Mobile-Banking-Sicherheit erfordert neue Strategien

Von Marc T. Hanne

Die Sicherheitskonzepte für das klassische Online-Banking lassen sich nur bedingt auf das Mobile Banking übertragen. Deshalb müssen neue, mehrstufige und mobilzentrierte Ansätze entwickelt werden, so der Autor. Sie müssen die richtige Balance zwischen Sicherheit und Nutzerfreundlichkeit finden. Das wiederum heißt: Die meisten Authentifizierungsvorgänge müssen im Hintergrund stattfinden. Red.

Das Bedrohungspotenzial von Cyber-Attacken nimmt kontinuierlich zu. Vor allem auch mobile Geräte stehen zunehmend im Fokus der Angreifer. Mobile Anwendungen mit sicherheitskritischem Charakter müssen deshalb umfassend geschützt werden. Ein wichtiger Bereich ist dabei das Mobile Banking.

Smartphones und sonstige smarte Geräte sind aus dem täglichen Leben nicht mehr wegzudenken. Ihre Funktionsvielfalt hat inzwischen ungeahnte Ausmaße angenommen und kontinuierlich kommen neue mobile Anwendungen hinzu. Ein Bereich, der momentan stark wächst, ist das Mobile Banking. Es bietet zwei entscheidende Vorteile: Zum einen können Anwender ihre Bankgeschäfte in deutlich komfortablerer Weise erledigen und zum anderen können Banken den mobilen Kanal für die enge Kundenkommunikation nutzen.

Gemäß einer Studie der internationalen Managementberatung Bain & Company ist die Zahl der Mobile-Banking-Nutzer in Deutschland von 2012 bis 2015 von fast null auf rund 20 Prozent gestiegen*. Der Trend wird sich fortsetzen, vor allem dann, wenn die von Verbrauchern heute noch verschiedentlich geäußerten Sicherheitsbedenken bei Bankgeschäften mittels mobiler Geräte ausgeräumt werden können.

Für den weiteren Erfolg des Mobile Banking ist es folglich von essenzieller Bedeutung, dass Finanzinstitute das Thema Sicherheit stärker in den Vordergrund rücken. Gefragt sind proaktive Schritte der Banken bei der Konzeption und Umsetzung neuer, strikter Sicherheitsstrategien und -richtlinien. Die von der EU verabschiedete und am 13. Januar 2018 in Kraft tretende „Payment Services Directive 2" (PSD2) wird ihr übriges dafür tun, den Druck auf Finanzdienstleister zu erhöhen, die Sicherheit ihres Online-Banking-Angebotes zu überprüfen, wird doch in der Richtlinie nicht nur der Internet Zahlungsverkehr neu geregelt, sondern starke Mehr-Faktor-Authentifizierung als obligatorisch eingeführt.

Zum Autor

Marc T. Hanne, Director of Sales, IAM Solutions DACH, CEE & Middle East, HID Global GmbH, Walluf

Mobil-zentrierter Sicherheitsansatz gefragt

Finanzinstitute haben in der Vergangenheit große Investitionen getätigt, um effiziente Security-Frameworks für das herkömmliche Online-Banking zu realisieren. Auf das Mobile Banking lassen sie sich allerdings nicht eins zu eins übertragen. Hier sind spezifische Herausforderungen zu beachten, vor allem hinsichtlich der starken Zunahme von Malware, die gerade Mobilgeräte adressiert. Wenn somit lediglich bestehende Online-Banking-Infrastrukturen und -Tools für das Mobile Banking genutzt werden, sind unweigerlich hohe Sicherheitsrisiken in Kauf zu nehmen. Es ist deshalb zwingend erforderlich, einen neuen Mobil-zentrierten Sicherheitsansatz zu wählen.

Im Mobile Banking muss bei der Festlegung einer Sicherheitsstrategie zunächst berücksichtigt werden, dass ein mobiles Gerät jederzeit abhandenkommen kann, zum Beispiel durch Diebstahl. Zudem ist zu beachten, dass mobile Anwendungen vor allem dann genutzt werden, wenn sie komfortabel zu verwenden sind. Anwender erwarten einen einfachen Zugriff auf Apps, Services und Inhalte, wobei eine hohe Sicherheit „quasi im Hintergrund" standardmäßig gewährleistet sein sollte. Deshalb

ist es extrem wichtig, die richtige Balance zwischen Security und User Experience zu finden.

Gefahren durch neue Nutzungsmöglichkeiten

Die vielfältigen Nutzungsmöglichkeiten mobiler Geräte bringen gleichzeitig zahlreiche Sicherheitsgefahren mit sich.

- Anwender öffnen E-Mails und Dateianhänge aus unbekannten Quellen, besuchen nicht vertrauenswürdige Webseiten und laden beliebige Apps herunter.

- Erschwerend kommt hinzu, dass vielfach die gleichen Login-Daten und Passwörter für unterschiedlichste Webseiten oder Anwendungen genutzt werden.

Dadurch sind mobile Geräte einer Vielzahl von Sicherheitsbedrohungen ausgesetzt, beispielsweise Phishing, Malware oder Social Engineering. Auch die zunehmende Nutzung öffentlich zugänglicher WLAN-Hotspots trägt unbeabsichtigt zu einer Bedrohung der Gerätesicherheit bei.

Sicherheit auf mehreren Ebenen

Um sichere Mobile-Banking-Services bereitzustellen und das Kundenvertrauen in die Sicherheit bei Bankgeschäften zu erhöhen, sind mehrstufige Sicherheitslösungen unverzichtbar. Sie müssen alle potenziellen Gefahren bei Transaktionen berücksichtigen und damit auch alle möglichen Angriffspunkte: Dazu gehören das Frontend, also das Anwendergerät, und das Backend, also die Bankanwendung, die die Legitimierung von Anwenderanfragen über mobile Geräte übernimmt, sowie der Kommunikationsweg. Doch was muss eine Sicherheitslösung für das Mobile Banking konkret bieten? Sechs Punkte sind entscheidend:

1. Unterstützung eines integrierten, mehrstufigen Sicherheitsansatzes: Mobile-Banking-Anwender wollen auch dann geschützt bleiben, wenn ihr Verhalten vielleicht nicht im Einklang mit Cyber Security Best Practices steht. Lösungen müssen deshalb mehrere Authentifizierungsmethoden unterstützen, um Kunden zweifelsfrei identifizieren zu können. Zudem muss eine End-to-End-Sicherheit hinsichtlich Gerät, Applikation, Verbindung und Backend-Server gewährleistet sein.

2. Einfache Festlegung und Konfiguration mehrerer Authentifizierungsmethoden für verschiedene Anwendungsfälle: Eine Lösung sollte flexibel konfigurierbar und mandantenfähig sein sowie beliebige Kombinationen von Authentifizierungsmethoden für unterschiedliche Kanäle, Nutzergruppen oder Bankgeschäfte ermöglichen. Mit einer solchen Lösung kann ein Finanzinstitut auch die Kosten gering halten, da alle Authentifizierungsanforderungen über eine einzige Plattform verwaltet werden können.

3. Mobile Application Security: Die Malware-Attacken auf mobile Applikationen nehmen kontinuierlich zu, Lösungen im Bereich Mobile Application Security müssen deshalb standardmäßig integriert sein. Sie sollten neben bekannten Verfahren zur Sicherung mobiler Applikationen unter anderem auch eine Erkennung von Debuggern, Emulatoren, Manipulationen und Code-Verschleierungen bieten.

4. Threat Intelligence zur Erkennung potenzieller Probleme auf Basis von Risikoanalysen vor und nach der Infizierung von Systemen und Anwendergeräten: Eine zukunftsweisende Mobile-Security-Lösung erkennt sowohl bekannte als auch neu auftretende Bedrohungen und nutzt Kontextinformationen wie das übliche Anwenderverhalten, Gerätekonfigurationen oder Bedrohungsprofile.

5. Strikte Compliance-Frameworks: Compliance-Regelungen sind wesentlich mehr als vorgeschriebene Methoden für das erfolgreiche Absolvieren jährlicher Audits. Die Konformität mit Anforderungen wie PSD2 und den PCI-DSS (Payment Card Industry Data Security Standard)-Vorgaben erhöht auch das Sicherheitsniveau des Mobile Banking, reduziert die Risiken der Bank und steigert das Vertrauen der Kunden. Zu beachten ist, dass die gewählte Mobile-Banking-Lösung Compliance-Frameworks als integrierte Funktion unterstützen sollte und nicht als Add-on.

Authentifizierung im Hintergrund

6. Starke Authentifizierung ohne Beeinträchtigung der User Experience: Einerseits ist es auf jeden Fall sinnvoll, eine Zweifaktor oder sogar Mehrfaktor-Authentifizierung für die Mobile-Banking-Sicherheit zu nutzen, andererseits ist aber zu berücksichtigen, dass der Anwender auch nicht zu viel Zeit für die Überprüfung seiner Identität und Zugriffsrechte bei der Abfrage seines Kontostands oder bei der Durchführung einer Überweisung verlieren will. Die Kundenbeeinträchtigung kann ohne Abstriche hinsichtlich der Sicherheit minimiert werden, indem die meisten Authentifizierungsverfahren „im Hintergrund" laufen, sodass Anwenderaktivitäten bei der Authentifizierung nur dann erforderlich sind, wenn sie aufgrund der Sicherheitsrichtlinien oder des Risikoprofils absolut nötig sind.

Mobile Banking wird weiter an Popularität gewinnen. Eine wichtige Voraussetzung für den durchschlagenden Erfolg wird aber sein, dass Finanzinstitute die Entwicklung und Implementierung von mehrstufigen Mobile-Security-Strategien weiter vorantreiben. Nur so können die Gefahren für Kundendaten minimiert und Reputationsverluste im Fall eines Sicherheitsvorfalls vermieden werden. Die Herausforderung für Banken liegt dabei darin, eine Lösung zu finden, die einerseits hohe Sicherheit garantiert, andererseits aber auch eine positive User Experience bietet. Schließlich wird die Akzeptanz der Nutzer das ausschlaggebende Kriterium für den Erfolg oder Misserfolg von Mobile-Banking-Verfahren sein.

Fußnote

* http://www.bain.de/press/press-archive/privatkunden-geschaeft-banken-machen-mobil.aspx