Fallbeispiele zum IT-Recht – Phishing & Auskunft

Nachdem wir uns in den letzten Ausgaben jeweils aus verschiedenen Perspektiven der so genannten Störerhaftung, also der Haftung für die Handlungen anderer, in der Regel der Nutzer des zur Verfügung gestellten Webangebots, gewidmet haben, sollen in dieser Ausgabe verschiedene aktuelle Entscheidungen unterschiedlicher Gerichte als Ausgangspunkt für unsere Fallbeispiele dienen.

Zum Thema Phishing liegt eine Entscheidung des Kammergerichts Berlin vor, die als Basis des ersten Fallbeispiels dient. Die Frage des Verschuldens des Bankkunden oder aber der Bank spielt in diesen Fällen eine entscheidende Rolle. Wie sicher ist das TAN-Verfahren?

Das zweite Fallbeispiel betrifft ein kürzlich vom Amtsgericht in München ergangenes Urteil, das auch eine hohe Relevanz in der Praxis hat: Muss mir der Betreiber einer Internetseite den Namen eines registrierten Nutzers nennen, wenn ich gegen diesen Nutzer vorgehen will weil er mich auf der Internetseite beleidigt hat? Was meinen Sie?

Versuchen Sie zunächst die aufgeworfenen Fragen anhand Ihres Rechtsgefühls selbst zu beantworten und vergleichen Sie anschließend mit dem tatsächlichen Ergebnis.

Hätten Sie auch so entschieden?

Fallbeispiel 1 - Phishing:

Bankkundin K wird Opfer einer so genannten Phishing-Attacke. Als sie an ihrem PC Überweisungen im Wege des Online-Banking vornehmen will öffnet sich nach Eingabe ihrer PIN auf der Internetseite der beklagten Bank B ein weiteres Fenster, das äußerlich der Internetseite der Bank entsprach. In diesem Fenster wurde darauf hingewiesen, dass die Anmeldung fehlgeschlagen sei. Es folgt die Aufforderung, zum Login vier noch unverbrauchte Transaktionsnummern (TAN) einzugeben, was die Kundin K auch tat. Am nächsten Tag wurden vom Konto der K Überweisungen an ihr unbekannte Personen in Höhe von 14.500,00 € vorgenommen. Die Bank verwendet das klassische TAN-Verfahren und nicht das etwas sicherer iTAN-Verfahren.

Frage:

Kann die Kundin K von der Bank B den durch Phishing verlorenen Betrag ersetzt verlangen?

Antwort:

Nur Teilweise (Hier: 70% des Schadens).

Das Kammergericht Berlin hat den Schaden nach Verschuldensmaßstäben geteilt. Sowohl der Kundin als auch der Bank kann ein Sorgfaltsverstoß vorgeworfen werden. Die Kundin kann daher nicht den ganzen Schaden, sondern eben nur 70% davon verlangen.

Die Klägerin hat ihre Pflicht zur Geheimhaltung ihrer Zugangsdaten schuldhaft verletzt, indem sie der Aufforderung zur Eingabe von vier TAN nachkam. Diese Pflicht beinhaltet nicht nur die sichere Verwahrung von Notizen dieser Zugangsdaten, sondern auch eine angemessene Reaktion auf objektiv begründete Verdachtsmomente. Ignoriert der Bankkunde solche Anzeichen, liegt darin eine Pflichtverletzung.

Nach Auffassung des Gerichts begründete die Aufforderung zur Eingabe von vier TAN zum Zwecke der Authentifizierung ein solches hinreichendes Verdachtsmoment. Denn die TAN dient üblicherweise nur zur Autorisierung eines Auftrages bzw. Anweisung und nicht zur Legitimation bei der Anmeldung zum Online-Banking; zumindest die Abfrage mehrerer TAN zu diesem Zwe-

cke muss als unüblich angesehen. Demzufolge hätte die Klägerin Veranlassung gehabt, auf dieses Verdachtsmoment hin den Vorgang zunächst abzubrechen und sich durch Rückfrage bei der Beklagten zu versichern, dass eine solche Vorgehensweise von dieser tatsächlich gefordert wird.

Dass die gefälschte Internetseite, auf welche die Klägerin geleitet worden ist, der tatsächlichen Internetseite der Beklagte täuschend ähnlich sah, stellt keinen ausreichenden Grund dar, die aufgezeigten Verdachtsmomente zu ignorieren. Von einem durchschnittlichen Nutzer des Online-Banking kann erwartet werden, dass er zumindest allgemeine Kenntnis von den Gefahren durch Manipulationen von Banken- bzw. Kundensoftware hat, so dass er bei Auftreten von konkreten Verdachtsmomenten auch dann angemessen reagiert, wenn er sich dem äußeren Anschein nach auf der Internetseite seiner Bank und damit in einer vorgeblich sicheren Umgebung befindet.

Ein weiterer Sorgfaltspflichtverstoß der Klägerin kann nicht mit der Begründung angenommen werden, die Klägerin habe es unterlassen, ihre Programme mit ausreichenden Virenschutzprogrammen abzusichern. Die Tatsache, dass auf dem Computer der Klägerin geheime Daten ausgespäht worden sind, erlaubt nicht den Schluss darauf, dass es insoweit an einem wirksamen Virenschutzprogramm mangelte. Es ist zu berücksichtigen, dass es verschiedene denkbare Möglichkeiten gibt, wie kriminelle Dritte an geheime Daten eines Kunden gelangen können, wie zum Beispiel durch einen Angriff auf den Zentralrechner, so dass sich der Schluss auf eine typische Ursache verbietet.

Eine Sorgfaltspflichtverletzung der Beklagten Bank ist aber darin zu sehen, dass die Beklagte noch zu einem Zeitpunkt das herkömmliche TAN System verwendete, als die von den Tätern gewählte Angriffsmethode des Abfragens mehrere TAN Nummern bereits hinlänglich bekannt war und in Form des neueren iTAN Systems ein wirksameres System zur Abwehr dieser Angriffe existierte. Eine Sorgfaltspflichtverletzung der Bank liegt zumindest dann vor, wenn sie ein System verwendet, das bei der Mehrzahl der Kreditinstitute nicht mehr im Einsatz ist und hinter dem Sicherheitsstandard des neueren Systems zurückbleibt. Entscheidend ist, dass das neue System gegenüber dem alten eine höhere Sicherheit bot und daher die Angriffsmöglichkeiten zumindest eingeschränkt hätte.

Bei Abwägung der verschiedenen Verschuldensanteile der Parteien ergibt sich nach Auffassung des Gerichts ein überwiegendes Mitverschulden der Beklagten, das die Richter mit 70% bewerten. Hierbei wurde insbesondere berücksichtigt, dass zum Zeitpunkt der schädigenden Handlung das von der Beklagten verwendete TAN System als überholt anzusehen war und der Missbrauch der erlangten TAN mit dem neueren iTan-System nicht möglich gewesen wäre.

(Das Urteil erging genau so vom Kammergericht Berlin am 29.11.2010, Az.: 26 U 159/09)

Fazit:

Das Gericht hat damit bereits die Verwendung des herkömmlichen TAN-Verfahrens durch die Bank als ein Mitverschulden der Bank für den entstandenen Schaden gewertet. Da die Mehrzahl der Banken bereits das neuere iTAN-Verfahren benutzt hat das Gericht die Verwendung des grundsätzlich unsichereren Verfahrens als unzureichend angesehen. Aber auch der Nutzer des Online-Banking muss kritisch mit dem Medium Internet umgehen und darf nicht Vorgänge, die ihm merkwürdig vorkommen müssen, einfach ignorieren. Insoweit hat das Gericht hier vernünftige Maßstäbe angelegt und kam so nachvollziehbar zu einer Quotelung 70:30 zu Lasten der Bank.

Seit dem 01.11.2009 ist übrigens der Haftungsmaßstab des damals neu eingefügten § 675v BGB anzuwenden, der aufgrund einer EU-Richtlinie (so genante SEPA-Richtlinie) eingefügt wurde. Der Bankkunde haftet danach nur für grobe Fahrlässigkeit und nicht für einfach fahrlässiges Verhalten. In dem hier entschiedenen Fall war diese Norm aber noch nicht anzuwenden, da der Vorfall vor Inkrafttreten des § 675v BGB stattfand.

Fallbeispiel 2 - Auskunft:

K betreibt mehrer Autohäuser. B betreibt eine Internetplattform, auf der sich registrierte Nutzer zum Thema Auto austauschen können. In diesem Forum haben verschiedene Nutzer Erfahrungsberichte veröffentlicht, die für K geschäftsschädigend sein können. Jedenfalls fühlt sich K durch die Äußerungen diskreditiert und geschädigt. Auf den Hinweis von K hat B unverzüglich die betreffenden Beiträge aus dem Forum entfernt. Darüber hinaus hat K Auskunft von B darüber verlangt, welche Nutzer sich hinter den Nicknamen, unter denen die Beiträge gepostet wurden, verbergen, um diese Nutzer im Anschluss direkt in Anspruch nehmen zu können. B weigert sich die verlangten Auskünfte zu erteilen.

Frage:

Hat K gegen B Anspruch auf Auskunftserteilung (Namen, Adressen der registrierten Nutzer)?

Antwort:

NEIN.

Als Betreiberin eines Internetforums, das den Nutzern inhaltliche Dienste anbietet und nicht nur Telekommunikationsleistungen zur Verfügung stellt, ist die Beklagte B Diensteanbieterin im Sinne des Telemediengesetzes (TMG). Nach § 14 Absatz 2 TMG darf der Diensteanbieter auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist. Die Voraussetzungen dieses Auskunftsanspruches sind schon deshalb nicht gegeben, da das Begehren der Klägerin keinem der genannten Zwecke dient. Ein Anspruch der Klägerin nach § 14 Absatz 2 TMG besteht daher nicht.

Eine analoge Anwendung dieser Vorschrift scheidet aus, da es sich erkennbar eine Ausnahmeregelung handelt, die keine Erweiterung über den ausdrücklich genannten Anwendungsbereich hinaus finden soll. So ist in § 12 TMG geregelt, dass der Diensteanbieter die für die Bereitstellung von Telemedien erhobenen personenbezogenen Daten für andere Zwecke nur verwenden darf, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat. Eine analoge Anwendung kommt daher nicht in Betracht.

Die Klägerin hat auch keinen Anspruch auf Auskunftserteilung aus §§ 242, 259 BGB, da es sich bei der Regelung in § 14 Absatz 2 TMG um eine spezieller Norm zu diesem allgemeinen Anspruch handelt, so dass ein Rückgriff auf den aus Treu und Glauben abgeleiteten Auskunftsanspruch ausscheidet. Auch hier schließt die Regelung in § 12 TMG der Auskunftserteilung aufgrund eines allgemeinen Auskunftsanspruches aus, da eben gerade keine Regelung vorliegt, die sich ausdrücklich auf Telemedien bezieht.

Da der Klägerin somit ein Auskunftsanspruch nicht zusteht, war die Klage abzuweisen. Soweit sich die Klägerin beleidigt oder verleumdet sieht, muss sie sich staatsanwaltlicher Hilfe bedienen und um gegebenenfalls im Wege der Akteneinsicht die gewünschten Kenntnisse zu erlangen. Da der Klägerin dieser Weg offensteht, ist sie auch nicht rechtlos gestellt.

(Das Urteil erging genau so vom AG München mit Urteil vom 03.02.2011, Az.: 161 C 24062/10)

Fazit:

Obwohl der Betreiber eines solchen Internetforums die erforderlichen Daten hat und der Geschädigte nachweislich Ansprüche gegen den einzelnen Nutzer hat oder dies zumindest nicht ausgeschlossen ist, besteht kein Auskunftsanspruch des Verletzten. Das Amtsgericht München geht hier streng nach den Vorschriften des Telemediengesetzes vor und verneint am Ende einen allgemeinen Auskunftsanspruch nach Treu und Glauben. Letzteres ließe sich jedoch auch anders lösen. Ein Anspruch nach Treu und Glauben wurde schon mehrfach von Gerichten herangezogen, wenn die Erteilung der Auskunft im jeweiligen Einzelfall als sachgerecht erschien.

Hier wird der Verletzte auf den strafrechtlichen Weg verwiesen, was in solchen Fällen stets ein gangbarer Weg ist. Er kann also Strafanzeige wegen Beleidigung und/oder Verleumdung stellen. Die Staatsanwaltschaft als Ermittlungsbehörde wiederum hat sodann die Möglichkeit über den genannten § 14 Absatz 2 TMG den Plattformbetreiber auf Auskunft in Anspruch zu nehmen. Wenn aber die Staatsanwaltschaft keinen Anfangsverdacht sieht, wird es zu einem Auskunftsverlangen nicht kommen. Und auch danach kann die Staatsanwaltschaft die Akteneinsicht wegen überwiegender schutzwürdiger Interessen des Beschuldigten verweigern. Der strafrechtliche Weg muss also nicht unbedingt zum Erfolg führen. Und schließlich darf nicht vergessen werden, dass dieser Weg zu einer Kriminalisierung der Nutzer des Forums führt, was nicht unbedingt erstrebenswert ist.

Timo Schutt
Rechtsanwalt & Fachanwalt für IT-Recht
www.schutt-waetke.de