Rabobank: **Visuelle** Authentifizierung vor dem **Rollout**

Von Swantje Benkelberg

Bei der niederländischen Rabobank geht die Umstellung auf ein neues Sicherheitsverfahren in die letzte Runde: Mit der Auslieferung des sogenannten Rabo-Scanners stellt die Bank flächendeckend auf ein Verfahren um, das in Deutschland bei einigen Banken unter dem Namen Photo TAN bekannt ist und auf dem Einscannen eines farbigen QR-Codes basiert, in dem die Transaktionsdaten verschlüsselt sind. Genutzt werden kann das Verfahren nicht nur im Online-Banking der Bank, sondern auch für das Online-Überweisungsverfahren Ideal, das dem deutschen Giropay entspricht.

Man-in-the Middle-Angriffe, Man-in-the Browser-Attacken, Angriffe auf SMS-basierte Lösungen mit Einmalpasswörtern - das Online Banking ist seit jeher ein attraktives Ziel für professionelle Hacker jeglicher Couleur. Hier befinden sich Kreditinstitute in einem steten Wettlauf mit der kriminellen Szene. Denn je ausgefeilter die Sicherheitsverfahren werden, desto ausgefeilter werden auch die Angriffe, die die Hacker entwickeln. Das gilt auch für Multi-Kanal-Lösungen zur Authentifizierung und digitalen Signatur

Bei dem Wettrennen haben Anbieter von Authentifizierungslösungen gegenüber den Hackern ein Manko: Ihre Lösungen müssen nicht nur funktionieren, sprich die jeweils aktuellen Angriffe abzuwehren in der Lage sein. Sie müssen auch noch benutzerfreundlich und einfach zu bedienen sein, denn sonst werden sie von den Bankkunden schlicht nicht akzeptiert.

Die niederländische Rabobank hat aus diesem Grund ein neues, visuelles Verfahren zur Authentifizierung im Online-Banking eingeführt, das höchste Sicherheit mit einer sehr einfachen und komfortablen Handhabung vereinen soll. Dabei wird der bisher genutzte und als ähnlich sicher geltende Random Reader abgelöst durch den sogenannten Rabo Scanner, der noch einfacher zu bedienen ist und weniger Eingaben vom Kunden verlangt.

Bei Commerzbank, Comdirect und Deutscher Bank läuft das nun von den Niederländern eingeführte Verfahren unter „Foto TAN" – nur mit dem Unterschied, dass hier ein separates Gerät zwar angefordert werden kann, jedoch erforderlich ist. Stattdessen funktioniert die Photo TAN auf mobilen Endgeräten bei deutschen Banken in Verbindung mit einer separaten App.

Die Rabobank hingegen setzt auf ein „Rabo Scanner" genanntes Gerät von Vasco, das bei dem Unternehmen auch unter dem Produktnamen Digipass läuft. Dabei ist die neueste Gerätegeneration mit einem Farbbildschirm und einer Kamera auf der Rückseite ausgerüstet.

Grundlage des Verfahrens ist die sogenannte Cronto-Sign-Technologie. Sie basiert auf einem farbigen QR-Code der nächsten Generation, in dem sämtliche Transaktionsdaten kodiert sind. Sie sollen von einem Angreifer weder ausgelesen noch verändert werden können.

Farbiger QR-Code als Grundlage

Das quadratische Feld mit dem QR-Code erscheint während einer Transaktion auf dem Bildschirm des Smartphones, Tablets oder PCs des Kunden. Dieser fotografiert die Grafik mit dem Rabo Scanner ab. Danach werden Transaktionsdaten wie Empfänger oder Betrag dekodiert und im Klartext auf dem Bildschirm des für die Transaktion genutzten Endgeräts angezeigt, sodass sie noch einmal überprüft werden können. Der Rabo Scanner generiert ein Einmalpasswort, das der Kunde an seinem Computer, Tablet oder Smartphone eingibt, um die Transaktion zu autorisieren. Sollten die angezeigten Transaktionsdaten von den vermeintlich eingegebenen abweichen, kann der Kunde die Transaktion abbrechen und es erneut probieren. Eine erneute Abweichung ist dann allerdings ein deutliches Zeichen für einen Betrugsversuch.

Um die Sicherheit dieses Verfahrens zu maximieren, verfügt der Rabo Scanner zudem über einen integrierten Kartenleser, in die der Kunde seine Bankkarte einstecken muss. Zudem muss er dabei die

entsprechende PIN in den Scanner eintippen. Das für die Authentifizierung benötigte Geheimnis liegt wie bei dem in Deutschland weit verbreiteten Sm@rt-TAN plus/optic-Verfahren auf dieser Karte und nicht im Scanner, so dass ein Rabo Scanner auch für mehrere Konten oder von mehreren Personen verwendet werden kann. Dies erhöht zum einen den Komfort für den Kunden und reduziert zum anderen die Kosten der Bank.

Fünf Anwendungsmöglichkeiten im Online-Banking

Da der Rabo Scanner ebenso wie sein Vorgänger Random Reader – eine klassische Kartenleser-Lösung – ein separates Gerät und nicht mit dem Internet verbunden ist, kann er von Angreifern und Hackern nicht kompromittiert werden.

Auch zum Gerät mit der Banking-Anwendung besteht keinerlei Verbindung, sodass diese Lösung selbst bei einem kompromittierten PC sicher ist. Damit reduziert der Rabo Scanner das Risiko von Man-in-the-Middle-Attacken und Malware und bietet sowohl dem Kunden als auch der Bank die Sicherheit, dass Zahlungsanweisungen nicht verändert wurden.

Im Online- und Mobile-Banking dient der „Rabo Scanner" fünf verschiedenen Zwecken:

- Sicherer Login in die Bankanwendung,
- Signieren von Aufträgen und Transaktionen im Internet- und Mobile Banking,
- Signieren von Verträgen über das o Internet Banking,
- Bestätigung von Änderungen im Internet Banking und
- Bestellen von Produkten im Rabo Internet Banking,

Auch zur Autorisierung von Transaktionen mit Ideal

Zudem kann er auch eingesetzt werden, um Kreditkartenzahlungen oder Zahlungsanweisungen über die in den Niederlanden sehr populäre Zahlungsplattform Ideal über das Online-Banking zu signieren. Ideal ermöglicht es Online-Händlern und ihren Kunden, Zahlungen in Echtzeit und unwiderruflich über das Konto des Kunden bei einer der angeschlossenen Banken abzuwickeln. Damit ist es dem deutschen Giropay vergleichbar. Es hat sich jedoch deutlich besser am Markt durchgesetzt, sodass es durchaus sinnvoll scheint, auch diese Transaktionen mit der neuen Technologie abzusichern.

Da die neue Authentifizierungslösung bereits beim Login in die Bankanwendung greift, sind Kunden, die bereits den Rabo Scanner einsetzen, nicht nur vor betrügerischen Eingriffen in ihre Transaktionen gefeit. Anders als bei Lösungen mit einer statischen PIN, die ausgespäht werden kann, bleiben auch persönliche Informationen wie etwa der Kontostand vertraulich.

Um die Benutzerfreundlichkeit weiter zu erhöhen, sind zwei Anwendungen von der Zwei-Faktor-Authentifizierung ausgenommen: Die Eröffnung eines neuen Kontos und Überweisungen zwischen zwei Konten des gleichen Kunden.

Handelsübliche Batterien

Dass der Rabo Scanner mit handelsüblichen Batterien arbeitet, die der Kunde bei Bedarf einfach selbst auswechseln kann, nützt der Bank und den Kunden gleichermaßen. Zum einen erspart es der Bank den Austausch des Gerätes, wenn eine geräteimmanente Batterie sich erschöpft. So verlängert sich dessen Lebensdauer. Dem Kunden erspart der Batteriewechsel das Anfordern eines neuen Gerätes und – im ungünstigsten Fall – eine Phase, in der er keine Online-Transaktionen mehr ausführen kann, weil die Batterien des alten Gerätes aufgebraucht ist, ein neues jedoch noch nicht vorliegt. Wann der Batteriewechsel erforderlich ist, signalisiert eine integrierte Anzeige.

Für internationale Kunden lässt sich der Rabo Scanner auch auf eine Bedienung in englischer Sprache umstellen.

18 Monate für den Rollout

Mit der Entscheidung für das neue visuelle Authentifizierungsverfahren traf die Rabobank auch die Entscheidung, dass der Rabo Scanner den bisher genutzten Random Reader komplett ersetzen sollte, sodass nur eine Lösung unterhalten und gewartet werden muss. Der Aufwand dafür ist beträchtlich: Alle 5,4 Millionen Exemplare des Vorgängermodells Random Reader müssen ausgetauscht werden. Weil vermutlich nur so die Akzeptanz beim Kunden gegeben ist, erhalten alle Kunden den neuen Leser kostenfrei.

Als Zeitplan für den Rollout wurde im September 2014 ein Zeitraum von 18 Monaten angegeben. Der Rollout begann im Januar 2015, und schon am Ende der dritten Januarwoche waren 250 000 Rabo Scanner an Privatkunden ausgegeben. Seit Februar werden pro Woche 125 000 Stück

versandt. Seit März wird der Scanner auch an Geschäftskunden ausgeliefert.

Der Übergang vom alten Kartenleser auf die neue Lösung ist dabei fließend. Kunden können das Vorgängermodell weiter benutzen, bis sie den neuen Robo Scanner erhalten haben. Wie es bei der Einführung neuer Sicherheitsstandards fast schon üblich ist, kursierten schon wenige Tage nach der Ankündigung der Umstellung auf das neue Verfahren Phishing-Mails und existierten gefälschte Webseiten, über die Bankkunden angeblich den Rabo Scanner anfordern konnten – natürlich gegen Preisgabe ihrer Login-Daten. Wie viele Kunden darauf hereingefallen sind, dazu macht die Bank keine Angaben. Sie hat jedoch wiederholt darauf hingewiesen, dass die Kunden nicht selbst aktiv werden müssen. Vielmehr werden sie automatisch benachrichtigt, wenn ihr Online-Banking auf die neue Lösung umgestellt wird.

Alter Leser automatisch deaktiviert

Zunächst bekam beziehungsweise bekommt jeder einzelne Kunde per Briefpost ein Schreiben mit allen notwendigen Informationen einschließlich des Termins seiner eigenen Umstellung. Sobald der Rabo Scanner versandt wird, findet der Kunde eine entsprechende Mitteilung in seiner persönlichen Mailbox innerhalb der Bankanwendung.

Der Scanner selbst wird von einem weiteren Brief begleitet, mit dem dem Kunden mitgeteilt wird, zu welchem Datum sein bisher genutzter Kartenleser deaktiviert wird. Das soll spätestens 35 Tage nach Erhalt des Rabo Scanners der Fall sein. Sobald der Kunde den neuen Scanner zum ersten Mal nutzt, wird der alte Kartenleser unverzüglich deaktiviert und der Kunde kann nur noch das neue Gerät nutzen. So soll ein schneller und kompletter Übergang sichergestellt und verhindert werden, dass Kunden weiterhin die alte Lösung nutzen.