www.jusletter.ch

Roman Kost

Plädoyer für ein neues Hackingstrafrecht

Strafbefreiung von «Ethical Hacking»

Seit 1992 ist Hacking in der Schweiz strafbar. Ob mit redlicher Absicht gehackt wird, spielt keine Rolle. Dieser Beitrag zeigt den Wert von ethischer IT-Sicherheitsforschung für Gesellschaft und Wirtschaft auf, beleuchtet die rechtliche Situation ethischer Hackerinnen und Hacker in der Schweiz und plädiert mit einem Revisionsvorschlag dafür, ethisches Hacking in der Schweiz zu legalisieren.

Beitragsart: Essay
Rechtsgebiete: Datenschutz, Strafrecht

Zitiervorschlag: Roman Kost, Plädoyer für ein neues Hackingstrafrecht, in: Jusletter 31. März 2025

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

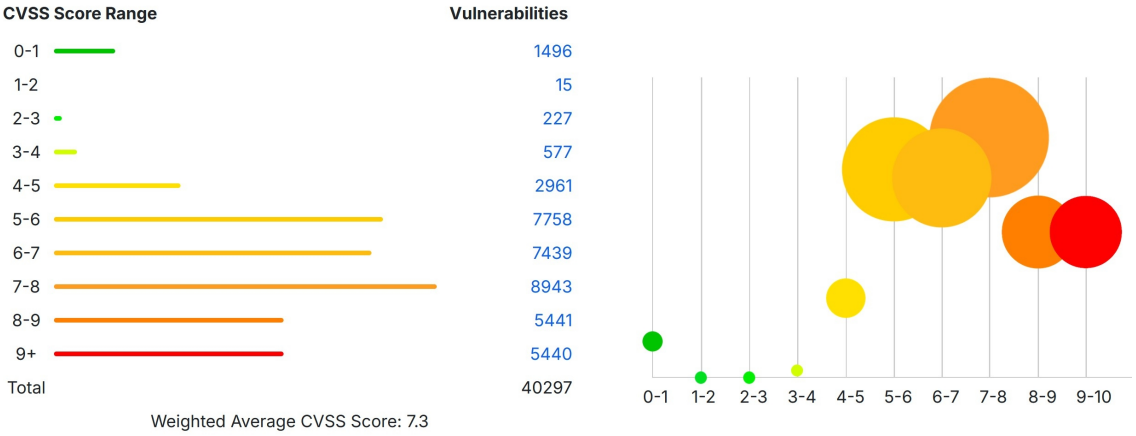
Inhaltsübersicht

1. Ausgangslage

[1] Seit 1999 werden im *Common Vulnerabilities and Exposures* (CVE) System Schwachstellen von IT-Systemen systematisch erfasst.[1,2] 2024 wurden im Schnitt täglich über 100 neue Schwachstellen veröffentlicht. Unter den über 40'000 neuen Schwachstellen im Jahr 2024 waren es insgesamt 5'440 (vgl. nachstehende Abbildung), die mit dem Risiko «kritisch» (Score von > 9) bewertet worden sind. Kritische Schwachstellen können z.B. die direkte Übernahme eines Systems aus der Ferne ermöglichen, einen sehr grossen Kreis an Systemen betreffen, enorme Auswirkungen auf Schutzziele haben oder sie zeichnen sich durch sehr geringe Komplexität aus und sind darum durch interessierte Akteure leicht ausnutzbar. 2014, nur zehn Jahre zuvor, waren es noch durchschnittlich 30 publizierte Einträge täglich, 2004 waren es noch keine fünf publizierten Schwachstellen am Tag.

[1] Allgemeiner Hinweis zu Links: Sämtliche Links wurden am 17. März 2025 geprüft und besucht. In den Fussnoten wird diese Angabe nicht mehr wiederholt. Wo möglich, wurden Permalinks (∞) eingefügt.

[2] Das CVE-System ist ein amerikanische Forschungs- und Entwicklungscenter im Bereich der Cybersecurity (NCS FFRDC) und wird technisch von der amerikanischen Non-Profit-Organisation MITRE betrieben. Es gilt heute weltweit als das zentrale Instrument zur Verwaltung von Sicherheitslücken. Das BACS/NCSC des Bundes ist als CVE Numbering Authority dem CVE-System angeschlossen.



CVE-Publikationen zwischen dem 1. Januar 2024 und dem 31. Dezember 2024 nach Risiko gruppiert (Stand: 15. März 2025).[3]

[2] Die rasant steigende Zahl von Sicherheitslücken ist eindrücklich. Sie läuft parallel zur Tatsache, dass Computertechnologie mittlerweile ubiquitär geworden und mit unserem Alltag vollständig verflochten ist. Die IT-Landschaften haben eine Komplexität angenommen, die oft nicht mehr bewältigt werden kann – selbst von IT-Fachleuten mit langjähriger Praxis. Cloudsoftware baut beispielsweise auf unzähligen Bibliotheken auf, die jede für sich genommen eine potentielle Gefahrenquelle darstellen kann. Nebst dem Smartphone sind vernetzte Uhren, Tracker und Medizinalgeräte – vom Herzschrittmacher über das Hörgerät zur Insulinpumpe – zu täglichen Begleitern geworden. Obschon heute nur erste Gehversuche bestehen, steht es ausser Frage, dass auch vernetzte Brillen, Kontaktlinsen oder Gehirnimplantate zum Thema werden. Es entsteht aber nicht nur Neues. An allen denkbaren und undenkbaren Orten ist Hard- und Software im Einsatz, die bereits ihr Lebensende erreicht hat und keine Updates mehr erhält. Im besten Fall sind solche Legacy Devices noch nicht vergessen gegangen und werden gar noch aktiv gewartet. Die Realität hingegen sieht düster aus. Fehlende Inventarisierung und ungepatchte Systeme haben sich zu einem der grössten Risikofaktoren gemausert. Was in dieser ganzen Komplexität bleibt, sind die «Normalsterblichen», die sich auf die Dienstleister, die Hersteller und den Staat verlassen müssen. Sie gehen ihrer täglichen Arbeit nach, interagieren mit den Behörden im Rahmen ihrer Rechte und Pflichten oder pflegen ihre sozialen Kontakte im Alltag mit anderen Menschen. All das ist abhängig von digitaler Technologie.

[3] Es steht ausser Zweifel, dass der Mensch sich und seine Umwelt auch in Zukunft weiter vernetzen wird. Diese ganz grundlegende Feststellung zwingt uns, *ethisch* handelnde Sicherheitsforscherinnen und -forscher vor Strafverfahren und Strafen zu schützen. Kriminelle Hacker müssen weiterhin verfolgt werden. Kriminelle Hacker verursachen enorme Schäden wirtschaftlicher Natur und bewirken beispielsweise durch Leaks oder Datenhehlerei die Verletzung von Persönlichkeitsrechten unzähliger Menschen.

3 Quelle Abbildung cvedetails.com (∞). Bei dieser Risikobewertung wird auf das Common Vulnerability Scoring System (CVSS) Methodologie der Non-profit Organisation FIRST abgestellt. Darin werden unter anderem Aspekte wie der Angriffsvektor und die -komplexität sowie die Auswirkungen des Angriffs abgebildet, vgl. https://www.first.org/cvss/ und ausführlich ENISA, State Of The Art Vulnerabilities, 2018/2019 (∞).

[4] *Ethical Hacking* steht synonym zum Begriff Sicherheitsforschung. Ethisch hacken heisst, Sicherheitslücken zu entdecken, die betroffenen Systembetreiber über die Sicherheitslücken aufzuklären und dadurch zu helfen, generell die Sicherheit aller Systeme zu verbessern. Wer so handelt, soll straflos bleiben. Ethische Hackerinnen und Hacker betreiben unverzichtbare Sicherheitsforschung. Sie tun Gutes und handeln im Interesse der Gesellschaft. Ich plädiere deshalb für ein revidiertes Hackingstrafrecht.

[5] Zuerst aber die Ausgangslage:

1.1. Pentesting und Bug Bounty-Programme

[6] Bei *Pentests* wird auf der Basis klarer vertraglicher Abmachungen versucht, in Systeme einzudringen. Die Angreifer beginnen ihre Untersuchungen oft ohne detaillierte Informationen zu den Systemen (Black-Box-Pentesting), was am ehesten externe Angriffe simuliert. Oder sie erhalten vom Auftraggeber gewisse Informationen zur System- und Netzwerkarchitektur, was eher dem Szenario interner Angriffe entspricht (White-Box-Pentesting).[4]

[7] Die EU hat mit dem *Digital Operational Resilience Act* (DORA) für den Finanzsektor (Art. 2 Ziff. 1 DORA) Pflichten eingeführt, die unter anderem die Einführung von Riskmanagement Frameworks (Art. 6) inklusive das Durchführen von Pentests enthalten, die sich an aktuellen Bedrohungen zu orientieren haben (Art. 26).[5] Schweizer Finanzinstitute sind ebenfalls in der Pflicht, Cyber-Risiken zu Managen und regelmässige Pentests durchzuführen.[6] Zwar besteht keine explizite Pflicht zu Pentesting für kritische Infrastrukturen der Schweiz, Art. 8 Abs. 1 und 2 des Informationssicherheitsgesetzes (ISG) verlangen hingegen die Implementation eines Risikomanagements, wobei Pentests zur Beurteilung der laufenden Risiken zum aktuellen Stand der Wissenschaft und Erfahrung gehören.

[8] Bei *Bug Bounty*-Programmen wird ein meist unbestimmtes Publikum dazu aufgerufen, Systeme innerhalb eines bestimmten Scopes auf Schwachstellen zu untersuchen. Anhand im Voraus festgelegter Kriterien werden die Teilnehmenden für ihre Meldungen kompensiert.[7]

[9] Beim Pentesting wie auch bei Bug Bounty-Programmen ist es ausschlaggebend, welche Regeln gelten.[8] Darf nach einem initialen Zugriff im System die Umgebung gescannt und nach weiteren Schwachstellen gesucht werden (lateral movement)? Darf auf Datensätze irgendwelcher Art und in irgendeiner Form zugegriffen werden? Besteht dafür eine Rechtfertigungsgrundlage im Hinblick auf datenschutzrechtliche Vorgaben? Wie verhält es sich damit, wenn eine Vielzahl vorab unbekannter Sicherheitsforscherinnen und -forscher durch das Bug Bounty-Programm angespro-

4 NIST SP 800–192, S. 55 f. Für Web Application-Pentesting siehe Florian Widmer, Web-Applikationssicherheit, digma 2005, S. 40 ff.; mit zahlreichen Hinweisen und Beispielen: OECD, Encouraging Vulnerability Treatment – Responsible management, handling and disclosure of vulnerabilities (∞), 3. Februar 2021, S. 60.

5 Siehe Wortlaut des DORA (∞). Ausführlich zum Thema: Thorsten Ammann/Yannick Zirnstein, DORA – IT-Sicherheit gesetzlich verordnet, in: Compliance Berater 2023, S.21.

6 FINMA-Rundschreiben 23/1, Operationelle Risiken und Resilienz – Banken, N 69 (∞).

7 Vgl. für amerikanische Behördenprogramme z.B. NIST SP 800–216, S. 9 und S. S 27.

8 Wolfgang Straub, Informatikrecht – Einführung in Softwareschutz, Projektverträge und Haftung, S. 253 f.; Damian K. Graf, Strafbarkeit von «Ethical Hacking», «Bug Bounty Hunting» und «Penetration Testing», in: Jusletter 12. Februar 2024, N 13 ff.; siehe dazu Sandro Germann/David Wicki-Birchler, Hacking und Hacker im Schweizer Recht, AJP 1/2020, S. 90 f.

chen werden soll? Das sind einige Fragen, die sich stellen, wenn man den Sicherheitsforscherinnen und -forschern einen rechtssicheren Handlungsrahmen geben will.

[10] Zusammengefasst: Pentesterinnen und Bounty-Jäger hacken mit Befugnis, solange sie sich an die Vorgaben halten. Diese Befugnis schliesst die Tatbestandsmässigkeit aus.[9] Ihnen droht weder ein Strafverfahren noch eine Strafe. Der hier diskutierte Revisionsvorschlag betrifft keine Hacks auf vertraglicher Basis, also weder Bug Bounty-Programme noch Pentesting-Aufträge. Ebenfalls werden keine neuen Pflichten eingeführt, weder sektoriell oder gar für alle Systembetreiber. Im Fokus steht nur der «freischaffende» Hacker mit altruistischer Intention.

1.2. Notstand

[11] Elegant ist der Ansatz von Isler/Kunz/Moll[10], welche die Strafbarkeit von Hacking unter den Voraussetzungen des rechtfertigenden Notstands als rechtmässig erachten. Dieser Ansatz ist deshalb elegant, weil er keiner Novelle des Hackerstrafrechts bedürfte, schon heute würde damit eine Lösung existieren. Der rechtfertigende Notstand nach Art. 17 StGB birgt jedoch verschiedene Stolpersteine, die es der juristischen Praxis und ganz besonders den technisch versierten Forschenden verunmöglichen, in einem rechtssicheren Rahmen zu arbeiten, sprich zu hacken.

[12] Ausgehend vom Grundgedanken passt die Rechtsfigur des Notstands auf die Situation ethischer Hacker auf den ersten Blick gut. Es erfolgt ein eigentlich rechtswidriger Eingriff in fremde Rechtsgüter, welcher rechtmässig ist, sofern ohne diesen Eingriff Rechtsgüter Dritter gefährdet wären. Diese zu schützenden Rechtsgüter müssen höher gewichtet sein als jenes, in das eingegriffen wird. Ethische Hackerinnen greifen prototypisch in das Rechtsgut des Computerfriedens ein und melden dann ihr Vorgehen und die Schwachstelle der Systembetreiberin, damit diese dann die Schwachstelle behebt und die Systemsicherheit steigert. Dadurch schützen sie zum einen eine Vielzahl von Rechtsgütern der Systembetreiberin, aber auch diverse Rechtsgüter anderer User dieser Systeme sowie von Personen, deren Daten auf diesen Systemen bearbeitet werden.

[13] Unter Computerfrieden ist analog zum Hausfrieden die Befugnis zu verstehen, über die eigenen virtuellen Räume ungestört zu herrschen und darin den eigenen Willen frei zu betätigen. Die Daten, die in diesem virtuellen Raum vorhanden sein können (aber nicht müssen), sind vom Computerfrieden und damit vom Hackingartikel Art. 143bis Abs. 1 StGB nicht erfasst. Das ungestörte Verfügungsrecht über Daten wird stattdessen durch den Tatbestand des Datendiebstahls (Art. 143 Abs. 1 StGB) und die Datenbeschädigung (Art. 144bis Abs. 1 StGB) geschützt.

[14] Es stellt sich hingegen die Frage, ob die gefährdeten Rechtsgüter, die man retten will, vor einem Hack überhaupt erkannt werden können. Die Systembetreiberin wie auch deren Rechtsgüter lassen sich unter Umständen eruieren oder abschätzen. Die Rechtsgüter mutmasslicher Dritter zu identifizieren, erscheint dagegen sehr schwierig. Blosse Vermutungen genügen nicht. Zu den zu rettenden Rechtsgütern im Sinne des Notstandsrechts zählen ausserdem nur absolut geschütz-

9 BSK StGB II-Weissenberger, Art. 143bis N 22; PK StGB-Trechsel/Crameri, Art. 143bis N 8; CP II-Monnier, in: Alain Macaluso/Laurent Moreillon/Nicolas Queloz (Hrsg.), Commentaire Romand, Code pénal II, Basel 2017 (zit. CR CP II-Verfasser), Art. 143bis N 11; Graf (Fn. 8), N 13.

10 Zum Ganzen m.w.H. Michael Isler/Oliver Kunz/Gina Moll, Strafbarkeit von Ethical Hacking (∞), 26. Juni 2023, N 137 ff. Im Deutschen Recht führt Klaas ebenfalls den Notstand zur Rechtfertigung von ethischem Hacking an und argumentiert, dass eine Dauergefahr resp. ein längerfristig angelegter Risikosachverhalt bestehe, der jederzeit in einen Schaden umschlagen kann: Arne Klaas, «White Hat Hacking» – Aufdecken von Sicherheitsschwachstellen in IT-Strukturen, in: MMR 2022, S. 189.

te Rechte, wie z.B. die körperliche Unversehrtheit, das Leben, die Freiheit oder das Eigentum.[11] Rein vertraglich geschützte Interessen genügen beim Notstand nicht, sind deshalb aber nicht etwa weniger schützenswert.

[15] Problematisch am Institut des Notstands ist sodann die Voraussetzung, dass die Gefährdung der Rechtsgüter *unmittelbar* bestehen muss.[12] Freilich stellt das Vorhandensein von Schwachstellen eine Gefahr dar, aber nicht automatisch auch eine unmittelbare. Die Unmittelbarkeit kann sich zwar auch so verhalten, dass zeitlich keine direkte Nähe mehr besteht, «die Abwehr aber später nicht mehr oder nur unter viel höheren Risiken möglich ist»; auch bei Dauergefahren ist eine Unmittelbarkeit gegeben.[13] Wenn überhaupt, lässt sich die Unmittelbarkeit aber erst nach dem erfolgreichen Hack feststellen. Damit wäre der Hack selbst aber nicht mehr von der Notstandssituation getragen und wirkt sich darum nicht mehr rechtfertigend aus.

[16] Wären diese Hürden aber einmal überwunden, ist die Abwägung zwischen Computerfrieden und dem geretteten Rechtsgut kaum mehr mit Schwierigkeiten verbunden. Die allermeisten Rechtsgüter sind höher zu gewichten als der Computerfrieden. Das gilt umso mehr, wenn es die Systembetreiberin selbst ist, die unsichere Systeme betreibt und dadurch eine Gefahr für die Rechtsgüter anderer schafft. Wohingegen nur der Computerfrieden selbst gerettet werden kann, der jedoch dafür zuerst verletzt werden musste, dürfte die Güterabwägung scheitern. Das wäre der Fall beim Hack eines Systems, bei welchem ausschliesslich das Rechtsgut des Computerfriedens des Betreibers verletzt würde.

[17] In der analogen Welt ergibt sich der Sinn, dass Unmittelbarkeit vorausgesetzt ist, zwanglos. Selbstverständlich soll niemand bestraft werden, der die Scheibe eines brennenden Geschäfts einschlägt, um die darin eingeschlossene Kundschaft zu retten. In der digitalen Welt kann die ethische Hackerin aber nicht zuverlässig feststellen, wie akut oder ob überhaupt die Rechtsgüter Dritter in Gefahr sind.

[18] Ebenfalls kann problematisch werden, dass für die vorzunehmende Notstandshandlung strikte Subsidiarität gefordert wird. Bestehen mildere Mittel, die ebenso zur Rettung der gefährdeten Rechtsgüter genügen würden, so müssen sie auch eingesetzt werden. Wendet man nicht das (für die handelnde Person erkennbare) mildere Mittel an, ist die Strafbarkeit nicht mehr per se ausgeschlossen. Hacking ist ein langwieriger, analytischer Prozess, dem in den allermeisten Fällen unzählige Versuche vorausgehen und unzählige Male die Angriffsmethode angepasst werden muss, bevor der Hack funktioniert. Sämtliche gescheiterten Versuche wären nicht von dieser Subsidiarität erfasst; sie waren gar nie mildestmöglich, weil gar nicht erst geeignet. Es ist offensichtlich, dass der rechtfertigende Notstand nicht für komplexe «Tat»-Handlungen geeignet ist, bei welchen man erst in mehreren Iterationen zum Ziel gelangt. Die Kinoversion der Hackerin, die sich in Windeseile von System zu System hackt, geht vollkommen an der Realität vorbei.

[19] Ein Problem darin, ethisches Hacken über eine Notstandssituation zu legalisieren, liegt also zum einen darin, dass die Sicherheitsforscher kaum je über das Vorliegen der Notstandselemente wissen. Das hingegen ist notwendiger Teil des subjektiven Tatbestands, damit das eigene Han-

11 Michel Dupuis et al. (Hrsg.), Petit commentaire CP, 2. Aufl., Basel 2017 (zit. PC CP), Art.17 N 13; BSK StGB I-Niggli/Göhlich, Art. 17 N 5.

12 Siehe dazu die zutreffende und detaillierte Kritik, die Unmittelbarkeit bei ethischem Hacking zu leicht anzunehmen in Graf (Fn. 8), N 24 bis 27; BSK StGB I-Niggli/Göhlich, Art. 17 N 14; PC CP (Fn. 11), Art.17 N 7.

13 Isler/Kunz/Moll (Fn. 10), N 146 f.

deln nach Art. 17 StGB rechtmässig ist.[14] Zum anderen verhindern die Methodik und die zeitlichen Aspekte eines Hacks die Möglichkeit, sich auf eine unmittelbare oder wenigstens zeitnahe Rettung berufen zu können. Der Hack und die Sicherheitsmeldung führen in aller Regel nicht unmittelbar zur Rettung von bedrohten Rechtsgütern, da immer noch zuerst das Handeln der Systembetreiberin notwendig ist. Anders würde es sich nur dann verhalten, wenn die Hacker die Sicherheitslücke auch gleich selbst stopfen würden.[15]

[20] Ganz zentral ist letzten Endes auch die Tatsache, dass ethisches Hacking in erster Linie von Neugier und dem Ziel getrieben ist, die Sicherheit von Systemen zu erhöhen. Ethisches Hacking trägt zwar den Rettungsgedanken in sich, dabei handelt es sich aber um ein langfristiges Ziel. Man könnte auch sagen, es ist eine «Begleiterscheinung», eine sehr willkommene und nützliche.

[21] Insgesamt ist der rechtfertigende Notstand nach Art. 17 StGB für ethische Hackerinnen und Hacker keine taugliche Grundlage, sich zu betätigen. Die digitale Welt ist genauso Teil der Rechtsrealität wie die analoge Welt. Lösungsansätze wie der rechtfertigende Notstand in seiner heutigen Form scheitern an neuen Phänomenen wie dem ethischen Hacken. Ein Ansatz wäre es, die traditionelle Figur des Notstands weiterzuentwickeln. Hält man an der heutigen Konzeption des Notstands aber weiterhin fest, lassen sich die enormen Unsicherheiten nicht ausräumen. Mit dem Instrument des Notstands nach Art. 17 StGB lässt sich ethisches Hacking nicht legalisieren.[16]

1.3. Strafbares Hacking

[22] Art. 143bis Abs. 1 StGB stellt auf Antrag unter Strafe, wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt. Eingedrungen werden muss auf digitalem Wege, worunter auch das direkte Benutzen einer Tatstatur eines Computers fällt.[17] Das Auslesen eines *hardcoded* (also im Code abgespeicherten) Passworts, um dieses Passwort dann zu benutzen, ist kein Hacking. Ein hardcoded Passwort in einem Binary stellt keine besondere Sicherung dar, es lässt sich mit einfachsten Bordmitteln auslesen und gilt gar als öffentlich zugänglich.[18]

[23] Anders verhält es sich hingegen mit einem Passwort, das auf einem Stück Papier notiert ist und sich in privaten Räumen befindet. Bereits das simple Benutzen von aufgefundenen Passwörtern fällt unter Art. 143bis Abs. 1 StGB, vorausgesetzt, die Passwörter sind nicht öffentlich zugänglich.[19] Auf die technischen Fähigkeiten der Täterschaft kommt es letztlich nicht an.

---

14 BSK StGB I-Niggli/Göhlich, Art. 17 N 24.

15 Das kommt durchaus vor und ist vor allem dann denkbar, wenn sich im gehackten System die Schwachstelle durch die Korrektur einer Konfiguration, das Updaten oder Patchen einer Komponente beheben liesse. Dabei stellt sich aber sofort die Frage nach Art. 144bis Abs. 1 StGB. Selbst kriminelle Hacker schliessen regelmässig die angetroffene Sicherheitslücke, nach dem sie sich Persistenz auf dem System verschaffen konnten. Sie verhindern damit, dass sich die Konkurrenz ebenfalls im System einnisten und es für ihre Zwecke missbraucht.

16 So auch Graf (Fn. 47), N 40 mit einer konzisen Zusammenfassung sämtlicher Problemstellung im Zusammenhang mit dem Notstand.

17 Auch die Kommunikation per Tastatur erfolgt auf «dem Wege von Datenübertragungseinrichtungen», vgl. Roman Kost, Hacking nach Art. 143bis Abs. 1 StGB – Ein Erfolgsdelikt, in: Jan Wenk/Marianne Lehmkuhl (Hrsg.), Cyber-Strafrecht – Aus Praxis und Theorie, Zürich, 2025, S. 6.

18 Mit dem Befehl strings kann man sich sämtliche Strings (Zeichenketten) ausgeben, die in einem Binary (ausführbare Datei) vorhanden sind. Trotzdem ist es im Fall «ModernSolution» zu einem Schuldspruch gekommen, wobei das Amtsgericht Jülich in 17 Cs-230 Js 99/21–55/23 ein Dekompilieren der Anwendung und anschliessendes Auslesen angenommen hat.

19 Vgl. BGer, 6B_1207/2018, 17. Mai 2019 resp. BGE 145 IV 185, E. 2.2.2; Kost (Fn. 17), S. 7 f.

[24] Hacking ist ein Erfolgsdelikt, bei dem der Erfolg eintritt, sobald die Täterschaft sich im System aufhält und dadurch der Computerfrieden verletzt ist.[20] Nicht relevant ist, ob die Möglichkeit besteht, Daten zur Kenntnis zu nehmen.[21] Es genügt der blosse Aufenthalt im virtuellen Raum, um strafbar zu werden.

[25] Nicht strafbar ist *Port Scanning*. Hier wird bloss mit einem Systemdienst in einer Art und Weise gesprochen, wie es vorgesehen ist.[22] Die dabei erhaltenen Informationen ermöglichen zwar unter Umständen Rückschlüsse auf Schwachstellen, in das gescannte System eingedrungen wird dabei aber nicht.

[26] Gelangen Hacker in ein *ungesichertes* System, so sind sie nicht wegen Hackings strafbar. Wer auf einem System einen Dienst laufen lässt, der über öffentliche Netze erreichbar ist und diesen Dienst nicht besonders schützt, hat kein Recht, die Strafverfolgungsbehörden beizuziehen und unerbetene Besucher verfolgen zu lassen. Darunter fallen auch Fälle von «path traversal», wo bei einem Dienst systematisch Pfade ausprobiert werden, um zu prüfen, ob die Zugriffsrechte korrekt gesetzt sind.

[27] Ein System ist z.B. dann nicht «besonders gesichert», wenn es keinerlei Schutzmechanismen aufweist. Es ist auch dann nicht besonders gesichert, wenn es bloss eine Sicherung mit Standardpasswörtern aufweist (z.B. im Herstellerhandbuch nachlesbar) oder die Konfiguration zwar individualisiert wurde, dabei aber dann bloss triviale Zugangsdaten verwendet wurden (z.B. admin:password oder user:12345678).[23] Daran würde sich auch nichts ändern, wenn sich ein Systembetreiber die Mühe macht, die Standardports des Dienstes zu ändern.

[28] Nach heute geltender Rechtslage sind ethische Hacker nach Art. 143bis Abs. 1 StGB strafbar. Sie setzen sich der Strafverfolgung aus, sobald sie sich zu erkennen geben.

1.4. Social Engineering

[29] Ins Repertoire der Hackingtechniken gehört auch das *Social Engineering*.[24] Unter Social Engineering werden alle Angriffsmethoden gefasst, die sich spezifisch auf den Menschen, dessen Verhaltensweisen und Psychologie beziehen. Mit Social Engineering wird der Mensch gehackt

20 Kost (Fn. 17), S. 8.

21 Anders wohl das BGer in BGE 130 III 28, E. 4.2, wo es festhält, dass es genüge, wenn keine Barrieren mehr bestünden, die an einer Kenntnisnahme von Daten ernsthaft hindern würden. Ebenso unter Verweis auf denselben BGE, Graf (Fn. 8), N 9.

22 Selbst Auffassung Graf (Fn. 8), N 9.

23 Kost (Fn. 17), S. 18; anderer Auffassung Damian K. Graf, in: Jürg-Beat Ackermann (Hrsg.), Wirtschaftsstrafrecht der Schweiz, 2. Aufl., Bern 2021, § 26 N 66 i.V.m. 47 f., wo auch banalste Kennwörter genügen sollen, ebenso Firewalls oder Verschlüsselungstechnologien, nicht aber Standardpasswörter. Standardpasswörter sind per se banal, weil sie in Bezug auf ein Produkt öffentlich bekannt sind. Firewalls beschränken sodann zwar den Traffic eines Systems, stellen aber auf Grund ihrer Funktionsweise keine Authentifizierungsmethode dar. Mit Verschlüsselung kann die Lesbarkeit von Daten beschränkt werden, sie schränkt hingegen nicht den Zugriff auf einen virtuellen Raum ein.

24 Die Politik- und Sozialwissenschaften erfassen unter dem Begriff «Social Engineering» alle Massnahmen, mit denen soziale Verhaltensweisen und Haltungen in Gesellschaften verändert werden können. Der Begriff wurde von Karl Popper eingeführt, vgl. Karl Popper, The Open Society and Its Enemies – Volume 1: The Spell of Plato, S. 17 f.

und nicht ein Datenverarbeitungssystem.[25] Schon dieser Umstand schliesst die direkte Anwendung von Art. 143bis Abs. 1 StGB aus; Menschen sind nicht vom Straftatbestand erfasst.[26]

[30] Damit ist auch klargestellt, dass die vorgeschlagene Legalisierung gerade Social Engineering-Methoden *nicht* umfasst, sondern ausschliesslich das Hacken von Systemen. Ethische Hackerinnen und Hacker dürfen also den Zugang zu Systemen nicht dadurch erlangen, indem sie zuerst einen Menschen hacken und dessen Zugangsdaten z.B. durch *Phishing*, einer ausgeklügelten Kommunikationsstrategie am Telefon oder durch das Versenden eines Trojaners[27] erschlichen haben.

[31] Bei Pentesting-Aufträgen wird Social Engineering in aller Regel vom Methodenkatalog und dem Scope ausgeschlossen. Das liegt daran, dass eine nahezu 100%ige Wahrscheinlichkeit besteht, dass irgendein Mensch überliststet wird. Mit genügend Zeit und Ressourcen lässt sich jedes System über den Faktor Mensch kompromittieren.

[32] Dass Social Engineering heute wie auch nach einer Legalisierung von ethischem Hacking strafbar bleiben soll, ist richtig, weil mit dieser Angriffsmethode kein Mehrwert für die Gesellschaft entsteht. Durch Social Engineering wird keine technische Lücke geschlossen. Man könnte anbringen, dass es erst durch Social Engineering möglich wurde, die internen Systeme zu testen. Das ist natürlich richtig. Die im internen Bereich eingesetzte Software lässt sich hingegen auch auf Sicherheitslücken prüfen, indem ein Testsetup aufgestellt wird. Anders verhält es sich nur bei Eigenentwicklungen, auf die man nicht ohne weiteres Zugriff hat.

[33] Sodann präsentiert sich die Gefährdungslage für Rechtsgüter betroffener Personen und Systembetreiber nicht gleich, wenn zuvor in ein an sich sicheres System mit erschlichenen Zugangsdaten eingedrungen wurde. Von öffentlichen Netzen heraus ausnutzbare Sicherheitslücken – und das ist der Fokus des Revisionsvorschlags – stellen die weitaus grössere Gefahr für betroffene Personen und Systembetreiber dar.

[34] Wenn auf der Basis der durch Social Engineering erlangten Resultate (meistens sind es Zugangsdaten) in Systeme eingedrungen wird, kann Art. 143bis Abs. 1 StGB zur Anwendung gebracht werden – nach heutigem Recht wie auch mit der vorgeschlagenen Legalisierung.[28] In diesen Fällen wird es auch weiterhin der Systembetreiberin anheimgestellt sein, ob sie diesen Rechtsbruch toleriert und auf eine Strafanzeige verzichtet oder nicht.

---

25 Zieht man das OSI-Modell zur Veranschaulichung hinzu, so sind wir auf Schicht 8 angelangt. Auf dieser Schicht ist der Mensch wie auch Organisationen und die Umwelt inkl. Staat angesiedelt. Es handelt sich dabei um eine inoffizielle Erweiterung der sonst ausschliesslich technischen Schichten 1 bis 7 des OSI-Modells.

26 Vermutlich anderer Auffassung ist ebenso wohl CR CP II-Monnier, (Fn. 9), Art.143bis N 12 mit Verweis auf Art. 143 N 18, wobei die Autoren wohl davon ausgehen, dass Social Engineering auch das Verwenden des Erschlichenen umfasst. Sie gehen in Bezug auf den Datendiebstahl sogar so weit, anzunehmen, dass durch Social Engineering erschlichene Daten wie Passwörter etc. unter Art. 143 Abs. 1 StGB fallen, obschon die Datensätze nicht aus einem Datenverarbeitungssystem entwendet wurden.

27 Der Social Engineering-Aspekt liegt hier im gezielten Aussuchen eines geeigneten Opfers und dem Cachieren des Trojaners als harmloses Dokument, um das Opfer zum Ausführen des Trojaners zu bewegen. Die Benutzung des Trojaners im Anschluss stellt dann wiederum Hacking dar.

28 A.M. und Social Engineering wohl als Hacking erfasst bei Graf, § 26 N 142.

2. Handlungsbedarf

[35] Bereits im Jahr 1990 hat der Europäische Rat in die Zukunft geblickt und festgehalten: «*The computer may well become the ‹Achilles› heel of the post-industrial society*».[29] Dass sich die strafrechtliche Legalisierung von ethisch handelnden Hackerinnen und Hacker aufdrängt, haben erste Länder bereits erkannt und einen gesetzlichen Rahmen geschaffen (vgl. Rz. 124 unten).

[36] Folgendes Argumentarium spricht für die Strafbefreiung auch in der Schweiz:

2.1. Hackingstrafrecht modernisieren

[37] Hintergrund der ersten Gesetzgebungsbemühung zum Hackingstrafrecht waren erste Vorstösse im Parlament in den 1970er Jahren, mit denen neue Tatbestände zur Bekämpfung der Wirtschaftskriminalität geschaffen werden sollten.[30] Später prägend und Thema in der Fragestunde an den Bundesrat waren zum Beispiel ein Hack mittels AHV-Nummern in das Videotext-System der Stadt Biel 1985, der mit einer Interpellation zur Sprache gebracht wurde, ein Hackerskandal in der BRD, welcher 1989 aufflog oder der Hack ins ETH-Rechenzentrum 1989.[31] Die Computerisierung ist mit diesen Vorfällen definitiv im Bewusstsein angekommen. Die vom Bundesrat eingesetzte Experten-kommission nahm sich denn auch dem neuen Phänomen der Computerkriminalität an. Parallel erarbeitete das *European Committee on Crime Problems* einen Bericht, der die Untersuchungsresultate seit 1985 zusammenfasst und 1989 publiziert wurde. Bereits in diesem Bericht finden die Beweggründe von Hackern und die Vorteile des Hackens für die Sicherheit Eingang.[32] In der Schweiz hingegen lag der Fokus des Gesetzgebers vollständig auf der Kriminalisierung; die Thematik der technischen Sicherheit und der Wert der Sicherheitsforschung wurde nicht aufgegriffen.[33]

[38] Am 2. März 1992 empfahl der Bundesrat dem Parlament eine Formulierung, die im subjektiven Tatbestand Bereicherungsabsicht (überschiessende Innentendenz) vorgesehen hatte, obschon das Eindringen in Systeme für sich betrachtet nichts mit Rechtsgütern der Vermögenssphäre zu tun hat.[34] Die vorgeschlagene Erstfassung kombinierte denn auch den Datendiebstahl mit Hacking im gleichen Tatbestand:

> «*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 verschafft, die nicht für ihn bestimmt und gegen unbefugten Zugriff besonders gesichert sind, oder auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in fremde, beson-*

29 European Committee on Crime Problems (ECCP), Report by the European Committee on Crime Problems, 1990, S. 3.

30 M.w.H. Christa Pfister, Hacking – Die Schweizer Hacking-Strafnorm (Art. 143bis StGB) im Vergleich mit den Bestimmungen der Cybercrime Convention, des Rechts der Europäischen Union, des deutschen und des österreichischen Strafrechts, Diss. Zürich 2008, S. 46. Bundesrat, Botschaft über die Aenderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (∞), 1991, BBl 1991 II 969, S. 979.

31 AB 1985 1275; AB 1989 394; AB 1990 479.

32 ECCP (Fn. 29), S. 53 «to grant a ‹premium› in cases in which the per petrator gives immediate notice of the access and of the loopholes used to the victim or to state authorities».

33 Vgl. Bundesrat (Fn. 30), 1011.

34 Bundesrat (Fn. 30), 1011. Vgl. Roman Kost, https://143bis.ch/kommentar/stgb-143bis/ (∞), ca. 2016.

> *ders gesicherte Datenverarbeitungsanlagen eindringt, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.*
>
> *2. Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.*
>
> *3. Handelt der Täter ohne Bereicherungsabsicht, so wird er, auf Antrag, mit Gefängnis oder mit Busse bestraft.*»

[39] Die vom Parlament am 17. Juni 1994 beschlossene und schliesslich per 1. Januar 1995 in Kraft gesetzte Fassung trennte den Datendiebstahl und das Hacking schliesslich, wobei für Hacking Art. 143bis StGB erschaffen wurde.[35]

[40] Im Hinblick auf die Bereicherungsabsicht hat man gleichzeitig eine Kehrtwende vollzogen:[36]

> «*Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.*»

[41] Damit wurde das ursprünglich *ex officio* mit Strafandrohung von bis zu fünf Jahren Zuchthaus verfolgte Hacking (in Bereicherungsabsicht) zu einem nur noch auf Antrag zu verfolgenden Hacking ohne Bereicherungsabsicht mit Strafandrohung von bis zu drei Jahren Gefängnis abgewandelt. Hacker, die in Bereicherungsabsicht handelten, sind so durch die Maschen geschlüpft.

[42] Im Zuge der AT-StGB Revision wurden per 1. Januar 2007 die Bezeichnungen der Strafarten angepasst (namentlich anstelle von Zuchthaus resp. Gefängnis, neu Freiheitsstrafe oder Geldstrafe). Mit der Umsetzung der Europäischen Cybercrime-Konvention, wurde das viel kritisierte und wenig sinnvolle Tatbestandselement «ohne Bereicherungsabsicht» schliesslich gestrichen.[37]

[43] Die heutige Fassung ist seit dem 1. Januar 2012 in Kraft. Der Hackingtatbestand ist damit im Wesentlichen unverändert geblieben. Er hat sich von Beginn an dadurch ausgezeichnet, dass sich der Gesetzgeber schwer darin tat, Hacking sinnvoll zu erfassen und zu bewerten. Hacking wurde stets im Kontext von Vermögensdelikten diskutiert und ausschliesslich negativ konnotiert, ohne die Chancen von Hacking zu erkennen.

[44] Als Gegenargument zur Legalisierung von ethischem Hacking wird damals wie heute oft angeführt, dass Hacking gefährlich sei. Ein Blick in die parlamentarischen Beratungen und Berichterstattungen belegt diese Angst. Die Gefährlichkeit wurde durchgehend angenommen, ohne sie aber näher zu erläutern. Die Überlegungen waren durchwegs, dass Hacking das Hausrecht der Systembetreiber verletze und danach ermögliche, unbefugt auf Daten zuzugreifen, solche zu stehlen oder zu löschen.[38] Für diese Ängste ist also nicht der eigentliche Aspekt des Hackings und des Computerfriedensbruchs verantwortlich, sondern was allenfalls *danach* folgt.

---

35 BBl 1994 III 256; AS 1994 2290.

36 Erstfassung gemäss Bundesbeschluss vom 17. Juni 1994, BBl 1991 II 969 (S. 258).

37 AT-StGB-Revision gemäss Bundesbeschluss vom 12. Februar 2002, (BBl 1999 1979); Bereicherungsabsicht aufgehoben mit Bundesbeschluss vom 18. Februar 2011, im heutigen Wortlaut in Kraft seit 1. Januar 2012, (BBl 2010 4697).

38 ECCP (Fn. 32), S. 19 ff. Vereinzelt findet auch die Gefahr «over criminalisation», a.a.O. S. 26, Erwähnung. Sämtlichen Berichten aus dieser Zeit ist hingegen gemein, dass sie die heutige Bedeutung und das Ausmass der Informationstechnologien nicht annähernd abschätzen konnten. Die Bedeutung der ethischen Sicherheitsforschung als zentraler Faktor zur Verbesserung der Sicherheit wurde damals noch nicht erkannt. Das verwundert auch nicht, schliesslich haben sich die Methoden, technische Sicherheit z.B. auch in die Produkteentwicklung miteinzubeziehen, enorm entwickelt.

[45] Würde man nun per se das Gegenteil behaupten und sagen, dass Hacking vollkommen ungefährlich ist, wäre das hingegen unredlich. Die Gefährlichkeit des Hackens in technischer Hinsicht kann dann bestehen, wenn Prozesse abstürzen, die allenfalls weitere Prozesse oder gar das ganze System in Mitleidenschaft ziehen könnten. Oder die gehackten Prozesse verhalten sich unerwartet und verändern gar Daten. Rückblickend auf die letzten 30 Jahre lässt sich aber festhalten, dass das eigentliche Hacken – also das Eindringen in ein System – nicht per se gefährlich ist. Es sind soweit ersichtlich keine Fälle bekannt, wo Schaden durch einen reinen Hack – also ausschliesslich durch das Eindringen in ein Datenverarbeitungssystem, wie es durch Art. 143bis Abs. 1 StGB unter Strafe gestellt wird – entstanden ist. Angegriffene Prozesse starten sich bei einem Absturz in aller Regel neu, wenn sie nicht ohnehin wie bisher einfach weiterarbeiten. Fälle wie DDoS (zu subsumieren unter der Nötigung nach Art. 181 StGB), Ransomware-Erpressung (Art. 156 StGB) oder simple Datenbeschädigung (Art. 144bis StGB) sind kein Hacking. Auch nach einer Legalisierung von Hacking sind sie strafbar (vgl. Rz. 130 ff. unten).

[46] Trotz skandalträchtiger Nachrichten und parlamentarischer Fragen an den Bundesrat, war die digitale Welt vor 30 Jahren noch in jeder Hinsicht beschaulich. War Hacking vor 30 Jahren nur sporadisch ein Thema im Parlament, lässt sich heute das Thema im parlamentarischen Betrieb kaum mehr in Zahlen fassen. Cybersicherheit hat alle Bereiche durchdrungen. In die heutigen Meldungen bringen es nur noch Sicherheitsvorfälle von enormem Ausmass, Hacks sind damit Teil der Normalität geworden. Art. 143bis Abs. 1 StGB bildet in Anbetracht seines Entstehungshintergrunds in keiner Weise mehr die enorm gesteigerte Gefahrenlage ab und wird der aktuellen Allgegenwart von vernetzter Technik nicht gerecht.

2.2. Strafverfahren bei ethischem Hacking

[47] Ein Strafverfahren hat einschneidende Konsequenzen. Man denke nur an Hausdurchsuchungen, Beschlagnahmungen und Freiheitsentzug. Das Verfahren dauert danach praktisch ausnahmslos lange. Neben der nervlichen Belastung stehen in dieser Zeit Bewerbungsprozesse in der Schwebe, insbesondere dort, wo Personensicherheitsprüfungen vorausgesetzt sind oder in sonstiger Weise erhöhte Anforderungen bestehen. Falsche Angaben im Rahmen eines Bewerbungsprozesses können ernsthafte arbeitsrechtliche Konsequenzen nach sich ziehen.

[48] Wurde früher noch angenommen, die Gefahr von Strafverfolgung sei gering, so hat sich das Bild mittlerweile geändert.[39] Grosse mediale Beachtung erhielt jüngst der Hack polnischer Züge, der Hack der CDU-App oder der Fall ModernSolutions.[40] Es sind zahlreiche weitere Fälle bekannt, bei denen Hersteller resp. Systembetreiber erst nach einem medialen Aufschrei und der Intervention der Gesellschaft der Wert der Schwachstellenmeldungen bewusst wurde. Nicht selten ist es erst die schlechte Publicity, die die Betreiber gehackter Systeme von Strafanzeigen abhält resp. zu deren Rückzug bewegt.

---

39 Vgl. z.B. Pfister (Fn. 30), S. 206, die (im Jahr 2007) noch zur Annahme gelangte, die Risiken seien gering und der Mehrwert zu klein.

40 Siehe zu den polnischen Zügen: Kantorkel, Das ist völlig entgleist (∞); zur CDU-App: Martin Holland, Sicherheitslücken in CDU-connect-App: Strafverfahren gegen Entdeckerin (∞), 4. August 2021; zu ModernSolution: Fabian A. Scherschel, Kommentar zu Modern Solution: Wer gemeinnützig handelt, wird bestraft (∞) und einschlägiges Urteil des Amtsgericht Jülich, 17 Cs-230 Js 99/21–55/23 (∞) vom 8. November 2024. Eine Liste von Strafverfahren gegen ethische Hacker findet sich hier: https://github.com/disclose/research-threats (∞).

[49] Erduldete Zwangsmassnahmen sind kaum wettzumachen. Beschlagnahmte private wie berufliche IT-Gerätschaften sind lange Zeit nicht mehr verfügbar; ganz abgesehen von den Implikationen, die sich für die Privat- resp. die Geheimsphäre ergeben – für die betroffene beschuldigte Person selbst oder deren Kundschaft. Sollte geistesgegenwärtig durch die beschuldigte Person eine Siegelung verlangt worden sein, folgen zeit- und kostenintensive Entsiegelungsverfahren, wenn sie denn überhaupt in den engen Bahnen der gerichtlich akzeptierten Argumentationslinien erfolgversprechend sind. In aller Regel können die beschuldigten Personen keine gesetzlichen Geheimnisschutzgründe vorbringen.[41]

[50] Wird der Rückzug des Strafantrags erreicht, ändert auch eine spätere Einstellung nichts mehr am entstandenen Aufwand (vgl. Art. 33 Abs. 1 bis 3 i.V.m. Art. 319 Abs. 1 lit. d StPO). Die verlorene Zeit in Haft, an Befragungen, Triagen, Verhandlungsterminen und in der Diskussion mit der Verteidigung kann man nicht ersetzen. Dass sich Lebenszeit mit Geld kompensieren liesse, ist eine Irrvorstellung. Kompensatorische Geldzahlungen sind, wenn sie denn überhaupt erfolgen, sehr bescheiden. Sie kommen ohnehin nur für ungerechtfertigten Freiheitsentzug in Frage, was heute bei der Verfahrenserledigung durch Rückzug des Strafantrags gerade bei Hacking nicht in Betracht kommt (Art. 430 Abs. 1 lit. a StPO): Der Hack war rechtswidrig, daher der Freiheitsentzug grundsätzlich nicht ungerechtfertigt. Es besteht letzten Endes die Gefahr, dass den ethischen Hackerinnen und Hackern trotz Einstellung die Verfahrenskosten überbunden werden; schuldhaft im Sinne des heute geltenden Hackerartikels hätten sie allemal gehandelt, trotz redlicher Absichten (Art. 426 Abs. 2 StPO).

[51] Wie gesehen, ist nach heutiger Rechtslage jegliche Art von Hacking strafbar. Das führt zur absurden Situation, dass sich ethische Hacker bei einer Meldung an die Betreiberschaft des gehackten Systems deren Willkür aussetzen. Es ist der «Profiteur» dieser Meldung der entscheidet, ob die meldende Person nun ein Strafverfahren zu gegenwärtigen hat oder nicht. Diese Situation ist auch deswegen absurd, weil sich solchen Strafverfahren nur jene ethischen Hacker aussetzen, die eruierbar sind, sprich, sich melden oder nicht (genügend) OPSEC[42] haben walten lassen. Auf OPSEC wird aber gerade deshalb oft verzichtet, weil man ohnehin mit guten Intentionen handelt und Meldung erstattet.

[52] Auch die OECD bestätigt die weit verbreitete Furcht vor Strafverfolgung in der Forscher-Community und erwähnt dabei diverse weitere Beispiele von ethischen Sicherheitsforschenden, die sich mit Strafverfolgung konfrontiert sahen. Hervorgehoben wird der enorme Chilling Effect, den die Strafandrohungen für ethische Hackerinnen haben.[43] Das erstaunt nicht, schliesslich funktioniert bei ethischen Hackerinnen der moralische Kompass noch, das im Gegensatz zu kriminellen Akteurinnen. Im Unterschied zu kriminellen Akteuren hat allein die blosse Androhung einer Strafe auf ethische Hackerinnen bereits Wirkung.[44]

[53] Gegen die Strafbefreiung ethischen Hackings wird oft angeführt, dass mit einer Strafbefreiung mehr gehackt werde. Das ist richtig, aber gleichzeitig unproblematisch. Strafbefreit werden nur jene Sicherheitsforscherinnen, die sich an die Vorgaben halten. Die Strafbefreiung von ethi-

41 Urteil 7B_313/2024 vom 24. September 2024, E. 4.3 (zur Publikation vorgesehen).

42 Operations resp. Operational Security bedeutet hier die Gesamtheit an Massnahmen, sich nicht erwischen zu lassen. Innerhalb der Hackingszene wird der Begriff anders als in der IT-Industrie benutzt, wo unter OPSEC die Massnahmen gefasst werden, die dem Schutz (kritischer) Daten und Informationssysteme dienen.

43 OECD (Fn. 4), S. 49 und insbesondere S. 52 f.

44 OECD (Fn. 4), S. 29 f. und S. 35.

schen Hackerinnen führt nicht dazu, dass sich dadurch mehr böse Hacker ans Werk machen. Böse Hacker hacken heute genauso oft wie nach der Einführung eines Strafbefreiungstatbestands. Auf kriminelle Hacker hat die Strafandrohung keinen Einfluss, das ist heute in Anbetracht der zahlreichen Cybercrimevorfälle eindrücklich bewiesen. *Black Hats* bleiben weiterhin strafbar.

[54] Der Kampf gegen kriminelle Hacker scheitert an einem anderen Ort: Die generalpräventive Wirkung abstrakter Strafandrohungen, ohne dass auch deren Durchsetzung gewährleistet wird, ist verschwindend gering. Wirkungsvoll kann die Strafandrohung bei Cyberdelikten nur dann sein, wenn den Strafverfolgern mehr Ressourcen zugewiesen werden, um Kompetenzen und Personal aufzubauen. Das heisst aber gerade nicht, den Strafverfolgern noch mehr Aufgaben zuzuweisen, neue Aufgaben werden notgedrungen einfach auf die gleichen Schultern verteilt. Es braucht dringend mehr motivierte und gut ausgebildete Fachleute, die bereit sind, sich in den Staatsdienst zu stellen.

[55] Sodann liegt es auf der Hand, dass die Legalisierung von ethischem Hacking mehr Sicherheitsforscherinnen und -forscher dazu animiert, tätig zu werden. Das wiederum wird die Zahl der Angriffsversuche wohl etwas erhöhen. Die Unterscheidung zwischen guten und bösen Angreifern wird insbesondere an der ersten Verteidigungslinie (Perimetersicherheit) nicht möglich sein. Das muss sie aber auch nicht, da Sicherheitsaspekte ohnehin unterscheidungslos zu greifen haben. Das Grundrauschen wird zwar etwas stärker, nur muss man auch sehen, dass nicht urplötzlich eine ganze Armada an ethischen Hackern hinzutritt.

[56] Die chronische Überlastung der Strafverfolgungsbehörden bedarf keiner weiteren Erläuterung. Bei ehrlicher Betrachtung der Kosten eines Verfahrens stellt man rasch fest, dass hinter den symbolischen Rechnungen für Amtshandlungen weitaus höhere Kosten stecken. Rapporte und jegliche Art von Einsatz binden Ressourcen direkt vor Ort und lösen später weitere Aufwendungen aus, Rapporte müssen beispielsweise geprüft und in die weitere Untersuchung miteinbezogen werden. Es kann der Beizug von externen Fachleuten notwendig werden, z.B. von Forensikern und Systemspezialisten. Das ist bei Hackingfällen und ganz generell bei Triagen mit grösserem Datenvolumen nicht mehr selten der Fall. Es entstehen zusätzlich Kosten, die je nach Fallkomplexität enorm zu Buche schlagen und sehr viel Einsatzzeit binden.

[57] Die derzeit herrschende Rechtslage treibt die Kosten aller Akteure in die Höhe, ohne dass es sich rechtfertigen liesse. Die Sicherheitsforscher und deren Verteidigerinnen wenden Geld resp. Zeit auf. Auch pro bono-Verteidigung kostet trotzt ausbleibenden monetären Folgen Ressourcen. Bei notwendiger amtlicher Verteidigung, die sich bei komplexen Sachverhalten, Hilfsbedürftigkeit des Hackers oder zur Wahrung der Chancengleichheit ergeben kann, muss der Staat gleichzeitig die Anklage wie auch die Verteidigung finanzieren. Der Staat hat in solchen Fällen widersinnige Verfahren gegen ethische Hackerinnen und Hacker zu führen und muss gleichzeitig dafür auf beiden Seiten Ressourcen binden, die andernorts besser eingesetzt wären.

[58] Strafbefreiung bedeutet nicht, einfach freie Hand zu haben. Die Sicherheitsforscherinnen und -forscher bleiben für ihre Handlungen weiterhin verantwortlich und haben sich strikte an die etablierten *Vulnerability Disclosure Regeln* zu halten. Auch *Vulnerability Owner* sind in der Pflicht. Sie schulden ihren Kunden sichere Produkte und profitieren finanziell durch die Teilnahme am Markt. Es ist also an ihnen, gemeldete Sicherheitslücken ernst zu nehmen und mit ethischen Hackerinnen einen angemessenen Umgang zu pflegen. Ohne zwischen diesen beiden Playern und

dem Staat nachhaltiges Vertrauen zu schaffen, werden wir die Problematik von exponentiellem Schwachstellenwachstum nicht in den Griff bekommen.[45]

[59] Das Problem sind nicht die *White Hats*, sondern die kriminellen Cyberakteure. Es ist darum konsequent, White Hats von Strafverfolgung auszunehmen und dadurch die Strafverfolgungsbehörden zu entlasten. Die strafrechtliche Verfolgung von ethischen Hackern ist wie aufgezeigt für die Allgemeinheit am Ende sogar schädlich.

2.3. Handeln im Interesse der Gesellschaft schützen

[60] Der Begriff «Hacker» und «Hackerin» ist leider noch in einigen Köpfen mit Kriminalität verbunden. Bei Lichte betrachtet heisst hacken nur, dass man mit einem Problem in einer Art und Weise umgeht, die nicht vorgesehen war.[46] Mit Blick auf Informationstechnologien kann das von kreativer Erweiterung der Funktionalität bis hin zum trickreichen Ausnutzen technischer Schwachstellen reichen.

[61] Ethische Hackerinnen und Hacker («White Hat Hacker») handeln in altruistischer Absicht.[47] Das schliesst nicht automatisch aus, dass nicht auch die Suche nach Anerkennung und das Zeigen der eigenen technischen Fähigkeiten wichtige Treiber sein können.[48] Die Anerkennung der Forschungstätigkeit stellt vielmehr sogar ein tragendes Element dar, das man zu Gunsten aller nutzen sollte.[49] Wer hingegen eigennützig handelt und nicht beabsichtigt, dass die aufgedeckten Sicherheitslücken geschlossen werden, handelt nicht ethisch und hat keine Strafbefreiung verdient («Black Hat Hacker»).[50]

[62] Dazwischen findet sich die Kategorie der *Grey Hats*[51], also jene Personen, die objektiv betrachtet nicht sauber eingeordnet werden können. Ein wirkliches Problem besteht bei Grey Hats aber nicht. Wer sich nicht für das Schliessen von Sicherheitslücken einsetzen will, sich also nicht für gemeinnütziges Handeln entschieden hat, erscheint nicht schutzbedürftig und verdient keine Strafbefreiung. Mag sein, dass jemand sich zu Beginn in erster Linie aus Geltungsdrang oder gar

45 Vgl. auch OECD (Fn. 4), S. 68 f.; Manuela Wagner/Oliver Vettermann, Verantwortungsbewusster Umgang mit IT-Sicherheitslücken (∞), Trier, 2023, S. 68 f.

46 Gehackt werden können neben technischen Systemen auch die Gesellschaft, Rechtssysteme etc. Für eine umfassende Beschreibung von Hacking in allen Facetten: Bruce Schneier, A Hacker's Mind, How To Powerful Bend Society's Rules, and How to Bend Them Back, New York, 2023.

47 Die Bezeichnungen Black, Grey resp. White Hat-Hacker wurden in erster Linie in kriminalsoziologischer Sicht wissenschaftlich aufgearbeitet. Zum Ganzen Begriffsthema: siehe Edith Huber, Cybercrime – Eine Einführung, 2019, S. 34 und 69; Christoph Einzinger, Phänomenologie von digitalen Delikten – Eine Tat- und Täteranalyse von Hackern, in: Thomas-Gabriel Rüdiger/Petra Saskia Bayerl, Cyberkriminologie – Kriminologie für das digitale Zeitalter, 2023, S. 426 f.; Gráinne Kirwan/Andrew Power, Cybercrime – The Psychology of Online Offenders, 2013, S. 53; vgl. auch Germann/Wicki-Birchler (Fn. 8), S. 86 f.; Graf (Fn. 8), N 6 f.; Bundesrat, Die Förderung des ethischen Hackings in der Schweiz (∞), S. 5 f.; EDÖB, Merkblatt White-Hat-Hacker/innen (WHH) (∞), N 9.

48 Vgl. Sylvain Métille/Joanna Aeschlimann, Infrastructures et données informatiques: quelle protection au regard du code pénal suisse?, ZStR 132/2024, S. 302, haben in diesem Zusammenhang die witzige Abwandlung «hackito ergo sum» resp. «Je hacke donc je suis» erfunden.

49 Vgl. z.B. die vom BSI genannte «Hall of Fame», BSI CVD-Leitlinie (∞), S. 6 unten.

50 Siehe Fn. 47.

51 Germann/Wicki-Birchler, (Fn. 8), S. 87, verorten die Greyhacker in jenem Personenkreis, der die Sicherheitslücken regelmässig veröffentliche und so die Benutzung durch Black Hats in Kauf nehme. Das kann sein, ist aber nicht der typische Fall. Grey Hats zeichnet aus, dass sie opportunistisch unterwegs sind und damit in aller Regel nicht ethisch handeln. Es kommt dazu: Sicherheitslücken werden bei ethischem Hacking grundsätzlich immer veröffentlicht, aber die Veröffentlichung geschieht im Rahmen eines Responsible Disclosure resp. Coordinated Vulnerability Disclosure Prozesses.

in der Absicht, sich zu bereichern, betätigt hat. Wer letztlich aber zum Wohle aller die Sicherheitslücke meldet, soll dennoch von Strafbefreiung profitieren können. Es wäre ohnehin unrealistisch anzunehmen, man könne jeglichen Missbrauch ausschliessen. Nur weil jemand grundsätzlich eine Notwehr- oder Notstandssituation provozieren und auf Beweisschwierigkeiten zu seinen Gunsten hoffen könnte, wird weder das Notwehr- noch das Notstandsrecht ernsthaft in Frage gestellt. Einzelne Bevorteilungen und opportunistische Verhaltensweise vermögen nicht, die enormen Vorteile und öffentlichen Interessen zu überwiegen.

[63] Das Veröffentlichen von Schwachstellen ist ein Hauptbestandteil und Kern ethischen Hackens. Für die Veröffentlichung gibt es unter den Stichworten «Responsible Disclosure», «Coordinated Vulnerability Disclosure» (CVD) oder auch «Software Vulnerability Disclosure» bereits anerkannte Vorgehensweisen. Die *European Union Agency for Network and Information Security* (ENISA), eine weltweit anerkannte Agentur mit enormen Fachwissen, hat evaluiert, dass CVD bezwecken, die gesellschaftlichen Vorteile durch geordnete Veröffentlichung von Schwachstellen maximieren zu können.[52] Der gesellschaftliche Nutzen ethischer Sicherheitsforschung und der Publikation von Schwachstellen ist unbestreitbar und wurde wiederholt auch auf globaler Ebene durch die UNO in Beschlüssen und Arbeitsberichten festgehalten.[53] Auch die internationale Standardisierungsorganisation ISO hat die Normen ISO/IEC 29147 und ISO/IEC 30111 für die Schwachstellenmeldung und -behandlung erlassen. Die ISO hält fest: «*Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk*».[54] Das BACS hat den Bedarf des geordneten Schwachstellenhandlings ebenfalls erkannt[55] und 2021 eine erste Version ihrer CVD Policy[56] publiziert. MELANI, eine Vorgängerorganisation des BACS, hielt schon 2015 ausdrücklich fest, dass klare gesetzliche Regelungen wünschenswert seien und hat hervorgehoben, dass nur dank der Meldungen von Sicherheitsforschern die Sicherheit verbessert werden könne.[57]

[64] Bruce Schneier, eine Koryphäe der Kryptologie und Cybersicherheit, hält im Endeffekt gar jegliche Art von Veröffentlichung – also notwendigenfalls auch als Full Disclosure ohne Koordination mit dem Hersteller – für besser, als das Zurückbehalten. Er verweist darauf, dass der kritische Blick der Öffentlichkeit der einzige verlässliche Weg ist, die Sicherheit zu erhöhen, wohingegen Geheimniskrämerei die Sicherheit aller nur verschlechtert.[58] *Full Disclosure* ist jedoch nur dann angezeigt, wenn sich der Hersteller schlicht um das Problem foutiert. In diesem Fall ist

---

52 ENISA, Economics of vulnerability disclosure (∞), 2018, S. 33, 4.4.1; ebenso Sven Herpig, Vulnerability Disclosure: Guiding Governments from Norm to Action –How to Implement Norm J of the United Nations Norms of Responsible State Behaviour in Cyberspace (∞), 2024, S.6 und 8, sowie Manuela Wagner/Oliver Vettermann (Fn. 45), S. 9 ff.; CVD-Policies sind kein Allheilsmittel, aber immerhin ein zentraler Baustein, vgl. dieselbigen, S. 81 ff.

53 Anstelle vieler: United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (A/76/153) (∞), 2021, S. 7, zit. United Nations, Responsibility sowie United Nations, *Developments in the field of information and telecommunications in the context of international security*, (A/79/214) (∞), 2024, S. 7, zit. United Nations, Developments.

54 ISO/IEC 29147:2020, Kap. «Scope», S. 1.

55 MELANI, Halbjahresbericht 2015/2 (∞), S. 8, Kap. 3.1.4 sowie Ankündigung einer eigenen CVD-Policy im 2019: MELANI, Halbjahresbericht 2019/2 (∞), S. 37.

56 BACS, Melden einer Schwachstelle (Coordinated Vulnerability Disclosure, CVD) (∞) sowie die zugehörigen Bedingungen: BACS, Rahmenbedingungen und Regeln (∞).

57 Halbjahresbericht 2015/2, S. 8, Kap. 3.1.4 (Fn. 55).

58 Mit diversen weiteren Argumenten zur Problematik: Bruce Schneier, Debating Full Disclosure, S. 191, in: ebd., Schneier on Security, 2008; ebd., Decrypting an iPhone for the FBI, S. 264, sowie The NSA Is Hoarding Vulnerabilities, S. 269, in: ebd., We have Root, 2019; ebd., Data Goliath, S. 174; ENISA, Good practice guide on vulnerability disclosure (∞), 2016, S. 25.

das Wissen um die Schwachstelle die einzige Möglichkeit der Nutzerinnen und Nutzer, Vorkehrungen zu treffen und notfalls auf die unsichere Hard- oder Software zu verzichten. Kurzfristig erhöht sich zwar durch Full Disclosure das Risiko, langfristig rechtfertigt sich dieser Umstand jedoch durch den Gewinn an Sicherheit.[59]

[65] Nicht ganz zu Unrecht hört man in der Diskussion mit Vertretern der IT-Branche den Vorwurf, dass Unternehmen, die eigentlich gute und wertvolle Produkte herstellen, durch die Berichterstattung über Schwachstellen stark bedrängt werden und dadurch Gefahr laufen, vernichtet zu werden. Das ist eine ernstzunehmende Befürchtung; die Auswirkungen der Medienberichterstattung über gehackte Unternehmen können in der Tat enorm sein. Der mediale Umgang ist nicht selten vom Bewirtschaften von Empörung getrieben. Es hat sich jedoch gezeigt, dass der transparente Umgang mit Sicherheitsvorfällen in der Öffentlichkeit mit Wohlwollen aufgenommen wird. Verheimlichen und Ausredensuchen dagegen hat starke negative Auswirkungen auf die Wahrnehmung eines Unternehmens. Darunter fällt auch die oft anzutreffende Reaktion, ethischen Hackern mit einer Strafanzeige zu begegnen. Diese Anzeigen geschehen in der Hoffnung, das Verhalten der angezeigten Person beeinflussen zu können und sie von öffentlicher Kommunikation abzuhalten. Haben sich die Sicherheitsforscher an die branchenüblichen Prinzipien der *Coordinated* resp. *Responsible Disclosure* gehalten, bewirken Anzeigen hingegen genau das Gegenteil. In solchen Fällen ist der Hersteller in der Verantwortung, sich selbst ebenfalls an die anerkannten Prinzipien zu halten. Dann wird einem Hersteller auch kein medialer Sturm der Entrüstung entgegenwehen. Halten sich ethische Hacker nicht an die Disclosure-Prinzipien, ernten sie ohne Ausnahme harsche Kritik und verlieren ihren Anspruch auf Straflosigkeit.

[66] Der Umgang mit Schwachstellen beschäftigt nicht nur Unternehmungen, sondern auch die Staaten. Dass Schwachstellen von staatlichen Akteuren zurückbehalten werden, ist seit einiger Zeit bekannt und wird unter dem Stichwort «No Disclosure» resp. «Weaponization» diskutiert. In den USA wird im Rahmen eines sog. «Vulnerabilities Equities Process» (VEP) resp. «Government Disclosure Decision Process» (GDDP) abgewogen, ob eine Schwachstelle publiziert wird oder nicht. Die Befürworter solcher Prozesse bringen in erster Linie vor, dass damit eine Vielzahl wichtiger Faktoren (z.B. Staatsinteressen und Sicherheitsinteressen) miteinbezogen und ausserdem Transparenz geschaffen werde.[60] Solche Prozesse seien einer Non Disclosure-Politik vorzuziehen. Deutschland diskutiert seit längerem die Implementierung eines solchen Prozesses.[61] Auf politischer Ebene führt der Verzicht auf eine Non Disclosure-Strategie oder zumindest das Einhalten eines transparenten Schwachstellenmanagements im Rahmen eines VEP/GDDP-Prozesses dazu, als glaubhafte Aussenpolitik wahrgenommen zu werden. Zu den positiven Wirkungen staatlicher Disclosure Policies gehören des Weiteren die Förderung von gegenseitigem Vertrauen und das Dämmen von Aufrüstungsspiralen.[62]

---

59 ENISA, Coordinated Vulnerability Disclosure policies in the EU (∞), 2022;
vgl. Markus Christen/Bert Gordijn/Michele Loi, The Ethics of Cybersecurity, S. 34 und 174.

60 Die deklassifizierte VEP-Policy der USA und ein Factsheet finden sich hier: Vulnerabilities Equities Policy and Process for the United States Government November 15 (∞), 2017; Factsheet (∞).

61 Vgl. zum Ganzen Sven Herpig, Governmental Vulnerability Assessment and Management Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities (∞), 2018 sowie Alexandra Paulus, Why Germany should practice the cyber norms it preaches: «The Case of a Vulnerabilities Equities Process» (∞), 2022.

62 United Nations, (Fn. 53), S. 7 und 14, sowie United Nations, Developments, S. 7 f.; ebenso Sven Herpig, (Fn. 52), S.10 ff.

[67] Die Schweiz behandelt in ihrer nationalen Cyberstrategie ebenfalls das Schwachstellenhandling durch Veröffentlichung. Dem BACS/NCSC wird dabei eine zentrale Rolle bei CVD resp. der Schwachstellenkommunikation zugewiesen.[63] Anders als das Stärken von «Bug Bounty»- und «Public-Trust»-Programmen finden sich leider keine Hinweise dazu, ethisches Hacken zu legalisieren oder wenigstens in Betracht zu ziehen.

[68] Ende 2023 hat sich der Bundesrat in einem relativ knappen Bericht über CVD-Policies der öffentlichen Verwaltung und bundesnahen Betrieben zur Cybersicherheit geäussert. Er hat dabei die Cybersicherheit als eine zentrale Herausforderung unserer Gesellschaft in der immer komplexer werdenden Umwelt anerkannt und hält fest: «*Für die Cybersicherheit ist es entscheidend, dass alles unternommen wird, um die Risiken von Schwachstellen in IKT-Systemen zu minimieren*» und weil «*sehr viele Angriffe Schwachstellen in IKT-Systemen ausnutzen, ist die Verhinderung und Schliessung von Schwachstellen von zentraler Bedeutung*».[64] Auch die vom Bundesrat und den Kantonen 2023 gutgeheissenen Nationalen Cyberstrategie hält deutlich fest, dass es für die Cybersicherheit «*von essenzieller Bedeutung [ist], dass die Entstehung solcher Schwachstellen wo immer möglich verhindert wird und bestehende Schwachstellen rechtzeitig erkannt und rasch behoben werden*».[65] In der Nationalen Cyberstrategie ist ethisches Hacking im Ziel «Sichere und verfügbare digitale Dienstleistungen und Infrastruktur» explizit mit einer Massnahme bedacht. So soll ethisches Hacking mit Bug Bounties und «Public-Trust»-Programmen institutionalisiert und dadurch gefördert werden, «*indem Rechtssicherheit für ethische Hacker verbessert wird*».

[69] Deutschland steht kurz vor einer seit Langem geforderten Legalisierung von ethischem Hacking. Im Referentenentwurf vom 4. November 2024 zur Modernisierung des Computerstrafrechts äussert sich das Deutsche Bundesministeriums der Justiz mit klaren Worten für die Legalisierung ethischen Hackens: «*Es muss verhindert werden, dass das Strafrecht von Handlungen abschreckt, die im gesellschaftlichen Interesse erfolgen und daher wünschenswert sind. Genau dies droht im Falle des Computerstrafrechts*». Der gesetzliche Status quo sei «*zum einen mit Unsicherheiten für die IT-Sicherheitsforschung verbunden und stellt zum anderen keine angemessene Reaktion auf zunehmend schwerere Angriffe dar*». Im Referentenentwurf wie auch im gleichentags publizierten Informationspapier wurde IT-Sicherheit zu Recht als die «*Achillesferse der Informationsgesellschaft*» bezeichnet.[66] Mit der angestrebten Revision wurde in Deutschland der richtige Weg eingeschlagen.Belgien, Frankreich, die Niederlande, Lettland und Litauen haben schon heute Vorbildcharakter (vgl. dazu unten Rz. 124).

[70] Die EU hat mit der NIS-2-Richtlinie den Mitgliedsländern Massnahmen zur Umsetzung vorgegeben, um das Niveau der Cybersicherheit u.a. von zentralen Kommunikationsdienstleistern und kritischer Infrastruktur auf ein hohes Niveau zu bringen (vgl. Art. 2 NIS-2). Darin werden wichtige Strukturen auf nationaler Ebene wie länderübergreifend kooperierende CSIRTs geschaffen, aber auch die Pflicht, CVD-Prozesse einzuführen und eine breite Palette anerkannter

63 NCSC, Grundsätze (∞); NCSC, Ziel: Sichere und verfügbare digitale Dienstleistungen und Infrastruktur (∞).

64 Bundesrat, Die Förderung des ethischen Hackings in der Schweiz (∞), 29. November 2023, S. 3. In diesem Bericht vom 29. November 2024 erfüllt der Bundesrat das Postulats 20.4594, Bellaiche, vom 17. Dezember 2020, welches CVD Policies und die Teilnahme an Bug-Bounty-Programmen für die öffentliche Verwaltung und bundesnahe Betriebe fordert. Der Bericht weist daher eine eingeschränkte Sicht auf ethisches Hacking auf.

65 Bundesrat, Nationale Cyberstrategie (NCS) (∞).

66 Referentenentwurf des Bundesministeriums der Justiz, Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts (∞) sowie Informationspapier (∞), 4. November 2024, S. 1 f.; zum streitbaren Element der Erforderlichkeit siehe unten Kap. 3.6.1; Manuela Wagner/Oliver Vettermann (Fn. 45), S. 71.

Risikomanagement-Methoden bis hin zur Sicherheit von Lieferketten. Gewisse Aspekte von NIS-2 trifft man auch in der Schweiz bereits an. Die NIS-2 Richtlinie sieht beispielsweise vor, die koordinierte Offenlegung von Schwachstellen zu erleichtern (Art. 12 NIS-2; was mit der CVD Policy des BACS angestossen wurde) und die Massnahmen dazu in einer nationalen Strategie festzulegen (Art. 7 Abs. 2 Bst. c NIS-2; vgl. die Nationale Cyberstrategie der Schweiz), wobei eine Koordinationsstelle bezeichnet werden muss (Art. 11 Abs. 5 Bst. c NIS-2; diese Rolle übernimmt das BACS, wenn seine CVD eingehalten ist).[67]

[71] Auch der *Cyber Resilience Act*[68] (CRA), der am 12. November 2024 in Kraft getreten ist, bezweckt die Stärkung der Cybersicherheit und legt dabei den Fokus auf *Produkte* mit digitalen Elementen (Erwägung 9 ff. CRA) und die Sicherheit der Verbraucher (Erwägung 1 CRA). Bereits in den ersten Sätzen hebt der CRA die Bedeutung von Cybersicherheit hervor: «*Die Cybersicherheit bedeutet eine der grössten Herausforderungen für die Union. [...] Cyberangriffe sind ein Thema von öffentlichem Interesse, da sie sich nicht nur auf die Wirtschaft der Union, sondern auch auf die Demokratie sowie die Sicherheit und Gesundheit der Verbraucher kritisch auswirken*». Im Hinblick auf die Produktentwicklung kann die Stossrichtung mit der Vorgabe von DevSecOps heruntergebrochen werden. Über den gesamten Lebenszyklus (von Entwicklung über Betrieb bis hin zu End Of Life) von Produkten muss Sicherheit zwingend miteinbezogen werden, worunter auch die Supply Chain Sicherheit inklusive der Empfehlung, Software Bill of Materials (SBOM) zu führen, fällt.[69]

[72] Im bereits erwähnten Bericht ist der Bundesrat Ende 2023 trotz allem zur Auffassung gelangt, dass die bestehenden Bug Bounty-Programme genügen würden und kein Handlungsbedarf für eine Revision des Strafrechts bestünde. Begründet wird diese Haltung damit, dass weiteres Potential existieren würde, die bereits bestehenden Massnahmen stärker zu nutzen. Das greift zu kurz und ist wohl dem stark beschränkten Fokus des Berichts auf Coordinated Vulnerability Disclosure-Strategien der öffentlichen Verwaltung geschuldet. Wenn weiteres Potential besteht, wird damit bei Lichte betrachtet bestätigt, dass ein Defizit besteht. Defizite als Grund anzuführen, nicht zu handeln, macht keinen Sinn. Auffällig ist ausserdem, dass der Bericht fälschlicherweise ethisches Hacking mit Hacking auf legaler Basis gleichstellt. Im Bericht fehlt denn auch eine fundierte Auseinandersetzung mit den zahlreichen wissenschaftlichen Arbeiten und Berichten von Behörden und Kommissionen der letzten Jahre. Die ausländischen Legislaturbemühungen finden ebenfalls keine Erwähnung, obschon sie deutlich in Richtung einer Legalisierung von ethischem Hacking zeigen.

[73] Mit Fokus auf die Wirtschaft lässt sich erkennen, dass ethisches Hacking zu besseren Hard- und Softwareprodukten führt. Unter Marktteilnehmern mit ähnlichen Produkten würde sich der Wettbewerb verstärken. Die bereits bestehenden Bildungsinstitutionen im Bereich der Cybersicherheit würden gestärkt, da in der Schweiz ein breiter und offener Diskurs innerhalb der ethischen Sicherheitsforschungs-Szene entstehen könnte. Die Schweiz würde sich im Wettbewerb an vorderster Front positionieren und ihre bestehenden Standortvorteile weiter ausbauen, wenn sie eine Legalisierung rasch umsetzt. Das gilt umso mehr, als das zentrale europäische Wirtschaftsschwergewicht Deutschland demnächst nachzieht.

---

67 Die NIS-2 (∞) Richtlinie ist seit dem 18. Oktober 2024 anwendbar. Zu den bestehenden Implementationen Bundesrat (Fn. 64), S. 9 und 12.

68 Der CRA (∞) wird per 11. Dezember 2027 anwendbar.

69 Begrifflichkeiten: Siehe Wikipedia-Einträge zu DevSecOps und SBOM. Das Führen von SBOM kann an Wichtigkeit kaum unterschätzt werden, stellt aber auch eines der grössten und wohl noch nicht gelösten Probleme der Softwareentwicklung dar.

[74] Die Strafbefreiung führt nicht zu mehr bösen Hackern, sondern zu mehr guten Hackern. Mehr ethische Hacker führen zu mehr Schwachstellenmeldungen und zu sichereren Systemen. Das wiederum erschwert die Arbeit der kriminellen Hacker, hilft wirtschaftliche Totalverluste z.B. durch Ransomwareangriffe zu verhindern und erhöht den Schutz aller Userinnen und User, die tagtäglich digital kommunizieren. Genau das sollte das Ziel eines modernen Hackingstrafrechts sein.

[75] Der politische Wille zur Stärkung der Cybersicherheit ist international aber auch in der Schweiz längst vorhanden, daran gibt es keine Zweifel. Der Handlungsbedarf ist ausgewiesen und wirksame Lösungsansätze würden existieren. Warum aber bestraft man ethisches Hacking – also das Handeln im Interesse der Gesellschaft – trotzdem?

[76] Zusammengefasst: Ethisches Hacking ist – ausgenommen, es besteht eine rechtliche Basis wie bei Pentests oder Bug Bounty-Programmen – in der Schweiz strafbar. Ob ethische Hacker bestraft werden oder nicht, ist der Willkür der Systembetreiber überlassen, die es in der Hand haben, Strafantrag zu stellen. In Anbetracht des gesellschaftlichen Nutzens von ethischem Hacking und der Bedeutung für die IT-Sicherheit und die Wirtschaft, ist diese Situation nicht haltbar. Die Legalisierung von ethischem Hacking ist überfällig.

3. Revisionsvorschlag

3.1. Strafbefreiung durch neuen Abs. 3 für Art. 143bis StGB

[77] Ein revidierter Hackingartikel könnte wie folgt aussehen; neu ist die Strafbefreiung in Abs. 3:

> [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.*
>
> [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.*
>
> [3] *Wer gemäss Absatz 1 in redlicher Absicht handelt und dem Betreiber des Datenverarbeitungssystems sein Vorgehen offenlegt, bleibt straffrei.*

3.2. Tatbestandselement «in redlicher Absicht»

[78] Die redliche Absicht stellt ein subjektives Tatbestandselement dar, das die Strafbefreiung ausschliesslich auf ethische Hacker beschränkt. Nur wer hackt, um Schwachstellen zu identifizieren und diese zu melden, um sie schliessen zu lassen, hackt redlich.[70] Die redliche Absicht ist keine Ausschliessliche, aber eine Zwingende. Wer zusätzlich danach trachtet, Anerkennung zu erhalten oder auf eine Belohnung hofft, handelt nicht unredlich. Die redliche Absicht hat im

[70] Verlangt sind diese zentralen ethischen Grundsätze, aber nicht auch ein ethischer Überbau. Denkbar wäre z.B., auf eine Form von Hackerethik (vgl. dazu Wagner/Vettermann [Fn. 45], S. 23) abzustellen, das ist hingegen nicht notwendig und würde nur die Komplexität erhöhen.

objektiven Tatbestand, der sich aus Abs. 1 ergibt, kein direktes Pendent. Es handelt sich um eine überschiessende Innentendenz.[71]

[79] Dass Strafbefreiung gemäss dem Revisionsvorschlag im Einklang mit der *Cybercrime Convention* (CCC, auch Budapest Convention genannt) steht und dass die Intention auch nicht rein altruistisch sein muss, ergibt sich direkt aus dem Wortlaut von Art. 7 Ziff. 2 der CCC: «*A* ***State Party may require*** *that the offence be committed by infringing security measures,* ***with the intent of*** *obtaining electronic data or other* ***dishonest or criminal intent*** *or in relation to an information and communications technology system that is connected to another information and communications technology system*». Nichts anderes tut der Revisionsvorschlag. Unter Strafe bleibt «dishonest» Hacking bestehen, straflos sein wird ausschliesslich «honest» Hacking.

[80] Art. 40 CCC sieht die Möglichkeit vor, durch eine schriftliche Notifikation des Zeichnerstaats zu «*erklären, dass er von der Möglichkeit Gebrauch macht, nach Artikel 2, 3, 6 Absatz 1 Buchstabe b, 7, 9 Absatz 3 und 27 Absatz 9 Buchstabe e zusätzliche Merkmale als Voraussetzung vorzusehen*». Mit dieser Regel soll den Vertragsparteien gestattet werden, bestimmte zusätzliche Elemente aufzunehmen, um den erfassten Sachverhalt der materiellen Tatbestände anzupassen. Damit wird bezweckt, konzeptionelle oder rechtliche Unterschiede der Konventionsstaaten ausgleichen zu können, die in einem Vertrag mit globalem Anspruch eher gerechtfertigt sind, als sie es in rein europäischem Kontext gewesen wären. Unter «Erklärungen» werden akzeptable Auslegungen verstanden, wohingegen «Vorbehalte» die Rechtswirkung Verpflichtungen zu modifizieren oder gar auszuschliessen umfasst.[72]

[81] Der Explanatory Report des Europarats bestätigt die vorstehende Interpretation von Art. 7 Ziff. 2 CCC ausdrücklich.[73] Es waren gerade die Befürchtungen verschiedener Zeichnerstaaten, dass die Forschung nach Sicherheitslücken tangiert würde, die Anstoss dafür gab, Art. 2 CCC offen zu formulieren. Auf Grund des klaren Wortlauts ist es nicht notwendig gewesen, eine Erklärung zur CCC im Sinne von Art. 40 CCC abzugeben, um die Anwendung von Art. 2 Abs. 1 CCC auf unredliches Hacking einzuschränken. Die Möglichkeit, nur unredliches Hacking zu bestrafen, besteht für die nationale Legislative nach Art. 2 Abs. 1 CCC *expressis verbis*. Es ist den Zeichnerstaaten unbenommen, ethisches Hacking, also redliche Absicht gemäss der vorgeschlagenen Revision, von Strafe auszuschliessen.

[82] Auf Absichten abzustellen, hat im Schweizer Strafrecht lange Tradition. Oft werden Absichten benutzt, um besondere subjektive Unrechtselemente zu umschreiben. Das tatbestandstypische Unrecht wird dadurch genauer bezeichnet, was zu einer Einschränkung der Strafbarkeit führt.[74] Liegen sie nicht vor, wird man nicht bestraft. Zahlreich anzutreffen ist die Bereicherungsabsicht und davon abgeleitete Absichten, z.B. beim Betrug resp. Computerbetrug (Art. 146 und 147 StGB), beim Wucher (Art. 156 StGB) oder der Zechprellerei (Art. 149 StGB) etc.

---

71 Allenfalls liesse sich das Offenlegen des Vorgehens als Pendent hinzuziehen. Die Bezeichnung als überschiessende Innentendenz hat jedoch keine praktische Bedeutung.

72 Council of Europe, Explanatory Report to the Convention on Cybercrime (∞), 23. November 2001, Rz. 315. Die Schweiz hat eine Erklärung abgegeben, dass Art. 2 CCC nur Anwendung findet, wenn Hacking unter Verletzung von Sicherheitsmassnahmen begangen wird (siehe «Vorbehalte und Erklärungen» (∞) als Anhang zur CCC). Die Erklärung wirkt als Vorbehalt. Es wird keine Rechtshilfe gewährt, sollte Hacking nicht durch überwinden einer Sicherheitsmassnahme begangen worden sein.

73 Council of Europe (Fn. 72), Rz 50: «Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence.»

74 Vgl. BSK StGB I-Niggli/Maeder, Art. 12 N 76.

[83] Benutzt man Absichten nicht, um Strafbarkeit, sondern wie hier, um Straflosigkeit näher zu spezifizieren, hat das wie bei subjektiven Unrechtselementen eine Einschränkung der Anwendbarkeit zur Folge: Nicht jeder Hack bleibt straffrei, sondern nur, wenn er von redlicher Absicht getragen ist. Diese redliche Absicht manifestiert sich schliesslich in der Meldung an die Systembetreiberin.

[84] Absichten zu beweisen, kann schwierig sein. In die Köpfe reinschauen, lässt sich trotz allgegenwärtiger Technologie noch nicht ganz. Diese Beweisschwierigkeiten sind aber nichts Neues, egal ob sie nun strafbegründende oder strafbefreiende Tatbestandselemente betreffen; in beiden Fällen werden auf der Basis von «*Erfahrungsregeln, Durchschnittsurteilen und Alltagstheorien aus den äusseren Umständen, insb. dem Hergang der Tat, Rückschlüsse auf die innere Einstellung*» gezogen.[75]

[85] Die Redlichkeit ergibt sich also grob heruntergebrochen unmittelbar aus dem «Tatverhalten» und aus dem Verhalten im Rahmen der Offenlegung gegenüber der Systembetreiberin. Es wird von den äusseren auf die inneren Tatsachen geschlossen. Diese Art der Beweisführung ist es denn auch, die opportunistisches Grey Hat-Hacking in die Schranken weist.

[86] Die Vorgehensweise während des Hacks, das Verhalten vor und nach dem Hack und die digitalen und analogen Spuren vereiteln es unredlichen Hackern, nach Belieben die Seiten zu wechseln und sich der Strafe zu entziehen. Mit böser Gesinnung starten und wenn man dann erwischt wird, rasch die Seite wechseln und ethisches Hacking vorgeben, ist nur auf den ersten Blick ein reales Szenario. Es würde bedeuten, dass die Strafverfolgungsbehörden den Hacker erwischen würden, noch bevor er seine Meldung machen konnte. Mit Blick auf die zeitlichen Dimensionen der Meldung (dazu sogleich), die ein ethischer Hacker einhalten muss, hätte er seinen Strafbefreiungsanspruch aufs Spiel gesetzt. Selbst wenn das der Fall wäre, würde eine Hausdurchsuchung und die anschliessende Auswertung der Gerätschaften einen böswilligen Hacker (der sich schliesslich entgegen der üblichen OPSEC-Massnahmen sogar noch erwischen lassen müsste) in Erklärungsschwierigkeiten bringen.

[87] Und gelingt es einem Grey Hat-Hacker dennoch ausnahmsweise einmal, sich als ethischer Hacker auszugeben, so ist das zu akzeptieren. Perfekte Regelungen gibt es genauso wenig wie perfekte Sicherheit. Die Schwachstelle muss in jedem Fall – also auch beim unwahrscheinlichen Fall eines Grey Hat-Hacks – gemeldet werden, was immer der Allgemeinheit zu Gute kommt.

3.3. Tatbestandselement «Betreiber des Datenverarbeitungssystems»

[88] Gemäss Revisionsvorschlag ist Adressat der Meldung die Systembetreiberin selbst und nicht eine behördliche Stelle. Damit wird dem BACS oder dem EDÖB nicht eine zusätzliche Aufgabe zugeteilt. Will man dennoch eine behördliche Meldestelle einführen, wären die Meldesysteme von BACS resp. EDÖB bereits vorhanden und würden sich anbieten.

[89] Der Vorschlag enthält keinen amtlichen Meldeweg. Es besteht kein Bedarf dafür, da sich der Hack im Verhältnis zweier (Rechts-)Subjekte zuträgt. Es spielt keine Rolle, ob es sich dabei um eine Betreiberschaft privater oder öffentlich-rechtlicher Natur handelt. Der Verzicht auf die

75 BSK StGB I-Niggli/Maeder, Art. 12 N 59, mit der Diskussion zur Beweisführung beim Eventualvorsatz; BGE 134 IV 26 E 3.2.

Meldung an eine amtliche Stelle entspricht der Ausgestaltung von Art. 143bis Abs. 1 StGB als Antragsdelikt.

[90] Die Betreiberschaft eines Systems zu identifizieren, ist für Hackerinnen selten mit Schwierigkeiten verbunden. Sind Webdienste betroffen, lassen sich die Kontaktdaten auf Webseiten finden, namentlich im Impressum, einer Datenschutzerklärung oder einer security.txt[76]. Bei Systemen, die keinerlei Webdienste laufen haben, können Informationen in Banner Messages enthalten sein. Weiter ist beispielsweise an *Reverse IP Lookups* zu denken, womit andere Domains identifiziert werden können, was wiederum Rückschlüsse auf die Betreiberschaft zulässt. Auch *eine Reverse Pointer-* oder *WHOIS-Abfrage* kann nützlich sein. Die Analyse eines Netzwerksegments kann unter Umständen die notwendigen Aufschlüsse oder Hinweise auf andere beteiligte Systeme ergeben. Letzten Endes besteht die Möglichkeit den Hoster oder ISP zu kontaktieren oder dann ein zuständiges CERT resp. CSIRT, das BACS oder die Strafverfolgungsbehörden um Hilfe bei der Identifikation anzufragen. Häufig wird dann der Kommunikationsweg hergestellt, in dem sich die Betreiberschaft zu erkennen gibt; Hoster, ISPs und Behörden geben keine direkten Auskünfte.

[91] Es ist im ureigensten Interesse der Betreiberschaft, intern eine angemessene Organisation aufzustellen und gegen aussen bekannt zu machen. Die Hacker haben ihr Mögliches zu tun und dürfen auf eine funktionierende interne Organisation vertrauen. Viele Länder haben zudem Transparenz- resp. Kennzeichnungspflichten eingeführt. Ordentlich aufgestellte Systembetreiber halten den Sicherheitsforschern eine security.txt vor, worin alle notwendigen Angaben – inkl. exakte Angaben zu einem sicheren Kommunikationskanal, einschlägige Policies und gewünschte Informationen – zu finden sind. Die Minimalvariante kann so aussehen:[77]

Contact: mailto:securityissues@example.com

Policy: https://example.com/.well-known/policy.txt

Encryption: https://example.com/pgp-key.txt

Canonical: https://example.com/.well-known/security.txt

Expires: 2026-01-01T00:00:01Z

Preferred-Languages: en, de

[92] Nicht wesentlich ist es, dass die Hacker die *rechtlich* korrekte Entität über den Hack orientieren, solange die Meldung am Ende an die verantwortliche Stelle gelangt. Diese Stelle sollte befähigt sein, die Schwachstelle zu beheben oder beheben zu lassen. Das heisst selbstverständlich nicht, dass die Meldung an irgendwen gehen kann, um der Offenlegungspflicht nachzukommen. Ausschlaggebend wird sein, dass man sich an jene Stelle wendet, die sich nach dem gewöhnlichen Lauf der Dinge und der allgemeinen Lebenserfahrung als die Zuständige ergibt. Jede irgendwie erdenkliche Abklärung muss nicht vorgenommen werden. Bei der initialen Mitteilung ist stets Zurückhaltung angezeigt und insbesondere bei Unklarheiten ratsam, nicht die vollständige Meldung mit sämtlichen Details oder gar einem *Proof of Concept* an eine Adresse zu senden, die man nicht vernünftig verifizieren konnte.

76 Siehe zum Inhalt RFC 9116 (∞).

77 Vgl. die Beispiele in RFC 9116 (∞), Ziff. 2.6 f. oder https://www.admin.ch/.well-known/security.txt (∞).

[93] Der Inhalt einer Schwachstellenmeldung ist vertraulich, da er sicherheitskritische Informationen enthält. Er darf nicht Dritten zugänglich gemacht oder gar publiziert werden (unmittelbares Full Disclosure).[78]

[94] Sollte sich die Betreiberschaft auf Meldung hin nicht rühren, also weder den Eingang der Meldung bestätigen oder die Meldung zwar bestätigen, aber dann keine weitere Kommunikation erfolgen lassen, sollten sich die Sicherheitsforscher um wiederholte Kommunikation bemühen. Es ist empfehlenswert, sich in solchen Situationen an die Prinzipien der *Responsible Disclosure* resp. *Coordinated Vulnerability Disclosure* zu halten. Zu denken ist dabei vorab an eine Meldung ans BACS.

3.4. Tatbestandselement «sein Vorgehen offenlegt»

[95] Das Offenlegen berührt im Wesentlichen zwei Dimensionen, eine Inhaltliche und eine Zeitliche.

[96] *Inhaltliche Dimension:* Es wird nicht vorgegeben, in welchem Detaillierungsgrad die Hacker ihre *Findings* zu kommunizieren haben. Selbstverständlich ist, dass die Offenlegung alles enthalten muss, dass die Systembetreiberin den Hack und damit die Schwachstelle nachvollziehen kann. Es ist dann an ihr, anhand der Meldung die relevanten Soft- und Hardwareteile resp. Systeme zu identifizieren und die Schwachstelle zu beheben. In aller Regel wird die Offenlegung auch die erkannten Schwachstellen enthalten, nur so kann das Vorgehen sinnvoll dokumentiert und nachvollzogen werden.

[97] Bei der initialen Kontaktaufnahme muss wie erwähnt insbesondere bei Unklarheiten über die zuständige Betreiberschaft vorsichtig vorgegangen werden. In solchen Fällen sollte die Meldung nur die zentralsten Angaben enthalten, sodass ein unzuständiger Dritter mit den Angaben nicht sein Unwesen treiben kann. Nachdem die Betreiberschaft zuverlässig festgestellt werden konnte, ist das gesamte Wissen um die Schwachstelle offenzulegen.

[98] Der Revisionsvorschlag verzichtet bewusst darauf, Detailvorgaben zum Inhalt zu machen. Es besteht breit abgestützter Konsens, was eine Schwachstellenmeldung zu enthalten hat. Typischerweise werden die betroffenen Produkte resp. Dienste angegeben und aufgezeigt, wie die Sicherheitslücke identifiziert und allenfalls reproduziert werden kann. Es kann auch der Code zu einem *Proof of Concept* enthalten sein. Soweit möglich und überhaupt bekannt, werden die funktionalen Auswirkungen der Schwachstelle umrissen.[79]

[99] Die ISO hat sich mit dem Offenlegen von Sicherheitslücken befasst und die Norm ISO/IEC 29147 entwickelt. Eng verzahnt mit dem CVD-Prozess nach ISO/IEC 29147 ist der *Vulnerability Handling-Prozess*, der ebenfalls eine Normierung mit ISO/IEC 30111 erfahren hat. Die ISO-Normen zum Offenlegen resp. jene zum koordinierten Veröffentlichen von Schwachstellen sind zwar nicht verbindlich, stellen aber dennoch *de facto* die Vorgehensweise dar, die in der IT-Branche erwartet und gelebt wird.[80] Das Abweichen von diesen in der Praxis anerkannten Standards sollte gut überlegt sein. In der Rechtsanwendung – namentlich bei der Beurteilung durch

78 Vgl. ISO/IEC 29147:2020, 6.2.1.

79 Vgl. ISO/IEC 29147:2020, 6.2.1. Richtigerweise werden auch in dieser ISO-Norm keine Vorgaben über das Notwendigste hinaus gemacht.

80 So auch Bundesrat (Fn. 64), S. 9 unten.

Gerichte – gelten solche Quellen als quasigesetzliche Leitlinie resp. als anerkannter Stand der Wissenschaft und Erfahrung im Sinne von Art. 139 Abs. 1 StPO.[81]

[100] *Zeitliche Dimension:* Es würde keinen Sinn machen, starre Fristen auf Gesetzesstufe festzulegen. Die bereits diskutierte Branchenüblichkeit und der herrschende Konsens zur *Responsible* resp. *Coordinated Vulnerability Disclosure* genügen. Als Richtschnur gilt: Die Findings sollten in einer initialen Fassung innerhalb von drei Tagen der Systembetreiberin gemeldet werden.

[101] Drei Tage bedeutet in Anlehnung an Art. 90 Abs. 1 StPO, dass die Meldung am dritten Tag nach dem Hack erfolgt sein sollte. Die Interpretation von Tagesfristen auf diese Weise ist im Schweizer Recht breit verankert.[82] Würde man Fristen in Stunden zur Anwendung bringen wollen, so würde die Stundenfrist nach Erkennen der Schwachstelle zu laufen beginnen. Die Systembetreiberschaft bestätigt der meldenden Person danach üblicherweise innert 3 Tagen die Meldung, sicher aber innert 7 Kalendertagen.[83] Dieser zeitnahe Austausch ist zentral, damit zwischen der Hackerin und der Betreiberschaft im Rahmen der Schwachstellenmeldung rasch eine Vertrauensbasis und eine gute Arbeitsbeziehung entstehen kann.[84] Je kritischer der Inhalt der Meldung ist, desto rascher sollte die Betreiberschaft die Meldung bestätigen und um die Behandlung bemüht sein.

[102] Der zeitliche Aspekt für die Meldung hat sich am Risiko zu orientieren, das sich aus Sicht der Hackerinnen ergibt. In die Risikobewertung aufzunehmen sind Aspekte wie die Art der Daten, die im System gehalten werden oder die Kritikalität des Systems für weitere Systeme. Aber auch die Kritikalität der gefundenen Schwachstelle in einer globalen Betrachtung kann ein Kriterium darstellen: Schwachstellen der Kategorie «Class Breaks» können eine ganze Kaskade an Security Breaches nach sich ziehen oder dadurch ganze Cyberökosysteme in ihrer Vertraulichkeit, Integrität und Verfügbarkeit tangieren.[85] Ein zweifellos zutreffendes Beispiel für einen derartigen Fehler war der *Heartbleed-Bug*, bei dem mit der Transportverschlüsselung (z.B. in https) ein fundamentaler Bestandteil der weltweiten Kommunikation betroffen war. Ob die Sicherheitslücke bereits aktiv, also «in the wild» ausgenutzt wird, ist ein weiterer zentraler Aspekt, den man zur Bewertung des Risikos beiziehen kann. Wird eine Sicherheitslücke bereits aktiv ausgenutzt, drängt sich sehr rasches Handeln durch die Melderin wie auch durch die Systembetreiberin auf.

[103] Keinen Sinn würde es machen, eine strikt objektive Sicht einzunehmen und von Hackerinnen zu verlangen, sie hätten sämtliche Aspekte in ihre Risikoeinschätzung miteinzubeziehen. Solche Anforderungen wären überzogen und haben im Schweizer Strafrecht auch keinen Halt.

[104] Fristen von beispielsweise 24h unter den ohnehin schon kurzen branchenüblichen drei Tagen führen zu mehr False Positive-Meldungen und verursachen nur Mehraufwand ohne wirklichen Nutzen. Ethische Hacker und Hackerinnen sind sich ihres Tuns bewusst und schätzen die

---

81 So stellt das Bundesgericht bspw. in konstanter Praxis auf Studien und Empfehlungen z.B. der Schweizerische Gesellschaft für Rechtsmedizin (SGRM) ab und erhebt deren Überlegungen zu Quasigesetz: Empfehlung zur Haaranalytik (BGer 1C_284/2022, E.2.3.3), Empfehlung betr. THC-Grenzwerten (BGE 145 IV 513 E. 2.3.3), Studie zum durchschnittlichen Reinheitsgehalt von Crystal-Meth (6B_504/2019 E. 2.2).

82 M.w.H. BSK StPO-Riedo, Art.90, N 1.

83 Das BACS bestätigt den Eingang von Meldungen innert 3 Arbeitstagen und triagiert innert 5 Arbeitstagen. Betrifft die Schwachstelle den Bund, so ist das BACS bemüht, die Lösungsfindung innert 60 Tage koordiniert zu haben, vgl. BACS, Rahmenbedingungen und Regeln (∞).

84 Vgl. ISO/IEC 29147:2020, 6.2.5 und ISO/IEC 30111:2020, 6.5.3.3 «timely manner».

85 Zum Begriff «Class Break» und den massiven Auswirkungen siehe Bruce Schneier, Click Here To Kill Everybody, New York, 2018, S. 31 ff. und 95, sowie Bruce Schneier, Class Breaks, 2017 (∞).

Lage in aller Regel akkurat ein. Sind sie der Auffassung, dass eine umgehende Meldung erfolgen muss, tun sie das auch.

[105] In Belgien hat man ethischen Hackern und Hackerinnen eine 72h-Frist vorgegeben, innert der die vollständige Meldung der Systembetreiberin sowie dem belgischen CSIRT *Centre for Cyber Security Belgium* (CCB) erfolgen muss. Innert 24h hat vorab eine initiale Meldung zu erfolgen (Art. 23. § 1er. 2° und 3°).[86] Litauen hat eine 24h-Frist eingeführt, nach welcher eine Meldung an das *National Cyber Security Centre* (Art. 25 Ziff. 3 Cybersicherheitsgesetz). Frankreich hat auf eine feste Fristensetzung auf Gesetzesstufe verzichtet; wenn Meldungen an das französische CSIRT, die *Agence nationale de la sécurité des systèmes d'information* (ANSSI), gehen, bestehen behördeninterne Fristen zur Bearbeitung der Meldung. Ebenfalls auf eine Frist wurde in den Niederlanden verzichtet.[87]

[106] Breite Akzeptanz besteht darin, die Schwachstellen grundsätzlich 90 Tage nach der Meldung der Öffentlichkeit bekannt zu machen.[88] Unbegründet ist die Befürchtung, eine solche Veröffentlichung würde zu einer Rufschädigung beitragen. Es ist gesellschaftlich akzeptiert, dass Fehler in Produkten vorkommen können, insbesondere bei Produkten, die IT-basiert sind. Nicht das Bekanntwerden von Sicherheitslücken ist das Problem, sondern schlechtes Handling von gemeldeten Schwachstellen. Hinhaltetaktiken oder gar Verschleierung sind es, welche den Ruf von Herstellern und Systembetreibern in Mitleidenschaft ziehen. Mit richtigem *Vulnerability Management* und angemessener Kommunikation kann im Gegenteil sogar ein guter Ruf gepflegt werden. Regelmässige Updates und das Patchen von Schwachstellen stellen bei den Abnehmerinnen und Abnehmer ein Kaufargument dar.

[107] Bemühen sich die Hacker und Hackerinnen nicht um eine zeitnahe Meldung, tun sie sich im Übrigen selbst keinen Dienst. Werden sie noch vor ihrer (zu späten) Meldung ermittelt, werden sie bedeutend mehr Mühe haben, ihr Tun als redliches Hacking darlegen zu können. Es ist daher so oder anders im eigenen Interesse der Sicherheitsforscherinnen, möglichst rasch der Offenlegungspflicht nachzukommen. Die Erfahrungen im Rahmen der Coordinated Vulnerability Disclosure zeigen denn auch auf, dass die Hackerinnen intensiv darum bemüht sind, ihre Entdeckungen laufend zu dokumentieren und die Betreiber der betroffenen Systeme rasch zu orientieren.

[108] Es ist wie aufgezeigt also sinnvoll, keine festen Vorgaben auf Gesetzesstufe zu erlassen. Sollte sich eine Revisionsvariante abzeichnen, bei der eine zentrale Meldestelle involviert ist und konkretere zeitliche Vorgaben den politischen Konsens besser abbilden, so sollten diese Vorgaben als Richtwerte und nur auf Stufe Verordnung definiert werden.

86 https://ccb.belgium.be/en/vulnerability-reporting-ccb (∞).

87 Eine Übersicht zum rechtlichen Stand von ethischem Hacking und Coordinated Vulnerability Policies in verschiedenen Ländern ist hier abrufbar: https://ethical-hacking.law (∞).

88 Vgl. das «Vulnerability Disclosure Cheat Sheet» (∞) des Open Worldwide Application Security Project (OWASP) oder die Google Vulnerability Handling Policy (∞).

3.5. Tatbestandselement «straffrei»

[109] Die CCC hatte zum Zweck, dass alle Zeichnerstaaten Hacking unter Strafe stellen.[89] Sie verbietet hingegen nicht, dass *ethisches* Hacking von Strafe ausgenommen wird. Art. 2 CCC sieht vor, dass die Konventionsstaaten die Strafbarkeit von der «unredlichen Absicht» abhängig machen dürfen (vgl. oben Rz. 78 ff.). Der Revisionsvorschlag ist wie bereits aufgezeigt, konventionskonform.

[110] Die Strafprozessordnung ermöglicht u.a. mit Art. 8 Abs. 1 StPO den Behörden, von Strafverfolgung abzusehen, *wenn es das Bundesrecht vorsieht*. In solchen Fällen wird gemäss Art. 8 Abs. 4 StPO die Nichtanhandnahme (Art. 310 StPO) resp. Einstellung (Art. 319 StPO) verfügt. Mit dem revidierten Hackingartikel würden inskünftig keine Strafverfahren mehr gegen ethische Hacker/Hackerinnen geführt. Art. 52 StGB gäbe zwar den Strafverfolgungsbehörden bereits heute die Möglichkeit an die Hand, von einer Strafverfolgung, einer Überweisung an das Gericht oder einer Bestrafung abzusehen, wenn Schuld- und Tatfolgen geringfügig sind. Art. 52 StGB findet hingegen kaum Anwendung und ist gerade bei Antragsdelikten sehr zurückhaltend anzuwenden.[90] In Anbetracht der heutigen Ausgestaltung des Hackingstrafrechts besteht keine Möglichkeit, auf dieser Basis von Strafverfolgung abzusehen; ganz abgesehen von den massiven Rechtsunsicherheiten, die durch die Umschreibung mit «geringfügigen» Schuld- und Tatfolgen im Kontext von Hacking weiterhin bestehen würden. Die Rechtswidrigkeit des Vorgehens würde zudem weiterhin bestehen. Untersuchungen bei Hacking sind komplex und aufwendig, was wie bereits aufgezeigt zur Auferlegung von Verfahrenskosten führen kann, selbst wenn auf eine Strafe verzichtet wird. Weder Art. 8 StPO noch Art. 52 Abs. 1 StGB genügen daher, um ethisches Hacking nach heutigem Recht von Strafe zu befreien.

[111] Die Formulierung des Revisionsvorschlags lehnt sich an die Strafbefreiungsregel des Landfriedensbruchs nach Art. 260 Abs. 2 StGB an. Wer sich nach Aufforderung aus der Ansammlung trotz an sich erfülltem Landfriedensbruch entfernt, «bleibt straflos». Wir haben also mit dem vorgeschlagenen Wortlaut eine bereits bekannte Formulierung, die mit den üblichen Auslegungsmethoden interpretiert werden kann.

[112] Etwas Ähnliches finden wir mit einer Kann-Formulierung bei den Ehrverletzungsdelikten, so z.B. in Art. 173 Ziff. 4 StGB. Eine Kann-Formulierung für Art. 143bis StGB wäre aber aus offensichtlichen Gründen der falsche Weg. Die Strafbarkeit ethischer Sicherheitsforscherinnen und -forscher darf nicht von den Überlegungen der Rechtsanwender abhängen.

[113] Strafbefreiung ist dem StGB also nicht fremd und lässt sich mit der vorgeschlagenen Formulierung «bleibt straffrei» ohne Rechtsunsicherheiten umsetzen.

---

89 Bundesrat, Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität (∞), 2010, BBl 2010 4697, S. 4703.

90 Jositsch/Schmid, StPO Praxiskommentar, 4. Aufl., Art.8 N 4; BSK StGB I-Riklin, Art. 52 N 28; Pfister (Fn. 30), S. 74.

3.6. Varianten

3.6.1. Meldepflicht an «zuständigen Stelle»

[114] Es wäre auch denkbar, neben der Offenlegung gegenüber der Systembetreiberin eine Pflicht zur Meldung **an eine zuständige Stelle** – auf Stufe Bund oder Kantone – einzuführen:

> [3] *Wer gemäss Absatz 1 in redlicher Absicht handelt und dem Betreiber des Datenverarbeitungssystems sowie der zuständigen Stelle sein Vorgehen offenlegt, bleibt straffrei.*

[115] Diese Lösung würde sich an die belgische und französische Regelung anlehnen und hat Vor- und Nachteile. Von Vorteil wäre diese Lösung, weil die zuständige Stelle über die sicherheitsrelevanten Umstände Kenntnis erlangt und die Schwachstellenveröffentlichung koordinieren oder die Koordination unterstützen könnte. Auch dem Datenschutz würde etwas mehr Nachdruck verliehen, da verletzliche Systeme in der Tendenz auch zu Datenschutzverletzungen führen. Das gilt insbesondere bei Konfigurationsfehlern oder ungepatchten Systemen, welche unter Umständen ein Verstoss gegen Art. 7 Abs. 1 DSG darstellen (vgl. auch Art. 1 Abs. 1 DSV und den Stand der Technik nach Abs. 4 lit. b DSV). Anders sieht es aus, wenn neue Lücken entdeckt werden, namentlich 0-*Day-Vulnerabilities*. Bei solchen neuen Lücken besteht der Vorteil einer staatlichen Meldestelle darin, dass diese Lücke zum Wohle der Öffentlichkeit in einem Coordinated Vulnerability Disclosure-Prozess bekannt gemacht werden.[91] Diese Meldungen kommen nicht nur der Schweizer Öffentlichkeit zu Gute, sondern der ganzen Welt. In diesem Prozess werden die Informationen zur Sicherheitslücke geordnet bekanntgegeben und dem Hersteller für die Behebung angemessene Zeit eingeräumt. In diesem Kontext wären dann auch eidgenössische Vulnerabilities Equities Prozesse resp. «Government Disclosure Decision»-Prozesse anzusiedeln (VEP/GDDP oben Rz. 66 f.).

[116] Auf der Stufe Bund wäre an das BACS oder den EDÖB zu denken. Beim BACS wäre das technischen Know-how sicher vorhanden, wohl auch beim EDÖB und ein Austausch unter diesen Bundesstellen würde naheliegen. Diese neue Meldepflicht würde bei der zuständigen Stelle zusätzliche Ressourcen notwendig machen, bereits heute ist die Situation angespannt. Für eine Ansiedlung beim EDÖB würde sprechen, dass der EDÖB bereits heute die Meldestelle für Datenschutzverletzungen ist, falls ein hohes Risiko für die Persönlichkeit oder die Grundrechte Betroffener besteht (Art. 24 Abs. 1 DSG). Das bestehende Meldesystem könnte um eine Meldefunktion erweitert werden.

[117] Auch ein föderalistischer Ansatz mit der Einführung einer kantonalen Meldestelle wäre denkbar. Die Strafverfolgung im Bereich des Hackings fällt regelmässig in die Zuständigkeit kantonaler Staatsanwaltschaften (vgl. z.B. Art. 22und 23 StPO). Denkbar wäre eine Meldepflicht direkt bei einer spezialisierten Abteilung einer Staatsanwaltschaft, was hingegen bei Diskussionen mit Sicherheitsforscherinnen wenig Begeisterung auslöst. Abgesehen von der bekanntermassen sehr kritischen Ressourcensituation der kantonalen Strafverfolgern, bestehen für diese geradezu untypische Konstellation soweit bekannt noch nirgends Prozesse, an die man anknüpfen oder sie zum Vorbild nehmen könnte. Verbleiben würden dann die kantonalen Datenschutzstellen,

[91] So ist das BACS eine durch MITRE akkreditierte Vergabestelle von CVE-Nummern und bietet professionelle Abläufe für die geordnete Veröffentlichung von Sicherheitslücken an. Im Jahr 2024 hat das BACS über 20 solcher Sicherheitslücken auf diese Weise veröffentlicht, darunter einige mit der Risikobewertung «Critical» und diverse mit Bewertung «High».

wo häufig bereits Prozesse für die Meldung von Datenschutzverletzungen bestehen, die sich aber grundsätzlich auf Vorfälle bei kantonalen und kommunalen Stellen beziehen.[92]

[118] Zu bevorzugen ist eine Lösung ohne neue Kompetenzen resp. Aufgaben, weder auf Stufe Bund noch Kanton: Zwar besteht dadurch tendenziell die Gefahr, dass das Wissen um die Sicherheitslücke verloren geht, wenn keine staatliche Stelle wie beispielsweise das BACS involviert ist. So besteh die Gefahr, dass die Sicherheitslücke stillschweigend behoben wird, was insbesondere bei bislang unbekannten Sicherheitslücken sehr bedauerlich wäre. Auf der anderen Seite muss man anerkennen, dass sich sehr häufig Privatrechtssubjekte gegenüberstehen und Hacking ein Antragsdelikt darstellt. Konsequenterweise wäre daher auch der gesamte Meldeprozess den Betroffenen zu überlassen. Es spricht so oder anders nichts dagegen, dass eine kompetente Stelle wie namentlich das BACS ein Merkblatt zum Umgang mit Schwachstellen zu Händen ethischer Hackerinnen und Hacker sowie den Systembetreibern erlässt.

3.6.2. Nur notwendige Vorgehensweise angewandt

[119] In Anlehnung an den deutschen Revisionsentwurf wäre es denkbar, eine Art Notwendigkeitsklausel einzuführen:

> [3] *Wer gemäss Absatz 1 in redlicher Absicht und nur soweit als notwendig handelt und dem Betreiber des Datenverarbeitungssystems sein Vorgehen offenlegt, bleibt straffrei.*

[120] Diese Formulierung bringt zum Ausdruck, dass nur jene Hacker und Hackerinnen straffrei bleiben sollen, die sich auf das Notwendigste beschränkt haben, um die Sicherheitslücke zu entdecken und auszunutzen. Sie lehnt sich stark an die in Deutschland diskutierte Wendung an, wonach eine Handlung nicht unbefugt ist, wenn «sie zur Feststellung der Sicherheitslücke erforderlich ist». Zwar ist dieses Ansinnen nachvollziehbar; es bestehen offensichtlich Ängste, den Sicherheitsforschenden zu sehr freie Hand zu lassen.

[121] Es gibt hingegen keinen sachlichen Grund, eine solche Formulierung aufzunehmen. Würde man diese Regelung einführen, hätte das zur Konsequenz, dass man sich bereits im strafbaren Versuch befindet, bevor ein Hack überhaupt funktioniert. Der Sicherheitsforschung ist inhärent, dass sie auf Trial & Error basiert, das gilt ganz besonders bei Black Box-Angriffen. Bis der Exploit wirklich funktioniert, wird der Angriff in unterschiedlichsten Iterationen getestet, bis er schliesslich im Zielsystem die beabsichtigte Wirkung entfaltet. Es ist im Rahmen des Coordinated Vulnerability Disclosures zudem üblich, der Meldung einen Proof of Concept beizufügen. In den seltensten Fällen ist dieser Proof auf den ersten Anhieb funktionsfähig.

[122] Ob eine Handlung notwendig war oder nicht, lässt sich nicht zum Vornherein herausfinden. Dieses Tatbestandselement kann daher in vielen Fällen von den Sicherheitsforschenden nicht kontrolliert werden, was dem ursprünglichen Ziel von mehr Rechtssicherheit zuwiderläuft. Die Rechtsunterworfenen stehen vor einer unmöglich einzuhaltenden Anforderung, was bei Straftatbeständen nicht haltbar ist. In Belgien existiert die Vorgabe, dass das Vorgehen notwendig und verhältnismässig sein muss, um die Sicherheitslücke zu entdecken und zu rapportieren. Diese Formulierung schwächt die Notwendigkeit wohl etwas ab und könnte dahingehend interpretiert werden, dass auch nicht notwendige Fehlversuche straffrei sein sollen, da sie für das Entde-

92 So z.B. in LU (§7 Abs. 1 KDSG) oder ZH (§ 12a Abs. 1 IDG).

cken und Rapportieren notwendig sind. Was in einem technischen Kontext «verhältnismässig» ist, dürfte aber kaum abschliessend eruierbar sein.

[123] Dass es im Rahmen eines Hacks nicht notwendig ist, Daten einzusehen, zu stehlen oder gar zu zerstören, ist offensichtlich. Solche Fälle bleiben aber auch weiterhin strafbar (vgl. Rz. 130 ff. unten), was zusätzlich belegt, dass eine Notwendigkeitsklausel überflüssig ist.

3.7. Andere Länder

[124] *Belgien*: Hacking ist nach 550bis §1er (Eindringen in Computersysteme) resp. 550bis §2 (Überschreiten der Zugangsberechtigung) und mit Qualifikationstatbeständen nach 550bis §3 des belgischen Strafgesetzbuchs strafbar. Ethisches Hacking ist seit dem 17. Mai 2024 nach Art. 23. § 1er. NIS2 erlaubt. Zuvor wurde ethisches Hacking bereits im Rahmen der am 15. Februar 2023 in Kraft getretenen Whistleblower-Gesetzgebung legalisiert. Innert 24h muss eine initiale Meldung erfolgen, innert 72h dann die vollständige. Die Meldung muss an die Systemverantwortlichen sowie das nationale CSIRT erfolgen. Vorausgesetzt ist weiter, dass die Tätigkeit nicht über das hinausgeht, «*qui était nécessaire et proportionné pour vérifier l'existence d'une vulnérabilité et pour la rapporter*». Die Schwachstelle darf nicht ohne vorgängig Erlaubnis durch das nationale CSIRT veröffentlicht werden, was auf eine interne Policy zur Veröffentlichung von Schwachstellen mit Vorbehalt zu Gunsten staatlicher Interessen zusammenhängen könnte (vgl. VEP/GDDP oben Rz. 66 f.).

[125] *Deutschland*: Hacking steht in Deutschland derzeit noch nach § 202c Abs. 1 StGB (Vorbereiten des Ausspähens und Abfangens von Daten) unter Strafe. Das deutsche Bundesministerium der Justiz hat einen Revisionsvorschlag zur Legalisierung von ethischem Hacking erarbeitet, der nächstens umgesetzt wird.[93] Der vorgeschlagene Lösungsansatz basiert auf dem Einfügen einer neuen Legaldefinition in § 202a Abs. 3 StGB, welcher definiert, was «nicht unbefugt im Sinne des Abs. 1» ist. Hacking ist nicht mehr strafbar, wenn der Hack in Absicht erfolgt, eine Sicherheitslücke festzustellen, diese Sicherheitslücke dem Systemverantwortlichen, Dienstleister, Hersteller oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet wird und dieser Hack zur Feststellung der Sicherheitslücke erforderlich ist. § 202a Abs. 3 StGB ist gleichermassen Anwendbar für den «Hackerparagrafen» § 202c Abs. 1 StGB. Der Revisionsvorschlag enthält keine Fristen, hingegen eine Art Notwendigkeitsklausel.

[126] *Frankreich*: Bereits seit dem 9. Oktober 2016 kennt Frankreich eine (fakultative) Strafbefreiung durch Article L2321-4 des Code de la Défense. Für die Zwecke der Sicherheit von Informationssystemen gilt der Verfolgungszwang nach Art. 40 der französischen Strafprozessordnung (Analog Art. 7 CH-StPO) unter der Voraussetzung nicht mehr, dass die Person in gutem Glauben handelt und sie die Schwachstelle *ausschliesslich* der ANSSI meldet. Es besteht keine Frist zur Meldung. Die ANSSI entscheidet über die weitere Behandlung der Meldung, wobei detaillierte Vorgaben auf Gesetzesstufe bestehen. Der Meldenden Person wird von Gesetzes wegen seitens der ANSSI Anonymität gewährt. Der Schutz ethischer Hacker vor Strafverfolgung erfolgt im französischen Modell also indirekt und nicht *ex lege*, sondern im Endeffekt über einen Opportunitätsentscheid durch die Strafverfolgungsbehörden resp. Anonymitätsversprechen. Der Entscheid, dass die Meldung ausschliesslich über die ANSSI erfolgen darf, dürfte wie in Belgien auch in

93 Siehe Fn. 66.

Frankreich mit einer staatlichen Policy zur Veröffentlichung von Schwachstellen mit Vorbehalt zu Gunsten staatlicher Interessen zusammenhängen.

[127] *Lettland*: In Lettland ist Hacking nach Art. 243 Strafgesetzbuch nur dann strafbar, wenn erheblicher Schaden entstanden ist. Da Hacking in aller Regel keinen Schaden verursacht, ist ethisches Hacking legal. Hingegen wird durch diese Art der Regelung an keinen Meldeprozess angeknüpft. Es ist damit nicht sichergestellt, dass Sicherheitsforschung der Allgemeinheit zugutekommt.

[128] *Litauen*: Seit dem 17. Juni 2021 ist mit Art. 25 des Cybersicherheitsgesetzes ethisches Hacking legalisiert. Das Vorgehen muss notwendig und verhältnismässig sein; die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen darf nur soweit als notwendig tangiert werden. Die Meldung der Schwachstelle hat innert 24h nach Abschluss der Schwachstellensuche an die betroffene Systembetreiberin sowie das nationale CSIRT zu erfolgen und hat der nationalen CVD-Policy zu entsprechen. Das Verwenden von missbräuchlich erlangten Passwörtern z.B. über Social Engineering ist explizit untersagt und lässt die Strafbefreiung entfallen (Art. 25 Ziff. 2 Abs. 6 Cybersicherheitsgesetz). Hält man sich nicht an diese Vorgaben, so ist Hacking nach Art. 198ź Strafgesetzbuch strafbar.

[129] *Niederlande*: Hacking ist in den Niederlanden nach Art. 138ab Strafgesetzbuch verboten. Gestützt auf erstinstanzliche Urteile hat die Generalstaatsanwaltschaft eine Behördenpraxis festgelegt und publiziert.[94] Ethisches Hacking wird nicht bestraft, wenn im Rahmen eines wesentlichen gesellschaftlichen Interesses gehandelt wurde und das Vorgehen verhältnismässig sowie notwendig war. Die Schwachstelle muss der betroffenen Organisation gemeldet werden; eine Frist wurde keine festgelegt.

Land	Grundlage	Frist	Meldestelle
Belgien	Art. 550bis Sw (Hacking) Art. 23 § 1er. NIS2 (Strafbefreiung)	72h	Systembetreiberin + Cyber Security Belgium (CCB)
Deutschland	§ 202c Abs. 1 Ziff. 1 StGB (Hacking) § 202a Abs. 3 StGB (Revisionsvorschlag zur Strafbefreiung)	Keine	Systembetreiberin, Hersteller oder Bundesamt für Sicherheit in der Informationstechnik (BSI)
Frankreich	Art. 323 ff. CP (Hacking) Art. L 2321-4 C. défense (Privilegierung)	Keine	Ausschliesslich: l'Agence nationale de la sécurité des systèmes d'information (ANSSI)
Litauen	Art. 198ź BK (Hacking) Art. 25 Ziff. 1 und 2 Cybersicherheitsgesetz (Strafbefreiung)	24h	Systembetreiberin + National Cyber Security Centre (NKSC)

94 Niederländische Generalstaatsanwaltschaft, Beleidsbrief «Responsible Vulnerability Disclosure» (∞), 14. Dezember 2020 mit Beilage 1 (∞) mit CVD-Broschüre und Beilage 2 (∞) mit Entscheidsammlung.

Land	Grundlage	Frist	Meldestelle
Lettland	Art. 243 KL (Hacking) (Strafbarkeit setzt erheblichen Schaden voraus)	Keine	Keine Vorgabe
Niederlande	Art. 138ab Sr (Hacking) Behördenpraxis (Strafbefreiung)	Keine	Systembetreiberin

Übersicht zur Legalisierung von ethischem Hacking in ausgewählten Ländern

4. Auswirkungen

4.1. Was weiterhin strafbar bleibt

[130] Der Revisionsvorschlag ist so ausgestaltet, dass ethische Hacker *keine* anderen Rechtsgüter tangieren dürfen, ausser den Computerfrieden. Verletzen Hacker andere Rechtsgüter – machen sie sich also unter einem anderen Titel strafbar – hat die Strafbefreiung keine Auswirkung auf diese Taten. Werden andere Rechtsgüter verletzt, können gleichzeitig Zweifel bestehen, ob sich die Handlungen auf eine ethische Gesinnung abstützen. Die Strafbefreiung würde dadurch aufs Spiel gesetzt.

[131] Mutieren die Sicherheitsforscher zu Vandalen und machen Datenbestände durch Löschung, Verschlüsselung etc. unbrauchbar, bleiben sie heute wie auch nach der Revision strafbar. Die Revision ändert nichts an der Tatsache, dass dieses Verhalten nicht toleriert wird. Ebenso wenig würde toleriert, wenn die Sicherheitsforscher die Offenlegung ihres Vorgehens von einem Preisgeld abhängig machen würden (Nötigung Art. 181 StGB und allenfalls Erpressung Art. 156 StGB), wobei die ethische Motivation in solchen Fällen ohnehin bereits verloren gegangen wäre und das Vorgehen nicht mehr straffrei ist. Kopieren die Hacker Datenbestände, so sind sie weiterhin Datendiebe (Datendiebstahl Art. 143 StGB oder unbefugtes Beschaffen von Personendaten nach Art. 179novies StGB).

[132] Die vorgeschlagene Revision hat einen engen Anwendungsbereich und legalisiert ausschliesslich die ethische Sicherheitsforschung im Anwendungsbereich von Art. 143bis Abs. 1 StGB. Folgende Phänomene von Cyberdelinquenz bleiben weiterhin strafbar, die Liste ist nicht abschliessend:

[133] *Social Engineering* ist auch nach der vorgeschlagenen Revision strafbar. Menschen zu Hacken, um Passwörter zu erlangen (z.B. Phishing) und danach in ein System einzudringen, ist weiterhin verboten. Bei diesem Vorgehen wird keine technische Schwachstelle erforscht und es werden keine Allgemeininteressen gefördert.

[134] *Brute Forcing* im Sinne eines (primitiven) Durchprobierens von Zugangsdaten bleibt ebenfalls strafbar, weil hier grundsätzlich keine Sicherheitslücke aufgedeckt, sondern eine Designschwäche ausgenutzt wird. Die Erforschung derartiger Designschwächen ist nicht per se falsch

oder strafbar.[95] Sie setzt hingegen nicht voraus, dass man in ein fremdes System eindringt. Sie lassen sich an einem eigenen Setup analysieren.

[135] *DoS*: Auch sämtlichen Varianten von *Denial of Service* sind nach der vorgeschlagenen Revision nicht zulässig. Wer Systeme durch Angriffe überlastet, hackt nicht im Sinne von Art. 143bis Abs. 1 StGB, deckt auch keine Sicherheitslücke auf und dient nicht der Gesellschaft.

[136] *Datendiebstahl* nach Art. 143 Abs. 1 StGB oder in seiner besonderen Form nach Art. 179novies StGB im Falle von Personendaten bleibt von der Legalisierung ethischen Hackings unberührt. Wer nach einem Hack in redlicher Absicht unerlaubt Daten kopiert, hat zwar in einer ersten Phase nicht das Rechtsgut des Computerfriedens verletzt, aber das ungestörte Verfügungsrecht über Daten. Hinzu kommt, dass dieses Verhalten für ethische Hacker atypisch wäre und sie ihre eigene redliche Absicht torpedieren. Wer als ethischer Hacker unterwegs ist, hat die Daten anderer zu respektieren.

[137] *Datenbeschädigung*: Auch das Löschen resp. Verändern inkl. Unbrauchbarmachen von Daten nach Art. 144bis Abs. 1 StGB bleibt von der vorgeschlagenen Legalisierung unberührt.

[138] *Ransomware Angriffe*: Die Kombination von Hacking nach Art. 143bis Abs. 1 StGB mit Datenbeschädigung (durch Verschlüsselung) und Erpressung nach Art. 156 StGB bleibt nach wie vor verboten. Mit ethischer Sicherheitsforschung hat dieses Tatverhalten nichts zu tun.

[139] *Spionage*, *Geheimnisverletzungen etc.*: Jegliche Form von Spionage ist auch nach der Legalisierung von ethischem Hacking mit Strafe bedroht. Die verschiedenen Formen des verbotenen Nachrichtendiensts nach Art. 272 ff. StGB, die Verletzung des Fabrikations- oder Geschäftsgeheimnisses nach Art. 162 StGB oder im politischen Kontext die Verletzung des Abstimmungs- und Wahlgeheimnisses nach Art. 283 StGB etc. bleiben nach wie vor strafbewehrt. Selbes gilt für die Tatbestände des Nebenstrafrechts wie z.B. die Verwertung fremder Leistung (Art. 5 UWG) oder die Verletzung von Fabrikations- und Geschäftsgeheimnissen (Art. 6 UWG).

4.2. Folgen der Strafbefreiung

[140] Die Schweiz hat jedes Interesse daran, möglichst rasch und konsequent ethisches Hacking auf eine legale Grundlage zu stellen. Ethische Sicherheitsforscherinnen und -forscher werden heute nicht tätig, da ihnen Strafverfolgung droht (Chilling Effect), obschon sie in redlicher Absicht und zum Wohle der Allgemeinheit handeln würden. Anders als kriminelle Hacker, die sich um bestehende Verbote foutieren, zeigen Strafandrohungen bei ethisch handelnden Personen Wirkung. Die Legalisierung von ethischer Sicherheitsforschung führt zu mehr gemeldeten Sicherheitslücken, die von den Kriminellen nicht mehr ausgenutzt werden können und nicht etwa zu mehr Cyberkriminalität.

[141] Ethisches Hacking stärkt die Sicherheit von digitalen Produkten, die heute allgegenwärtig sind und zugleich das Fundament hochentwickelter Herstellungsprozesse darstellen. Ohne digitale Technologie läuft heute nichts mehr. Umso wichtiger ist es, ein rechtliches Umfeld zu schaffen, das Sicherheit bietet. Legalisiert die Schweiz ethisches Hacking, bewirkt sie gleichzei-

95 Man denke an die anfällige Implementation der Registrar PIN-Funktion von Wifi Protected Setup (WPS), wo im Jahr 2011 mit geschickter Analyse von Stefan Viehböck die Anzahl notwendiger Versuche für eine Exhaustiv Search von 100 Mio. auf lediglich noch 1'000 PINs reduziert werden konnte. Die Angriffszeit reduzierte sich von mehreren Jahren auf durchschnittlich wenige Stunden. Mit diesem PIN erhielt der Angreifer dann den WLAN-Schlüssel. Vgl. reaver wps (∞) auf Google Code.

tig, dass der Schweizer Forschungs- und Produktionsstandort nicht nur konkurrenzfähig bleibt, sondern im internationalen Vergleich zu den Vorreitern gehört. Ein rechtssicherer Rahmen für die Sicherheitsforschung stärkt letztlich die digitale Infrastruktur und die digitale Souveränität der Schweiz.

[142] Die vorgeschlagene Revision legalisiert ethisches Hacking ähnlich wie das belgische und litauische Recht auf Stufe Gesetz. Deutschland wird in naher Zukunft ebenfalls die Legalisierung umsetzen. Rechtsstaatliche und demokratiepolitische Schwierigkeiten, wie sie beim französischen und niederländischen Modell bestehen, werden mit dem vorgeschlagenen Wortlaut verhindert und eng den Schweizer Gepflogenheiten gefolgt. Die Zeit ist reif, dass die Schweiz das Hackingstrafrecht weiterentwickelt und zukunftsfest gestaltet. Der vorgeschlagene Abs. 3 für Art. 143^{bis} StGB ist eine valable Möglichkeit dazu.

Roman Kost, Rechtsanwalt, MLaw, BSc in Information & Cyber Security, Luzern.