Verdachtsmeldung von Personen, Branchenspezialisten/Behörden, Fachmedien, etc.;[126]

(c) *Threat Intelligence* aus Drittquellen;

(d) Kritische neue Technologien sowie alarmierendes passives Verhalten/Positionierung der Betreiber in Bezug auf Cybersicherheit.

165 Erhärtet sich bei den Analysten des NTC aufgrund der daraus gewonnen Informationen der Verdacht, dass relevante Sicherheitslücken (und somit eine Gefahr im Sinne des Notstands) bestehen, so wird ein Initiativprojekt gestartet.

166 Waren die objektiven Notstandsvoraussetzungen im Nachhinein nicht gegeben, weil beispielsweise eine angenommene Gefahr nicht vorlag (sog.

---

124 «A Code Smell is a surface indication that usually corresponds to a deeper problem in the system.», Fowler Martin: CodeSmell, Beitrag vom 9. Februar 2006, <martinfowler.com/bliki/CodeSmell.html> (zuletzt besucht am 25. Juni 2023).

125 Ähnlich führte dies bereits das NCSC in England ein; vgl. National Cyber Security Centre (NCSC UK): NCSC Scanning Information, <https://www.ncsc.gov.uk/information/ncsc-scanning-information> und Scanning the Internet for Fun and Profit, <https://www.ncsc.gov.uk/blog-post/scanning-the-internet-for-fun-and-profit> (zuletzt besucht am 25. Juni 2023).

126 So etwa in der jüngst durch das NTC veröffentlichen technischen Sicherheitsanalyse der App *Tiktok* des chinesischen Herstellers ByteDance. Die Analyse resultierte aus Verdachtsmeldungen aus dem Ausland (Behörden, Medien etc.) sowie auf Anregung des NCSC, vgl. Nationales Testinstitut für Cybersicherheit (NTC): Technische Sicherheitsanalyse Mobile App «Tiktok», Begutachtung der Sicherheitsrisiken aus Schweizer Perspektive, <https://www.ntc.swiss/hubfs/NTC-security-analysis-tiktok-v1.0-de.pdf?hsCtaTracking=eb438ecd-a370-4935-b105-8eba59b68220%7Cd6f23147-1db5-4f44-9575-d48332f2b4d9Y> (zuletzt besucht am 25. Juni 2023).

Putativnotstand), so wird die Tat in Anwendung von Art. 13 Abs. 1 StGB zu Gunsten des Täters nach dem Sachverhalt beurteilt, den er sich vorgestellt hat.[127]

167 Bei Initiativprojekten könnte dies etwa der Fall sein, wenn aufgrund Anzeichen in einem System auf eine entsprechende Gefahr in einem anderen System geschlossen wird, die sich nach erfolgter Erprobung nicht bestätigt. In einem solchen Fall wäre nicht von einem strafbaren Versuch, sondern von einem rechtfertigenden Putativnotstand auszugehen. In den anderen Fällen, in denen das Eindringen und somit das tatbestandsmässige Handeln nach Art. 143bis Abs. 1 StGB gelingt, gilt die Gefahr grundsätzlich als bestätigt.

168 Alleiniges Ziel von Initiativprojekten ist das Aufdecken von Sicherheitslücken in gesellschaftlich relevanten Zielsystemen. Dabei informieren die Analysten die betroffenen Betreiber über die daraus gewonnen Erkenntnisse, damit die betroffenen Betreiber die aufgedeckten Sicherheitslücken schliessen sowie Sicherheitslücken öffentlich bekannt werden und entsprechende Präventionsschritte unternommen werden können. Das Handeln zum Zweck der Behebung des Notstands ist dem Vorhaben der Initiativprojekte inhärent. Die Initiativprojekte orientieren sich dabei an einem verlässlichen, vorkonzipierten Prozess, welcher vollständig und primär dem Dienst an die Systemsicherheit verpflichtet ist.

169 Dies grenzt Initiativprojekte insbesondere von weiteren Formen des *Ethical Hackings* ab, wo ein Hacker etwa zum Zweck der Selbstprofilierung (selbst wenn keine direkte Bereicherungsabsicht vorliegt) einen ähnlichen Penetrationstest durchführt. Letztere werden sich aufgrund der fehlenden subjektiven Komponente «zum Zweck der Behebung der Gefahr» nicht auf den rechtfertigenden Notstand nach Art. 17 StGB berufen können.

(e) Zwischenfazit: Notstand

170 Der Notstand nach Art. 17 StGB kann ein allfälliges tatbestandsmässiges Handeln nach Art. 143bis Abs. 1 StGB und Art. 144bis Abs. 1 StGB bei der Durchführung von Initiativprojekten in den meisten relevanten Fällen rechtfertigen.

---

[127] StGB Annotierter Kommentar-MAUSBACH/STRAUB, Art. 17 N 13; BSK StGB-NIGGLI/GÖHLICH, Art. 17 N 25; vgl. BGE 129 IV 6, E. 3.2.

Bei der Rechtfertigung über den Notstand nach Art. 17 StGB unterscheiden sich die Handlungen und Bestrebungen im Rahmen von Initiativprojekten in entscheidender Weise vom medial breit diskutierten Fallbeispiel des Klima-Aktivismus. In jüngster Zeit haben sich mehrere Schweizer Gerichte mit der Frage befasst, ob Straftaten von Klimaaktivisten (insb. Hausfriedensbruch bei Demo-Aktionen) unter Anrufung des Klimaschutzes durch Art. 17 StGB gerechtfertigt werden können. Diese Frage wurde höchstrichterlich im Urteil 6B_1295/2020 vom 26. Mai 2021 (BGE 147 IV 297) beantwortet, in welchem das Bundesgericht das Notstandsargument verwarf:[128]

Das Bundesgericht legte den Begriff der «unmittelbaren Gefahr» rechtsmethodisch aus und kam zum Schluss, dass Naturkatastrophen, welche infolge der globalen Erderwärmung auftreten, nur dann als «unmittelbare Gefahr» im Sinne von Art. 17 StGB qualifiziert werden können, wenn ein Täter in der Erkenntnis, dass ein solches Ereignis unmittelbar bevorsteht, handeln muss, um ein bestimmtes (!) Rechtsgut zu retten. Die Aktivisten hätten vorliegend aber Allgemeinrechtsgüter – wie etwa die Umwelt oder die Gesundheit der Gesamtbevölkerung – retten wollen. Die Aktivisten hätten nicht gehandelt, um ein bestimmtes Rechtsgut zu schützen, sondern um die Öffentlichkeit durch einen symbolischen Akt auf eine Problematik aufmerksam zu machen. Somit konnten sich diese nach Auffassung des Bundesgerichts auch nicht auf einen Putativnotstand berufen.

Im Rahmen von Initiativprojekten werden im Unterschied dazu individuelle Rechtsgüter konkret geschützt: Zwar verfolgt das NTC seinerseits übergeordnet auch den Schutz von Allgemeinrechtsgüter (öffentliche Sicherheit, etc.), bei der Durchführung eines Initiativprojekts an einem konkreten Zielsystem lässt sich jedoch ganz konkret zuordnen, welche individuellen Rechtsgüter (namentlich die Rechtsgüter der konkret Systemberechtigten und der Nutzer des Zielsystems) vor einem jederzeit möglichen Angriff auf das Zielsystem über die bislang unerkannten Sicherheitslücken geschützt werden. Daher sind die Kriterien, welche das Bundesgericht für eine unmittelbare Gefahr aufstellt, bei Initiativprojekten grundsätzlich erfüllt.

Der Notstand kann sodann bekanntlich nur subsidiär geltend gemacht werden. Darunter ist im Wesentlichen zu verstehen, dass die Verletzung des fremden Rechtsguts das einzige resp. mildeste geeignete Mittel zur Abwehr der Gefahr darstellt. Nachdem das Bundesgericht bereits die unmittelbare Gefahr verneinte, nahm es in seinen Erwägungen keine Überprüfung der

[128] Vgl. zum Ganzen auch: CAPRARA, Klimaaktivisten.

weiteren Voraussetzungen von Art 17 StGB vor,[129] äusserte sich jedoch indirekt unter dem Titel der Wahrung berechtigter Interessen zum Erfordernis der absoluten Subsidiarität und verneinte diese implizit mit Verweis auf eine Vielzahl anderer legaler Methoden, mit welchen das Ziel der Aktivisten erreicht werden könnte.

Auch in Bezug auf das Kriterium der absoluten Subsidiarität unterscheiden sich Initiativprojekte entscheidend von den Aktivitäten der Klimaaktivisten. Einerseits ist eine Schwachstellenanalyse ein direkt geeignetes Mittel, um bislang unentdeckte Sicherheitslücken in einem Zielsystem aufzudecken, darüber zu informieren und somit den Schutz des Systems sicherzustellen resp. die inhärente Gefahr zu bannen, dass diese Sicherheitslücken für böswillige Angriffe ausgenutzt werden. Die Handlung ist direkt zielgerichtet und hat nicht einen «symbolischen Charakter», wie es das Bundesgericht bei den Handlungen der Aktivisten unterstellte. Aufgrund der spezifischen Charakteristiken der Zielsysteme ist es denn meist auch nicht möglich, die Gefahr für ein betroffenes Zielsystem auf andere Weise frühzeitig abzuwehren.

5.5.2. Weitere Rechtfertigungsgründe

5.5.2.1. Aussergesetzlicher Notstand

171 Art. 17 StGB kann lediglich zum Schutz von Individualrechtsgütern angerufen werden. Zur Wahrung von Rechtsgütern der Allgemeinheit wird in der Literatur und Rechtsprechung ein ausser- bzw. übergesetzlicher Notstand diskutiert.[130] Nebst grundsätzlicher Kritik an der Existenzberechtigung eines solchen Rechtfertigungsgrunds herrscht auch bei den Befürwortern die Meinung vor, dass einzig die höchsten Güter eines Landes, wie etwa sein Bestand, seine Unabhängigkeit, territoriale Integrität usw. notstandsfähige Rechtsgüter der Allgemeinheit sein können.[131] Etwaige weitere öffentliche Interessen wären, wenn

[129] Vor dem Bundesgericht überprüfte das Waadtländer Kantonsgericht in seinem Urteil Jug 2020/333/371 vom 22. September 2020, E. 6.1.2 und 6.3 die entsprechende Argumentation der Aktivisten unter der Voraussetzung der absoluten Subsidiarität und kam zum Schluss, dass diese nicht erfüllt sei. Dabei erachtete das Kantonsgericht die gewählten Handlungen (Tennisspielen in Bankfiliale) nicht als ein geeignetes Mittel, die Gefahren, welche mit dem Klimawandel verbunden sind, abzuwenden. Ebenfalls erachtete es die Begehung der Straftaten (Hausfriedensbruch) nicht als erforderlich, um die schädigenden Folgen der globalen Erwärmung zu bekämpfen und stellte sich dabei insbesondere auf den Standpunkt, dass die Gefahr auch anders hätte abgewendet werden können. Beachtlich ist hier noch, dass das Waadtländer Kantonsgericht zuvor aber zumindest das Vorliegen einer unmittelbar drohenden Gefahr durch den Klimawandel bejaht hatte.

[130] Vgl. BGE 94 IV 68, E. 2; STRATENWERTH, AT I, S. 249; kritisch BSK StGB-NIGGLI/GÖHLICH, Art. 17 N 5.

[131] STRATENWERTH, AT I, S. 249.

überhaupt, über die Wahrnehmung berechtigter Interessen zu rechtfertigen. Daneben werden die weiteren Voraussetzungen nach Art. 17 StGB vorausgesetzt.[132]

172 Cyberangriffe auf staatliche Infrastrukturen können selbstredend die staatlichen Interessen i.e.S. gefährden, und Initiativprojekte tragen über die Erhöhung der Cybersicherheit indirekt zur Wahrung dieser Interessen bei. Dennoch bietet der aussergesetzliche Notstand wohl kaum je einen geeigneten (ergänzenden) Rechtfertigungsgrund für die Handlungen in Zusammenhang mit Initiativprojekten. Da so oder anders die Voraussetzungen nach Art. 17 StGB erfüllt sein werden, können entsprechende Handlungen direkt über den Notstand nach Art. 17 StGB bzw. subsidiär über die Wahrnehmung berechtigter Interessen gerechtfertigt werden.

5.5.2.2. Wahrung berechtigter Interessen

173 Nebst den gesetzlich normierten Rechtfertigungsgründen kann sich ein Täter unter gegebenen Umständen auf die Wahrung berechtigter Interessen als gewohnheitsrechtlich anerkannter Grund zum Ausschluss der Rechtswidrigkeit berufen.[133]

174 Die Rechtfertigung über die Wahrung berechtigter Interessen dient der Durchsetzung verfassungsmässig garantierter Freiheitsrechte[134] oder der Herstellung sozial erwünschter und gebilligter Zustände auf Kosten der Beeinträchtigung anderer Interessen.[135] Anders als beim Notstand wird bei der Wahrung berechtigter Interessen keine Gefahr gegen ein (anderes) Rechtsgut abgewehrt, vielmehr erfolgt die Verletzung des einen Rechtsguts in Durchsetzung eines Interesses, welches wichtiger zu werten ist als die Verletzung.[136] Aufgrund der dadurch begünstigten Gefahr einer durch den Täter vollzogenen Interessenverrechnung, wird diese Rechtsfigur in der Lehre stark kritisiert.[137]

175 Grundsätzlich könnte jedes schutzwürdige private oder öffentliche Interesse in Betracht kommen. Nach bundesgerichtlicher Rechtsprechung gelten indes für die Wahrnehmung berechtigter Interessen ähnliche Restriktionen wie beim Notstand: Einerseits bedarf es einer Interessenabwägung, wobei die verfolgten Interessen die verletzten deutlich überwiegen müssen. Andererseits muss die

---

132 BGE 94 IV 68, E. 2.

133 Praxiskommentar StGB-Trechsel/Geth, Art. 14 N 10 und 13 ff.

134 Ursprünglich entstand diese Rechtsfigur im Disput um die Grenzen der Pressefreiheit.

135 BSK StGB-Niggli/Göhlich Carola, Vor Art. 14 N 66; Donatsch/Tag, Strafrecht I, S. 274.

136 BSK StGB-Niggli/Göhlich, Vor Art. 14 N 70.

137 Vgl. Payer, Interessen, S. 193, mit entsprechenden Hinweisen; kritisch auch BSK StGB-Niggli/Göhlich, Vor Art. 14 N 67.

Handlung darüber hinaus auch ein angemessenes Mittel zur Erreichung des angestrebten Zwecks sein.[138]

176 Auf den Rechtfertigungsgrund der Wahrung berechtigter Interessen kann sodann nur ausgewichen werden, wenn die vorherrschende Interessenskollision gesetzlich nicht bereits abschliessend entschieden ist oder für die Abwägung keinen prozessualen Mechanismus kennt.[139] Ein Anrufen dieses Rechtfertigungsgrunds ist daher beispielsweise bei einer konkreten Bedrohung eines individuellen Rechtsguts nicht möglich, da Art. 17 StGB diese Fälle der Rettung von Individualrechtsgütern vor unmittelbaren Gefahren durch die Begehung strafbewehrter Taten abschliessend regelt.[140] Gemäss der bundesgerichtlichen Rechtsprechung kommt eine entsprechende Rechtfertigung nur in Ausnahmefällen in Betracht.[141] Entsprechend wurde die Wahrung berechtigter Interessen auch in den wenigsten Fällen höchstrichterlich bejaht.[142]

177 Mit Initiativprojekten wird durch die Erhöhung der Cyber- und allgemeinen Datensicherheit die Herstellung eines sozial erwünschten und gebilligten Zustands verfolgt. Dabei kommt der Cybersicherheit in der Schweiz auch politisch ein erhöhter Stellenwert zu.[143]

178 Dennoch ist im Kontext von Initiativprojekten nicht primär auf die Rechtsfigur der Wahrnehmung berechtigter Interessen zurückzugreifen, denn nebst den erwähnten (Allgemein-)Interessen werden im Rahmen von Initiativprojekten primär konkrete Rechtsgüter geschützt. Das Anrufen des Rechtfertigungsgrunds der Wahrnehmung berechtigter Interessen hat daher hinter Art. 17 StGB zurückzutreten. Indes ist für Fälle, bei denen die Berufung auf den Notstand nicht verfängt (beispielsweise aufgrund der fehlenden Unmittelbarkeit der Gefahr), je nach Umständen eine Berufung auf die Wahrnehmung berechtigter Interessen denkbar.

---

138 BSK StGB-NIGGLI/GÖHLICH, Vor Art. 14 N 67 mit Hinweisen auf BGE 129 IV 6; 127 IV 135; 120 IV 208; auch PAYER, Interessen, S. 191 f.; Handkommentar StGB-WOHLERS, Art. 17 N 12; DONATSCH/TAG, Strafrecht I, S. 272 f.

139 BGE 120 IV 208, E. 3a; Urteil des BGer 6B_880/2017 vom 4. Juli 2018, E. 3.4.2; Urteil des BGer 6B_200/2018 vom 8. August 2018, E. 3.2.

140 PAYER, Interessen, S. 190.

141 BGE 120 IV 208, E. 3a.

142 Bejaht etwa in BGE 113 IV 4 für die Rechtfertigung von Verkehrsdelikten eines Begleiters eines Fahrradrennens; vgl. BSK StGB-NIGGLI/GÖHLICH, Vor Art. 14 N 73 mit einer Übersicht der beurteilten Fälle, wobei die Rechtfertigung über die Wahrung berechtigter Interessen grossmehrheitlich abgelehnt wurde. So wurden unter anderem bei der Beurteilung von Nötigungshandlungen durch politische Aktivisten unter Anrufung des Klimaschutzes eine entsprechende Rechtfertigung mit der Begründung abgelehnt, dass den Aktivisten alternativ eine «eine grosse Palette legaler (insb. politischer und medialer) Möglichkeiten» zur Verfügung gestanden hätten (vgl. BGE 129 IV 6, E. 3.5, 3.7).

143 Vgl. insbesondere die Verabschiedung der neuen nationalen Cyberstrategie (NCS) im April 2023: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-94237.html> (zuletzt besucht am 25. Juni 2023).

5.5.2.3. (Mutmassliche) Einwilligung der Verletzten

179 In Bezug auf eine Rechtfertigung über eine (mutmassliche) Einwilligung der Verletzten sei auf Rz 58 ff. verwiesen.

180 Zu ergänzen ist sodann, dass eine Einwilligung in Bezug auf Art. 143bis Abs. 2 StGB aufgrund der Ausgestaltung als abstraktes Gefährdungsdelikt ausgeschlossen ist.[144]

5.6. Strafantragsberechtigung nach Art. 143bis Abs. 1 StGB und Art 144bis Abs. 1 StGB

181 Bei Art. 143bis Abs. 1 StGB sowie Art. 144bis Abs. 2 StGB handelt es sich um Antragsdelikte, entsprechend wird eine Handlung erst auf Strafantrag hin untersucht. Im Gegensatz dazu werden Widerhandlungen nach Art. 143bis Abs. 2 StGB von Amtes wegen verfolgt.

182 Im Rahmen von Initiativprojekten werden Zielsysteme getestet mit dem alleinigen Ziel, allfällige Sicherheitslücken aufzudecken und die Betreiber zu informieren, sodass solche Sicherheitslücken geschlossen werden können. Initiativprojekte dienen somit in erster Linie der Cybersicherheit des Zielsystems. Vor diesem Hintergrund ist anzunehmen, dass die Betreiber eines betroffenen Zielsystems mehrheitlich von einem Strafantrag absehen werden. Die Möglichkeit eines Strafantrags kann jedoch nicht per se ausgeschlossen werden. So gibt es immer wieder Fälle, in denen gegen Analysten von Initiativprojekten oder andere *Ethical Hacker* Strafanzeigen erhoben werden.[145]

183 Die Antragsfrist beträgt gemäss Art. 31 StGB drei Monate. Sie beginnt mit dem Tag zu laufen, an welchem der antragsberechtigten Person der Täter sowie die Tat bekannt wird.[146]

184 Vorliegend entspricht dies auch der Karenzfrist von 90 Tagen, welche das NTC den Betreibern nach Kommunikation von Sicherheitslücken für deren Behebung ansetzt. Nebst den Betreibern sind je nach Sachverhalt auch andere Personen antragsberechtigt (dazu sogleich). Nach Ablauf der 90-tägigen Frist ist das Risiko eines Strafantrags somit zwar nicht komplett gebannt (es bestünde immer noch die Möglichkeit, dass beispielsweise ein betroffener Nutzer erst später von den Tatumständen erfährt), es kann sich jedoch in Bezug auf den Betreiber nach

---

144 Die Einwilligung hat vom konkret betroffenen Rechtsgutträger zu erfolgen, den es bei abstrakten Gefährdungsdelikten gerade nicht gibt (vgl. Handkommentar StGB-WOHLERS, Vorbemerkungen zu den Art. 14 ff. N 6).

145 Vgl. etwa die Strafanzeige der CDU gegen eine deutsche Entwicklerin, nachdem diese Sicherheitslücken in der CDU-Wahlkampf App entdeckte (vgl. GRÜNER, Hacker-Verfahren), oder die Strafanzeige der E-Commerce-Unternehmung Modern Solution gegen einen Programmierer in Deutschland, welcher im daraufhin eingeleiteten Strafverfahren erstinstanzlich freigesprochen wurde (vgl. Heise Online: Modern Solution: Staatsanwaltschaft scheitert mit Anklage gegen IT-Experten, <https://heise.de/-9182813> [zuletzt besucht am 25. Juni 2023]).

146 Statt vieler: BGE 121 IV 272, E. 2.a.

Ablauf der 90 Tage seit Kommunikation der Sicherheitslücke nicht mehr materialisieren.[147]

185 Zum Strafantrag ist gemäss Art. 30 StGB jede Person berechtigt, welche durch die entsprechende Tat verletzt worden ist. Dabei ist nicht jeder, «dessen Interessen durch die strafbare Handlung irgendwie beeinträchtigt werden, sondern nur der Träger des unmittelbar angegriffenen Rechtsguts»[148] verletzt und somit strafantragsberechtigt. Der Träger des angegriffenen Rechtsguts ergibt sich erst durch die Auslegung des betreffenden Tatbestands.[149]

186 In der Praxis können sich bei der Beurteilung der Strafantragsberechtigung im Cyberstrafrecht einige Abgrenzungsschwierigkeiten ergeben, und es drängt sich eine je nach Sachverhalt differenzierte Handhabung des Antragsrechts auf.[150] Der Kreis der Strafantragsberechtigten kann somit je nach vollzogener Tathandlung variieren. Grundsätzlich ist der Verfügungsberechtigte der Datenverarbeitungsanlage zum Strafantrag berechtigt. Darunter fällt nebst dem Anbieter von Dienstleistungen (Provider) auch der Benutzer dieser Dienstleistungen, wie beispielsweise der Inhaber eines E-Mail-Accounts.[151]

187 In der Literatur wird indes diskutiert, dem Provider das Antragsrecht (analog dem Vermieter beim Hausfriedensbruch) abzusprechen. Beim Hausfriedensbruch beinhaltet das geschützte Rechtsgut «die Befugnis […], über die bestimmten Räume ungestört zu herrschen und darin den eigenen Willen frei zu betätigen.»[152] Derselbe Schutz (für den digitalen Raum) lässt sich auch Art. 143bis Abs. 1 StGB entnehmen. Es ist somit davon auszugehen, dass dem Eigentümer einer Server-Infrastruktur das Antragsrecht abgeht, wenn er einen Teil der Infrastruktur an Dritte «vermietet». Meist erfolgt eine solche «Vermietung» nicht etwa über Teile des physischen Servers, sondern über das Zurverfügungstellen von Kapazitäten des Servers (Rechenzeit, Arbeitsspeicher, Festplattenspeicher etc.). Dies geschieht vielfach über Sub-Systeme, welche über vom Host-System abgeschottete eigene Prozesse laufen. Beim Eindringen in ein solches Sub-System ist nur das Rechtsgut des Benutzers des Sub-System verletzt, der Betreiber oder Eigentümer des Host-Systems kann in der Regel über dieses Sub-System keine Herrschaft ausüben, mithin hat er kein Antragsrecht. Anders verhält es

147 Eine Information an den vom Strafantrag resp. der Strafanzeige Betroffenen erfolgt nicht unbedingt innerhalb der Antragsfrist, womit bei einer fristgerechten Erhebung des Strafantrags eine Information an die beschuldigte Person auch nach den 90 Tagen erfolgen kann.

148 Statt vieler: BGE 128 IV 81, E. 3; 118 IV 209, E. 2; 111 IV 63, E. 3.

149 BGE 87 IV 105, E. 2; Praxiskommentar StGB-Trechsel/Geth, Art. 30 N 2.

150 Zum Ganzen: Online Kommentar StGB-Kost, Art. 143bis.

151 Vgl. Urteil des BGer 6B_456/2007 vom 18. März 2008; Obergericht Zürich, Urteil UE140147 vom 13. September 2014, E. 6.2.1.

152 BGE 112 IV 31, E. 3.

sich, wenn der Angreifer aus der virtuellen Umgebung des Sub-Systems in das Host-System vordringt.

188 Unklar scheint die Situation etwa bei unberechtigten Zugriffen auf E-Mail-Accounts, insbesondere in Fällen, in denen der Nutzer des geschützten Kontos keinen Strafantrag stellt. E-Mail-Accounts sind meist keine Sub-Systeme, vielmehr ist es so, dass der Serviceprozess, welcher auf dem Server läuft, je nach Zugangsdaten andere Inhalte zeigt. Somit liegt der Schluss nahe, dass neben dem Nutzer des E-Mail-Accounts auch der Provider zum Strafantrag berechtigt ist.

5.7. Weitere Tatbestände

189 Nebst Art. 143bis und 144bis StGB gibt es im Schweizer Strafrecht auch noch weitere Bestimmungen, welche in Zusammenhang mit Initiativprojekten potenziell zur Anwendung gelangen könnten.

5.7.1. Strafbarkeit nach Art. 179^{novies} StGB

> ***Art. 179^{novies} StGB Unbefugtes Beschaffen von Personendaten***
>
> *Wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*[153]

190 Art. 179^{novies} StGB schützt die datenschutzrechtlich besonders behandelten schützenswerten Personendaten (Art. 3 lit. c DSG) strafrechtlich. Darunter fallen abschliessend Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe und administrative oder strafrechtliche Verfolgungen und Sanktionen.[154]

191 Geschütztes Rechtsgut sind dabei primär die Persönlichkeitsrechte der Personen, auf die sich die Daten beziehen, wobei auch über den Schutz des Gewahrsams des Dateninhabers diskutiert wird.[155]

192 *Beschaffen* bedeutet das Überwinden oder Umgehen der Zugangssperre, da der Tatbestand verlangt, dass die besonders schützenswerten Daten nicht frei

---

153 Änderung mit Totalrevision DSG per 1.09.2023: *Wer unbefugt besonders schützenswerte Personendaten, die nicht für jedermann zugänglich sind, beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*

154 Vgl. BSK DSG-BLECHTA, Art. 3 N 30.

155 Dazu BSK StGB-RAMEL/VOGELSANG, Art. 179^{novies} N 4 ff., diese Diskussion wirkt sich insbesondere auf die Frage der Strafantragsberechtigung des Dateninhabers aus.

zugänglich sein dürfen.[156] Es bedeutet nicht notwendigerweise das Begründen einer eigenen Verfügungsgewalt über die Daten (etwa sichern, herunterladen, o.Ä.), die blosse Kenntnisnahme der Daten genügt. Ein Eindringen in eine Datenverarbeitungsanlage ohne Kenntnisnahme der entsprechenden Daten erfüllt den Tatbestand indes nicht.[157]

193 Das Risiko einer Tatbegehung nach Art. 179^novies StGB bei der Durchführung von Initiativprojekten[158] wird somit entscheidend vom Verhalten der durchführenden Personen nach Eindringen in die fremde Datenverarbeitungsanlage sowie von der Sensibilität der zu erwartenden Daten im Zielsystem abhängen. Sobald ein Analyst bei einem Penetrationstest auf besonders schützenswerte Daten stösst, sollte er die Sicherheitslücke nicht weiter explorieren (vgl. dazu auch die Rahmenbedingungen und Regeln des NCSC, zu deren Einhaltung sich das NTC verpflichtet).[159]

5.7.2. Daten auf fremden Geräten (Art. 45c FMG i.V.m. Art. 53 FMG)

194 Gemäss Art. 45c FMG dürfen Personendaten[160] auf fremden Geräten nur dann durch fernmeldetechnische Übertragung (Art. 3 lit. c FMG) bearbeitet werden, wenn der Bearbeiter den betroffenen Benutzer zuvor über die Bearbeitung und ihren Zweck informiert hat und den Letzteren darauf hingewiesen hat, dass er die Bearbeitung ablehnen kann.[161] In Verbindung mit Art. 53 FMG kann eine vorsätzliche sowie fahrlässige Verletzung dieser Bestimmung strafrechtlich mit einer Busse von bis zu 5'000 Franken sanktioniert werden.[162]

195 Unter fernmeldetechnische Übertragung fallen nach Art. 3 lit. c FMG das elektrische, magnetische, optische oder andere elektromagnetische Senden oder Empfangen von Informationen über Leitungen oder Funk (insbesondere Internet-Übertragung und Übermittlung via Mobilfunknetze). Die Bestimmung richtet sich an alle, die mit den genannten Techniken Personendaten bearbeiten, nicht nur an Fernmeldedienstanbieter. Dabei ist mit *Bearbeiten* die Speicherung, der Zugriff und jede sonstige Bearbeitung gemeint.[163] Der Gesetzgeber wollte insbesondere Eingriffe wie die Installation und Nutzung von sog. *Cookies*,

---

156 Botschaft 1991, 1011.

157 So BSK StGB-RAMEL/VOGELSANG, Art. 179^novies N 23 explizit zum *Hacking*.

158 Vgl. GERMANN/WICKI-BIRCHLER, Hacking, S. 89, welche das Risiko insbesondere bei den *Hacking*-Methoden *Phishing*, *Spear-Phishing*, *Malware* und *Ransomware* verortet sehen, da diese Methoden die technische Fähigkeit haben, dem *Hacker* direkt Daten (jeglicher Art) zugänglich zu machen.

159 Nationales Zentrum für Cybersicherheit (NCSC): Rahmenbedingungen und Regeln <www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html> (zuletzt besucht am 25. Juni 2023).

160 Vgl. Handkommentar DSG-ROSENTHAL/JÖHRI, Art. 45c N 6.

161 VASELLA, Social Media, S. 262.

162 Art. 53 FMG.

163 Handkommentar DSG-ROSENTHAL/JÖHRI, Art. 45c N 4; zum Begriff des Bearbeitens, Botschaft 2003, 7987.

Web-Bugs oder *Spyware* erfassen.[164] Die Definition von Personendaten ergibt sich aus Art. 3 lit. a DSG, das Bearbeiten anonymer Daten ist nicht erfasst.[165] Nicht erfasst sind ausserdem Techniken, mit denen zwar in Kombination mit weiteren Daten ein Personenbezug hergestellt werden könnte, dieser aber nicht vorgesehen ist.[166]

196 Werden im Rahmen von Initiativprojekten beispielsweise Logdaten mit Personenbezug zu Drittpersonen auf einem fremden Gerät generiert, so könnte dies (aufgrund der fehlenden entsprechenden Information an die Betroffenen) ein Verstoss gegen Art. 45c FMG darstellen.

5.7.3. Konkurrenzen

197 Art. 143bis Abs. 1 und 143bis Abs. 2 StGB stehen zueinander in echter Konkurrenz. Sodann ist Art. 143bis Abs. 1 StGB im Verhältnis zu den übrigen Cyberdelikten namentlich zu den Art. 143 und 144bis Ziff. 1 sowie zu Art. 179^{novies} StGB[167] subsidiär resp. wird die Tathandlung von Art. 143bis Abs. 1 StGB konsumiert, so etwa bei Art. 144bis Ziff. 1 StGB.[168]

198 Echte Konkurrenz zu Art. 144bis Ziff. 1 ist ausnahmsweise dort denkbar, wo durch das tatbestandsmässige Verhalten nach Art. 143bis Abs. 1 StGB, neben den im Rahmen dieser Bestimmung verletzten Berechtigten noch weitere Personen gefährdet werden. Dies wäre etwa der Fall, wenn jemand Daten löscht in einem Datenverarbeitungssystem, welches einem Dritten gehört, der nicht Datenberechtigter ist.[169] Zwischen Art. 143bis und Art. 144bis Ziff. 2 StGB kann regelmässige echte Konkurrenz angenommen werden, da sich das Gefährdungspotential von *Malware* nicht im reinen Eindringen erschöpft.[170]

199 Daneben steht Art. 45c FMG zu den Tatbeständen des Computerstrafrechts in echter Konkurrenz, da ein anderes Rechtsgut geschützt ist.[171]

5.8. Internationale Strafzuständigkeit der Schweiz

200 Die Computerdelikte sind regelmässig Distanzdelikte, somit ergeben sich bei deren Verfolgung auch Fragen der internationalen Strafzuständigkeit.

---

164 Botschaft 2003, 7987; vgl. VASELLA, Social Media, S. 262; Handkommentar DSG-ROSENTHAL/JÖHRI, Art. 45c FMG N 8.

165 Handkommentar DSG-ROSENTHAL/JÖHRI, Art. 45c FMG N 7 und 19.

166 Ibid., Art. 45c FMG N 20.

167 Bei Art. 179^{novies} StGB wird teilweise aufgrund der Verschiedenheit der Rechtsgüter (Persönlichkeitsrechte vs. Verfügungsgewalt) für echte Konkurrenz argumentiert, so etwa BSK StGB-RAMEL/VOGELSANG, Art. 179^{novies} N 33.

168 BSK StGB-WEISSENBERGER, Art. 143bis N 30-33; DONATSCH et al., StGB, Art. 143 N 1.

169 BSK StGB-WEISSENBERGER, Art. 144bis N 80.

170 BALTISSER, Datenbeschädigung, S. 130 f.

171 Handkommentar DSG-ROSENTHAL/JÖHRI, Art. 45c FMG N 29.

201 Die territoriale Anwendbarkeit des Schweizer Strafgesetzbuch ist in den Art. 3 ff. geregelt (in Bezug auf die CCC insbesondere auch Art. 6 StGB).

202 Angeknüpft wird gemäss Art. 3 StGB an den Begehungsort. Dieser definiert sich nach Art. 8 StGB, wobei ein Verbrechen oder Vergehen als dort begangen gilt, «wo der Täter es ausführt oder pflichtwidrig untätig bleibt, und da, wo der Erfolg eingetreten ist».[172]

203 Im Bereich der Cyberdelikte gilt als Ausführungsort grundsätzlich der Ort, an dem sich der Täter bei der Auslösung der die Prozesse auslösenden Programmbefehle aufhält.[173] Dabei ist es regelmässig der Fall, dass der Ort, an dem ein Täter handelt (z.B. an seinem eigenen Computer) nicht mit demjenigen übereinstimmt, an dem sich die Daten oder die Datenverarbeitungsanlage befinden, auf die eingewirkt wird.[174] Ein vom Handlungsort getrennter, zusätzlicher Anknüpfungsort (über den Erfolgsort) nach Art. 8 StGB kann indes nur bei Verletzungs- und bei konkreten Gefährdungsdelikten (Erfolgsdelikten), nicht aber bei schlichten Tätigkeits- oder abstrakten Gefährdungsdelikten vorliegen (vgl. jedoch unten Rz 206 f.).[175]

204 Bei den Cyberstraftatbeständen sind die Datenbeschädigung (Art. 144bis Ziff. 1 StGB) und der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB) typische Erfolgsdelikte. Die unbefugte Datenbeschaffung (Art. 143 StGB) und die Datenfälschung (Art. 251 StGB) werden als schlichte Tätigkeitsdelikte qualifiziert. Die Deliktsnatur des unbefugten Eindringens in eine Datenverarbeitungsanlage (Art. 143bis Abs. 1 StGB) ist nicht eindeutig geklärt, wobei teilweise im Sinne eines schlichten Tätigkeitsdelikts argumentiert wird,[176] andere Meinungen hingegen von einem Verletzungs- oder konkreten Gefährdungsdelikt ausgehen.[177] Um abstrakte Gefährdungsdelikte handelt es sich sodann bei Art. 143bis Abs. 2 sowie Art. 144bis Ziff. 2 StGB.[178]

205 Aufgrund des oben zu Art. 8 StGB Ausgeführten hätte dies zur Folge, dass die Tätigkeitsdelikte und die abstrakten Gefährdungsdelikte lediglich dann in der Schweiz verfolgt werden könnten, wenn der Täter diese in der Schweiz ausgeführt hat. Dies selbst wenn auf eine in der Schweiz gelegene Datenverarbeitungsanlage eingewirkt würde.[179]

---

172 Art. 8 Abs. 1 StGB.

173 Wirtschaftsstrafrecht-Graf, S. 1023.

174 Ibid., S. 1022.

175 BSK StGB-Popp/Keshelava, Art. 8 N 9.

176 Wirtschaftsstrafrecht-Graf, S. 1022.

177 BSK StGB-Weissenberger, Art. 143bis N 6, mit weiteren Hinweisen.

178 Wirtschaftsstrafrecht-Graf, S. 1022.

179 Müller, cloud computing, S. 308; vgl. auch Wirtschaftsstrafrecht-Graf, S. 1022 f.

206 Dieses Resultat wurde aufgrund der Natur von Cyberdelikten zu Recht als unbefriedigend kritisiert. Das Bundesgericht hat der Kritik in seiner neueren Rechtsprechung Rechnung getragen und verlangt für eine Anknüpfung nicht mehr einen eigentlichen Erfolg, sondern «un rattachement territorial».[180] Dieses Kriterium ist für die strafrechtliche Anknüpfung in der Schweiz insbesondere dann gegeben, wenn die betroffene Datenverarbeitungsanlage oder die Daten sich in der Schweiz befinden.[181] Faktisch kann also sowohl das Handeln eines Täters in der Schweiz mit Einwirken auf Datenverarbeitungsanlagen oder Daten im Ausland, als auch der umgekehrte Fall, eine Strafzuständigkeit in der Schweiz begründen. Selbst wenn der Täter aus dem Ausland handelt, die Datenverarbeitungsanlage ebenfalls im Ausland ist (z.B. Cloudsystem), der Geschädigte jedoch seinen Sitz in der Schweiz hat, kann dies eine Schweizer Strafzuständigkeit begründen.[182]

207 Zuletzt könnte auch ein ausländischer, sich aktuell in der Schweiz befindlicher Täter, welcher eine Straftat, die unter das CCC fällt, vollumfänglich im Ausland und gegen ausländische Opfer begangen hat, gestützt auf Art. 6 StGB in der Schweiz verfolgt und verurteilt werden.[183]

6. Fazit

208 Analysten handeln im Rahmen von Initiativprojekten regelmässig tatbestandsmässig im Sinne von Art. 143bis Abs. 1 StGB, sofern sie sich nicht auf straflose Vorbereitungshandlungen (wie etwa *Portscanning,* etc.) beschränken. Je nach den konkreten Umständen der Schwachstellenanalysen ist auch ein (kollaterales) tatbestandsmässiges Handeln nach Art. 144bis Ziff. 1 StGB gegeben.

209 Als strafrechtlicher Rechtfertigungsgrund können sich Analysten auf den Notstand nach Art. 17 StGB berufen, sofern sie die diskutierten Voraussetzungen erfüllen. Insbesondere braucht es vor der Durchführung eines Initiativprojekts konkrete Anzeichen für das Vorhandensein von Sicherheitslücken im Zielsystem. Sodann ist bei der Durchführung von Initiativprojekten die Eingriffsintensität in Nachachtung des Prinzips der Subsidiarität bzw. der Interessenabwägung möglichst gering zu halten und die Initiativprojekte müssen dem Zweck der Beseitigung der Gefahr dienen.

210 Die Veröffentlichung von Erkenntnissen aus Initiativprojekten ist nicht tatbestandsmässig im Sinne von Art. 143bis Abs. 2 StGB, sofern eine darin

[180] Vgl. BGE 141 IV 336, E. 1.2.
[181] Wirtschaftsstrafrecht-Graf, S. 1023 f.
[182] Müller, cloud computing, S. 309.
[183] Wirtschaftsstrafrecht-Graf, S. 1024.

dokumentierte Sicherheitslücke vor Veröffentlichung bereits vollständig behoben wurde, oder aber der Detailierungsgrad der Publikation es einem Dritten nicht oder nur mit erheblichem Mehraufwand ermöglicht, darauf basiert eine entsprechende Tathandlung nach Art. 143bis Abs. 1 StGB selbst vorzunehmen.

Literaturverzeichnis

ACKERMANN et al., Strafrecht	Jürg-Beat Ackermann/Patrick Vogler/Laura Baumann/Samuel Egli, Strafrecht Individualinteressen, Gesetz, System und Lehre im Lichte der Rechtsprechung, Bern 2019.
BALTISSER, Datenbeschädigung	Annina Baltisser, Datenbeschädigung und Malware im Schweizer Strafrecht, Der Tatbestand des Art. 144bis StGB im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, Diss. Zürich, Zürcher Studien zum Strafrecht Bd. 69, Zürich 2013.
BSK DSG-BEARBEITER/IN	Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz (DSG)/Öffentlichkeitsgesetz (BGÖ), 3. Aufl., Basel 2014.
BSK StGB-BEARBEITER/IN	Marcel Alexander Niggli/Hans Wiprächtiger (Hrsg.), Basler Kommentar Strafrecht (StGB), 4. Aufl., Basel 2019.
CAPRARA, Klimaaktivisten	Tommaso Caprara, Straftaten von Klimaaktivisten gegen Grossbanken können nicht gerechtfertigt werden, forumpoenale 2/2022 S. 137 ff.
DOLDER/WÜEST, IT-Recht	Fritz Dolder/Candid Wüest, Entscheidungen zum schweizerischen IT-Recht, 2016.
DONATSCH et al., StGB	Andreas Donatsch/Stefan Heimgartner/Bernhard Isenring/Hans Maurer/Marcel Riesen-Kupper in: Andreas Donatsch (Hrsg.), StGB/JStG Kommentar, Mit weiteren Erlassen und Kommentar zu den Strafbestimmungen des SVG, BetmG, AIG und OBG, 21. Aufl., Zürich 2022.
DONATSCH, Strafrecht III	Andreas Donatsch, Strafrecht III, Delikte gegen den Einzelnen, 11. Aufl., Zürich 2018.
DONATSCH/TAG, Strafrecht I	Andreas Donatsch/Brigitte Tag, Strafrecht I, Verbrechenslehre, 10. Aufl., Zürich 2021.
GERMANN/WICKI-BIRCHLER, Hacking	Sandro Germann/David Wicki-Birchler, Hacking und Hacker im Schweizer Recht, AJP 2020 S. 83 ff.
GRÜNER, Hacker-Verfahren	Sebastian Grüner, Hacker-Verfahren wegen CDU-Wahlkampf-App eingestellt, 17. September 2021, verfügbar unter: <www.golem.de/news/connect-app-hacker-verfahren-wegen-cdu-

	wahlkampf-app-eingestellt-2109-159658.html> (zuletzt besucht am 25. Juni 2023).
Online Kommentar StGB-KOST	Roman Kost, Kommentar zu Art. 143bis – Unbefugtes Eindringen in ein Datenverarbeitungssystem, verfügbar unter: <143bis.ch/kommentar/stgb-143bis/> (zuletzt besucht am 25. Juni 2023).
MÄDER, Verschlüsselung	Lukas Mäder, «Verschlüsselung hinkt Jahre hinterher»: Der Schweizer Messenger Threema setzte bis vor kurzem auf veraltete Kryptografie, NZZ vom 9. Januar 2023, verfügbar unter: <www.nzz.ch/technologie/threema-schweizer-messenger-hatte-schwaechen-bei-verschluesselung-ld.1719543> (zuletzt besucht am 25. Juni 2023).
MÜLLER, cloud computing	Jérémie Müller, For et droit pénal applicable au cloud computing, forumpoenale 5/2013 S. 306 ff.
NAFZGER, Safe Harbor	Sandro Nafzger, Legal Safe Harbor – So werden ethische Hacker entkriminalisiert, verfügbar unter: <www.bugbounty.ch/legal-safe-harbor/> (zuletzt besucht am 25. Juni 2023).
PATERSON/SCARLATA/TUONG TRUONG, Threema	Kenneth G. Paterson, Matteo Scarlata, Kien Tuong Truong, Three Lessons from Threema, verfügbar unter (mit Möglichkeit zum Download): <breakingthe3ma.app/> (zuletzt besucht am 25. Juni 2023).
PAYER, Interessen	Andrés Payer, Zur Wahrnehmung berechtigter Interessen im Strafrecht, recht 2020 S. 186 ff.
PAYER, Klimawandel	Ders., Klimawandel und strafrechtlicher Notstand, ex ante 2/2020 S. 21 ff.
Praxiskommentar StGB- AUTOR/IN	Stefan Trechsel/Mark Pieth (Hrsg.), Schweizerisches Strafgesetzbuch – Praxiskommentar, 4. Aufl., Zürich 2021.
Handkommentar DSG-ROSENTHAL/JÖHRI	David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.
SCHMID, Computer	Niklaus Schmid, Computer- sowie Check- und Kreditkartenkriminalität – Ein Kommentar zu den neuen Straftatbeständen des schweizerischen Strafgesetzbuches, Zürich 1994.

StGB Annotierter Kommentar-AUTOR/IN	Damian K. Graf (Hrsg.), StGB Annotierter Kommentar, Bern 2020.
STRATENWERTH, AT I	Günter Stratenwerth, Schweizerisches Strafrecht – Allgemeiner Teil I: Die Straftat, 4. Aufl., Bern 2011.
STRATENWERTH/BOMMER, BT I	Günter Stratenwerth/Felix Bommer, Schweizerisches Strafrecht – Besonderer Teil I: Straftaten gegen Individualinteressen, 8. Aufl., Bern 2022.
VASELLA, Social Media	David Vasella, Kapitel 7: Social Media und Datenschutz / II. – III., in: Oliver Staffelbach / Claudia Keller (Hrsg.), Social Media und Recht für Unternehmen, Zürich 2015.
Wirtschaftsstrafrecht-AUTOR/IN	Jürg-Beat Ackermann (Hrsg.), Wirtschaftsstrafrecht der Schweiz. Hand- und Studienbuch, 2. Aufl., Bern 2021.
Handkommentar StGB-WOHLERS	Wolfgang Wohlers, Schweizerisches Strafgesetzbuch – Handkommentar, 4. Aufl., Bern 2020.

Materialienverzeichnis

(in chronologischer Reihenfolge)

Botschaft über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung) sowie betreffend die Änderung des Bundesgesetzes über die wirtschaftliche Landesversorgung (Strafbestimmungen) vom 24. April 1991, BBl 1991 II 969 ff. (zitiert: Botschaft 1991)

Botschaft zur Änderung des Fernmeldegesetzes (FMG) vom 12. November 2003, BBl 2003 7951 ff. (zitiert Botschaft 2003)

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010, BBl 2010 4697 ff. (zitiert: Botschaft 2010)

Botschaft zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen) vom 2. Dezember 2022, BBl 2023 84. (zitiert Botschaft 2023)

Nationales Zentrum für Cybersicherheit (NCSC): Nationale Cyberstrategie (NCS) vom April 2023, <https://www.newsd.admin.ch/newsd/message/attachments/76793.pdf> (zuletzt besucht am 25. Juni 2023)

Webseiten

Blog Yes We Hack: Abusing S3 Bucket Permissions, <blog.yeswehack.com/yeswerhackers/abusing-s3-bucket-permissions/> (zuletzt besucht am 25. Juni 2023)

Centre for Cyber Security Belgium (CCB): Vulnerability Reporting to the CCB, <ccb.belgium.be/en/vulnerability-reporting-ccb> (zuletzt besucht am 25. Juni 2023)

CERT-EU: Coordinated Vulnerability Disclosure Policy, <cert.europa.eu/coordinated-vulnerability-disclosure-policy> (zuletzt besucht am 25. Juni 2023)

Council of Europe, Treaty Office: Reservations and Declarations for Treaty No. 185 – Convention on Cybercrime, <www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0> (zuletzt besucht am 25. Juni 2023)

European Union Agency for Cybersecurity: Coordinated Vulnerability Disclosure Policies in the EU, April 2022, <https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu> (zuletzt besucht am 25. Juni 2023)

Fowler Martin: CodeSmell, Beitrag vom 9. Februar 2006, <martinfowler.com/bliki/CodeSmell.html> (zuletzt besucht am 25. Juni 2023)

Google: Google Project Zero Vulnerability Disclosure, <googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html> (zuletzt besucht am 25. Juni 2023)

Hacktricks Boitatech: AWS-S3, <hacktricks.boitatech.com.br/pentesting/pentesting-web/buckets/aws-s3> (zuletzt besucht am 25. Juni 2023)

Heise Online: Modern Solution: Staatsanwaltschaft scheitert mit Anklage gegen IT-Experten, <https://heise.de/-9182813> (zuletzt besucht am 25. Juni 2023)

Nationales Zentrum für Cybersicherheit (NCSC): Rahmenbedingungen und Regeln, <www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/schwachstelle-melden/scope-and-rules.html> (zuletzt besucht am 25. Juni 2023)

National Cyber Security Centre (NCSC UK): NCSC Scanning Information, <https://www.ncsc.gov.uk/information/ncsc-scanning-information> (zuletzt besucht am 25. Juni 2023)

National Cyber Security Centre (NCSC UK): Scanning the Internet for Fun and Profit, <https://www.ncsc.gov.uk/blog-post/scanning-the-internet-for-fun-and-profit> (zuletzt besucht am 25. Juni 2023)

Nationales Testinstitut für Cybersicherheit (NTC): Technische Sicherheitsanalyse Mobile App «Tiktok», Begutachtung der Sicherheitsrisiken aus Schweizer Perspektive, <https://www.ntc.swiss/hubfs/NTC-security-analysis-tiktok-v1.0-de.pdf?hsCtaTracking=eb438ecd-a370-4935-b105-8eba59b68220%7Cd6f23147-1db5-4f44-9575-d48332f2b4d9Y> (zuletzt besucht am 25. Juni 2023)

Nationales Testinstitut für Cybersicherheit (NTC): Vulnerability Disclosure Policy, <https://www.ntc.swiss/ueber-uns/rechtsdokumente> (zuletzt besucht am 16. Juni 2023)

Open Web Application Security Project (OWASP): Vulnerability Disclosure Cheat Sheet, <cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html> (zuletzt besucht am 25. Juni 2023)

Schweizerische Post: Swiss Post bug bounty programme, Securing digital trust, <www.post.ch/en/about-us/responsibility/swiss-post-bug-bounty?shortcut=bug-bounty> (zuletzt besucht am 25. Juni 2023)

UN Office of Information and Communications Technology: United Nations Responsible Disclosure & Reporter Acknowledgment Policy, <unite.un.org/content/united-nations-responsible-disclosure-reporter-acknowledgment-policy> (zuletzt besucht am 25. Juni 2023)

US Department of Homeland Security: Vulnerability Disclosure Program Policy and Rules of Engagement, <https://www.dhs.gov/publication/vulnerability-disclosure-program-policy-and-rules-engagement> (zuletzt besucht am 25. Juni 2023)

Glossar

Browser	Software-Anwendung zur Darstellung von Webseiten im World Wide Web oder allgemein von Dokumenten und Daten. Benutzeroberfläche für Webanwendungen, die es Benutzern ermöglicht, Webseiten aufzurufen, Links zu folgen, Formulare auszufüllen und andere Interaktionen mit Webseiten durchzuführen.
Brute-Forcing	Cyber-Angriffsmethode, um Passwörter und andere Zugangsdaten zu knacken. Bei einer Brute-Force-Attacke testet der Angreifer meist mittels eines Automatisierungstools eine Liste an häufigen Wörtern oder Buchstabenkombinationen und probiert sie der Reihe nach durch, bis ein Zugang geknackt ist.
Bug Bounty-Programm	Eine durch Unternehmen, Interessenverbände, Privatpersonen oder Regierungsstellen betriebene Initiative, in welcher für das Identifizieren oder Bekanntmachen von Sicherheitslücken in Software, Anwendungen oder Webdiensten meistens Prämien in Geld- oder Sachpreisen ausgelobt werden.
Code Smell	Oberflächlicher Hinweis auf tieferliegende Probleme in einem System
Cookies	Ein Cookie ist eine Textinformation, die im Browser auf dem Endgerät des Betrachters jeweils zu einer besuchten Website gespeichert werden kann. Das Cookie wird entweder vom Webserver an den Browser gesendet oder im Browser von einem Skript erzeugt.
Cross-Site-Scripting (XSS)	Eine an Webanwendungen gerichtete Cyber-Angriffsmethode, die über Code-Injektion schädliche Skripts an den Browser eines Benutzers zur Ausführung sendet
Daten	Gemäss Definition in Rz 28
Datenverarbeitungsanlage	Gemäss Definition in Rz 28
Denial of Service	Cyber-Angriffsmethode, bei der ein Server gezielt mit so vielen Anfragen bombardiert wird, dass das System die

	Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall nicht mehr verfügbar ist.
Ethical Hacking	Gemäss Definition in Rz 23
Exploit	Programm, Code, Script, oder Plugins für ein Hacking Tool, mit welchem ein Hack auf eine Datenverarbeitungsanlage ausgeführt werden kann.
Firewall	Vorinstallierte Schutzvorrichtung von Datenverarbeitungsanlagen/Systemen gegen fremden Zugriff über ein Netzwerk
Hacker	Person, die Hacks durchführt
Hacking/Hacks	Gemäss Definition in Rz 22
Hardware	Alle technisch-physischen Komponenten eines Datenverarbeitungssystem (im Unterschied zu Software)
Malware	Software (wie z.B. Schadprogramme, Viren, Würmer usw.), die in Datenverarbeitungssysteme eindringen oder dort implementiert werden und Störungen oder Schäden verursachen können.
NCSC	Nationales Zentrum für Cybersicherheit
Netzwerk	Zusammenschluss verschiedener technischer, primär selbstständiger elektronischer Systeme, der die Kommunikation der einzelnen Systeme untereinander ermöglicht.
NTC	Nationales Testinstitut für Cybersicherheit
Patch	Aktualisierung für Software/Betriebssystemen, die Korrekturen vornimmt und/oder Sicherheitslücken schliesst
Penetrationstest	Test der Sicherheit von vernetzten Komponenten und Anwendungen eines Netzwerks/Datenverarbeitungssystems mit Mitteln und Methoden, die tauglich sind, um unautorisiert in das System einzudringen (Penetration).
Phishing	Unrechtmässige Beschaffung von persönlichen Daten über gefälschte Websites, E-Mails oder Kurznachrichten

	mit dem Ziel, bspw. Zugangsdaten des Opfers erhältlich zu machen (Form des Social-Engineerings).
Portscan	Technik, um offene Netzwerkports bei einem Datenverarbeitungssystem zu identifizieren. Dafür werden systematisch spezielle Datenpakete an die unterschiedlichen Ports von einem Zielsystem gesendet und dabei die Fehlermeldungen und Antworten analysiert.
Proof of Concept	Technische Darlegung eines *Exploits*, wobei dieser auf eine für das Zielsystem unschädliche Funktion reduziert wird.
Ransomware	Software (wie z.B. Schadprogramme, Viren, Würmer usw.), die den Zugriff auf Daten und Systeme einschränken oder unterbinden und nur durch die Bezahlung von Lösegeldforderungen wieder freigibt.
Reverse-Engineering	Rückentwicklung eines bestehenden Systems, meist zum Verständnis der Architektur, Funktionsweise und internen Strukturen allf. zur Nachentwicklung
Safe Harbor	Institutionalisiertes Framework, worin Personen, die (System-)Schwachstellen ohne betrügerische oder böswillige Absicht untersuchen und melden, denen Straffreiheit garantiert wird, wenn sie gewisse Kriterien einhalten.
Schwachstellenanalyse / Vulnerability Assessment	Ganzheitliche Sicherheitsanalyse eines Zielsystems, welche regelmässig auch Penetrationstests umfasst.
Server	Computerprogramm oder Gerät, welches Funktionalitäten, Dienstprogramme, Daten oder andere Ressourcen bereitstellt, damit andere Geräte oder Programme darauf zugreifen können, meist über ein Netzwerk.
Sicherheitslücke	Schwachstelle, Anfälligkeit oder Lücke in einer Datenverarbeitungsanlage, die zum unbefugten Eindringen in ein Datenverarbeitungssystem ausgenutzt werden könnte.
Social-Engineering	Cyber-Angriffsmethode, bei dem Menschen manipuliert werden, dass sie gegen normale Sicherheitsverfahren und bewährte Praktiken verstossen, um sich beispielsweise

	unbefugten Zugang zu einem Datenverarbeitungssystem zu verschaffen.
Software	Alle nicht technisch-physikalischen Funktionsbestandteile eines Datenverarbeitungssystems (im Unterschied zu Hardware), insbesondere Programme
Spyware	Software, welche Informationen über ein System resp. die sich darauf befindlichen Daten sammelt oder das Verhalten der Benutzer ausspioniert.
Threat Intelligence	Evidenzbasierte Information über Cyberangriffe, die von Experten für Cyber-Security geordnet und analysiert wird.
Web-Bug	Ein kleines grafisches Bild oder ein Stück Code, das in eine Webseite oder eine E-Mail-Nachricht eingebettet ist, um Informationen über die Besucheraktivitäten auf einer Website oder in einer E-Mail zu sammeln