Bank intern
Der Insider-Report für den leitenden Banker: ●aktuell ●kompakt ●kritisch ●unabhängig
Spezial

Düsseldorf, 25-04-2022 XXV. Jahrgang Beilage zu Nr. 17/2022

Vorsicht Falle: Sparkassen und Volksbanken als Opfer von Phishing-Attacken

– von RA Dr. **Jan-David Jansing** & RA **Anne Lilli Breitkreutz**,
VOELKER & Partner Reutlingen –

Die aktuelle Kriminalstatistik zeigt es deutlich: Auch Kriminelle arbeiten seit Corona lieber aus dem 'Homeoffice' – der Anteil von Raub und Diebstahl sinkt und Online-Betrug nimmt rapide zu. Immer häufiger werden auch Kunden von **Sparkassen** und **Volksbanken** zu Opfern von Phishing-Attacken – und damit auch die Banken selbst, die bei der Regulierung dann in einem Spannungsfeld zwischen kundenfreundlicher Erstattung und mühsamer Schadensabwälzung auf die Kunden stehen: In der Anwaltspraxis stellen wir fest, dass manche Bank viel zu freigiebig reguliert – während andere Banken viel zu pauschal eine Autorisierung durch den Kunden oder dessen grobe Fahrlässigkeit unterstellen. Beides ist nicht richtig, da alle Fallgestaltungen stets einer akribischen Aufklärung in tatsächlicher und rechtlicher Hinsicht bedürfen (Faustformel: Anwaltskosten für die Sachaufklärung etc. fast immer fünfstellig). Dies gilt erst recht deshalb, weil sich die Rechtslage völlig unterschiedlich darstellt, je nachdem welches Legitimationsverfahren verwendet wurde (ChipTAN, SMS-TAN, PushTAN): So stellen wir fest, dass gerade im Zuge der Einführung der aktuellsten, vermeintlich 'modernsten' Verfahren (z. B. die **S-pushTAN**-App oder **VR-SecureGo**) ungleich größere technische und rechtliche Probleme auftreten als z. B. beim vermeintlich altmodischen ChipTAN-Verfahren.

> Fast immer werden Bankkunden unter einem Vorwand – etwa einer angeblich erforderlichen Systemaktualisierung – über eine Phishingmail dazu verleitet, ihre PIN-Nummer etc. auf einer vermeintlich 'echten' (tatsächlich aber gut imitierten) Homepage ihrer Bank einzugeben. Da sowohl Mail als auch Homepage sehr authentisch gestaltet sind (und nicht mehr – wie früher – mit massenhaft Rechtschreibfehlern durchsetzt), können Kunden die Täuschung oftmals nicht erkennen – was im Streitfall den Vorwurf des grob fahrlässigen Verhaltens erschwert: Denn wer nicht erkennen kann, dass er sich nur vermeintlich im vertrauten Online-Banking der eigenen Bank befindet, dem kann man auch nicht vorwerfen, er habe leichtfertig Daten an Dritte weitergegeben.

Sodann werden die Kunden telefonisch von einem angeblichen Bankmitarbeiter kontaktiert, der diese zur Preisgabe von TANs bewegt – mit welchen der schadensstiftenden Überweisung zugestimmt wird. Auch hier agieren die Betrüger professionell, indem sie mit einer Rufnummern-ID anrufen, welche tatsächlich von der Bank stammt und indem sie sich als Vertreter des tatsächlich zuständigen Kundenbetreuers ausgeben (dessen Namen sie im Online-Banking gelesen haben).

> Täter nutzen auch gezielt den Umstand aus, dass vielerorts aktuell die Umstellung der Legitimationsverfahren von ChipTAN auf app-basierte Verfahren erfolgt – indem sie mit betrügerisch entwendeten Daten die Legitimations-Apps 'kapern'. Dies ermöglicht es den Tätern, selbst unbegrenzt Überweisungen aus dem Online-Banking auszuführen – ohne, dass sie den Kunden noch telefonisch dazu veranlassen müssten, ihnen eine TAN mitzuteilen. Die Täter haben leichtes Spiel, weil viele Kunden wegen der Umstellung des Legitimationsverfahrens tatsächlich aktuell von ihren Banken kontaktiert wurden – so dass es ihnen plausibel erscheint, wenn sie die Bank (vermeintlich) noch einmal telefonisch darum bittet, bei der abschließenden Einrichtung der 'pushTAN-App' o. ä. mitzuwirken (sog. 'Social Engineering').

Impressum
markt intern Verlagsgruppe – **kapital-markt intern** Verlag GmbH, Grafenberger Allee 337a, D-40235 Düsseldorf. Tel.: +49 (0)211 6698 199, Fax: +49 (0)211 6698 777. www.kmi-verlag.de. Geschäftsführer: Dipl.-Kfm. Uwe Kremer, Rechtsanwalt Gerrit Weber, Dipl.-Ing. Günter Weber. Gerichtsstand Düsseldorf. Handelsregister HRB 71651. Vervielfältigung nur mit Genehmigung des Verlages.

Bank intern Herausgeber: Dipl.-Ing. Günter Weber. Redaktionsdirektoren: Dipl.-Kfm. Uwe Kremer, Rechtsanwalt Gerrit Weber. Chefredakteur: Rechtsanwalt Dr. Axel J. Prümm. Redaktionsbeirat: Dipl.-Ing. Dipl.-Oen. Erwin Hausen, Christian Prüßing M.A., Dipl.-Oec. Curd Jürgen Wulle. Druck: Theodor Gruda, www.gruda.de. ISSN 1615-522X

Ist die betrügerische Überweisung 'geglückt', verlangt der Kunde meist von seiner Bank nach § 675u S. 2 **BGB** die Erstattung des Betrags – mit der Begründung, dass er der Überweisung nicht zugestimmt habe. Viele Banken tendieren dazu, diesem Kundenbegehren allzu schnell nachzugeben und den Betrag zu erstatten. Dabei sollte unbedingt in Betracht gezogen werden, den Kunden nicht einfach kampflos zu entschädigen, sondern den Vorgang genau zu untersuchen (jedenfalls bei größeren Beträgen).

Denn teilweise bestehen gute Chancen, dass sich die Bank doch mit Erfolg auf eine Autorisierung berufen kann – obwohl sie selbst bei streitigen Zahlungsvorgängen nach § 675w BGB mit erheblichen Beweispflichten belastet ist. Hierbei kommt es stark auf die Umstände des Einzelfalls an – wie etwa, welches Legitimationsverfahren verwendet wurde oder was über den betrügerischen Tathergang bekannt ist (Letzteres setzt viel Know-how voraus, um die Schwachstellen der Systeme im Streitfall erkennen und argumentativ für die Bank nutzen zu können). So besteht z. B. beim ChipTAN-Verfahren mit der derzeitigen **BGH**-Rechtsprechung (vgl. BGH, Urteil vom 26.01.2016, Az.: XI ZR 91/14) die Möglichkeit, dass sich die Bank auf den Beweis des ersten Anscheins beruft – sofern sie anhand bestimmter Protokolle nachweisen kann, dass eine Authentifizierung erfolgt ist und der Zahlungsvorgang ordnungsgemäß aufgezeichnet, verbucht sowie nicht durch Störungen beeinträchtigt ist. Denn das ChipTAN-Verfahren wird wegen seiner Abschottung (vom Endgerät, auf dem der Kunde das Online-Banking betreibt sowie auch sonst vom Internet) von den Gerichten als 'praktisch unüberwindbar' eingestuft. Anders ist dies bei SMS- oder app-basierten Verfahren, welche nach diesen Maßstäben (bislang) nicht als sicher angesehen werden können: Die Bank handelt sich also u. U. Nachteile bei der Beweisführung gerade dadurch ein, dass sie auf die vermeintlich moderneren Legitimationsverfahren umstellt. Man muss also genau zwischen Zeitgeist (*"Alles bequem mit dem Handy machbar!"*) und Sicherheit abwägen und darf sich nicht darauf verlassen, dass das neueste System per se das 'sicherste' ist – bloß weil es vom jeweiligen **Sparkassen-** oder **Volksbankenverband** aktuell vermarktet wird.

BUNDESGERICHTSHOF

Eine sorgfältige Sachverhaltsaufklärung ist auch erforderlich um ggf. eine grob fahrlässige Verletzung von Kundensorgfaltspflichten nachzuweisen – denn ein daraus resultierender Schadensersatzanspruch der Bank ist häufig deren einzige Möglichkeit, um sich schadlos zu halten. Hier ist oft festzustellen, dass Banken im Rahmen des internen Beschwerdemanagements viel zu schnell die grobe Fahrlässigkeit bejahen (*"Das System ist sicher; der Schaden kann daher nur durch Fahrlässigkeit verursacht worden sein!"*), obwohl der Grat zwischen einfacher und grober Fahrlässigkeit in der Praxis äußerst schmal ist. Will man mit der Argumentation bei Gericht bestehen (wo eine starke Tendenz vorherrscht, den Kunden in Schutz zu nehmen), bedarf es einer genauen Aufklärung jedes Einzelfalls – z. B. wie der Kunde seine Legitimationsdaten preisgegeben hat, welche Warnhinweise die Bank ihm vorher gegeben hatte usw. – Der Teufel steckt im Detail!

Dies gilt auch für die Verteilung der Darlegungs- und Beweislast und der damit verbundenen Prozessstrategie: Durch gezieltes Bestreiten von Tatsachen kann es der Bank z. B. gelingen zu verhindern, dass der Kunde den Anscheinsbeweis durch Darlegung eines möglichen alternativen Geschehensablaufs erschüttert. Dies setzt aber voraus, dass die Bank bereits von Anfang an bei der Kundenkommunikation jedes Wort abwägt, um sich im späteren Prozess keine Argumente abzuschneiden (Falsch: *„Es ist klar, dass Ihr Computer gehackt wurde."* / Richtig: *"Wir haben keine Auffälligkeiten beim Zahlungsvorgang festgestellt; Sie geben aber an, dass Ihr Computer gehackt worden sei…"*). Denn oft ist davon auszugehen, dass es weder der Bank noch dem Kunden gelingen wird, alle Einzelheiten aufzuklären und zu beweisen – weshalb man alles daran setzen muss, sich diese Unsicherheit durch geschicktes prozessuales Taktieren selbst zu Nutze zu machen.

Fazit: Phishing ist und bleibt ein Massenphänomen – aber es gibt nicht die 'eine' richtige Strategie im Umgang damit. Es bedarf vielmehr eines gesteigerten Problembewusstseins und einer genauen Analyse jedes Einzelfalls – auch zur Vermeidung künftiger Schäden.