Strafbarkeit des Verwendens mittels Phishing erlangter Kontonummern, PINs und TANs (z.B. in Form der Eingabe in den Computer zum Zwecke der unberechtigten Vornahme von Überweisungen) wegen versuchten Computerbetrugs

Gericht

KG Berlin

Datum

02.05.2012

Aktenzeichen

(3) 121 Ss 40/12 (26/12)

Branche/ Lebenslage

Phishing,PIN,Kontonummer,TAN,versuchter Computerbetrug,§ 263a StGB,Phishing-Attacke,unautorisierte Überweisung

Akteure

Täter, Opfer

Wer haftet?

Grundsätzlich Täter, vorliegend jedoch kein versuchter Computerbetrug

Haftungsart

Freiheitsstrafe oder Geldstrafe

Haftungsumfang

Freiheitsstrafe bis zu fünf Jahre

Haftungsbegründendes Verhalten

Versuch eines Computerbetrugs, hier (-)

Technische Umstände

Versuch der Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf

Persönliche Umstände

Vorsätzliches, rechtswidrige und schuldhafte Begehung eines Straftat

Möglichkeiten der Haftungsvermeidung

–

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Der Täter hatte mittels sog. Phishing von anderen Personen Kontonummern, PINs und TANs erlangt.

Bei dem sog. Phishing handelt es sich um den Versuch, vertrauliche Daten von Internetnutzern zu entwenden. Hierzu werden eine Vielzahl gefälschter Emails versandt, die den Empfänger auf manipulierte Webseiten locken, damit dieser dort vertrauliche Passwörter offenbart (vgl. m. w. N. Weidemann, in: BeckOK StGB, 37. Edition Stand: 01.02.2018, Lexikon des Strafrechts, Computerkriminalität, B. Einzelne Erscheinungsformen, VII. Phishing Rn. 9-9-1).

Fraglich war nun, in welchem Moment der Täter durch die Benutzung der erlangten Daten zur Verwirklichung eines Computerbetrugs (§ 263a StGB) unmittelbar ansetzt (§ 22 StGB) und die Straftat somit versucht. Des Computerbetrugs macht sich strafbar, wer das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, Verwendung unrichtiger oder unvollständiger Daten, unbefugte Verwendung von Daten oder sonst unbefugte Einwirkung auf den Ablauf beeinflusst, um sich oder einem Dritten auf Kosten eines anderen einen rechtwidrigen Vermögensvorteil zu verschaffen. Ein Versuch zur Tat liegt erst dann vor, wenn zur Tatbestandverwirklichung unmittelbar angesetzt wird.

Das KG Berlin traf hierzu folgende Feststellungen:

> *Hat ein Täter widerrechtlich Konto-, Identifikations- und Transaktionsnummern sowie Zugangscodes von anderen Benutzern des Internets mittels Phishing erlangt, liegt ein Ansetzen zur Verwirklichung des Straftatbestands des Computerbetrugs im Sinne des § 22 StGB erst dann vor, wenn er diese Daten verwendet, indem er sie beispielsweise in den Computer eingibt, um so eine von dem tatsächlich Berechtigten nicht autorisierte Überweisung zu tätigen. Die Einrichtung von Zielkonten, eine fingierte polizeiliche Anmeldung und das Abfangen von Kontounterlagen können dagegen zwar auf einer Täuschungshandlung beruhen, stellen jedoch noch keinen versuchten Computerbetrug dar (juris Rn.4, Leitsatz).*

ANMERKUNGEN

Das KG Berlin konkretisiert mit der vorliegenden Entscheidung, ab welchem Zeitpunkt bzw. durch welche Handlungen im Falle des Verwendens mittels Phishing erbeuteter Daten ein unmittelbares Ansetzen zur Begehung eines Computerbetrugs anzunehmen ist.