Betrugsgefahr bei Onlinebanken?

1. Kompetenzen

Die Schülerinnen und Schüler sollen ...

1. sich Vorgehensweise und Umfang der im Artikel beschriebenen Betrugsfälle im Onlinebanking erschließen.
2. die Bedeutung funktionsfähiger Sicherheitssysteme für die Geschäftsmodelle der Onlinebanken herausarbeiten.
3. sich exemplarisch mit der Bedeutung von „Vertrauen“ im Wirtschaftsgeschehen sowie den Herausforderungen der Digitalisierung für Verbraucherinnen und Verbraucher auseinandersetzen.

2. Aufgaben

1. *Fassen Sie die im Artikel dargestellten Betrugsfälle im Onlinebanking in eigenen Worten zusammen. Legen Sie die Vorgehensweise der Täter dar.*
2. *Beschreiben Sie die vonseiten der Anbieter getroffenen Sicherheitsmaßnahmen.*
3. *Erläutern Sie in diesem Zusammenhang die Geschäftsbeziehungen zwischen den Smartphonebanken wie N26 und Fidor sowie den traditionellen Institutionen wie den Volks- und Raiffeisenbanken. Arbeiten Sie die zwischen diesen auftretenden Konfliktlinien heraus.*
4. *Erschließen Sie sich die Bedeutung funktionsfähiger Sicherheitssysteme für die Geschäftsmodelle der Smartphone- und Onlinebanken.*
5. *Erörtern Sie anhand des vorliegenden Beispiels die Bedeutung von „Vertrauen“ im alltäglichen Wirtschaftsgeschehen. Diskutieren Sie in diesem Zusammenhang, wie sich eine Zunahme von Betrugsfällen im Onlinebanking auf das Verhalten der Verbraucherinnen und Verbraucher auswirken könnte.*
6. *Setzen Sie sich exemplarisch mit den Vorteilen und Herausforderungen der Digitalisierung aus Verbrauchersicht auseinander. Überprüfen Sie hierzu, welchen Nutzen das Onlinebanking im Vergleich zu traditionell organisierten Bankgeschäften stiftet und inwieweit sich auf der anderen Seite Unsicherheiten erhöhen.*

Betrugsgefahr bei Onlinebanken?

Die Dienstleister der Genossenschaftsbanken warnen vor Betrugsgefahr im Zahlungsverkehr mit Smartphonebanken. Die betroffenen Institute wehren sich.

Bislang waren es Einzelfälle. Die ein oder andere Volksbank und Sparkasse hatte sich in den vergangenen Wochen über Smartphonebanken wie N26 oder Fidor beschwert. Der Vorwurf: Die Konkurrenten würden nicht genug tun, um Betrügereien zu verhindern. Jetzt sprechen zwei Rundschreiben aus dem Sektor der Genossenschaftsbanken dafür, dass die Probleme deutlich größer als bislang angenommen sein könnten. In den Schreiben ist von steigenden Schäden im Onlinebanking die Rede und davon, welche Rolle falsche Konten bei den Smartphonebanken spielen.

Die genossenschaftliche R+V Versicherung, die Schadensfälle durch Onlinebanking-Betrug für Volks- und Raiffeisenbanken absichert, verschickte Anfang Juni einen Brief mit der Überschrift: „Drastische Zunahme von Schäden bei Zahlungsvorgängen im Onlinebanking“. Neben der Zahl der Fälle seien auch die Schadensbeträge erheblich angestiegen und lägen aktuell deutlich über den Werten der vergangenen Jahre, heißt es in einer „Aktuellen Information“, die dem Handelsblatt vorliegt. „Wir hatten 2019 bereits knapp 300 Schäden“, sagte eine R+V-Sprecherin auf Anfrage. Insgesamt summiere sich der Aufwand auf rund fünf Millionen Euro. Das sei bereits deutlich mehr als der Durchschnitt der vergangenen drei Jahre. In einem Fall sei es um 350 000 Euro gegangen.

In dem Informationspapier nimmt der Versicherer explizit Bezug auf Smartphonebanken. Die R+V schildert das Vorgehen der Betrüger, das „in einer Vielzahl der Schadensfälle“ genutzt worden sei, wie folgt: Der Täter eröffnet mit fiktivem Namen ein Konto „meist bei Direktbanken (wie zum Beispiel N26 oder Fidor Bank) und häufig im Video-Ident-Verfahren“. Danach spähen die Täter die Zugangsdaten der Volksbank-Kunden aus und lösen betrügerische Überweisungen zugunsten ihrer gefälschten Konten aus. „Betrügern gelingt es derzeit - trotz der gezielten Warnhinweise der Banken - verstärkt an Zugangsdaten zum Onlinebanking von Bankkunden zu gelangen. Dabei missbrauchen sie insbesondere das mobileTan-Verfahren zulasten der Kontoinhaber“, erläutert die R+V. Einen ähnlichen Hinweis gab vergangene Woche auch DZ Compliance Partner, eine Servicegesellschaft, die für kleinere Volks- und Raiffeisenbanken Dienstleistungen im Bereich Geldwäsche- und Betrugsprävention anbietet. „Aktuell kommt es vermehrt zu betrügerischen Zahlungsaufträgen zugunsten von Konten bei Direktbanken, beziehungsweise insbesondere bei Finanz-Start-ups“, heißt es in einem Rundschreiben der Servicetochter der DZ Bank. „Je nach Einzelfall der Transaktion kann es sinnvoll sein, eine telefonische persönliche Rückbestätigung von Ihrem Kunden einzuholen“, steht in dem Hinweis, der dem Handelsblatt vorliegt. DZ Compliance Partner stellt anlassbezogene Hinweise in ein System, auf das etwa 350 bis 400 der insgesamt 875 deutschen Genossenschaftsbanken Zugriff haben. Solche Hinweise würden sich generell aus Presseberichten sowie Hinweisen der Finanzaufsicht Bafin speisen, heißt es in Finanzkreisen.

Zahlen der Bafin legen nahe, dass in diesem Jahr gehäuft Probleme bei Onlinebanken auftreten. Bis zum 18. Juni habe es im laufenden Jahr insgesamt 3 497 Kundenbeschwerden gegeben. Davon hätten 839 Beschwerden - also fast jede vierte - Online- oder Direktbanken betroffen, sagte eine Bafin-Sprecherin. Im vergangenen Jahr lag der Anteil der Onlinebanken bei den Beschwerden bei knapp 19 Prozent. Im laufenden Jahr habe die Behörde „zum einen verstärkt Beschwerden erhalten, die sich damit befassen, dass Direktbankkonten zur Abwicklung betrügerisch veranlasster Zahlungen genutzt werden. Weiterhin war die Erreichbarkeit und die Bearbeitungsgeschwindigkeit bei der Abwicklung von Geschäftsvorgängen Gegenstand von Beschwerden.“ […]

Ein weiterer Vorwurf der Genossenschaftsbanken richtet sich ebenfalls vor allem gegen N26. Das Institut sei nicht schnell genug erreichbar, um Betrugsfälle zu verhindern. Das Zeitfenster für einen erfolgreichen Überweisungsrückruf sei kurz, da Täter die Geldbeträge „schnellstmöglich“ weiterleiten, heißt es in dem Schreiben der R+V. „Dies wird durch die meist nur schlechte Erreichbarkeit bei den gewählten Direktbanken zusätzlich erschwert“, schreibt die Versicherung. „Hier dauert die Kontaktaufnahme sowohl telefonisch, per Fax oder per Internet oft Tage.“ […]

Die so gescholtenen Onlinebanken wehren sich gegen die Vorwürfe der Konkurrenz: „Unsere Verifikationsmaßnahmen sind sicher, und wir entwickeln diese Verifikationsstandards kontinuierlich weiter“, betont Max Schertel, Leiter Business Operations bei N26, dem Handelsblatt. Eine Sprecherin ergänzte, die Online-Verifikationsverfahren seien genauso sicher wie andere Legitimationsverfahren im Banking. Bei der Kontoeröffnung seien mehrere Sicherheitsstufen in den Prozess eingebunden. Allerdings hatte die Bafin N26 vor Kurzem verpflichtet, eine bestimmte Zahl ihrer Bestandskunden erneut zu überprüfen und ihre Prozesse und Arbeitsabläufe schriftlich zu fixieren, weil der Behörde die Geldwäschekontrollen des Instituts nicht genügten. Die Fidor Bank bestätigte zwar, dass sie „wie alle anderen Banken gelegentlich von betrügerischen Kontoeröffnungen betroffen“ sei. Die Kontroll- und Überwachungsmaßnahmen seien aber in den vergangenen zwei Jahren laufend intensiv verbessert worden und insgesamt „sehr erfolgreich“. In den Monaten Januar bis Mai 2019 seien „mehr als 99 Prozent“ aller Kontoeröffnungen „unbelastet“ gewesen. Der Anspruch Fidors gehe aber dahin, die Kontoeröffnungen zu 100 Prozent von missbräuchlichen Mustern frei zu halten.

Auch gegen den Vorwurf der zu langen Reaktionszeiten wehren sich die Banken. „Wir hatten Schwierigkeiten mit unserer Erreichbarkeit, aber mittlerweile sind wir unter sämtlichen Telefonnummern erreichbar, speziell die spezifischen Telefonnummern für den Zahlungsverkehr und die Nummern unserer Geldwäsche-Abteilung“, sagte N26-Manager Schertel. „Die Anliegen werden taggleich bearbeitet“, so Schertel. […] Die Fidor Bank betont ebenfalls, sie sei für andere Banken und Kunden sowie Dritte sowohl telefonisch als auch per E-Mail sehr gut zu erreichen. Für die Kommunikation mit anderen Banken stünden neben den normalen Wegen für Kunden weitere E-Mail-Adressen und Telefonnummern der Compliance-Abteilung zur Verfügung. […]

Quelle: Osman, Y./Atzler, E., Handelsblatt, Nr. 119, 25.06.2019, 26