

Strafbarkeit des Einforderns von Geld zur Vermeidung weiterer DDoS-Attacken als (versuchte) Erpressung, Strafbarkeit von DDoS-Attacken in Tateinheit hierzu wegen Computersabotage

Gericht

LG Düsseldorf

Datum

22.03.2011

Aktenzeichen

3 KLS 1/11

Branche/ Lebenslage

Erpressung, DDoS-Attacke, Distributed Denial-of-Service-Attacke, Hackerangriff, Computersabotage, Geldforderung, § 253 StGB, § 303b StGB

Akteure

Täter, Opfer

Wer haftet?

Täter

Haftungsart

Freiheitsstrafe oder Geldstrafe

Haftungsumfang

Hier: Gesamtfreiheitsstrafe von zwei Jahren und zehn Monaten

Haftungsbegründendes Verhalten

Erfüllung der Straftatbestände der gewerbsmäßigen Erpressung in Tateinheit mit Computersabotage und der versuchten gewerbsmäßigen Erpressung

Technische Umstände

Herbeiführung der Überlastung eines EDV-Systems mittels eines Bot-Netztes

Persönliche Umstände

Vorsätzliche Begehung einer Straftat

Möglichkeiten der Haftungsvermeidung

-

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Der Angeklagte beabsichtigte, mittels eines sog. Bot-Netztes die Internetseiten einzelner Pferdewetten-Anbieter zu überlasten, falls diese nicht auf eine zuvor geäußerte und mit einer entsprechenden Drohung verbundenen Zahlungsaufforderung reagierten.

Zur Untermauerung seiner Drohung griff er die [Server](#) eines Unternehmens mit seinem Bot-Netz an, das unter der Last zeitweise außer Betrieb ging. Um weiteren Umsatzausfällen zu entgehen, kam das Unternehmen der Geld-Forderung des Angeklagten nach.

Gegenüber weiteren Pferdewetten-Anbietern ging der Angeklagte in der gleichen Weise vor. Nicht alle der attackierten Unternehmen kamen seiner Forderung nach.

Das Landgericht begründete die Strafbarkeit des Angeklagten wie folgt:

Sogenannte DDos-Attacken auf die Server von Internetfirmen über ein Bot-Netz erfüllen den Tatbestand der (gewerbsmäßigen) Computersabotage gem. § 303b Abs. 1 Nr. 2, Abs. 2 StGB (juris Rn. 62).

Sofern gleichzeitig die jeweiligen Unternehmen von dem Täter aufgefordert werden, Zahlungen zur Vermeidung der Attacken an ihn zu leisten, liegt eine tateinheitlich begangene (gewerbsmäßige) Erpressung gem. § 253 Abs. 1, Abs. 4 S. 2 1. Alt. StGB vor (juris Rn. 58).

ANMERKUNGEN

Bei einem sog. „Denial-of-Service“ werden fremde IT-Systeme gezielten überlastet, die dann die vom Betreiber gewünschten Funktionen jedenfalls vorübergehend nicht mehr erfüllen können und so die Bearbeitung aller Anfragen verweigern. Wird diese Überlastung dadurch herbeigeführt, dass von einer Vielzahl fremder Systeme koordiniert massenhaft Anfragen auf IT-Systeme eingehen, so spricht man von einem „Distributed Denial-of-Service“ (vgl. eingehend Popp, jurisPR-ITR 25/2011 Anm. 6). Im vorliegenden Fall wurde die DDos-Attacke mittels eines sog. Bot-Netztes herbeigeführt. Dabei übernimmt der Täter durch einen Trojaner zumindest teilweise die Kontrolle über fremde Rechner und missbraucht diese dazu, die erwähnten massenhaft koordinierten Anfragen auf das anvisierte System durchzuführen.

Solche DDos-Attacken unterfallen dem Straftatbestand der Computersabotage gem. § 303b Abs. 1 Nr. 2 StGB. Damit verknüpfte Erpressungen bzw. Erpressungsversuche begründen eine Strafbarkeit nach § 253 StGB.

Darüber hinaus gilt es darauf hinzuweisen, dass der Tatbestand der Computersabotage (§ 303b StGB) eine „erhebliche“ Störung der betroffenen Datenverarbeitung, also eine Beeinträchtigung des reibungslosen Systemablaufs von einigem Gewicht, voraussetzt. Zu den Kriterien, nach denen sich die Erheblichkeit bemisst, zählen dabei insbesondere der Aufwand an Zeit, Kosten und Mühen, der für die Beseitigung der Störung notwendig ist (Popp, jurisPR-ITR 25/2011 Anm. 6).