Strafbarkeit des Phishings als Computerbetrug

Gericht

LG Bonn

Datum

07.07.2009

Aktenzeichen

7 KLs 1/09

Branche/ Lebenslage

Phishing, Computerbetrug § 263a StGB, Schadprogramme

Akteure

Angeklagter, Mittäter, Ermittlungsbehörde

Wer haftet?

Angeklagter

Haftungsart

Gewerbs- und bandenmäßig begangener Computerbetrug (§§ 263a Abs. 1, Abs. 2, 263 Abs. 5 StGB)

Haftungsumfang

4 Jahre Freiheitsstrafe

Haftungsbegründendes Verhalten

Tatherrschaft im Rahmen einer bandenmäßig begangenen Durchführung mehrerer Phishing-Attacken und daraufhin folgender Geldtransaktion zu Lasten der angegriffenen Konteninhaber

Technische Umstände

Infizierung von fremden Computern mit einer Schadsoftware ermöglicht das technische Aufzeichnen der Eingabe von Autorisierungsdaten im Online-Banking

Persönliche Umstände

Der Angeklagte handelte vorsätzlich, insbesondere auch hinsichtlich der Verursachung eines Vermögensschadens bei den betroffenen Kontoinhabern

Möglichkeiten der Haftungsvermeidung

–

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Der Angeklagte war im Rahmen von Phishing-Attacken für den Betrieb und die Weiterentwicklung des Systems der tatbegehenden Gruppe zuständig. Bei einer Phishing-Attacke gelangen die Angreifer durch die Zwischenschaltung zwischen die Kommunikation von Bankkunden und Bank (etwa über die Verlinkung zu gefälschten Webseiten, z.B. über den Link in einer E-Mail) an Daten des Bankkunden, um dessen Konto unbefugt zu belasten. Der Angeklagte überwachte und verwaltete insbesondere die Verzeichnisse über die eingesetzten.

Darüber hinaus pflegte er das eingesetzte Botnetzwerk der Gruppe. Ab einem späteren Zeitpunkt war der Angeklagte auch in die Koordination der technischen Weiterentwicklung der eingesetzten Schadprogramme involviert.

Der Angeklagte wurde vom Gericht wegen gewerbs- und bandenmäßig begangen Computerbetrugs (§§ 263a Abs. 1, Abs. 2, 263 Abs. 5 StGB) verurteilt. Mit der Vornahme von Überweisungen unter Verwendung der abgegriffenen Autorisierungsdaten, sei der Computerbetrug begangen worden:

> *Da das Merkmal der Unbefugtheit nach herrschender Auffassung in Anlehnung an § StGB § 263 StGB „betrugsspezifisch“ auszulegen ist, ist die Verwendung von Daten dann als unbefugt anzusehen, wenn sie gegenüber einer natürlichen Person Täuschungscharakter hätte. Das ist unter der Voraussetzung gegeben, dass die Befugnis des Täters zur Inanspruchnahme der Computerleistung zur Geschäftsgrundlage gehört, so dass sie auch beim Schweigen der Beteiligten als selbstverständlich vorausgesetzt werden kann. Dies ist insbesondere auch bei der Eingabe vertraulicher Zugangs- und Transaktionsdaten (PIN und TAN) im Rahmen des Onlinebankings der Fall, wenn die Legitimationsdaten durch Phishing erlangt wurden.*

Hierbei befand das Gericht, dass der Täter sich sowohl hinsichtlich selbst getätigter Überweisungen mit den abgegriffenen Daten, als auch hinsichtlich der Überweisungen durch andere Personen der Gruppe strafbar gemacht hatte, weil ihm auch diese Handlungen zuzurechnen waren:

> *Die Tatbeiträge des Angeklagten waren so wesentlich, dass ohne sie die Taten nicht durchführbar gewesen wären. Ohne seine Koordinierung im Bereich der Trojanerentwicklung und der Koordinierung der Spam-Attacken, also der Verteilung der Schadsoftware, wäre es gar nicht erst zur Infizierung der Rechner der Geschädigten gekommen.*

ANMERKUNGEN

Das Gericht setzte sich mit den Fragen auseinander, ob und ab wann bei Phishing-Attacken und daraufhin folgender Vornahme von unbefugten Überweisungen ein Computerbetrug im Sinne des § 263a StGB vorliegt. Außerdem benannte es Kriterien für die Annahme mittäterschaftlichen und bandenmäßigen Handelns.