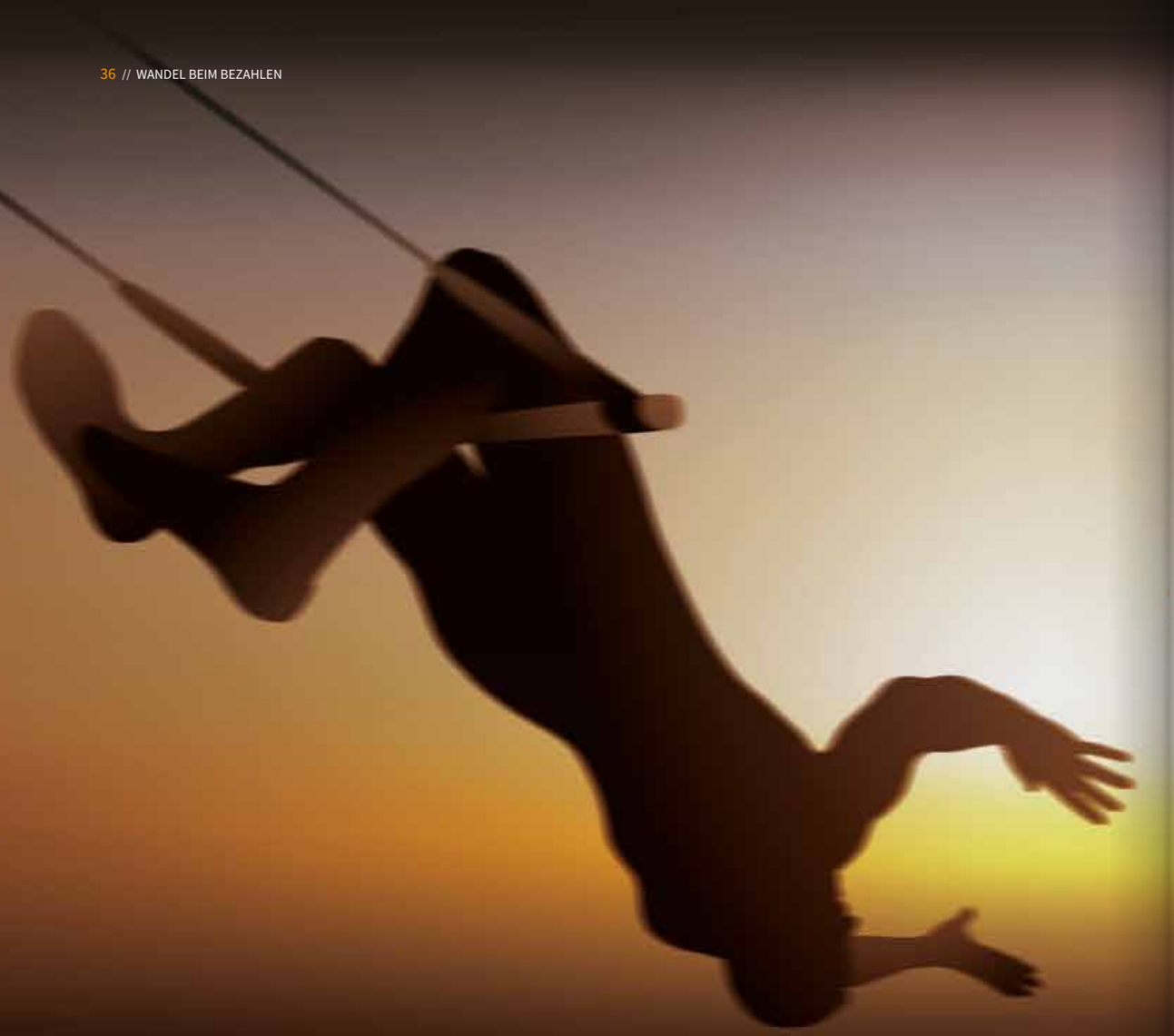

ALLES IM GRIFF

Sicherheit im girocard-System

Wenn ein Akrobat am Trapez durch die Lüfte schwebt, einen Salto schlägt, sich blind darauf verlässt, dass sein Partner in der richtigen Sekunde zur Stelle ist, um ihn im Flug aufzufangen, dann stockt so manchem Zuschauer der Atem. Doch Akrobatik setzt neben intensivem Training und Vertrauen in aller Regel auf ein weiteres, zentrales Element, das auf den Tribünen oft gar nicht auffällt, weil der Blick nach oben gerichtet ist: ein Netz, das im Ernstfall für Sicherheit sorgt.

Was für den Trapezkünstler das physische Netz ist, das ihn auffängt und vor Verletzungen bewahrt, ist beim Bezahlen ein enges Geflecht aus sichernden Maßnahmen, welche die Deutsche Kreditwirtschaft ständig überprüft, ausbaut und optimiert.

Ein Händler benötigt zunächst ein von der Deutschen Kreditwirtschaft zugelassenes Terminal und muss über entsprechende Verträge registriert sein. Damit ist immer eine klare und nachvollziehbare Zuordnung zu einem der Bank bekannten Händlerkonto gegeben und der Händler ist eindeutig identifizierbar. Zudem können Transaktionen nur über einen zugelassenen Netzbetreiber abgewickelt werden. Der kryptographisch abgesicherte Datensatz, der für die Gutschrift auf dem Händlerkonto benötigt wird, entsteht durch eine Abfolge von Kommandos zwischen Terminal und Karte. Dies geschieht nur beim Stecken der Karte oder bei einer kontaktlosen Transaktion bei sehr geringem Abstand zum Terminal, so dass ein unbeabsichtigtes Zahlen verhindert wird.

Zudem ist es Vorgabe des EMV-Standards, nach dem kontaktlose Zahlungen auch im girocard-System erfolgen, dass keine Transaktion durchgeführt wird, wenn das Terminal mehrere Karten gleichzeitig im Feld erkennt. Die korrekte Implementierung des Standards wird durch akkreditierte Testlabore überprüft und ist Voraussetzung für die Zulassung und damit auch die Betriebserlaubnis durch die DK.

Zwei Faktoren für regelmäßige Kontrollen

Als weitere Schutzmaßnahme erfolgt nach mehrmaligem Bezahlen nur durch Vorhalten regelmäßig eine Zahlungsfreigabe über einen zweiten Faktor, z. B. die PIN. Laut gesetzlicher Vorgabe (EBA RTS) kann das kartenausgebende Institut wählen, ob bspw. nach maximal fünf Transaktionen in Folge oder maximal 150 Euro in Summe in aufeinanderfolgenden Transaktionen die erneute Freigabe über die PIN oder eine alternative Authentifikationsmöglichkeit (z. B. biometrische Verfahren) nötig ist. Wie die Grenze innerhalb dieses Rahmens konkret gesetzt wird, entscheidet das kartenausgebende Institut. Der Kunde wird vom Terminal darauf hingewiesen, wenn eine Authentifikation nötig ist.

Auch der Karteninhaber ist Teil des Netzes

Je engmaschiger und stabiler das Netz, umso besser kann es seine Aufgabe erfüllen. Deswegen hat auch der Karteninhaber gewisse Pflichten: Er muss stets sorgsam mit Karte und PIN umgehen. Dazu gehört, dass er seine PIN geheim hält – denn nur dann kann sie ihre Aufgabe erfüllen. Auch das regelmäßige Prüfen der Kontobewegungen – im Onlinebanking oder mithilfe des Kontoauszugs – ist wie bisher Teil der Pflichten des Karteninhabers. Unregelmäßigkeiten sollten Kunden umgehend ihrem Institut melden.

Kommt die girocard oder das Smartphone mit der digitalen girocard abhanden, so sollte die Karte sofort beim kartenausgebenden Institut oder über den zentralen Sperr-Notruf 116 116 gesperrt werden. Ein Diebstahl sollte zusätzlich bei der Polizei angezeigt werden.

Rechtmäßig ist eine Transaktion schlussendlich nur, wenn alle technischen Voraussetzungen erfüllt sind und der Kunde die Zahlung aktiv autorisiert. Im Falle einer kontaktlosen Transaktion ohne starke Kundenauthentifizierung bedeutet das, der Karteninhaber selbst muss seine (physische oder digitale) Karte aktiv und willentlich an das Terminal halten. Im Falle einer missbräuchlichen Kartennutzung haftet grundsätzlich die Hausbank, solange der Karteninhaber sorgsam mit der Karte umgegangen ist. ///