Keine Entwarnung beim Kreditkartenbetrug

Von Jörg Reuter

Wenngleich in einigen Ländern Europas die Verluste durch Kreditkartenbetrug 2019 gesunken sind, kann Jörg Reuter keine Entwarnung geben. Zum einen hat die kriminelle Szene Start-ups und unter dem Eindruck der Corona-Pandemie neu gestartete Online-Shops ins Visier genommen. Zum anderen hat auch die starke Kundenauthentifizierung ihre Grenzen in der Sicherheit der dafür genutzten Mobiltelefone. Unter Sicherheitsaspekten bricht der Autor deshalb eine Lanze für das Mobile Payment. Hier macht die Tokenisierung den Hackern das Leben zumindest schwerer. Red.

Mehr als 1,5 Milliarden Euro Verlust durch Kreditkartenbetrug sind europäischen Banken 2019 entstanden. Das zeigt die diesjährige Ausgabe der „European Fraud Map" von Fico. Im Durchschnitt über alle Länder hinweg nahmen die Verluste um 2 Prozent im Vergleich zu 2018 ab, wobei sich das Betrugsniveau in den einzelnen Ländern sehr unterschiedlich gestaltet.

Großbritannien bleibt mit rund 620 Millionen Pfund Verlust der Spitzenreiter in Bezug auf das absolute Betrugsvolumen, obwohl die Verluste durch Kreditkartenbetrug dort im vergangenen Jahr um über 50 Millionen Pfund beziehungsweise acht Prozent abnahmen. Auch in zahlreichen anderen europäischen Ländern konnte das Vorjahresniveau leicht gesenkt oder zumindest weitestgehend gehalten werden. Doch diese Erfolge sind nicht zwingend von Dauer – aus verschiedenen Gründen.

Kampf gegen Cyberkriminelle noch längt nicht gewonnen

Die Gegenmaßnahmen der einzelnen europäischen Länder und ihrer Finanzinstitute im Kampf gegen den Kreditkartenbetrug tragen zwar teilweise Früchte, trotzdem ist der Kampf gegen die Cyber-Kriminellen noch längst nicht gewonnen.[1)] Besonders erfolgreich gestaltet sich die Entwicklung in Norwegen und Portugal. Hier nahmen die Verluste um 16 beziehungsweise 13 Prozent ab – die höchsten prozentualen Abnahmen innerhalb Europas. In Deutschland nahmen die Verluste nur geringfügig – um 1 Prozent – ab. Ungarn und Polen hingegen sind mit jeweils 17 Prozent mehr Verlust die Länder mit den höchsten prozentualen Anstiegen von 2018 auf 2019 – gefolgt von Rumänien, Griechenland und Italien mit 14, 12 und 10 Prozent.

Die Abnahme in Großbritannien ist vor allem darauf zurückzuführen, dass dort 2018 die sogenannten „Data Compromise Events" – also massive Datenlecks – geradezu explodierten und so zu einem Anstieg der Schadensumme von über 100 Millionen Pfund führten. Generell ist das Betrugsniveau auf dem Inselstaat 2019 nach wie vor das höchste in ganz Europa.

An die Kreditkartendaten kommen die Kriminellen dabei erfahrungsgemäß nach wie vor insbesondere über einen altbewährten Weg: Datenbank-Hacks bei Online-Händlern oder seltener bei Banken und Finanzdienstleistern. Dabei herrscht in der Regel eine Art Arbeitsteilung in der Szene.

– So gibt es Experten für das eigentliche Hacking der Datenbanken,

– dann kommen Spezialisten für die Infiltration und das Abgreifen der Daten aus den Systemen auf den Plan

– und schlussendlich diejenigen, die diese Daten dann über das Darknet oder andere Kanäle verkaufen. Die Kriminellen, die die Daten dann tatsächlich nut-

Jörg Reuter, Consultant Fraud & Financial Crime, FICO Fair Isaace Germany GmbH, Bensheim

zen, sind in der Regel also nicht dieselben, die die Daten ursprünglich gestohlen haben. Das erschwert die Ermittlungen und strafrechtliche Verfolgungen in diesen Fällen.

Kriminelle Szene profitiert von Covid-19

Die in diesem Jahr veröffentlichte Studie „Dark Web Price Index 2020" von Privacy Affairs zeigt: Kreditkartenbetrug ist für Kriminelle attraktiv.[2)] So kostet eine geklonte Mastercard inklusive PIN durchschnittlich 15 US-Dollar. Bedenkt man, dass bei Datendiebstählen gerade im Online-Handel meist mehrere Millionen Datensätze unrechtmäßig entwendet werden, machen die Cyber-Kriminellen, die diese Karten zur Verfügung stellen, hier ein Riesengeschäft. Aber auch diejenigen, die die geklonten Karten erwerben, stehen dem in nichts nach: Pro Karte sind oftmals mehrere Tausend Euro zu holen – zumindest, wenn die Betrüger schnell genug zuschlagen.

Dabei spielt der aktuelle E-Commerce-Boom aufgrund der Pandemie den Verbrechern in die Hände. Denn derzeit sprießen so viele Online-Shops wie noch nie in so kurzer Zeit aus dem Boden, da immer mehr Händler die ausbleibende Lauf- und Ladenkundschaft online kompensieren müssen. Und nicht alle neuen Online-Shops haben von Anfang an schon umfangreiche Sicherheitsvorkehrungen implementiert, um sich und ihre Kunden gegen Cyber-Kriminelle ausreichend abzusichern.

Fintechs als neue Opfer

Auch wenn die Cyber-Kriminellen das bestehende Netz aus Banken, Online-Shops und Kunden noch längst nicht abgegrast haben, nehmen Hacker und Betrüger schon die nächsten Opfer ins Fadenkreuz: Fintechs, also Technologieunternehmen im Finanzsektor – und dabei vor allem Start-ups. Die Vorstellung, dass ein Fintech von Anfang an alle genutzten Systeme und Dienste vollumfänglich absichern kann, ist wohl eher Wunschdenken. Der Innovationsdruck führt vielmehr dazu, dass die Sicherheit zumindest anfangs nicht immer ganz oben auf der Prioritätenliste steht.

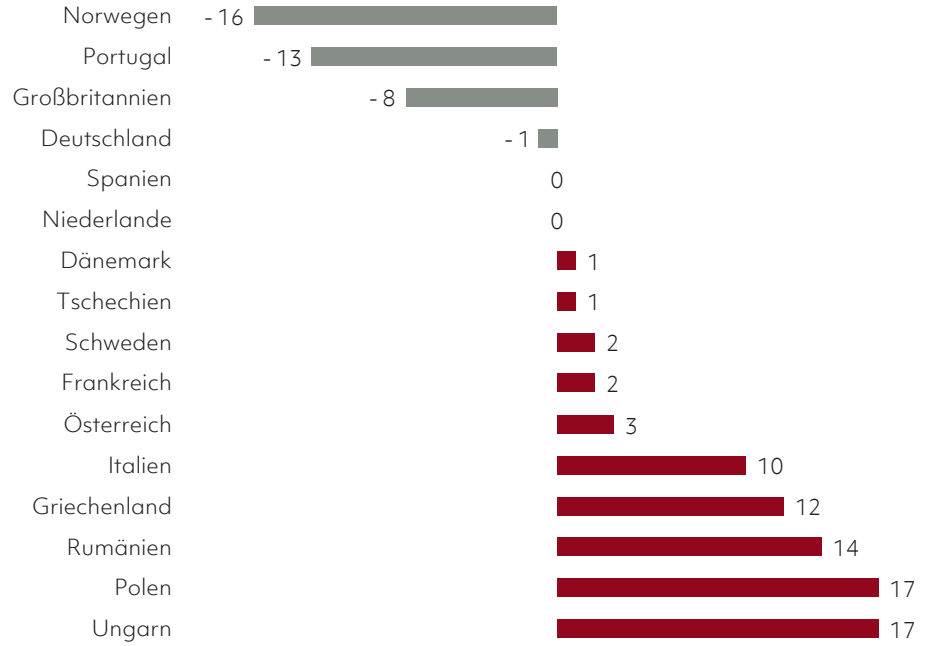
Die bisher im Vergleich zu großen Banken noch überschaubare Zahl an Kunden bei den einzelnen Fintechs ist wohl der Hauptgrund dafür, warum hier bislang noch wenige Data Breaches zu verzeichnen sind. Allerdings sind Fintechs nicht per se unsicherer als traditionelle Banken. Tatsächlich gibt es hier auch durchaus Vorreiter, die von Anfang an mit einem tiefgehenden „Security Mindset" ihr Business aufbauen und betreiben.

In den Finanz- und Wirtschaftsnachrichten in Deutschland hat – mit Ausnahme von Corona – in den vergangenen Monaten vor allem ein Thema die Schlagzeilen dominiert: Der Fall Wirecard. Und auch wenn jetzt aus dem verbliebenen Vorstand des einstigen Dax-Unternehmens Stimmen laut werden, dass die Geschäfte doch regulär fortgeführt werden, stehen doch alle Zeichen auf Zerfall. Die Unsicherheit und Berichterstattung rund um den Fall ruft schon Phishingbetrüger und Scammer auf den Plan. Wenn Wirecard auseinanderbricht, ist davon auszugehen, dass weitere Cyber-Kriminelle nicht lange auf sich warten lassen – auch wenn Hacker üblicherweise eher Händler statt die „Card Issuer" beziehungsweise Zahlungsdienstleister angreifen. Die Zahl der Datenlecks bei den „dicken Fischen" nimmt aktuell eher ab, was zeigt, dass die Sicherheitsmaßnahmen hier massiv hochgefahren wurden.

Multi-Faktor-Authentifizierung mit Grenzen

Doch was können Banken und Verbraucher nun tatsächlich tun, um es den Cyber-Kriminellen zumindest so schwer wie möglich zu machen? Ein Mittel ist die Multi-Faktor-Authentifizierung. Hierbei wird die Zugangsberechtigung beispielsweise zu einer Online-Banking-App durch mehrere voneinander unabhängige Merkmale überprüft, beispielsweise eine Kombination aus Sicherheitsfrage und SMS-PIN oder Passwort und Fingerabdruck. Indem man die relativ anfälligen Passwörter als einzige Authentifizierungsfaktoren aus der Schusslinie nimmt und mit deutlich sichereren Merkmalen ergänzt beziehungsweise sie sogar komplett ersetzt, haben Hacker es sehr viel schwerer, entsprechend gesicherte Accounts zu knacken. Wenn allerdings die komplette Authentifizierung über ein und dasselbe Smartphone erfolgt, sich dort Malware einnistet und diese dann sowohl den Authenticator als auch die Banking-App kompromittiert, kommt auch die Multi-Faktor-Authentifizierung an ihre Grenzen.

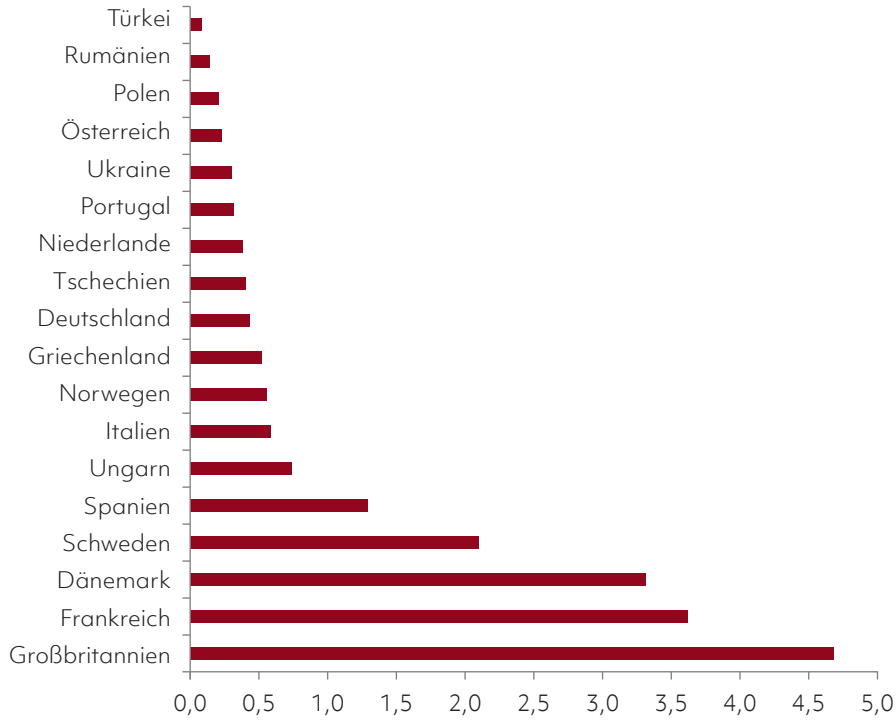
Abbildung 1: Verluste durch Kartenbetrug nur in wenigen Ländern rückläufig



Prozentuale Veränderung der Betrugsverluste durch Kreditkartenbetrug 2019 versus 2018

Quelle: Fico

Abbildung 2: Europäischer Kreditkartenbetrug – Verhältnis zu den Gesamtausgaben



Basispunkte – Verluste durch Kreditkartenbetrug in Cent pro 100 Euro

Quelle: Fico

Dafür gibt es weitere bewährte Mittel und Wege, mit denen effektiv gegen Kreditkartenbetrug vorgegangen werden kann. Gerade Machine Learning und Advanced Analytics helfen dabei, außergewöhnliche Verhaltensmuster von angeblichen Bankkunden, die beispielsweise auf Identitätsdiebstahl oder geklaute Kartendaten hinweisen, zu erkennen. So analysieren entsprechende Lösungen sämtliche Transaktionen in Echtzeit, um mögliche Kompromittierungen zu erkennen und den Betrug schon im Entstehen zu verhindern.

Tokenisierung hilft

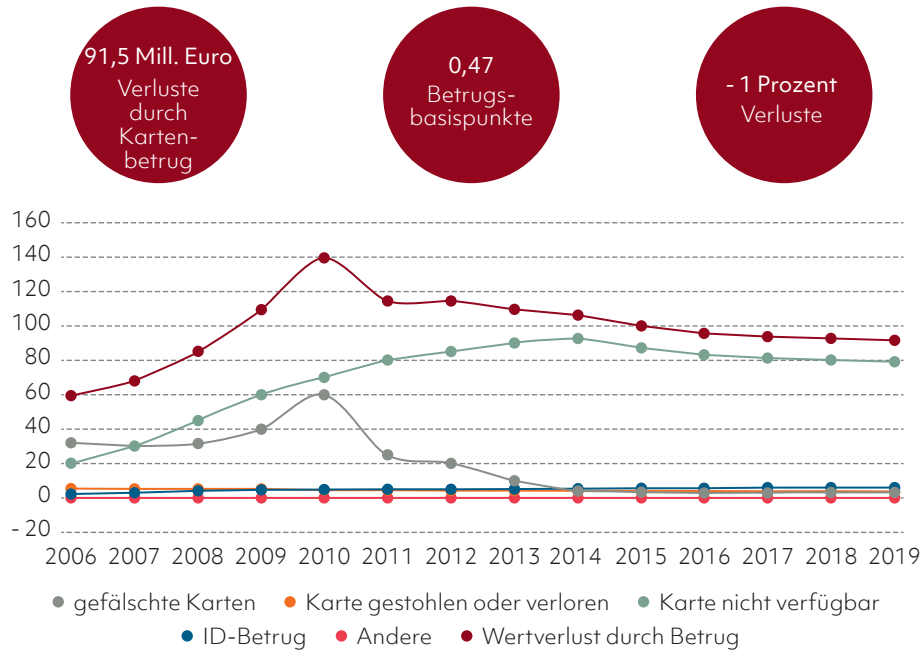
Ein weiteres Mittel gegen Kreditkartenbetrug kann das immer beliebter werdende kontaktlose Zahlen per Smartphone sein. Immerhin nutzten laut einer Umfrage der Postbank im August 2019 bereits elf Prozent der Deutschen das kontaktlose Bezahlen per Smartphone oder Smartwatch.[3)] Diese Zahl dürfte in den vergangenen zwölf Monaten noch einmal spürbar angestiegen sein.

Solche Zahlungsarten sind für Kriminelle aufgrund der eingesetzten Technik deutlich schwieriger anzugreifen. Denn sowohl Google Pay als auch Apple Pay – und andere Smartphone-Zahlungsmöglichkeiten auf NFC-Basis – nutzen für die Absicherung des Datenaustauschs die sogenannte „Tokenization". Hierbei wird jeder einzelne Zahlungsvorgang mit einem eigenen Einmal-Token geschützt, der zufällig erzeugt wird und direkt nach Beendigung des Vorgangs seine Gültigkeit verliert. Die Zahlungsvorgänge sind zudem so kryptografisch abgesichert, dass ein Abgreifen der NFC-Kommunikation (das sogenannte NFC-Grabbing) praktisch keine Aussicht auf Erfolg hat.

Nachdem aktuell das Betrugs-Reporting in ganz Europa im Rahmen von PSD2 immer noch im Standardisierungsprozess steckt, kann es tatsächlich noch ungeahnte Veränderungen in der europäischen Betrugslandschaft geben. Sicher ist jedoch, dass, während der Fokus aktuell noch auf Kreditkartenbetrug und vor allem dem sogenannten „Card not Present"-Betrug liegt, neue Bedrohungsszenarien vor allem im digitalen Finanzbereich verstärkt entstehen. Denn in vielen Ländern erfährt das digitale Banking allgemein hohe Wachstumsraten.

Betrachtet man die Zeit rund um die Weltfinanzkrise 2007/2008, ist ein starker gleichzeitiger Anstieg der Betrugsverluste erkennbar. Analog dazu führt auch die Rezession als Folge der Corona-Pandemie zu einem Anstieg von Betrugsdelikten. Einer der Gründe da-

Abbildung 3: Deutscher Kreditkartenbetrug – 2006 bis 2019 (in Millionen Euro)*



*Rot hervorgehoben: Werte 2019

Quelle: Fico

für ist, dass sich gerade in wirtschaftlich schwierigen Zeiten manche Menschen dazu verleiten lassen, sich zumindest in kriminellen Grauzonen zu bewegen und beispielsweise als sogenannte „Mules" oder Strohmänner zu arbeiten – also als Personen, die kriminell erworbenes Geld im Auftrag Dritter von einem Konto auf ein anderes transferieren – ein Akt der Geldwäsche. Gleichzeitig nimmt aber auch die Kreditkartennutzung aufgrund der wachsenden Beliebtheit des Online-Shoppings stark zu. Hier kann sich dann das altbekannte Sprichwort „Gelegenheit macht Diebe" bewahrheiten.

Betrugsmigration innerhalb Europas

Aber auch weitere Trends zeichnen sich ab: In Deutschland nehmen sogenannte Scams und Social Engineering stark zu. Es gibt hier viele Spielarten. Neben dem altbekannten „Enkeltrick" nutzen Betrüger etwa zunehmend detaillierte Kenntnisse über die Lebensumstände ihrer Opfer aus, die sie zuvor vor allem über deren Social-Media-Aktivitäten ausgespäht haben. So lassen sich nicht nur in vielen Fällen Passwörter zurücksetzen – die hier eingesetzten Sicherheitsfragen lassen sich teilweise schon mit einem Blick auf Facebook oder Instagram beantworten – so gewonnene Kenntnisse ermöglichen es den Betrügern darüber hinaus, sich beispielsweise als Handwerker auszugeben, wenn das Opfer gerade das Haus renoviert. Besonders perfide wird das Ganze, wenn sich die Ganoven – ganz aktuell – als Mitarbeiter des Reiseveranstalters ausgeben, wenn das Opfer sich gerade um eine Erstattung im Rahmen einer Stornierung aufgrund von Covid-19 bemüht.

Und dann ist da noch die Betrugsmigration innerhalb Europas: Wenn in einzelnen Ländern die Maßnahmen gegen Betrug verschärft werden, ist absehbar, dass die Kriminellen in Länder migrieren, wo das Sicherheitsniveau noch nicht so hoch ist. Wir dürfen also auf die weiteren Entwicklungen in Sachen Finanzbetrug sehr gespannt sein.

Fußnoten
1) https://www.fico.com/europeanfraud/
2) https://www.privacyaffairs.com/dark-web-price-index-2020/
3) https://www.der-bank-blog.de/kontaktloses-bezahlen-trend/studien/mobile-payment-studien/37656399/