

Positionspapier zur fehlenden Strafbarkeit von Phishing- und Spoof-Attacken im Internet

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder mit ca. 120 Mrd. Euro Umsatz und mehr als 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Mehr als 600 Direktmitglieder gehören dem Mittelstand an. BITKOM setzt sich insbesondere für eine Verbesserung der rechtlichen und politischen Rahmenbedingungen in Deutschland, für eine Modernisierung des Bildungssystems und für die Entwicklung der Informationsgesellschaft ein.

■ Hintergrund zu Phishing- und Spoof-Attacken

In den letzten Monaten tritt eine zunächst aus dem englischsprachigen Raum bekannte Form der Internetkriminalität zunehmend auch im deutschsprachigen Internet auf. Mit so genannten „Phishing-Mails“ (sprachlich abgeleitet von „Password-Fishing“) wird versucht, durch eine täuschende Gestaltung von massenhaft versandten E-Mails die Empfänger dazu zu verleiten, die Zugangsdaten (Benutzername oder Kontonummer und Passwort) für sicherheitsrelevante Anwendungen wie Online-Banking, Online-Shops oder andere E-Commerce-Anwendungen preiszugeben. Meist verlinken die Phishing-Mails auf Webseiten (sog. „Spoof“-Seiten), die in ihrer äußeren Gestaltung das Erscheinungsbild der Originalseiten der jeweiligen Anwendung, wie z.B. von Banken, nachahmen. Die Nutzer werden – oft unter Androhung erheblicher Konsequenzen bei Nichtbefolgung – aufgefordert, ihre Zugangsdaten und gelegentlich sogar weitere sensible Daten (z.B. Kreditkartennummern oder sogar Karten-PINs etc.) auf diesen Seiten anzugeben. Zuletzt wurden Fälle bekannt, in denen ganze Online-Shops täuschend echt nachgeahmt wurden, nur um auf diese Weise an die Zugangsdaten getäuschter Nutzer zu gelangen.

Die gewonnenen Daten werden von den Tätern dann zur unbefugten Nutzung der Bank- und Nutzerkonten und damit zur Begehung oft sehr folgenreicher Straftaten missbraucht. Aufgrund der inzwischen erreichten hohen Qualität der täuschenden E-Mails und Webseiten werden trotz aller Aufklärungsbemühungen immer wieder Internetnutzer Opfer dieser Attacken. Hierdurch führt das Phänomen Phishing bzw. Spoof auch über die konkreten Schadensfälle hinaus zu einer wachsenden Verunsicherung der Bürger bei der Nutzung von elektronischen Geschäftsanwendungen und ist damit geeignet, das wirtschaftliche Potenzial dieses Bereichs zu gefährden.

Angesichts der stark zunehmenden Problematik bereitet es nicht nur betroffenen Online-Banken und -Unternehmen, sondern auch den Ermittlungs- und Strafverfolgungsbehörden erhebliche Sorge, dass das Phishing- und Spoof-Phänomen strafrechtlich kaum erfasst werden kann.

■ Die bisherige Rechtssituation

In Frage kommen grundsätzlich Strafbarkeiten wegen Betrugs nach § 263 StGB und wegen Ausspähen von Daten nach § 202a StGB. Beim Betrug stellt sich allerdings das Problem, dass die angestrebte Preisgabe der Zugangsdaten wohl weder als Vermögensverfügung (die Zugangsdaten an sich sind keine vermögenswerten Güter) noch als konkrete schadensgleiche Vermögensgefährdung (sie schafft lediglich die Voraussetzungen für die Herbeiführung eines Vermögensschadens in einem weiteren Akt) angesehen werden kann. Auch liegt noch kein unmittelbares Ansetzen zu einer später mit den Daten geplanten Straftat (in den meisten Fällen Computerbetrug nach § 263a StGB) vor. Die Strafbarkeitsschwelle wird damit erst erreicht, wenn die Täter die Daten nach erfolgreichem Datenklau zur wirtschaftlichen Schädigung der Opfer nutzen. Das Versenden der Phishing-E-Mails und das Aufsetzen von Spoof-Seiten, die zunächst die einzigen sichtbaren Handlungen sind, bleiben hingegen derzeit als Vorbereitungshandlungen straffrei.

Hiergegen bietet auch der Tatbestand des § 202a StGB (Ausspähen von Daten) keine Handhabe, da tatbestandlich schon keine Daten im Sinne des Absatzes 2 betroffen sind. Denn Objekt der Ausspähung sind nicht die beim Online-Anbieter elektronisch gespeicherten Daten, sondern die eben nicht elektronisch oder anders gespeicherten bzw. übermittelten Informationen beim Nutzer. Zudem fehlt es insoweit an der besonderen Sicherung gegen den unberechtigten Zugriff. Schließlich fehlt bei § 202a StGB auch eine Versuchsstrafbarkeit, was die Ermittlungsbehörden, die oft nur von der Phishing- bzw. Spoof-Attacke selbst, nicht aber von eventuellen Erfolgsfällen Kenntnis haben, vor Schwierigkeiten stellt.

Auch die aktuell geplante und bereits in den Bundestag eingebrachte Neuregelung zu Spam-E-Mails wird hier keine Abhilfe schaffen können, da diese allein auf „kommerzielle Kommunikationen per elektronischer Post“ abstellt. Diese Beschränkung auf Werbe-E-Mails schließt aber gerade die in betrügerischer Absicht abgefassten Phishing-E-Mails von der Anwendbarkeit aus, obgleich auch sie massenhaft verschickt werden und sogar wesentlich größere Schäden anrichten können. Auch Spoof-Seiten erfasst die gesetzliche Neuregelung nicht.

■ Rechtliche Lösungsmöglichkeit

Es erscheint deshalb erforderlich, einen speziellen Straftatbestand zu schaffen. Dieser sollte es mit Strafe bedrohen, elektronische Nachrichten oder Webseiten in betrügerischer Absicht so zu gestalten, dass der Empfänger der Nachricht bzw. der Besucher der Webseite über den wahren Absender bzw. Urheber getäuscht und damit zur Preisgabe geheimer Informationen verleitet wird, die dann zur Täuschung im Rechtsverkehr eingesetzt werden können.

Das Delikt sollte vorzugsweise als abstraktes Gefährdungsdelikt ausgestaltet sein, um nicht im Einzelfall den Nachweis eines Erfolges notwendig zu machen, der für die Ermittlungsbehörden auch bei Kenntnis einer Phishing- bzw. Spoof-Attacke oft nur schwer feststellbar ist. Alternativ müsste bei Ausgestaltung als Erfolgsdelikt zumindest eine Versuchsstrafbarkeit bestehen.

Auch wenn es sich bei Phishing und Spoof – wie auch bei Spam und anderen internetbezogenen Attacken – nicht um nationale, sondern um originär internationale Phänomene handelt, ist dennoch die Einführung einer nationalen Strafvorschrift sinnvoll. Über die Regeln des internationalen Strafrechts wird in vielen Fällen die Anwendbarkeit des deutschen Rechts zu begründen sein. Gerade das zuletzt vermehrte Auftreten deutschsprachiger Phishing-E-Mails und Spoof-Seiten zeigt zudem, dass erkennbar auch gerade der deutsche E-Commerce-Markt

im Visier der Täter ist. Diese sind offenbar in vielen Fällen auch in Deutschland ansässig; andernfalls können sie zumindest über die internationale Rechtshilfe ermittelt und verfolgt werden. Auch andere Länder haben bereits oder diskutieren die Strafbarkeit von Phishing- und Spoof-Attacken, so z.B. die Vereinigten Staaten Strafbarkeiten wegen „Identity Theft“ nach 18 U.S.C. § 1028(a)(7) oder nach dem neuen CAN-SPAM Act (18 U.S.C. § 1037).

BITKOM regt deshalb die Einführung eines Straftatbestands entweder im Fünfzehnten Abschnitt des Besonderen Teils des StGB (Verletzung des persönlichen Lebens- und Geheimnisbereichs, §§ 201ff. StGB) oder – vorzugsweise, da es sich im Regelfall um die Vorbereitung von gegen das Vermögen gerichteten Straftaten handelt – im Bereich der Vermögensdelikte an. Dieser könnte wie folgt formuliert sein:

als abstraktes Gefährungsdelikt:

Wer eine elektronische Nachricht oder ein Angebot in Tele- und Mediendiensten so gestaltet, dass Empfänger der Nachricht oder Nutzer des Angebots über den wahren Absender oder Anbieter getäuscht und dadurch verleitet werden sollen, geheime Informationen preiszugeben, die zur Täuschung im Rechtsverkehr eingesetzt werden können, wird mit Freiheitsstrafe bis ... oder mit Geldstrafe bestraft.

als Erfolgsdelikt mit Versuchsstrafbarkeit:

(1) Wer sich fremde Informationen, die zur Täuschung im Rechtsverkehr eingesetzt werden können, dadurch verschafft, dass er elektronische Nachrichten oder Angebote in Tele- und Mediendiensten so gestaltet, dass der Empfänger der Nachricht oder der Nutzer des Angebots über den wahren Absender oder Anbieter getäuscht und dadurch zur Preisgabe der Information verleitet wird, wird mit Freiheitsstrafe bis ... oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

Berlin, den 22. März 2005