Bundesministerium
der Justiz

14. September 2023

Ergebnisprotokoll des 1. Symposiums zum Thema: „Besteht Reformbedarf im Computerstrafrecht?“ am 30. Juni 2013 (9.00 bis 13.00 Uhr) im Bundesministerium der Justiz

I. Begrüßung

Herr Dr. Böhm, Abteilungsleiter der Abteilung II – Strafrecht – im Bundesministerium der Justiz betonte in seinen Begrüßungsworten, dass ein Meinungsaustausch von Expertinnen und Experten unterschiedlicher Fachrichtungen besonders wichtig sei, da die Digitalisierung in allen Bereichen voranschreite und es zu immer neuen Kriminalitätsphänomenen käme. Ob diese auch die Schaffung neuer Straftatbestände erfordere, müsse fortlaufend geprüft werden.

II. Eingangsstatements und Diskussion

1. Themen der Eingangsstatements

„Ist das Computerstrafrecht grundsätzlich ein geeignetes Instrument zum Schutz kritischer Infrastrukturen?“
Vortragend: Herr Prof. Dr. Brodowski, Universität des Saarlandes

„Vom Computer- zum Internetstrafrecht? Bedarf es einer Neustrukturierung?“
Vortragend: Herr Prof. Dr. Hilgendorf, Universität Würzburg

„Werden die Tatbestände des Computerstrafrechts den gegenwärtigen Erscheinungsformen der Internet- und Computerkriminalität gerecht? Kann strafbares Verhalten ausreichend geahndet werden? Gibt es Bedarf zur Entkriminalisierung oder für neue Straftatbestände?“
Vortragend: Frau Oberstaatsanwältin Komp, Generalstaatsanwaltschaft Köln und
Frau Rechtsanwältin Nadeborn, Berlin

„Neue Erscheinungsformen von Computerkriminalität –"Identitätsdiebstahl", Deepfakes, Doxing und Co. Sollte § 42 BDSG in das Kernstrafrecht überführt werden?“
Vortragend: Frau Prof. Dr. Schiemann, Universität zu Köln

2. Diskussion

Es bestand Konsens bei den Expertinnen und Experten und den wortnehmenden Diskussionsteilnehmerinnen und -teilnehmern darüber, dass es keiner grundlegenden Neustrukturierung der Computerstraftaten i. e. S. bedarf.

Trotz neuer Kriminalitätsphänomene lägen keine relevanten Strafbarkeitslücken bei Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit informationstechnischer Systeme vor, u. a. aufgrund allgemein gefasster, technik-neutraler Regelungen, der Existenz flankierender Vorbereitungsdelikte und der Überlappung mit weiteren Straftatbeständen (etwa Betrug bei „Identitätsdiebstahl“). Neue Formen sozialschädlichen Verhaltens durch die fortschreitende Digitalisierung und das Internet müssten nicht immer auch die Schaffung neuer Straftatbestände zur Folge haben.

Strafrecht sei und müsse „ultima ratio“ bleiben. „Restrisiken“, d. h. kleinere Strafbarkeitslücken, müssten akzeptiert werden. Wichtiger sei in diesem Zusammenhang, die Medienkompetenz der Nutzenden zu stärken und die Sicherheitsarchitekturen der Systeme zu verbessern.

Vereinzelte Anpassungen seien aber denkbar, etwa die Einfügung einer Legaldefinition der „Überwindung der Zugangssicherung“.

Einer Strafbarkeit eines sog. „digitalen Hausfriedensbruchs“ bedürfe es nach überwiegender Meinung nicht. § 202a StGB sei bereits ein weitreichender Tatbestand, der hohen Schutz entfalte.

Die Frage, ob man Hersteller oder Betreiber strafrechtlich haftbar machen solle, wenn Computersysteme nicht ausreichend sicher seien, da nicht von jeder Bürgerin/jedem Bürger erwartet werden könne, dass sie/er den Sicherheitsvorkehrungen ausreichend nachkäme bzw. nachkommen könne, wurde diskutiert und weitgehend als zu weitreichender Eingriff kritisiert.

Eine mögliche Überführung des § 42 BDSG in das Kernstrafrecht wurde kontrovers diskutiert und Probleme in diesem Zusammenhang aufgezeigt. Eine Überführung erhöhe die Sichtbarkeit dieser Regelung, die ein „Schattendasein“ führe. Ob eine Überführung einen Mehrwert für die Strafbarkeit anderer, „neuer“ Kriminalitätsphänomene habe, wurde aber in Frage gestellt, da für den Tatbestand des § 42 BDSG eine wissentliche und gewerbsmäßige Handlung erforderlich sei, § 42 BDSG im Gegensatz zu § 202a StGB nur nicht allgemein zugängliche Daten erfasse, es sich um ein absolutes Antragsdelikt handele und Änderungen des Antragserfordernisses zu Überlastungen der Ermittlungsbehörden führen könnten.

Integritätsverletzungen im Zusammenhang mit sog. „Innentätern“ (wenn ein Passwort durch einen Berechtigten zu einer Straftat genutzt werde) seien ebenfalls ausreichend geschützt - zumindest solange die höchstrichterliche Rechtsprechung § 202a StGB so extensiv auslege wie bisher. Dagegen wurde angeführt, dass eine extensive Auslegung von Straftatbeständen zu Rechtsunsicherheiten führe. Wann ein „nicht unerhebliches Überwinden der Sicherheitsvorkehrung“ im Sinne des § 202a StGB vorliege, werde in der Rechtsprechung unterschiedlich

behandelt. Lösungsmöglichkeit könne eine Definition sein, wann ein „nicht unerheblicher Aufwand“ zur Überwindung der Zugangssicherung vorliege. Bagatellfälle müssten weiterhin ausgeschlossen sein. Auch die Frage des „Dateneigentums“ sei rechtlich nicht ausreichend geklärt.

Den Schutz kritischer Infrastrukturen (KRITIS) sahen die Vortragenden ausreichend durch das Strafrecht geschützt, insbesondere da auch hier bei Angriffen in der Regel neben den Computerdelikten im engeren Sinne weitere Straftatbestände verwirklicht würden, etwa bei Ransomware-Attacken der Straftatbestand der Erpressung gemäß § 253 StGB. Der Ansicht, höhere Strafrahmen zur Abschreckung von Angriffen auf KRITIS seien weder erforderlich, noch sei insoweit ein Mehrwert zu erwarten, stand die Meinung entgegen, der Straftatbestand des § 303b StGB (Computersabotage) decke den Schutz kritischer Infrastrukturen nicht ausreichend ab. Es sei insbesondere eine Strafrahmenerhöhung bei Angriffen auf KRITIS erforderlich, nicht aus präventiven Gründen, sondern vielmehr um die gesellschaftlichen Gefahren und den erhöhten Unrechtsgehalt wiederzugeben, der Angriffen auf KRITIS immanent sei.

Eine Erhöhung der Strafrahmen der §§ 202a ff. StGB wurde lediglich im Zusammenhang mit der Strafverfolgung als ggf. erforderlich angesehen, um die Anwendung des § 100a StPO zu ermöglichen, damit Ermittlungen ausgeweitet werden könnten. Hiergegen wurde vorgebracht, dies sei unverhältnismäßig, da die Aufnahme in den Katalog des § 100a StPO ein höheres Unrecht voraussetze, das nicht einfach durch Verschiebung des Strafrahmens geschaffen werden könne.

Die Frage, ob der IT-Sicherheitsbranche Straffreiheit gewährt werden müsse, wurde kontrovers diskutiert. Schwierigkeiten bei der Abgrenzung white/grey/black-hat-Hacker wurden dargelegt. Die Meinungen, dass das Hacking in allen Formen weiterhin grundsätzlich strafbewehrt bleiben müsse und entgegengesetzt dazu, dass die IT-Sicherheitsbranche nicht der Gefahr ausgesetzt sein dürfe, sich strafbar zu machen, standen sich kontrovers gegenüber. Verschiedene Lösungsmöglichkeiten wurden angesprochen, etwa die Schaffung eines Ausschlusstatbestandes in § 202a StGB.

Strafbarkeitsrisiken wurden auch im Zusammenhang mit Ransomware-Opfern diskutiert, die das geforderte Lösegeld zahlten, sich damit aber unter Umständen nach § 129 Satz 2 StGB strafbar machten, da sich die Zahlungen unschwer unter „Unterstützungen“ subsumieren ließen. Es bestünde zwar die Möglichkeit, den Straftatbestand in diesen Fällen teleologisch zu reduzieren, hier sprach man sich aber für mehr Rechtssicherheit durch angepasste Gesetzgebung aus, um nicht die Opfer zu kriminalisieren.

III. Nächstes Symosium

Die Diskussion soll im nächsten Symposium fortgesetzt werden, das am 4. Oktober 2023 stattfinden soll. Schwerpunktthema soll u. a. der Schutz der IT-Sicherheitsforschung im Zusammenhang mit Datenschutz, Urheberrecht und Geschäftsgeheimnisgesetz sein.