

# Bankkarten und Sicherheit: Immer noch ein Thema?

**Referent:** Prof. Dr. Dipl.-Ing. Manfred Pausch

**Protokoll:** Iris Speiser

Zu Beginn der Veranstaltung wies Prof. Pausch auf Fälle in jüngerer Vergangenheit hin, in denen es zu Manipulationen an Geldautomaten gekommen ist. So werden z.B. Vorsatzschlitze vor den Karteneinzügen angebracht, die während des Einziehens der Bankkarte den Magnetstreifen auslesen. Zusätzlich kommen aufgesetzte Tastaturen zum Einsatz, die die PIN-Eingabe des Kunden protokollieren. Derartige Manipulationen sind für den Kunden kaum erkennbar – zumal die Kartenschlitze und Tastaturfelder der verschiedenen im Einsatz befindlichen Geldautomatenmodelle unterschiedlich aussehen. Der Kunde verfügt daher nicht über Referenzbilder unmanipulierter Automaten.

Allgemein lassen sich bei der Beurteilung der Sicherheit von Bankkarten verschiedene Risikogruppen unterscheiden:

## **Risiko "Erraten" oder "Errechnen" der PIN**

Das grundsätzliche Risiko des PIN-Verfahrens besteht darin, dass die Berechtigung einer Person zum Kontenzugriff ausschließlich anhand der Karte geprüft wird. Der Kunde legitimiert sich durch den Besitz der Karte sowie die Kenntnis der PIN. Beide Merkmale können auch bei anderen Personen zutreffen, ohne dass dies durch die verwendeten technischen Maßnahmen feststellbar wäre.

Unter den Begriff Bankkarten fasst man sowohl die ec-Karten als auch Kreditkarten. Ihre Funktionen sind ähnlich; so kann mit beiden Geld an Geldautomaten abgehoben werden. Beide Systeme arbeiten derzeit mit Magnetstreifen und PIN Authentisierung. Es bestehen jedoch Unterschiede bei der Erzeugung und Prüfung der PIN.

Bei ec-Karten wird die aus dem Masterschlüssel des jeweiligen Instituts und den auf der Karte enthaltenen Daten (Bankleitzahl, Konto-Nummer. und Kartenfolgenummer) ein individueller Schlüssel generiert, mit dessen Hilfe wiederum die PIN generiert wird. Dabei findet das "Triple-DES-Verfahren" als Verschlüsselungsverfahren Anwendung. Die PIN selbst wird nicht auf der Karte gespeichert.

Die PIN-Generierung von Kreditkarten erfolgt nach einem ähnlichen Verfahren, wie bei ec-Karten, allerdings wird hier nur das einfache DES-Verfahren eingesetzt.

Das Errechnen der PIN ist nur dann möglich, wenn es gelingt, die bei der Erzeugung der PIN verwendete DES-Verschlüsselung zu brechen. Das einfache DES-Verfahren kann mit der heutigen Technik in wenigen Stunden gebrochen werden; das zur PIN-Generierung bei ec-Karten verwendete Triple-DES-Verfahren gilt dagegen nach dem heutigen Stand der Technik als sicher.

Eine weitere Gefahr liegt schlicht im Erraten der PIN. Ein 4-stelliger PIN-Code ermöglicht theoretisch 10.000 mögliche Ziffernkombinationen. An den Geldautomaten wird aber erst nach drei Fehlversuchen die Karte eingezogen. Die Wahrscheinlichkeit, die PIN zu erraten liegt daher theoretisch bei 1:3.333. Einige Kombinationen, z.B. "0000" werden allerdings nicht verwendet, wodurch sich die Wahrscheinlichkeit eines erfolgreichen Rateversuchs erhöht.

Die Ermittlung der PIN durch einen unbefugten Dritten kann zudem dadurch erleichtert werden, dass die Häufigkeit der Ziffern in der PIN nicht gleichverteilt ist. Die PIN wird nämlich im Hexadezimalsystem erzeugt, in dem 16 Ziffernwerte existieren. Erst in einem zweiten Schritt erfolgt eine Umsetzung in das Dezimalsystem. Dies hat zur Folge, dass manche Ziffern statistisch häufiger abgebildet werden als andere. Bei Kenntnis dieser statistischen Häufung, erhöht sich die Trefferwahrscheinlichkeit erheblich.

Laut Auskunft der Banken kommt zwar inzwischen ein neues Verfahren zum Einsatz, dass keine derartige statistischen Häufungen mehr hervorbringe. Prof. Pausch zweifelt jedoch an dieser Aussage.

Einerseits kann auch durch andere Verfahren nicht erreicht werden, dass 16 durch 10 ohne Rest teilbar wird. Zum anderen sind Fälle bekannt, in denen die Kunden trotz Umstellung auf das neue PIN-Verfahren dieselbe PIN behielten, was bei Verwendung eines anderen Verfahrens doch recht unwahrscheinlich ist. Bisher haben die Banken noch keinen Sachverständigen Einblick in das neue Verfahren gewährt, so dass die Aussage der Banken, das neue Verfahren sei sicher, nicht durch unabhängige Dritte geprüft werden kann.

### **Risiko "Kopieren der Karte"**

Magnetkarten können relativ einfach mit handelsüblichen Magnetkartenlesegeräten vervielfältigt werden. Duplizierte von Bankkarten können derzeit in Deutschland aber grundsätzlich nicht missbraucht werden, da die Karten neben dem Magnetstreifen zusätzlich über ein kapazitives Merkmal verfügen, das nicht kopierbar ist. Eine kopierte Karte würde daher von Geldautomaten in Deutschland als Fälschung erkannt werden. Im Ausland wird hingegen nur der Magnetstreifen geprüft; Kopien können dort somit nicht erkannt werden.

Das kapazitive MM-Merkmal hat jedoch den Nachteil, dass es recht störanfällig ist. Insbesondere Temperatur- und Luftdruckschwankungen können die elektrostatischen Eigenschaften verändern und zu Erkennungsfehlern führen. Viele Banken deaktivieren daher die Prüfung des MM-Merkmals an Wochenenden, um das versehentliche Einziehen gültiger Karten zu vermeiden. Das Risiko eines Missbrauchs wird hierdurch ausgerechnet an solchen Tagen erhöht, an denen dem Kunden die Sperrung seiner Karte erschwert ist.

Abhilfe kann hier ein zusätzlicher Chip auf der Karte schaffen. Auf den in Deutschland im Verkehr befindlichen ec-Karten sind zwar oftmals Chips angebracht; genutzt werden diese bisher jedoch lediglich als Geldkartenfunktion. Etliche Kreditkartensysteme werden derzeit auf die Chip-Technologie umgestellt (so z.B. VISA); die Umrüstung der Geldautomaten hinkt jedoch hinterher.

### **Risiko "Postweg"**

Viele Banken senden Ihren Kunden sowohl Karten als auch PIN per Post zu. Zwar werden Karte und PIN in der Regel getrennt verschickt; oftmals erfolgt aber keine Prüfung des Zugangs des ersten Briefes vor Versand des zweiten. Durch Häufungen der Sendungen sind diese leicht zu erkennen. Es sind Fälle bekannt, in denen Postmitarbeiter die Sendungen abgefangen haben.

### **Risiko notierte PIN**

Der deutsche Bundesbürger verfügt heutzutage durchschnittlich über ca. 8 Karten, die über ein Autorisierungsmerkmal wie PIN, Passwort o.ä. verfügen. Die Memorierung einer solchen Anzahl von Zugangscodes ist Personen, die diese Fähigkeit nicht trainiert haben, in der Regel nicht möglich. Dem Kunden bleibt daher oft nichts anderes übrig, als sich die Nummern zu notieren. Dieses Problem wird wohl erst gelöst werden, wenn biometrische Merkmale verwendet werden.

### **Risiko "technische Mängel der Geldautomaten"**

Insbesondere ältere Geldautomaten hatten technische Mängel, die es erlaubten, unberechtigt Geld zu entnehmen.

Eine beliebte Methode war die Entnahme von Teilbeträgen. Von dem Geldscheinstapel im Ausgabefach wurde nur ein Teil entnommen; der Rest wurde im Ausgabefach belassen. Nach einer gewissen Zeit zogen die Automaten nicht entnommenes Geld wieder ein; eine Abbuchung erfolgte in solchen Fällen nicht. Das wieder eingezogene Geld wurde in einem separaten Fach gesammelt, ohne dass eine Zuordnung der einzelnen eingezogenen Beträge zu den Kunden möglich gewesen wäre.

Die Banken haben inzwischen auf diesen Trick reagiert. Die Geldautomaten messen jetzt die Dicke der ausgegebenen Scheine und vergleichen sie mit der Dicke wieder eingezogener Beträge. Zudem werden in dem Einzugsfach Trennblätter zwischen den eingezogenen Scheinen eingelegt, wodurch teilweise entnommene Beträge dem jeweiligen Kunden zugeordnet werden können.

Eine andere Variante ist die so genannte "Marlboro-Methode". Hierbei wird der Geldausgabeschacht vom Täter verklemmt, so dass der Kunde kein Geld erhält. Nach dem Weggang des Kunden kann der Betrag dann vom Täter herausgefischt werden.

In jüngerer Vergangenheit sind auch Fälle bekannt geworden, in denen durch Manipulation des Kartenschlitzes die Kartenrückgabe verhindert wurde. Nachdem sich der Kunde ohne Karte entfernt hat, gelangt der Täter mit Hilfe einer Schlinge an die Karte.

### **Risiko "Systemmängel"**

Nach Angaben der Banken ist die PIN einer Karte ausschließlich bei der Bank hinterlegt; eine Prüfung der sollte daher ausschließlich online möglich sein. Es gibt jedoch Vorfälle, die darauf hindeuten, dass dies im Ausland nicht immer der Fall zu sein scheint. Die Dauer des Auszahlungsvorganges oftmals derart kurz, dass in dieser Zeit unmöglich eine Online-Verbindung zum autorisierenden Kreditinstitut aufgebaut werden konnte. Dieses Phänomen ist nur durch zwei Möglichkeiten erklärbar: Entweder ist die Aussage der Banken falsch, dass die PIN ausschließlich beim kontoführenden Institut hinterlegt ist und bei jedem Kontenzugriff eine Online-Autorisierung stattfindet - oder es erfolgt eine Autorisierung durch die ausländische Bank ohne Prüfung der PIN.

Die Logfiles der Bankrechenzentren weisen übrigens oftmals den Eintrag "Sekundärautorisierung" auf. Die Banken liefern jedoch keine befriedigende Erklärung für diese Einträge.

Offenbar ist es auch innerhalb Deutschlands möglich, trotz fehlerhafter PIN eine Auszahlung zu erhalten. So haben in Berlin und Olpe Kunden trotz falsch eingegebener PIN Geld erhalten. Die Vorgänge wurden in dem ZDF-Magazin "WiSo" dokumentiert. Die Ursache der Fehlfunktion konnte seinerzeit nicht geklärt werden, dennoch soll der Fehler nach Angaben der betroffenen Banken inzwischen behoben worden sein.

In den Risikobereich der Systemmängel ist auch der Missbrauch von Kreditkartennummern einzuordnen, die durch Software automatisch generiert wurden. In Fällen, in denen solche automatisch generierte Nummern zufällig mit echten Kreditkartennummern übereinstimmen, kann dies zu unberechtigten Abbuchungen bei dem betroffenen Karteninhaber führen.

### **Risiko "Ausspähen der Kartendaten"**

Kundendaten können auf verschiedene Weise ausgespäht werden. Die einfachste Methode ist, sich in die Nähe des Kunden zu stellen und diesen direkt zu beobachten.

Technische Hilfsmittel erregen jedoch weniger Aufmerksamkeit des Kunden. Die Kartendaten können durch Vorsatzgeräte an den Kartenschlitz, die PIN durch Kameras oder manipulierte Tastaturen. Besonders dreist gehen Täter vor, die falsche Geldautomaten aufstellen. In der Regel handelt es sich um "echte" Geldautomaten, die zuvor anderorts gestohlen wurden.

Das Ausspähen der Daten ist die derzeit häufigste Missbrauchsart bei Bankkarten. Dem Kunden kann daher nur empfohlen werden, besonders wachsam zu sein.

### **Diskussion:**

Nach Prof. Pauschs Vortrag wurden von den Zuhörern noch einige Fragen aufgeworfen, über die teilweise intensiv diskutiert wurde.

- ***Was sollte ein Kunde tun, der trotz Eingabe der richtigen PIN am Geldautomaten kein Geld ausgezahlt bekommt?***

Dieses Phänomen kann verschiedene Ursachen haben. Meistens wird es sich um eine Fehlfunktion des Geldautomaten handeln. In diesem Fall wird keine Kontobelastung durch die Bank erfolgen. Es ist aber nicht auszuschließen, dass der Geldautomat in einer Weise manipuliert wurde, dass das Geld im Ausgabeschacht zurückgehalten wird und nach dem Weggang des Kunden von einem Unbefugten entnommen werden kann.

Es ist daher ratsam, bei der Bank sobald wie möglich zu prüfen, ob tatsächlich eine die Belastung des Kontos erfolgt ist.

- **Wie ist die Sicherheit von Chip-Karten die bei der elektronischen Signatur eingesetzt werden – insbesondere da die ZPO in 292a einen Anscheinsbeweis für die Echtheit elektronisch signierter Dokumente vorsieht?**

Die bei der qualifizierten elektronischen Signatur verwendeten Verfahren sind Prof. Pausch nicht im Detail bekannt; akkreditierte Zertifikatsaussteller unterliegen allerdings der Kontrolle der verwendeten Technik durch das BSI, so dass in diesem Fall von einem hohen Sicherheitsstandard auszugehen ist.

- **Wie ist die Risikoverteilung zwischen "Erraten" und Ausspähen von Kartendaten zu bewerten?**

Nach den bisherigen Erfahrungen ist das Ausspähen von Kartendaten wesentlich verbreiteter.

- **Im Ausland werden von Geldautomaten bei der Geldausgabe Quittungen ausgegeben. Haben diese einen Beweiswert?**

Nein, derartige Quittungen haben – jedenfalls nach deutschem Recht – keinen Beweiswert, da es durchaus denkbar ist, dass durch technische Fehlfunktionen Geld ohne Quittung oder Quittungen ohne Geld ausgegeben wird.

- **Könnten die Bilder von Überwachungskameras als Beweismittel der Geldentnahme dienen?**

Im Geldautomaten selbst wird lediglich die Stückelung des ausgegebenen Geldbetrages dokumentiert. Die Überwachung des kapazitiven MN-Merkmals wird übers Wochenende oft abgeschaltet, da es sich – insbesondere bei wechselnden Witterungsbedingungen – als störanfällig erwiesen hat. Eine Falschgeldprüfung im Automaten findet nicht statt, lediglich Größe und Dicke der Scheine wird geprüft. Die Bilder der Überwachungskameras können zwar helfen, die Person am Geldautomaten zu identifizieren (sofern sie nicht

maskiert war). Zur Dokumentation der technischen Vorgänge im Automaten sind die Bilder jedoch in der Regel ungeeignet.

- Stellen biometrische Verfahren eine Alternative zum Bankkartensystem dar? Reine biometrische Verfahren können durchaus eine Alternative darstellen. Derzeit sind die meisten Verfahren aber noch nicht hinreichend ausgereift und verursachen zu viele Fehlidentifizierungen. Dies mag hinzunehmen sein, sofern eine alternative Zugangsprüfung durch einen Menschen möglich ist, für Geldautomaten, die auch am Wochenende ohne menschliche Kontrolle operieren, sind die Verfahren aber noch zu unsicher. Etwas realistischer ist die Ersetzung der PIN-Eingabe durch ein biometrisches Verfahren, wobei lediglich ein Abgleich des biometrischen Merkmals mit einem Referenzmuster erfolgt, das z.B. auf einem auf der Karte aufgebracht Chip gespeichert ist. Dies würde zumindest das Risiko des Ausspäehens der PIN und das Problem der notierten PINs ausschließen.