Wie sicher ist das Bezahlen mit dem Mobiltelefon?

Zu den Vorteilen des kontaktlosen, mobilen Bezahlens gehören die Durchführung von Transaktionen innerhalb von Sekundenbruchteilen, die benutzerfreundliche Bedienung der digitalen Kreditkarten und das Bezahlen von Kleinbeträgen ohne PIN-Eingabe. Jedoch wird mit Mobile Payment seitens der Kunden häufig ein höheres Sicherheitsrisiko in Verbindung gebracht.

Unter anderem wird bemängelt, dass sich Malware aufs Mobiltelefon bringen und theoretisch Speicherkarteninhalte stehlen lässt. Zudem besteht die Befürchtung, dass von digitalen Kreditkarten übertragene Kreditkartendaten von Betrügern abgehört und für weitere Transaktionen missbraucht werden könnten.

Betrugsszenarien

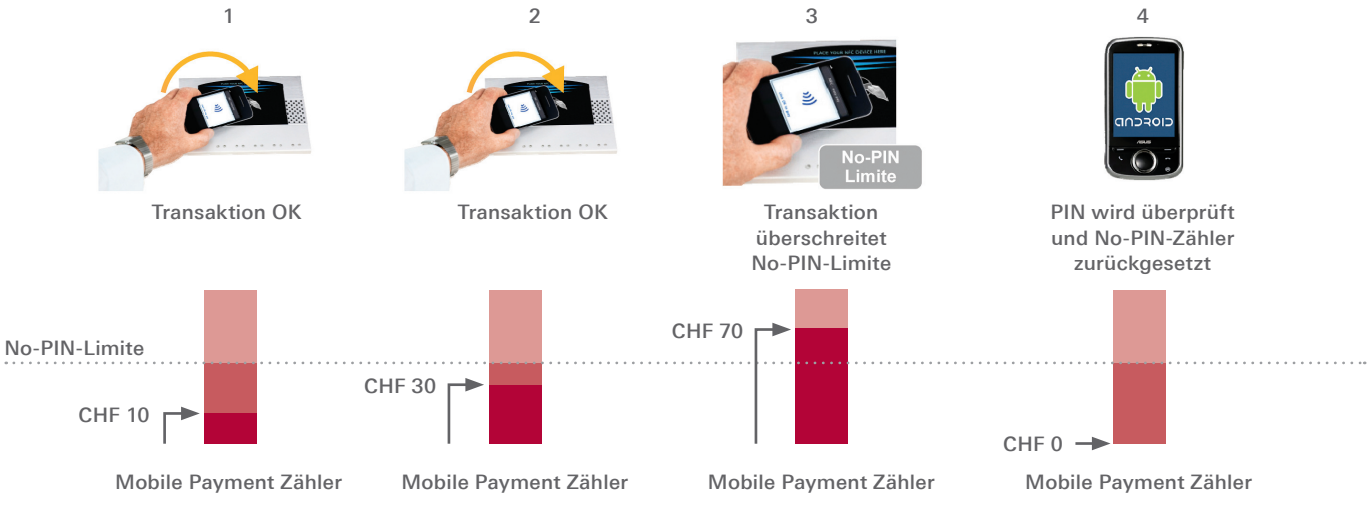
Diese Befürchtungen werden weiter verstärkt, indem potenzielle Sicherheitslücken von kontaktlosen Kreditkarten sowie mit der NFC-Technologie (Near Field Communication) ausgerüsteten Mobiltelefonen in zahlreichen Artikeln rege diskutiert werden. Beispielsweise werden Szenarien beschrieben, in welchen Betrüger mit speziellen Lesegeräten über Distanz die Kreditkartendaten von Passanten auslesen können, auch wenn deren Smartphones in den Taschen der Opfer bleiben. Zwar demonstrieren so genannte Paycardreader eindrücklich, wie einfach verschiedene für eine Kreditkartentransaktion notwendige Daten ausgelesen werden können. Dazu gehören insbesondere die Kartennummer, die Gültigkeitsdauer sowie der Transaktionsbetrag. Jedoch kann der für eine erfolgreiche Transaktion ebenfalls benötigte Name des Karteninhabers nicht ausgelesen werden und die für die Erstellung von Kreditkarten-Klonen benötigten Informationen sind somit nicht vollständig.

Hoher Schutz

Entgegen der weit verbreiteten Annahmen bietet die für Mobile Payment erforderliche zusätzliche Schnittstelle auf NFC-Basis der bei korrekter Umsetzung im Zusammenspiel mit gängigen Sicherheitsmechanismen einen hohen Schutz gegen verschiedene Angriffsvektoren wie Abhörangriffe oder Malware. Einerseits stellt die Kreditkartenindustrie mit den Payment Card Industry (PCI) Standards hohe Sicherheitsanforderungen, um den Missbrauch von Kreditkartendaten zu verhindern. Andererseits werden in den Spezifikationsdokumenten seitens der Kreditkartenkartenorganisationen umfangreiche Sicherheitsanforderungen gestellt. Zudem werden von den Kreditkarten herausgebenden Banken verschiedene Massnahmen zur Reduktion des finanziellen Risikos sowie Methoden im Bereich des Betrugsmanagements eingesetzt, um die Erfolgsquote von Angriffen möglichst gering zu halten.

Neben der Einhaltung verbindlicher Standards seitens der Kreditkartenindustrie und technischer Massnahmen, wie der Verschlüsselung von Transaktionen und der Authentifizierung nach aktuellstem Standard, bieten folgende grundlegende Mechanismen den entscheidenden Schutz vor Missbrauch:

No-PIN Transaktionen Zähler



Ein als *No-PIN Transaktion Zähler* bekannter Mechanismus schränkt die Anzahl Transaktionen ein, die bei Kleinbeträgen ohne PIN-Eingabe durchgeführt werden können. Um zu verhindern, dass ein Betrüger ein gestohlenes Mobiltelefon für Kreditkartenzahlungen nutzen kann, reduziert dieser Zähler die Anzahl Transaktionen unter CHF 40.

Sobald die No-PIN-Transaktions-Limite überschritten wurde, wird der Karteninhaber aufgefordert, seine PIN einzugeben, bevor die nächste Transaktion durchgeführt werden kann. Der theoretische Verlust ist normalerweise durch die AGBs seitens der Kreditkarten herausgebenden Bank gedeckt. Das finanzielle Risiko bei der Transaktion von Kleinbeträgen ohne Karteninhaber-Prüfung ist somit als relativ gering einzustufen.

Ein verwandtes, als *Offline Transaktionen Zähler* bekanntes, Verfahren zählt in regelmässigen Abständen, ob die Identität des Kreditkarteninhabers durch eine Online-Verbindung zum Kreditkartenherausgeber überprüft worden ist.

Der Karteninhaber kann nur eine bestimmte Anzahl an Offline-Transaktionen durchführen. Ist ein bestimmtes Limit erreicht, wird dieser aufgefordert, die Transaktion mit der PIN zu bestätigen.

Lohnenswerte Angriffsziele?

Viele der von Sicherheitsexperten als theoretisch möglich eingestuften Angriffe auf kontaktlose und mobile Bezahlungsmethoden konnten bis heute unter realen Bedingungen nicht durchgeführt werden. Bei einer nüchternen Betrachtung der potenziellen Schwachstellen sowie der bestehenden technischen Sicherheitsmassnahmen stellt sich heraus, dass andere Angriffsmethoden erfolgversprechender sind. Zur häufigsten Betrugsart gehören heutzutage Fälle im Online-Handel, wo die Kreditkarte physisch nicht vorgezeigt werden muss. Dabei werden durch Phishing, gefälschte Internetdienste, Zugriff auf E-Mail-Konten oder Datenlecks gestohlene Kreditkartendaten zum Kauf von Dienstleistungen und Produkten im Internet missbraucht. Dieses Betrugsmuster macht über 80% der Gesamtverluste aus.

Bei der aktuellen Diskussion potenzieller Sicherheitsrisiken im Bereich des mobilen Bezahlens wird häufig ausser Acht gelassen, dass die neue Technologie bestimmte Sicherheitsaspekte auch verbessert, insbesondere durch oben beschriebene Sicherheitsverfahren. Aufgrund der steigenden Komplexität von Mobiltelefonen und der damit verbundenen potenziellen Schwachstellen ist davon auszugehen, dass das Sicherheitsrisiko durch Malware oder Abhörangriffe auf Mobiltelefone tendenziell zunimmt. Dieses Risiko ist jedoch kalkulierbar und sehr gering, sofern die Mobile-Payment-Anwendung korrekt umgesetzt, grundlegende Sicherheitseinstellungen bestehen und vom Benutzer nicht umgangen werden können.

Leo Niedermann, Detecon (Schweiz) AG
leo.niedermann@detecon.com

Offline Transaktionen Zähler