Lebenslauf

Johannes Burr

Geboren am 26. März 1980 in Bonn. 1996/1997 AFS-student an der Whitehouse High School, U.S.A. 1999 Abitur am Konrad-Adenauer-Gymnasium Meckenheim. Anschließend Wehrdienst beim PzBtl. 214 in Augustdorf. 2000 bis 2005 Studium der Rechtswissenschaften an der Rheinischen Friedrich-Wilhelms-Universität Bonn. 2005 Erstes Juristisches Staatsexamen. Seit 2006 Promotion bei Prof. Dr. Martin Böse.

Promotionsvorhaben

Die strafrechtliche Bewertung von Identitätsdiebstahl im Internet mittels Phishing und Pharming

Der alte Lehrbuchfall vom angeblichen Gasmann, der die Gutgläubigkeit und Sorglosigkeit von Privatpersonen missbraucht und sich durch Täuschung Zutritt zu einer Wohnung erschwindelt, um dort vermögensschädigende Straftaten begehen zu können, hat inzwischen eine moderne Variante erhalten. Eine neue Facette herkömmlicher Trickdiebstähle und Trickbetrügereien trägt im Zeitalter des Internets den Namen „Phishing" und hat in den zurückliegenden Monaten in rasanter Geschwindigkeit die Aufmerksamkeit der Öffentlichkeit erfahren. Keinesfalls verwunderlich. Umfragen zufolge war in Deutschland bereits jeder zweite Internetnutzer Adressat einer Phishing-Mail. Weltweit wurden im zweiten Halbjahr 2005 anderthalb Milliarden Phishing-Versuche registriert, im Schnitt annähernd 8 Millionen pro Tag.
Hinter dem Kunstwort Phishing, dessen Etymologie noch umstritten ist, verbirgt sich eine moderne Form des Trickbetruges, bei dem der Täter den Versuch unternimmt persönliche Zugangsdaten des Opfers auszuspionieren, um diese anschließend für einen finanziellen Missbrauch zu verwenden. Schätzungen zufolge verursacht Phishing weltweit jährlich Schäden in Milliardenhöhe, wobei die Tendenz steigend ist. Phishing avanciert inzwischen zu einem hochorganisierten Betätigungsfeld der internationalen Kriminalität.
Dabei vollzieht sich der klassische Phishingangriff in drei Schritten:
Zunächst werden potentielle Opfer durch den massenhaften Versand von offiziell wirkenden, tatsächlich jedoch gefälschten E-Mails mittels eines trügerischen Links zu einer gefälschten, aber täuschend echt aussehenden Website gelockt. Diese scheinbar bekannte und vertrauenswürdige, in Wahrheit jedoch lediglich der Originalseite ähnelnde Webpage soll dem Opfer suggerieren, er kommuniziere mit dem ihm bekannten und von ihm ausgewählten Internetanbieter (z.B. einem Geldinstitut, Onlineauktionshaus u.ä.), und soll ihn zur gutgläubigen Preisgabe sensibler und vertraulicher Zugangsdaten verleiten.
Daran anknüpfend kann der Täter die erlangten Zugangsdaten verwenden und beispielsweise mittels erbeuteter PIN- und TAN - Nummern unter Ausschöpfung des Transaktionslimits eine Überweisung vornehmen, die auf ein inländisches Konto eines oft ahnungslosen Mittelsmannes erfolgt.
In dem dritten und letzten Schritt wird der überwiesene Betrag von dem getäuschten Werkzeug des Täters abgehoben und das Geld zumeist per Western Union an einen Empfänger im Ausland weitergeleitet. Damit ist das ergaunerte Geld gewaschen und der Phishingangriff abgeschlossen.
In strafrechtlicher Hinsicht stellt sich die Frage, ob das geltende Recht ausreicht, um auf dieses Phänomen des Internetzeitalters reagieren zu können, oder ob – wie teilweise behauptet – Handlungsbedarf seitens des nationalen Gesetzgebers besteht. Dabei wird insbesondere die Frage kontrovers diskutiert, ob bereits diejenigen Handlungen, welche zu Beginn des Phishingangriffs erfolgen, also das Versenden der E-Mails und das Einrichten und Bereitstellen der korrespondierenden Internetseite, von geltenden Straftatbeständen erfasst werden. Ziel der Promotionsarbeit ist es, auf diese Diskussion einzugehen, den diesbezüglichen Meinungsstand in der juristischen Literatur und Rechtsprechung zu untersuchen, die einzelnen Standpunkte zu beleuchten und eigene Lösungsansätze auszuarbeiten.
Darüber hinaus wird es Aufgabe der Arbeit sein, auf die Strafbarkeit neuerer Erscheinungsformen des Phishings einzugehen, wie etwa dem sogenannten „Pharming" oder „Keylogging".