Hans-Joachim Massenberg

Wie sicher sind **Online-Zahlungen?**

Monat für Monat erscheinen im Schnitt neun Millionen neue Schadsoftwareprogramme, mit denen kriminelle Hacker Online-Banking-Kunden deutscher Kreditinstitute angreifen wollen (Abbildung 1). Diese Zahl mag schockieren, doch die Kreditinstitute kommen dank schneller und flexibler Präventionsmaßnahmen sowie funktionierender Sicherheitssysteme gut mit dieser Herausforderung zurecht. Online-Banking ist und bleibt sicher und wird auch in der Bevölkerung – mit zunehmender Tendenz – als sicher wahrgenommen.

Dies spiegelt sich nicht zuletzt in steigenden Nutzerzahlen und in verschiedenen Umfrageergebnissen wider: Nach einer Erhebung des Bankenverbandes von Juni 2014 etwa nutzen 54 Prozent der Befragten Online-Banking; damit ist ihre Zahl gegenüber der vorherigen Befragung aus dem Jahr 2010 in allen Altersgruppen gestiegen. 50 Prozent aller Befragten finden Online-Banking sicher oder sehr sicher, 2010 waren es nur 35 Prozent. Von den Online-Banking-Nutzern selbst halten sogar 84 Prozent Online-Banking für sicher oder sehr sicher.

Online-Bezahlverfahren auf dem Vormarsch

Um Online-Einkäufe zu bezahlen (Abbildung 2), spielen die traditionellen Verfahren Überweisung, Lastschrift, Kreditkarte und Bargeld (bei Nachnahme) weiter eine große Rolle. Auf dem Vormarsch sind zudem sogenannte Internet-Bezahlverfahren (Abbildung 3), die sich häufig der üblichen Zahlverfahren als Grundlage bedienen. Ihr Umsatzanteil liegt derzeit lediglich bei 2,8 Prozent aller Online-Zahlungen, ihr Anteil an Bezahltransaktionen sogar nur bei 0,9 Prozent. Gleichwohl gaben 2014 55 Prozent der in einer Erhebung der Deutschen Bundesbank Befragten an, Internet-Bezahlverfahren im Online-Einkauf zu nutzen.

Wir sind uns sicher: Mit wachsender Bedeutung des E-Commerce wird auch der Bedarf nach Zahlverfahren für den Online-Einkauf weiter steigen. Wenn auch ihr Umsatzniveau gegenwärtig noch immer vergleichsweise gering ist, so hat dieses doch in jüngster Zeit stark zugenommen. Der Umsatz im stationären Handel hingegen verharrt auf relativ konstantem Niveau. Diese Entwicklung wird noch unterstützt durch die zunehmende Konvergenz von E-Commerce und stationärem Handel, da immer mehr Händler ihre Waren sowohl online als auch im Ladengeschäft anbieten. Dabei verschwimmt die Grenze zwischen den Absatzwegen zusehends.

Neue Wettbewerber, neue Regeln

Das starke Wachstum im E-Commerce und die zunehmende Konvergenz von Online- und stationärem Handel haben den Aufstieg neuer Verfahren und neuer Anbieter befördert, auch von Nichtbanken. Solche Drittdienste sind bis heute nicht gesondert reguliert, werden aber – richtigerweise – mit der gerade novellierten EU-Zahlungsdiensterichtlinie (PSD II) in das Zahlungsdiensteaufsichtsrecht miteinbezogen. Die PSD II soll noch 2015 in Kraft treten und wird dann binnen zwei Jahren in das nationale Recht umzusetzen sein.

Sie führt drei neue Kategorien von Dienstleistern ein: Zahlungsauslösedienste, Kontoinformationsdienste und Drittherausgeber von Zahlungsinstrumenten. Um diesen Diensten europaweit einen Zugang zu ermöglichen, müssen ihnen die Kreditinstitute eine neue standardisierte Kontoschnittstelle bereitstellen. Mit der neuen Zahlungsdiensterichtlinie dürfte der Zugang der Kunden zum Online-Banking aufgrund von Sicherheitsvorgaben aufwändiger werden, denn schon der Log-in zum Konto muss dann mit einem Einmal-Token, zum Beispiel mit einer TAN, erfolgen.

Online-Sicherheit heute – ein Gesamtpaket

Doch wie sieht der Zugang zum Konto heute aus? Und wie bekommen Banken und Sparkassen die anfangs genannten neun Millionen neuen Schadsoftwareprogramme in den Griff, die Monat für Monat auf ihre Sicherheitssysteme und ihre Kunden losgelassen werden? Die heute im Wesentlichen eingesetzten Legitimationsverfahren – und damit Sicherheitsverfahren –

Dr. Hans-Joachim Massenberg, Mitglied der Hauptgeschäftsführung, Bundesverband deutscher Banken e. V., Berlin

Das Vertrauen der deutschen Kunden in die Online-Banking-Angebote der Kreditinstitute wächst. Zu Recht, meint der Autor. Mit Blick auf das Aufkommen neuer Verfahren und Anbieter bei Zahlungen im E-Commerce begrüßt er die EU-Zahlungsdiensterichtlinie PSD II. Und sieht mit ihr dennoch auch Gefahren verbunden: Mit Ausweitung des Zugangs zum Bankkonto durch Drittdienste könnte in seinen Augen die Zahl der versuchten Angriffe allein deshalb schon zunehmen, weil Kunden sich in manchen Fällen schwertun dürften, legitime Drittdienste von kriminellen Pseudodienstleistern zu unterscheiden. Und schon heute ist das sogenannte Social Engineering, ein für Betrüger oftmals viel versprechender Weg, bei dem beispielsweise durch das Vortäuschen falscher Tatsachen der Kunde zur Herausgabe persönlicher Zugangsdaten verleitet wird. Hier helfe nur Prävention und Information des Kunden. (Red.)

sind iTAN, mobileTAN (TAN als SMS auf Mobiltelefon), chipTAN (TAN-Generator), photoTAN (als App wie mit Zusatzgerät) und nun auch beginnend die Biometrie.

Die Gesamtsicherheit eines Legitimationsverfahrens besteht dabei nicht nur aus dem für den Kunden sichtbaren Teil wie der iTAN, der chipTAN oder der photoTAN. Es kommt vor allem auch auf eine agile, intelligente Hintergrundsicherheit an. Mit anderen Worten: Das Sicherheitspaket wird geschnürt aus den für den Kunden sicht- und anwendbaren Verfahren („Front End") und den Hintergrundsystemen der Banken („Back End"). Die Komponenten müssen passen und zusammenwirken, sodass das Gesamtsystem die Vielzahl der Angriffe auf die Kunden parieren kann.

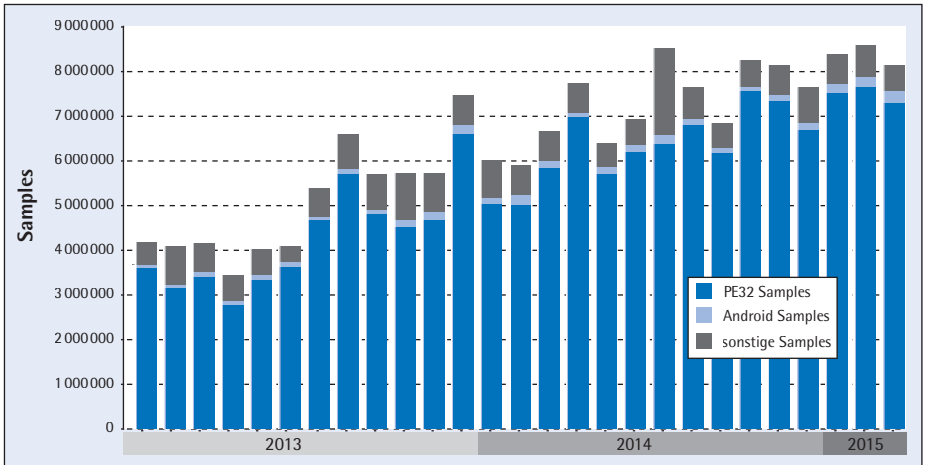
Hauptangriffsziel Endanwender

Aus eigenen Untersuchungen ist bekannt, dass die Schäden im Online-Banking in Deutschland nur einen Basispunkt ausmachen – also nur 0,01 Prozent des jeweiligen Transaktionsvolumens. Dieses vergleichsweise geringe Ausmaß der Schäden ist ganz wesentlich auf die Sicherheitsmaßnahmen zurückzuführen. Das „Gesamtpaket Sicherheit" funktioniert, nicht nur beim Front End der Kunden.

Wenn es Attacken gibt, sind der Endanwender und seine Computer- (oder Smartphone-)Ausrüstung Hauptangriffsziel für die Kriminellen. Angegriffen wird vor allem durch Social Engineering: Falsche Tatsachen werden dem Bankkunden vorgetäuscht und sollen ihn zu unüberlegten Handlungen wie die Herausgabe geheimer Zugangsdaten verleiten. Zum Social Engineering gehört aber auch die heimliche Installation von Schadsoftware auf Mobiltelefonen und Rechnern oder die Durchführung einer gefälschten „Testüberweisung".

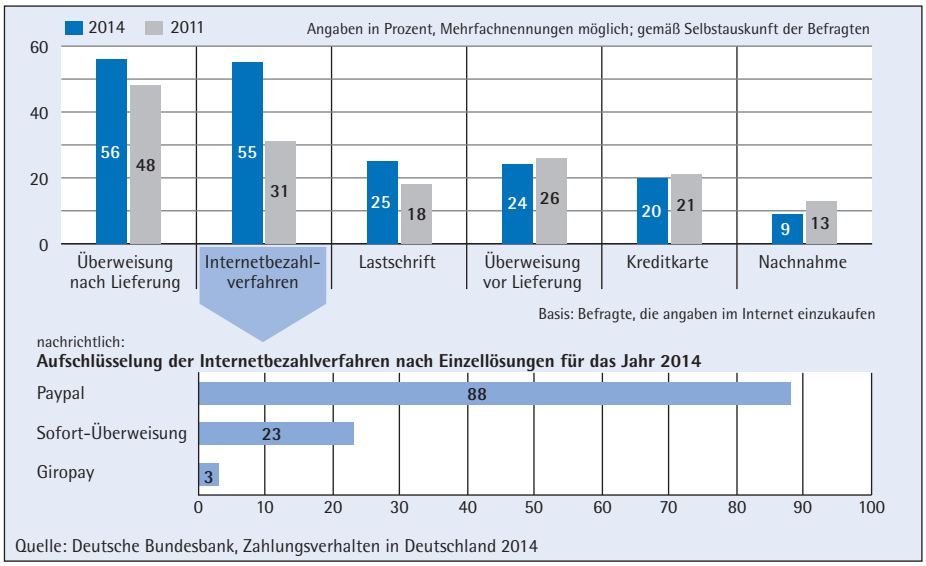
Hinzu kommt, dass die Kriminellen mangelnde Sorgfalt und Sicherheitsvorsorge beziehungsweise technische Schwachstellen mit Schadsoftware ausnutzen. In der Praxis wird zumeist eine Kombination beider Elemente – Social Engineering und Schadsoftware – benutzt. Zusätzlich greifen die Kriminellen Begleitprozesse des Online-Banking an, um an Geheimnisse heranzukommen. Beispiele sind der Postweg (zum Beispiel der Diebstahl von Initialisierungsbriefen durch Aufbrechen des

Abbildung 1: Spot – Angriffe auf Online-Banking-Kunden – annähernd 9 Millionen neue Schadsoftwaren pro Monat



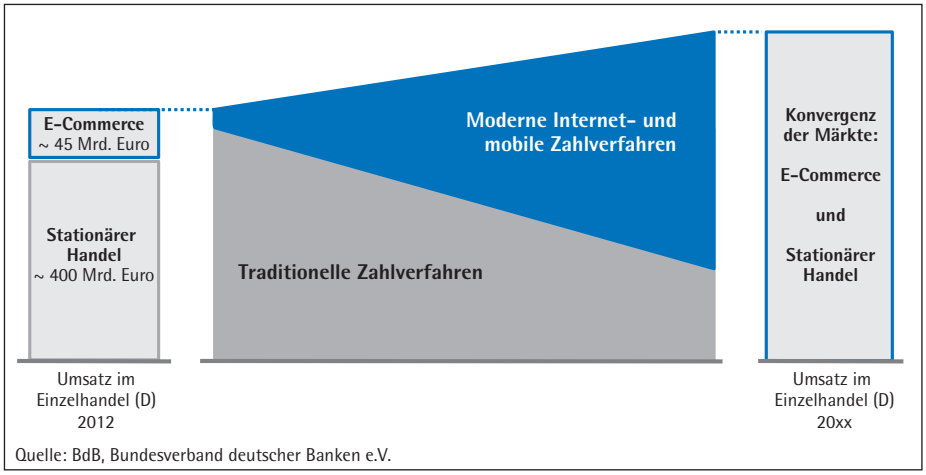
Quelle: BdB, Bundesverband deutscher Banken e.V.

Abbildung 2: Bezahlen beim Online-Einkauf 2014 und 2011



Quelle: Deutsche Bundesbank, Zahlungsverhalten in Deutschland 2014

Abbildung 3: Internetbezahlverfahren wird große Zukunft vorausgesagt



Quelle: BdB, Bundesverband deutscher Banken e.V.

Tabelle: Moderne Online-Zahlverfahren erfüllen zugleich Anforderungen von Käufern und Händlern

	Moderne Online-Zahlverfahren	Traditionelle Zahlverfahren			
		Kreditkarte	Vorkasse	Lastschrift	Rechnung
Einfach	• Ein Passwort, ein Klick, fertig • ID vorausgefüllt • Lieferanschrift-hinterlegt	• Händische Eingabe von Kreditkarten-daten • ... jedoch reagie-ren Schemes	• Onlinebezahlung mit mehreren Eingabefeldern • Alternativ unbequeme Offline-Zahlung	Händische Eingabe von Bankdaten erforderlich	• Nach Erhalt Ware: • Onlinebezahlung mit mehreren Eingabefeldern • ... Alternativ unbequeme Offline-Zahlung
Sicher für Käufer	Käufer erhält bei Betrug oder Nicht-lieferung Geld zurück	Käufer erhält bei Betrug oder Nichtlieferung Geld zurück	kein Käuferschutz - Käufer nach Bezahlung „auf sich allein gestellt"	8 Wochen Rück-buchungsmöglich-keit für Käufer	Käufer durch nach-trägliche Zahlung vollständig geschützt
Sicher für Händler	Händler hat Zahlungsgarantie mit einigen Aus-nahmen	In der Regel nur wenige Rück-buchungen	Händler voll-ständig geschützt	Händler mit Risiko der Rückbuchung	Keine Absicherung des Händlers (Forde-rungskauf kosten-intensiv)
Sofort	Händler und Käufer erhalten Realtime-Bestätigung	Kreditkartenzah-lung durch Bank-autorisierung sofort für Kunde und Händler bestätigt	Händler erhält Bestätigung mit unregelmäßiger Verzögerung	Keine sofortige Bestätigung	Händler hat bei Versand der Ware noch keine Bestäti-gung der Zahlung

Quelle: Bundesverband deutscher Banken e.V.

Briefkastens) oder Prozesse der Telefongesellschaften (etwa zur Bestellung von Dubletten-SIMs).

Prävention und Information

Es ist zu befürchten, dass mit der Ausweitung des Zugangs zum Bankkonto durch Drittdienste aufgrund der PSD II die Zahl der Angriffsversuche steigen könnte. Warum? Zwar wird durch die neue Aufsicht über Drittdienste auf den ersten Blick die Sicherheit von Internetbezahlverfahren erhöht. Doch könnten Kriminelle versuchen, sich per Social Engineering als legitimierter Drittdienst auszugeben und dies für Angriffe ausnutzen, da viele Nutzer legitime Drittdienste kaum von kriminellen „Pseudo-Drittdiensten" unterscheiden können. Sollte dieses Szenario eintreten, werden Institute und beaufsichtigte Drittdienste gemeinsam handeln müssen.

Als A und O gegen Social Engineering helfen Prävention und Information des Kunden. Hierzu hat der Bankenverband verschiedene Broschüren veröffentlicht, die online und offline erhältlich sind:

- Dubioses Stellenangebot: Finanzagent (Juli 2014)
- Wie schütze ich mich vor Phishing? (August 2014)
- Online- und Mobile-Banking – sicher über Browser und App (September 2014)
- Vorsicht: Betrug per Telefon (März 2015)

Im Sinne ihrer Kunden stellen die Bankverfahren den Faktor Sicherheit eindeutig in den Vordergrund. Sie kommen damit aber auch einer Auflage der Bankenaufsicht (BaFin) nach, die unabhängig von der Risikoeinschätzung der Bank und der Risikoklasse einer Transaktion sichere Verfahren fordert: Transaktionen über 30 Euro müssen genauso abgesichert werden wie über 5 000 Euro. Demgegenüber weisen moderne Online-Zahlverfahren oft Praktikabilitätsvorteile für Käufer und Händler auf, die mit den Schlagwörtern „einfach, sicher, sofort" beschrieben und beworben werden (Tabelle).

Da sie perspektivisch zusätzliche Dienstleistungen in das Online-Zahlverfahren integrieren werden (beispielsweise Rabattsysteme, Finanzierungsangebote), dürfte ihre Attraktivität künftig noch zunehmen. Klar ist: Die Kunden haben berechtigte Erwartungen an Online-Zahlungen. Sie wollen nicht mit Sicherheitsmaßnahmen „belästigt" werden, gleichwohl nicht auf Sicherheit verzichten. Sie wollen sich einfach und schnell registrieren und genauso einfach und schnell bezahlen können.

Alle diese Anforderungen erfüllt das neue Bezahlverfahren der deutschen Banken und Sparkassen mit dem Namen „Paydirekt", das bis Ende 2015 an den Start gehen soll und in dem das Girokonto der Kunden eine Schlüsselrolle spielt. Das neue mobile Bezahlverfahren bietet gleichermaßen Sicherheit und Benutzerfreundlichkeit für Käufer und Händler. Dadurch, dass die deutschen Banken und Sparkassen an einem Strang ziehen, wird zudem eine wettbewerbsfähige Bezahllösung mit einem großen, der Bank oder Sparkasse bereits bekannten Nutzerkreis angeboten.

Als Sicherheitspaket bietet Paydirekt ein adaptives Authentifizierungsverfahren, das neben dem Sicherheitsmerkmal „Wissen" (geheimes Kennwort des Benutzers, in Kombination „Benutzername + Passwort") dynamisch den zweiten Sicherheitsfaktor „Besitz" beisteuert. So wird schon heute sichergestellt, dass das Verfahren entsprechenden regulatorischen Vorgaben der BaFin entspricht. Für das Merkmal „Besitz" kann das dem Benutzer bekannte Verfahren aus dem jeweiligen Online-Banking seiner Bank (dezentrale 2-Faktor-Authentifikation) oder alternativ ein von Paydirekt zur Verfügung gestelltes Verfahren (zentrale 2-Faktor-Authentifikation) genutzt werden.

Zusammenfassend lässt sich sagen: Der Kunde ist heute überall im Internet unterwegs, nutzt dort einfache Zugangsmechanismen und verlangt deshalb von den Banken nicht nur ein vertrauenswürdiges und sicheres, sondern auch ein schnelles und einfaches Banking. Hier bietet sich den Banken die Chance, kundenorientierte Angebote zu gestalten, die maßgeschneidert ins Zeitalter der Digitalisierung passen.

In diesem Zusammenhang ist es wichtig, dass für alle Marktteilnehmer im Zuge der neuen Regulierung EU-weit gleiche Anforderungen gelten. Ungeachtet dessen aber gilt nach wie vor: Vertrauen in die Sicherheit, Stabilität und Zuverlässigkeit ihrer Online-Verfahren ist das Asset der Banken! Kunden können ihr Geld mit Banken seit Jahrzehnten sicher transferieren und werden dies auch weiterhin tun. Es bleibt also dabei: Online-Zahlungen sind sicher.

Dieser Beitrag basiert auf einer Rede des Autors beim Zahlungsverkehrssymposium 2015 der Deutschen Bundesbank am 15. Juni 2015 in Frankfurt am Main. Zwischenüberschriften sind teilweise von der Redaktion eingefügt. Die vollständige Präsentation des Autors zum Redebeitrag kann unter www.bundesbank.de oder www.kreditwesen.de abgerufen werden.