Секция «44.2 Актуальные вопросы права немецкоязычных стран (на немецком языке)»

Strafrechtliche Verantwortlichkeit für DDos-Angriffe und Botnetze gemäß dem deutschen Strafgesetzbuch

Научный руководитель – Маджумаев Мурад Мамедович

Шамарокова Екатерина Алексеевна

Студент (бакалавр)

Российский университет дружбы народов имени Патриса Лумумбы, Юридический факультет, Москва, Россия

E-mail: k.shamarokova@yandex.ru

Das Wachstum digitaler Technologien und die Verbreitung von Informationssystemen haben zu einem Anstieg der Cyberkriminalität geführt, einschließlich DDoS-Angriffen und der Nutzung von Botnetzen, die darauf abzielen, den Betrieb von Systemen zu stören und wirtschaftlichen Schaden zu verursachen. In Deutschland sind die grundlegenden Bestimmungen der strafrechtlichen Verantwortlichkeit für solche Handlungen im Strafgesetzbuch verankert. Für die rechtliche Qualifizierung von DDoS-Angriffen und Botnetzen sind insbesondere die §§ 202a, 202b, 303a und 303b StGB von Bedeutung, die die Verantwortlichkeit für unbefugten Zugang, das Abfangen von Daten, Datenmanipulation sowie Computersabotage festlegen [1].

Ein DDoS-Angriff (Distributed Denial of Service) ist ein Cyberangriff, der die Funktionsfähigkeit eines Informationssystems durch massenhafte Anfragen stört, wodurch das System überlastet wird und für Nutzer nicht mehr erreichbar ist [2]. Solche Angriffe werden häufig mithilfe von Botnetzen durchgeführt – Netzwerken infizierter Geräte (PCs, Server, Smartphones oder IoT-Geräte), die von einem Angreifer gesteuert werden [3]. Der Einsatz von Botnetzen ermöglicht die Koordination einer großen Anzahl von Geräten und erhöht dadurch die Angriffskraft erheblich.

Eine der zentralen strafrechtlichen Normen Deutschlands im Bereich des Schutzes der Informations ist § 202a StGB, der die Strafbarkeit des unbefugten Zugangs zu Daten (Ausspähen von Daten) regelt.

§ 202a StGB stellt den unbefugten Zugang zu Daten unter Strafe, wenn diese durch besondere Sicherungsmaßnahmen geschützt sind und der Täter diese Schutzvorrichtungen überwindet [1]. Zu solchen Handlungen gehören beispielsweise das Umgehen von Authentifizierungssystemen, der Einsatz von Schadsoftware oder das Knacken von Passwörtern. Die Strafandrohung für diese Tat beträgt Freiheitsstrafe bis zu drei Jahren oder Geldstrafe [1].

§ 202b StGB sieht eine Strafbarkeit für das unbefugte Abfangen von Daten aus nicht öffentlich zugänglichen Systemen oder mittels elektromagnetischer Ausstrahlung vor [4]. Dazu zählen etwa das Abfangen von Netzwerkverkehr, der Einsatz von Programmen zur Paket-Analyse oder die Installation von Schadsoftware zum verdeckten Erlangen von Informationen.

Die Sanktion für dieses Delikt beträgt Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe [4].

Von großer Bedeutung für die Bekämpfung der Cyberkriminalität ist ferner § 303a StGB, der die Strafbarkeit der Datenveränderung regelt.

Nach dieser Vorschrift sind Handlungen strafbar, die darauf gerichtet sind, Daten unbefugt zu löschen, zu verändern, zu unterdrücken oder unbrauchbar zu machen [1]. Unter Daten versteht man in diesem Zusammenhang Informationen, die elektronisch gespeichert oder übertragen und von Computersystemen verarbeitet werden.

Die objektive Tatseite des Delikts besteht in einem unbefugten Eingriff in die Struktur oder den Inhalt von Daten, der zu deren Beschädigung oder Verlust führt. Im Kontext von DDoS-Angriffen kann diese Norm Anwendung finden, wenn eine Überlastung des Systems zu einer Beschädigung oder zum Verlust von Daten führt, etwa bei einem Ausfall von Datenbanken oder bei Störungen im Serverbetrieb [5].

Die Strafandrohung für diese Tat beträgt Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Für die rechtliche Einordnung von DDoS-Angriffen ist insbesondere § 303b StGB maßgeblich, der die Strafbarkeit der Computersabotage festlegt.

Nach § 303b StGB sind Handlungen strafbar, die die Datenverarbeitung erheblich stören oder die Funktionsfähigkeit eines Informationssystems beeinträchtigen [1].

Die objektive Tatseite äußert sich in der Zerstörung oder Beschädigung von Daten, in Eingriffen in deren Verarbeitung, im Blockieren von Computersystemen sowie in der Schaffung von Hindernissen für das ordnungsgemäße Funktionieren der informationstechnischen Infrastruktur. DDoS-Angriffe stellen ein typisches Beispiel für Computersabotage dar, da die Koordination einer großen Anzahl infizierter Geräte eine erhebliche Belastung für den Zielserver erzeugt, den Systembetrieb stört und das Ausmaß des Angriffs deutlich erhöht. Dies kann zur vorübergehenden Nichtverfügbarkeit von Diensten sowie zu wirtschaftlichen Verlusten führen.

Der Grundtatbestand sieht eine Freiheitsstrafe bis zu drei Jahren oder Geldstrafe vor. Im Falle eines erheblichen Schadens oder eines Angriffs auf kritische Infrastrukturen kann die Strafe bis zu zehn Jahre Freiheitsstrafe betragen [1].

Die durchgeführte Analyse der Vorschriften des deutschen Strafgesetzbuches zeigt, dass in Deutschland ein umfassendes und logisch aufgebautes System zur Bekämpfung der Cyberkriminalität geschaffen wurde. Der Gesetzgeber unterscheidet klar zwischen verschiedenen Angriffen auf die Informationssicherheit: Während die §§ 202a und 202b StGB auf den Schutz der Vertraulichkeit und Geheimhaltung von Daten abzielen, gewährleisten die §§ 303a und 303b deren Integrität und Verfügbarkeit.

Eine besondere Rolle nimmt dabei die Einordnung von DDoS-Angriffen als Computersabotage gemäß § 303b StGB ein. Dieser Ansatz erkennt an, dass moderne Cyberangriffe nicht lediglich technische Zwischenfälle darstellen, sondern ernsthafte Eingriffe in die Funktionsfähigkeit gesellschaftl bedeutsamer Infrastrukturen sind. Die Festlegung strenger Sanktionen – bis zu zehn Jahren Freiheitsstrafe in qualifizierten Fällen – spiegelt das Bestreben Deutschlands wider, ein hohes Maß an digitaler Souveränität zu gewährleisten und wirtschaftliche Interessen im Zeitalter der umfassenden Digitalisierung zu schützen. Somit passt sich das deutsche Strafrecht fortlaufend der Entwicklung von Botnetzen an und bietet wirksame Mechanismen sowohl zur Bekämpfung des unbefugten Zugangs zu Informationen als auch zum Schutz der Funktionsfähigkeit globaler Informationssysteme.

Источники и литература

1 German Criminal Code (Strafgesetzbuch – StGB)

2 Bundesamt für Sicherheit in der Informationstechnik (BSI). The State of IT Security in Germany 2024

3 Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023

4 UNODC SHERLOC. German Criminal Code — Section 202a, 202b, 303a–303b (cybercrime provisions)

5 Bundeskriminalamt (BKA). Bundeslagebild Cybercrime 2024