

Sicher kontaktlos

In Berichten über angebliche Sicherheitslücken bei Kontaktlos-Karten ging in den vergangenen Wochen einiges durcheinander: Debit- und Kreditkarten wurden fälschlicherweise in einen Topf geworfen.



Elektronischer Datenklau ist beim kontaktlosen Bezahlen so gut wie ausgeschlossen.

Funkende Karten, abgefischte Daten und die Vorstellung, dass die Karte jederzeit den Aufenthaltsort verrät – bei der Berichterstattung unter anderem des Spiegels und der Wirtschaftswoche über die angebliche Sicherheitslücken bei Kontaktlos-Karten ging in den vergangenen Wochen einiges durcheinander. In einer Stellungnahme weist der Deutsche Sparkassen- und Giroverband (DSGV) darauf hin, dass eine Kommunikation zwischen den Girogo-Karten und zugelassenen Terminals nur über wenige Zentimeter hinweg möglich sei. Daher sei es nicht vorstellbar, dass Informationen über größere Abstände unbemerkt ausgelesen werden. „Um zum Beispiel Bewegungsprofile des Kunden zu erstellen, sind zwei bis drei Meter hohe Antennen erforderlich, die dann die Karte anfunken müssten. Dies würde wohl kaum unbemerkt

bleiben“, erläutert Jens Stolte von der Beratungsfirma stolte consult.

Ein weiterer Irrtum ist die Vorstellung, dass eine Kontaktlos-Karte unablässig funkt, also Signale aussendet. Doch alle

Eine Girogo-Transaktion kann nur an einem Terminal durchgeführt werden, das über eine Händlerkarte mit Sicherheitsmodul verfügt

mit der Nahfunk-Technologie NFC (Near Field Communication) ausgestatteten Karten sind passiv und reagieren nur, wenn sie von einem entsprechenden Terminal angefunkt werden.

Zusätzliche Sicherheit

Zudem kann eine kontaktlose oder kontaktbehaftete Girogo-Transaktion nur an einem Terminal durchgeführt werden, das über eine Händlerkarte mit

einem Sicherheitsmodul verfügt. Dies ist ein zusätzlicher Sicherheitsaspekt für Händler, etwa Tankstellenunternehmer, da alle Umsätze nur dem Bankkonto des Händlers gutgeschrieben werden können, auf

den die Händlerkarte ausgestellt wurde.

Auch im Hinblick auf die auslesbaren Daten herrschte Verwirrung, denn Debit- und Kreditkarten wurden hier ohne Unterscheidung in einen Topf geworfen. Der DSGV betont, dass bei dem neuen Kontaktlosverfahren Girogo keine personenbezogenen Daten ausgelesen werden können. „Bei Bezahlvorgängen wird lediglich das Datum, die Uhrzeit, der Be-

trag und die anonymisierte Händlerkartenummer gespeichert. Für den Kunden sind die Angaben ausreichend, um den Überblick über seine Finanzen zu behalten, für jeden anderen sind diese Informationen jedoch ohne Wert“, so der DSGV. Mit den aus der Karte auslesbaren, nicht personenbezogenen Daten, die zudem – mit von der deutschen Kreditwirtschaft zugelassenen Verfahren – verschlüsselt werden, können über andere Wege keine Bezahltransaktionen durchgeführt werden.

Kreditkarte antwortet mit Kartenummer

Etwas anders sieht es bei den mit der Kontaktlos-Technologie ausgestatteten Kreditkarten von Mastercard und Visa aus. Hier antwortet die Kreditkarte bei einem kontaktlosen Bezahlvorgang mit der Kartenummer und diese kann sehr wohl bei einigen Onlinehändlern zur Zahlung eingesetzt werden. Doch das Problem ist hier weniger die NFC-Technologie als vielmehr die Weigerung der internationalen Kreditkartenorganisationen, bei Zahlungen im Online-Handel generell auf ein weiteres Sicherheitsmerkmal zu bestehen. Die Deutsche Kreditwirtschaft fordert seit langem von den Kreditkartenorganisationen, solche unautorisierten Zahlungen zu unterbinden. Doch bisher stößt diese Forderung auf taube Ohren. „Die Kreditkartenorganisationen nehmen mögliche Betrugsfälle in Kauf, da sie fürchten, bei einem aufwändigeren Zahlvorgang Umsätze zu verlieren“, erläutert Stolte.

Dagmar Ziegner