cards Karten cartes

Ein Service
der Zeitschrift für Zahlungsverkehr
und Kartendienstleistungen

EMV unter Beschuss

sb – Zu Recht kann die Kartenbranche auf die gute Zusammenarbeit aller Beteiligten im Umgang mit der Datumsproblematik bei Seccos-5-Chipkarten des Herstellers Gemalto verweisen. Nur dadurch, dass alle an einem Strang zogen, konnte ein noch größerer Imageschaden für das Medium Karte vermieden werden.

Nachdem erst einmal eine Lösung gefunden war, wurde der Umgang mit den fehlerhaften Karten dann aber zum Wettbewerbsthema. Im Bemühen, die Kundschaft zu beruhigen, wetteiferten die Marktteilnehmer um die schnellste „Reparatur" beziehungsweise den schnellsten Austausch fehlerhafter Karten. Während die Gruppe der Sparda-Banken am 20. Januar 2010 den Austausch von rund 400 000 Karten ankündigte, wurde andernorts die Ausrüstung der Geldautomaten mit der Software zur Fehlerkorrektur vorangetrieben – und dies gelang vielfach schneller als ursprünglich anvisiert. Bei der Postbank etwa war sie für alle rund 1 600 Automaten am 28. Januar 2010 abgeschlossen. Die Stadtsparkasse München meldete am 2. Februar 2010 den Vollzug, der DSGV am 17. Februar 2010. An allen 25 700 Sparkassen-Geldautomaten können seitdem Karten „repariert" werden.

„Chip and PIN is broken"

Kaum ist bei diesem Thema Ruhe eingekehrt, hat die Kartenbranche jedoch mit einem neuen Imageproblem zu kämpfen. Wieder geht es um den Chip. Doch diesmal steht einmal mehr die sensible Sicherheitsfrage im Vordergrund. Forscher der Security Group am Computer Laboratory der Universität Cambridge veröffentlichten am 12. Februar 2010 ein Arbeitspapier mit der Überschrift „Chip and PIN is broken". Dessen Grundaussage lautet: Aufgrund einer fundamentalen Schwachstelle im EMV-Protokoll ist es mit geringem technischen Aufwand möglich, mit gestohlenen Original-EMV-Chipkarten unter Eingabe einer beliebigen PIN unentdeckt betrügerische Zahlungen durchzuführen, ohne die Geheimnummer zu kennen.

Basis ist ein sogenannter „Man in the middle"-Angriff. Mit einem Kartenadapter wird dabei der Verkehr zwischen einer Originalkarte und dem Terminal über einen PC mit einer speziellen Schnittstelle umgeleitet. Alle Nachrichten zwischen Terminal und Karte leitet der PC unverändert weiter. Nur wenn das Terminal ein Verify-PIN-Kommando an die Karte schickt, fängt er diesen Befehl ab und antwortet mit dem Code 0x9000, der dem Terminal signalisieren soll, dass die PIN gültig ist. Die falsche PIN wird nicht an die Karte zurückgesendet, sodass der Fehlbedienungszähler nicht tangiert wird. Dem Kartenchip wird vorgespiegelt, das Terminal unterstütze keine PIN-Verifikation und habe die Karteninhaberverifikation entweder übersprungen oder das Unterschriftsverfahren verwendet, sodass die Transaktion erfolgreich abgeschlossen werden kann. Lediglich an Geldautomaten funktioniert das Verfahren nicht, weil dort nicht der Kartenchip, sondern der Server der Bank die PIN prüft.

Unumstritten sind die Ergebnisse der Studie nicht – vor allem deshalb, weil der skizzierte Angriffsversuch nur bei älteren Chipversionen funktioniert. Auch der ZKA wiegelt ab: Deutsche Girocards und Kreditkarten sind von dem von den Forschern beanstandeten Fehler nicht betroffen. Denn die in Deutschland für die Seccos-Chips verwendeten EMV-Spezifikationen böten bereits Mechanismen zur Abwehr des beschriebenen Angriffsszenarios. Auch vor dem Hintergrund der Untersuchung aus Cambridge gelte daher das hohe Sicherheitsniveau von Chip und PIN.

Ein neuerlicher Imageschaden sind die entsprechenden Schlagzeilen gleichwohl. Sie sind Wasser auf die Mühlen all jener, die die Sicherheit des PIN-Verfahrens grundsätzlich bezweifeln – und könnten damit auch in gerichtlichen Entscheidungen zu Haftungsfragen ihre Spuren hinterlassen. Dass das beschriebene Angriffsverfahren nur bei bestimmten Chips funktioniert, ändert daran nichts. Denn wenn die Forscher dort eine Lücke im System entdecken konnten, warum sollten Kriminelle dann nicht auch bei Seccos-Chips eine andere finden? Angesichts der endlosen Diskussionen um die PIN wird der Trend wohl langfristig in Richtung Biometrie gehen. Auch dabei sollte man sich aber keine Illusionen über eine hundertprozentige Sicherheit machen. Die gibt es schließlich auch beim Bargeld nicht.

cardtech weiter unabhängig

Der Netzbetreiber cardtech Card & POS Service GmbH ist unabhängig und wurde nicht an Easycash verkauft, wie in der November-Ausgabe von cards Karten cartes fälschlicherweise berichtet. Das 1990 gegründete Unternehmen ist nach wie vor selbstständig. Easycash übernahm nicht etwa cardtech, sondern den Geschäftsbereich CardCash der BV-Zahlungssysteme GmbH des Bank-Verlags Köln. Die Redaktion bittet die Verwechslung zu entschuldigen.