Kurzinformation
Cyberkriminalität

1. Definition und Aktualität

Der Begriff der Cyberkriminalität (Cybercrime) umfasst nach einer verbreiteten, auch vom Bundeskriminalamt (BKA) verwendeten Definition im Kern diejenigen Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne, vgl. BKA, Bundeslagebild Cybercrime 2016, S. 2 [abrufbar unter https://www.bka.de]). Generell ist im Bereich der Cyberkriminalität eine starke Zunahme von Straftaten zu verzeichnen. So stieg die Zahl der in Deutschland als Cybercrime im engeren Sinne erfassten Straftaten 2016 gegenüber dem Vorjahr um 80,5 % auf 82.649 Straftaten; die Aufklärungsquote lag bei 38,7 % (Bundeslagebild Cybercrime 2016, S. 5).

2. Geltendes deutsches Strafrecht

Im deutschen Strafrecht existiert eine Vielzahl von Straftatbeständen, die Erscheinungsformen der Cyberkriminalität pönalisieren (vgl. hierzu Lampe/Hegmann, in: Münchener Kommentar zum StGB, 3. Auflage 2017, Vorbemerkung zu § 93 Rn. 30). In der Praxis sind vor allem relevant:

- § 202a StGB – Ausspähen von Daten. Hiernach macht sich strafbar, wer „unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft".

- § 202b StGB – Abfangen von Daten. Strafbar macht sich, wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft.

- Fälschung beweiserheblicher Daten sowie Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB). Erfasst wird hier die Täuschung einer Person durch die Fälschung von Daten. Durch einen Dateninhaber werden Daten gefälscht bzw. verfälscht und zur Täuschung im Rechtsverkehr genutzt. Dies kann etwa durch die Zusendung von E-Mails unter Vorspiegelung realer Identitäten erfolgen. Das Opfer soll so zur Preisgabe von relevanten Daten veranlasst werden.

WD 7 - 3000 - 167/18 (6. August 2018)

– § 303a StGB – Datenveränderung – stellt das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten unter Strafe. Die Tathandlungen werden anschaulich auch als „elektronische Sachbeschädigung“ bezeichnet. Der Straftatbestand der Computersabotage (§ 303b StGB) schützt anknüpfend an § 303a StGB vor allem die Datenverarbeitung selbst. Die Tatvariante des § 303b Absatz 1 Nr. 2 StGB, die einschlägig ist, wenn eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich gestört wird, dass Daten in der Absicht, einem anderen Nachteil zuzufügen, eingegeben oder übermittelt werden, erfasst regelmäßig auch die weit verbreiteten Denial of Service-Angriffe (DoS-/DDoS-Angriffe) sowie die Verbreitung und Verwendung von Schadsoftware unterschiedlicher Art, etwa in Gestalt sogenannter Trojaner, Viren, Würmer usw. (vgl. Bär, DRiZ 2015, 432).

Verletzte Rechtsgüter sind bei diesen Tatbeständen „in erster Linie private Interessen an einer nicht abgehörten Kommunikation, aber auch das öffentliche Interesse an der vertraulichen Übermittlung von Nachrichten. Die Dimension von globaler, massenhafter Datenausspähung, die den persönlichen Informations- und Geheimnisbereich praktisch schutzlos erscheinen lassen, kann die Staatsschutzqualität solcher Operationen begründen“ (Lampe/Hegmann a.a.O.).

3. Aktuelle Reformvorhaben auf nationaler Ebene

Nach Ansicht der deutschen Bundesländer weisen die oben genannten Strafvorschriften Schutzlücken auf: So würden derzeit nur Daten geschützt, nicht aber IT-Systeme selbst, und gegen die massenhaften unbemerkten Infiltrationen durch Botnetze und Schadsoftware, DDos-Attacken und das Ausspähen von Daten durch international agierende Cyber-Kriminelle könnten sich selbst aufmerksamste Nutzer nicht wehren. Der Bundesrat hat daher am 2. März 2018 einen Gesetzentwurf zur wirksameren Bekämpfung von Cyberkriminalität verabschiedet, mit dem er Computer und IT-Systeme besser vor Hackerangriffen und unbefugter Benutzung schützen möchte (BT-Drs. 19/1716). Der Entwurf sieht einen neuen Straftatbestand § 202e StGB – „Unbefugte Benutzung informationstechnischer Systeme“ – vor, der den unerlaubten Zugriff auf informationstechnische Systeme mit einem Freiheitsentzug von bis zu zehn Jahren unter Strafe stellen soll. Der Gesetzentwurf wurde dem Bundestag zugeleitet.

* * *