

Magnetstreifen-Daten\*, Eurocheque-Karte: Mit Geduld und Geschick Geheimcodes dechiffriert

## Hacken statt knacken – Bankraub à la carte

Risiko für zwanzig Millionen Bankkunden: Schwindel mit Eurocheque-Karten

**Banker reden nicht gern darüber: Bankräuber neuen Typs plündern Tag für Tag mit gestohlenen und verfälschten Eurocheque-Karten, per Geldautomat, die Konten argloser Kunden. Schon fürchten Fachleute, daß**

**es einer Computer-Mafia gelingt, den geheimen Karten-Kode zu entschlüsseln – auf einen Schlag ließen sich bundesweit aber Millionen Mark erbeuten, die möglichen Folgen reichen „bis zur Systembedrohung“.**

Verblüfft sah sich der Universalschleifer Ralf Steynen, 22, immer wieder die Kontoauszüge 44 bis 46 an. Die 18 Positionen auf den drei Bankzetteln lauteten alle gleich: „Geldautomat“.

Innerhalb einer Woche waren an drei verschiedenen elektronischen Zahlstellen in Köln insgesamt 9200 Mark abgeboben worden – allerdings, beteuert Steynen, nicht von ihm.

Er hatte seine Eurocheque-Karte, die den Bargeld-Bezug aus Automaten ermöglicht, auch weder verlegt noch verloren, sondern „stets bei mir gehabt“. Daß ein Dieb mit Steynens Karte abkassiert hat, sei mithin ebenfalls ausgeschlossen.

Steynen ist die Sache schleierhaft, er hat „gar keine Erklärung, wie das passieren kann“. Dagegen hatte die Stadtsparkasse Köln, bei der Steynen ein Girokonto unterhält, sofort ihre Version parat: Nur der Kontoinhaber selbst oder jemand aus seinem „privaten Bereich“ sei imstande, mit der Plastikkarte und der geheimen „Persönlichen Identifikations-Nummer“ (PIN) die Automaten anzuzapfen.

Tatsächlich kommt es schon mal vor, daß einer seine Kontoüberziehung zu kaschieren versucht, indem er einfach behauptet, ein Fremder müsse sich seiner Karte bedienen haben. Doch die Gewißheit, mit der die Stadtsparkasse im Fall Steynen den vermeintlichen Täter ortete, ist brüchig geworden.

\* Der Strichcode der Eurocheque-Karte wird auf dem Computer-Bildschirm sichtbar gemacht, einzelne Daten werden durch ein besonderes EDV-Programm ausgewiesen. Beispiel: Die Karte wurde zuletzt am 14. Dezember 1985 an einem Geldautomaten benutzt (die ersten vier Ziffern der dritten Zeile bedeuten: 348. Tag, letzte Jahresziffer 5).



Kundin am Geldautomaten: Diebe schielen über die Schulter

Denn bundesweit häufen sich neuerdings mysteriöse Vorfälle, bei denen ahnungslose Bankkunden per Elektronik ausgeplündert werden. Bankraub geschieht heutzutage nicht länger mehr nur so, wie es das Publikum aus der Presse und aus dem guten alten Kintopp kennt.

Der Typ des Schränkens, der sich wie einst, in der Ära der Berliner Ringvereine, die legendären Gebrüder Sass mit Schneidbrenner und Brecheisen an den Tresor heranrobbt, ist womöglich bald ebenso passé wie der listige Riffiganove wie der Draufgänger mit der

Strumpfmassage oder der Brutalo, der sich nach dem Vorbild von Bonnie und Clyde im Schalterraum Geiseln greift und notfalls umlegt.

An die Stelle des klassischen Panzerknackers tritt zunehmend der intelligente Hacker, der, statt Geldschränke aufzuschweißen, mit Geduld und Geschick Magnetstreifen manipuliert und Geheimcodes dechiffriert. Die Bankräuber neuen Typs zielen auf eine der verwundbarsten Stellen des Geldgewerbes: die blau-rote Eurocheque-Karte, von der zur Zeit bundesweit rund 20,2 Millionen Exemplare im Umlauf sind.

Die Plastikkarte ist nicht mehr sicher. Computer-Bastler und kriminelle Automatenknacker haben vielfach bewiesen: Statt echter EC-Karten akzeptieren die technisch aufwendigen Geldautomaten (Stückpreis: 120 000 Mark) auch von Kriminellen hergestellte Duplikate.

Und: Der vierstellige PIN-Kode, der Schlüssel zum elektronischen Safe, läßt sich mit diversen Tricks auskundschaften – ohne daß der Kartenbesitzer die Preisgabe der vertraulichen Zahlenkombination bemerkt.

Banker sprechen nicht gern darüber, doch schon vergeht kaum ein Tag ohne ein Dutzend oder mehr Fälle von elektronischem Banküberfall. Allein in Hamburg registriert die Kripo, so Hauptkommissar Günter Heerdt, einschließlich vorgetäuschter Straftaten „je Arbeitstag durchschnittlich einen Fall mißbräuchlicher Scheckkarten-Benutzung“.

Das Risiko, Opfer eines Bankomaten-Betrugs zu werden, ist hoch. Fast jeder westdeutsche Haushalt besitzt mittlerweile eine automatentaugliche Eurocheque-Karte, nahezu zehnmillionenmal pro Monat wird der Bargeld-Service an den rund 2700 bislang installierten EDV-Schaltern in Anspruch genommen.

Und die Gefahr für den Kunden steigt, je mehr Kriminelle sich daranmachen, den Kartenkode statt Panzerschränken zu knacken. Katastrophale Auswirkungen auf die Vertrauenswürdigkeit der Branche sind zu erwarten, wenn sich herumspricht, was das Fachblatt „Krimi-

### „Schneller als eine normale Abhebung“

nalistik“ bereits festgestellt hat: Die ins Automaten-system eingebauten „Sperren, die sich Experten mit hoher Sachkenntnis ausgedacht hatten und für absolut sicher hielten“, seien schon jetzt „nicht mehr unüberwindbar“.

Die Gegenseite sieht es genauso. „An die Original-Scheckkarten und die PIN-Nummern heranzukommen“, brüstet sich der Kölner Computerfreak Günter Jonas\*, 33, gehe „schneller als eine normale Abhebung“. Gemeinsam mit einem 46jährigen Kumpan holte sich der gelernte Kraftfahrzeugmechaniker um die Jahreswende 1985/86 bei 192 illegalen Automatenauszahlungen 78 500 Mark aus den gepanzerten Schatztruhen.

Fremde Konten zu plündern ist so simpel, daß kriminelle Tüftler-Typen, die auf die Falschgeld-Produktion spezialisiert sind, es künftig viel leichter haben könnten. „Geldautomaten auszurauben“, urteilt das Computer-Magazin „Chip“, sei „viel einfacher, als Blüten zu drucken“.

Schlimmer noch: Bankfachleute müssen sich bereits darauf einrichten, daß

\* Name von der Redaktion geändert.

# WIR VERMIETEN AUTOS. SO ODER SO. Z. B. GOLF SYNCRO



SPORTIVE WERBUNG MÜNCHEN

Es gibt kaum so unterschiedliche Situationen und Anforderungen wie beim Autofahren. Ein Auto soll z.B. für Geschäftsreisen, für die Freizeit, für Sonne, Regen und Schnee geeignet sein.

Damit Automieten nicht zum Abenteuer wird, vermieten wir Autos nach Maß. Unter mehr als 50 verschiedenen Fahrzeugen können Sie genau den Wagen mieten, der Ihren ganz persönlichen Ansprüchen entspricht. Z.B. mit sportlichem Flair, mit mehr Komfort und mit mehr Sicherheit. Einen sportlich weißen Golf syncro oder einen Quattro von Audi, oder ...



**DIE SPORTLICHEN WEISSEN.**



**Klassische Bankräuber im Film\***: Passé ist der Typ des Schränkens . . .

sich das organisierte Verbrechen des neuen Kriminalitätszweiges annimmt. Wenn erst einmal der elektronische Kode der EC-Karten – das bestgehütete Geheimnis der Branche – komplett entschlüsselt ist, könnten mafiäartige Gangs auf einen Schlag an vielen Orten Millionen und aber Millionen abkassieren – eine Art GAU im Geldgewerbe.

„Mit einer großen Zahl von Duplikaten, die durch eine organisierte Fälscherbande zum gleichen Zeitpunkt an den

### **Die Geheimzahl empfangen die Täter über Funk**

Geldausgabeautomaten eingesetzt werden“, warnte bereits vor vier Jahren der Münchner Scheckkarten-Spezialist Siegfried Otto, seien „Angriffe mit hohen Verlusten – bis zur Systembedrohung – möglich“.

Schon mit vergleichsweise schlichten Methoden, wie sie zur Zeit bei EC-Kriminellen gängig sind, lassen sich ansehnliche Beträge abkassieren. Dem Kölner Jonas etwa ist es, wie er dem SPIEGEL berichtete, sogar gelungen, jemandem 8000 Mark abzunehmen, dessen EC Karte er „nie in der Hand gehabt“ hat.

Das ging so: An einem Geldautomaten, vor dem Eingabeschlitz für die Scheckkarte, montierten Jonas und sein Komplize ein Gehäuse von sechseinhalb Zentimeter Tiefe. Inhalt: ein Magnetstreifen-Lesegerät mit Sender.

Wenn ein argloser Bankkunde seine Karte in den Schlitz steckte, empfingen die Täter über Funk nicht nur den kompletten Datensatz, der im Magnetstreifen auf der Kartenrückseite gespeichert ist, sondern auch die persönliche Geheimzahl, die der Kunde in die Auto-

stik nichts anfangen konnte, meldete eine Leuchtschrift dem düpierten Kunden: „Karte eingezogen.“

Verdattert verließen die Geprellten dann gewöhnlich den Tatort. Weil die Schalter schon geschlossen waren, konnten sie die vermeintliche Panne auch nicht sofort reklamieren.

Sogar ein Angestellter der Kölner Stadtparkasse fiel auf den Trick herein. Er hielt den Automatenanbau in der Filiale Rodenkirchen für ein zusätzliches Sicherheitssystem. Mit der Karte des Bankers hob das Duo binnen vier Tagen mehr als 36 000 Mark ab.

Um die erbeuteten Eurocheque-Karten selber einsetzen zu können, mußten die Gauner die jeweils passende vierstellige PIN ausbaldowern. Zu diesem Zweck hatten sie die Nummern-Tasten zuvor mit Make-up eingepinselt. Die Fingerabdrücke der geleiteten Kunden verrietern dann, welche Ziffern gedrückt worden waren.

Die richtige Reihenfolge ermittelten die Kartenklauer durch simples Auspro-



. . . mit Schneidbrenner und Brecheisen: **Klassische Bankräuber vor Gericht\***

matentastatur tippte – eine solche Funkbrücke erklärt womöglich auch den Fall des Universalschleifers Steynen.

Die Magnetstreifen-Daten übertrugen die heimlichen Lauscher auf Blankokarten, mit denen sie sich zu Hunderten in einem Computerladen eingedeckt hatten. Stückpreis: fünfzig Pfennig.

Später verfeinerte Jonas das Verfahren noch. Er konstruierte ein Vorsatzgerät, das die echten Eurocheque-Karten gleich einbehielt.

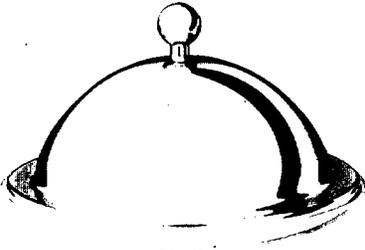
Ganz einfach: Die Täter steckten eine unbedruckte Blankette in die Box. Sobald ein Bankkunde seine Originalkarte einsob, beförderte er damit die Dummy-Karte in den Automaten. Und weil das Gerät mit dem wertlosen Stück Pla-

bieren – bei vier Stellen gibt es höchstens 24 Kombinationsmöglichkeiten. Sie kopierten deshalb die Magnetstreifen der Originalkarten auf Blanketten, von denen sie, weil der Apparat beim dritten Fehlversuch die Karte schluckt, eben schlimmstenfalls sieben Stück opfern mußten.

Mit den Kleckerbeträgen, die von den Kartenausgebern als Tageslimit festgesetzt sind, mochten sich Jonas und sein Komplize nicht begnügen. Regulär wirft so ein Automat, je nach Institut, maximal tausend oder auch zweitausend

\* Oben: Spielfilm-Szene aus „Riffifi“; unten: Angeklagte Erich und Franz Sass mit Verteidiger (vorn) 1932 in Berlin.

# 1.870 ausgezeichnete Restaurants zum Verschenken.



Machen Sie jemanden per Geschenk zum Feinschmecker. Mit den 1.870 Restaurants im Aral Schlemmer-Atlas 1987. Ausgezeichnet mit Schlemmer-Kochlöffeln. Beschrieben in Wort und Bild. Die Restaurants mit den besten Küchen Deutschlands haben fünf Schlemmer-Kochlöffel. Die mit empfehlenswerter Regionalküche einen. Und die dazwischen haben zwei, drei und vier Schlemmer-Kochlöffel.

Der Aral Schlemmer-Atlas ist das ideale Geschenk für jemanden, der ein Gourmet ist. Oder einfach gerne ißt. Gut bürgerlich oder fürstlich. National oder international. Klassische Küche oder Nouvelle Cuisine.

Und damit der Gang zu den Gängen auch problemlos verläuft, weisen viele detaillierte Karten und Stadtpläne den Weg. Die 1.870 Restaurants kosten ganze DM. 39,80. An Aral-Tankstellen, in Buchhandlungen und den Buchabteilungen der Kaufhäuser.



**Schlemmer-Atlas.**

Aral in Brix \* 24444 #



**Scheckkarten-Fälscherwerkstatt (in Köln):** „Einfacher, als Blüten zu drucken“

Mark aus, wenn er mit einer vom selben Bankhaus ausgestellten Eurocheque-Karte gefüttert wird; an anderen Geräten („Fremdverfügungen“) gibt es nur 400 Mark pro Tag.

Bei jeder Abhebung notiert der Geldautomat auf dem Magnetstreifen das Datum – die Karte ist dann für diesen Tag gesperrt. Doch die Sicherung läßt sich knacken: Wenn die ganze Magnetpiste mit den ursprünglichen Daten kopiert und die Originalkarte nach Gebrauch damit wieder beschrieben wird, nimmt der Automat nicht wahr, daß die Karte für diesen Tag eigentlich schon verbraucht ist.

Er habe „nur auf die Schwachstellen in den Sicherheitssystemen der Banken hinweisen“ wollen, verteidigte sich Günter Jonas vor Gericht: „Daß das Geld so leicht herausgekommen ist, hat mich selbst gewundert.“ Zurückgeben konnte er es „hinterher verständlicherweise nicht mehr“.

Daß solche Täter Nachahmer finden, scheint unausweichlich. Denn der Bankraub à la carte birgt weniger Gefahren als herkömmliche Hold-ups und das traditionelle Schränker-Handwerk: Kein Täter macht sich mehr die Finger schmutzig, es geht ohne Gewalt und Drohung ab, und das Risiko der Automatenplünderer, von Augenzeugen identifiziert zu werden, ist äußerst gering.

Nur durch dummes Ungeschick flogen die ansonsten cleveren Kölner Bankautomatenknacker auf. Sie fingerten während der Schalterstunden im Foyer der Sparkassenfiliale im Vorort Bayenthal so auffällig an der Apparatur herum, daß ein Kassierer stutzig wurde und eine im Vorraum installierte Videokamera einschaltete. Als die Photos in den

Lokalzeitungen veröffentlicht wurden, stellten sich die Kartentricks der Polizei.

Noch kecker als die Kölner Kartentricks gingen Betrüger in Braunschweig, Wolfsburg und Bremervörde ans Werk. Als Kartenfalle benutzten sie ein selbstgebasteltes Kästchen, von dem die Bankkunden glaubten, es handle sich um eine Vorrichtung zum Öffnen der Foyertüren, hinter denen sich die Automaten befanden.

Die Täter schraubten zunächst die Platte mit dem Schlitz für die EC-Karte ab. An der freigelegten Stelle befestigten sie ihr eigenes Gerät, das neben einer Öffnung für die Karte auch eine Tastatur für die PIN-Eingabe enthielt.

Der Zusatzapparat ließ vier verschiedene Lämpchen aufleuchten. Das erste befahl: „Karte einführen“, dann signalisierte das zweite: „Geheimzahl eingeben“ – die Kunden gehorchten brav.

## **Schadenssumme wird gehütet wie das Bankgeheimnis**

obschon, wie Banken-Sprecher später betonten, „an den Türen niemals die PIN abgefragt“ wird. Nach dem dritten Lämpchen („Eingabe bestätigen“) flackerte die Anzeige „Technischer Fehler“ auf, der sich auch mittels „Korrektur“-Taste nicht beheben ließ.

Als sich weder die Tür öffnete, noch der tückische Mechanismus die Scheckkarte wieder herausrückte, machten sich die immer noch vertrauensseligen Kunden auf den Weg zu einer Fernsprechkabine. Die Telefonnummer, die für den Fall eines Defekts auf dem Gerät angegeben war, erwies sich natürlich als frei erfunden. Unterdessen bauten die Gano-

ven ihre Trickbox samt Inhalt ab. Mit den erbeuteten Eurocheque-Karten wurden in den folgenden Wochen quer durch die Republik Automaten ausgeräubert.

Nach Ansicht der Braunschweiger Kripo kann „davon ausgegangen werden, daß es sich bei den Tätern um eine überregionale Tätergruppe handelt, die auch weiterhin mit dieser ‚Arbeitsweise‘ bei anderen Banken auftreten wird“. Die bislang durch Scheckkarten-Schwindel aufgelaufene Schadenssumme hüten Westdeutschlands Kreditinstitute so gut wie das Bankgeheimnis.

An Warnungen vor EC-Kriminalität hat es nicht gefehlt. Bereits 1982 mahnte

der die Eurocheque-Karten hergestellt werden: Die Geldautomaten lesen nur die Informationen, die als Strichcodes in dem braunen Eisenoxid-Streifen auf der Rückseite gespeichert sind. Und die, sagt Siegfried Otto, Vorsitzender der Geschäftsführung der Wertpapierdruckerei Giesecke & Devrient, sind „durch relativ leichte Übertragung der Magnetpiste auf andere Karten zu duplizieren“.

Otto muß es wissen: Sein Familienunternehmen, 1852 in Leipzig gegründet, ist nicht nur Marktführer im Drucken von Aktien, weltweiter Lieferant von Banknoten und einzige Privatfirma, die sich mit der Berliner Bundesdruckerei in die Herstellung des westdeutschen Papiergeldes teilt, sie hat auch das Monopol auf die Fabrikation der EC-Karte.

Über die „Buffering“ genannte Methode, Magnetstreifen zu vervielfältigen, kursieren in der Hacker-Szene amüsante Anekdoten. Bereits Anfang der siebziger Jahre kopierte ein amerikanischer Student die Datenpiste eines gültigen

U-Bahn-Monatstickets, indem er ein Tonband-Schnipsel auf die Karte legte und mit einem warmen Bügeleisen darüberfuhr. Die Kodierung des Tickets wurde dabei auf das Magnetband übertragen, das, auf eine entwertete Karte geklebt, wie ein gültiger Fahrausweis benutzt werden konnte.

Ganz so einfach sind Eurocheque-Karten nicht zu fälschen. Immerhin kann, wer keine Blanko-Karten kaufen will, sich auch Plastik-Rechtecke passend zurechtschneiden und ein Stück Videoband draufkleben.

Um funktionsfähige Fälsifikate herzustellen, bedarf es zwar spezieller Magnetstreifen-Lesegeräte. Aber die gleichen „Durchzugsleser“, die in den Automaten eingebaut sind, werden vom einschlägigen Versandhandel an jedermann vertrieben. Ein Münchner Versender warb für den Kartenleser „Elcomatic“ in einer Zeitschriften-Anzeige sogar mit dem ausdrücklichen Hinweis, daß das Gerät „auch für Bank- und Geldautomaten-Anwendungen“ geeignet sei.

Ein halbwegs geübter Bastler kann anhand der mitgelieferten Bedienungsanleitung das Lesegerät an seinen Heimcomputer anschließen und auf dem Bildschirm sichtbar machen, was auf der Magnetpiste steht. Was die Zeichen – maximal 107 in 29 „Feldern“ – bedeuten, ist in einer leicht zugänglichen Banken-Broschüre nachzulesen, Titel: „Aufbau und Feldbelegung der 3. Spur von Ma-

## 4.231 ausgezeichnete Hotels zum Verschenken.



Kein Problem. Im Aral Schlummer-Atlas sind sie alle drin. Die bürgerlichen mit einem Stern, die der internationalen Spitzenklasse mit fünf Sternen. Und die dazwischen mit zwei, drei und vier Sternen. Alle ausführlich in Wort und Bild beschrieben. Wem also den Aral Schlummer-Atlas 1987 schenken?

Zum Beispiel jemandem, der gern verreist. Privat oder geschäftlich. Jemandem, den Sie gern auf die Reise schicken würden. Für kurz oder lang. Jemandem, der gern übernachtet. Einfach oder gediegen. Jemandem, der häufig Konferenzen abhält. Auf Deutsch oder simultan auf Chinesisch.

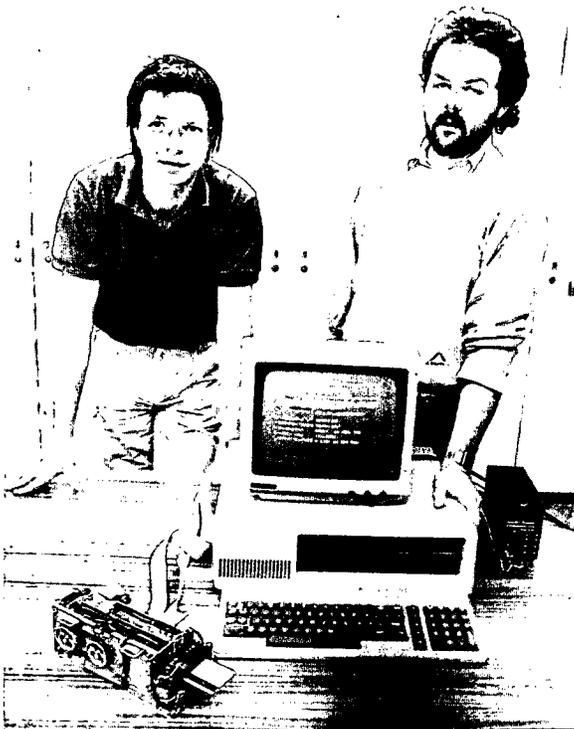
Oder jemandem, der gern direkt an der Reiseroute haltmacht. In Hotels oder Motels. Kurz und gut: Jemandem, dem Sie den Weg zu den Sternen weisen wollen. Mit vielen detaillierten Karten und Stadtplänen.

Die 4.231 Hotels kosten ganze DM 39,80. An Aral-Tankstellen, in Buchhandlungen oder den Buchabteilungen der Kaufhäuser.



## Schlummer- Atlas.

Aral in Bix \* 24444 #



**TV-Reporter Lehnardt, Ammann\***  
Lesegerät vom Versandhändler

Wolfgang Starke, Geschäftsführer des Deutschen Sparkassen- und Giroverbandes (DSGV), man dürfe „nicht darüber hinwegsehen, daß die neuen Techniken ohne entsprechende Sicherheitsvorsorge und Schutzmaßnahmen neuen Gefährdungen durch kriminelle Angriffe ausgesetzt sind“.

Im Dezember 1983 stellte die Bonner Unternehmensberatung SCS in einem Gutachten für die Bundespost fest, daß Magnetkarten mit nur geringem Kostenaufwand zu fälschen seien. Schon im Jahr darauf wurde, wie die Bundesregierung verlaublich, „erstmalig auch die Verwendung einer total gefälschten Karte“ an Bankautomaten bekannt.

Gegen das Zinken und Linken feilt auch die hohe Druckerkunst nicht, mit

\* Mit Magnetstreifen-Lesegerät und Heimcomputer.

gnetstreifen auf Eurocheque-Karten zur Benutzung im institutsübergreifenden Geldausgabeautomaten-System“.

Durch schlichtes Kopieren des Magnetstreifens lassen sich jene Datenfelder manipulieren, die bei der Automatenbenutzung verändert werden: der sogenannte Fehlbedienungszähler und der Tag der letztmaligen Verfügung.

Wie einfach die Automaten auf diese Weise zu täuschen sind, führten die Hamburger Fernsehjournalisten Thomas Ammann und Matthias Lehnhardt im „ARD-Ratgeber Technik“ vor: Sie hoben mit einer einzigen – Ammanns eigener – Eurocheque-Karte an einem Tag bei sechs verschiedenen Automaten je 400 Mark ab.

Das sei völlig unmöglich, hatten die Automaten-Betreiber bis dahin behauptet. Udo Einhoff, Sprecher des Bun-

der fremden sowie bis zu 2000 Mark bei der eigenen Bank abgehoben werden können.

Mit einer Karte etwa, die am Freitagnachmittag nach Schalterschluss einem Dieb in die Finger fällt, kann der mit einigem Geschick bis Montag früh, wenn die Bank die Verlustanzeige erhält, eine schöne Summe aus den Automaten ziehen: bis zu 9600 Mark.

Diebe ergattern die Plastikkärtchen oft bei Einbrüchen in Autos oder Wohnungen. Häufig warten die Kartengänger auch direkt vor den Bankautomaten auf ihre Opfer, weil sie denen dann gleich bei der PIN-Eingabe über die Schulter schielen und so die Geheimzahl ausspähen können.

Sobald die Scheine im Ausgabefach rascheln, verhalten sich viele Leute, wie Polizeibeamte berichten, auf merkwürdi-



**Fernsehteam beim Praxistest:** An einem Tag aus sechs Automaten je 400 Mark

desverbandes deutscher Banken, räumt seither immerhin ein, daß es ein gewisses „Risiko“ gebe – allerdings sei es „so gering, daß wir es in Kauf nehmen“.

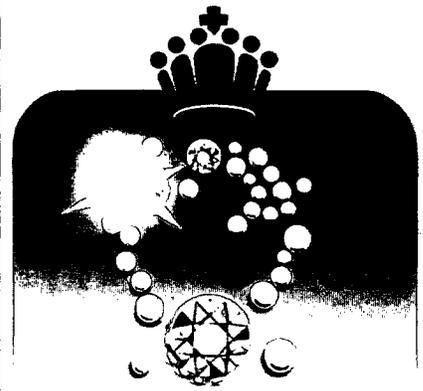
Gering ist das Risiko freilich nur für das Kreditgewerbe, das sich fast immer vor der Haftung drücken kann. Denn Betrügereien mit manipulierten Magnetstreifen setzen in der Regel voraus, daß sich Diebe zunächst mal fremde Scheckkarten aneignen und die dazu passenden Geheimzahlen in Erfahrung bringen. Und weil ihnen dazu meistens die Leichtfertigkeit von Karteninhabern verhilft, haben die Banken ein treffliches Argument, den Schaden auf die Kunden abzuwälzen.

Da kommen happige Beträge zusammen, auch ohne elektronische Datenveränderung. Bis eine gestohlene Karte gesperrt wird, vergehen – zumal wenn ein Wochenende dazwischen liegt – oft mehrere Tage, an denen jeweils 400 Mark bei

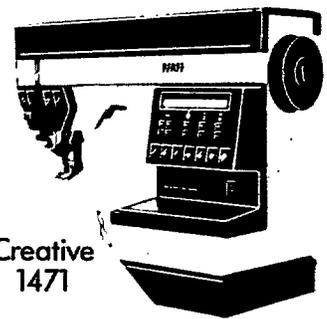
ge Weise leichtsinnig: Sie konzentrieren sich ganz auf das Nachzählen der Banknoten, die vergleichsweise viel wertvollere Scheckkarte aber stecken sie achtlos rasch in die Jackett- oder Gesäßtasche – und weg ist sie.

Langfinger, die keinen Blick auf die PIN-Tasten werfen konnten, rufen häufig beim rechtmäßigen Kartenbesitzer unter dem Vorwand an, sie seien bei der Bank angestellt und müßten die Geheimzahl wissen, um die Scheckkarte zu sperren. Kriminalist Heerdt: „Und die Leute fallen darauf rein.“

Als nützlich erweist es sich für einen Dieb auch, wenn er mit der Karte gleich die Briefftasche entwendet. „Irgendwo“, so ein Fachmann vom Banken-Verband, „haben die meisten Leute sich in ihren persönlichen Unterlagen die Nummer notiert.“ Kenner finden sie immer, etwa indem sie „im Telefonnotizbuch unter ‚G‘ wie ‚Geheimzahl‘ suchen“, wie Er-



Schenken Sie ein  
Jewel besonderer  
Art... die Krone  
von **PFAFF**



Creative  
1471

- Eine Nähmaschine mit höchstem elektronischem Nähkomfort
- für fürstliche Kreativitäts-Ansprüche.
- Und Kreativität ist einer der Schlüssel zum Glücklichein!
- Die Pfaff Creative vereint alles was Nähen zum Vergnügen macht
- und sticht wie von Hand – sogar den Kreuzstich!



**PFAFF**®

Die führende deutsche  
Nähmaschinenmarke mit  
dem guten Kundendienst.

Prospekte  
und Beratungsservice  
Telefon 0721 / 4001 540  
Pfaff, 75 00 Karlsruhe 41

## Wie klein sind 41 x 21 x 50 cm?

So klein, daß es dafür bestimmt noch Platz in Ihrem Büro gibt? Sie täten gut daran, ihn zu nutzen.

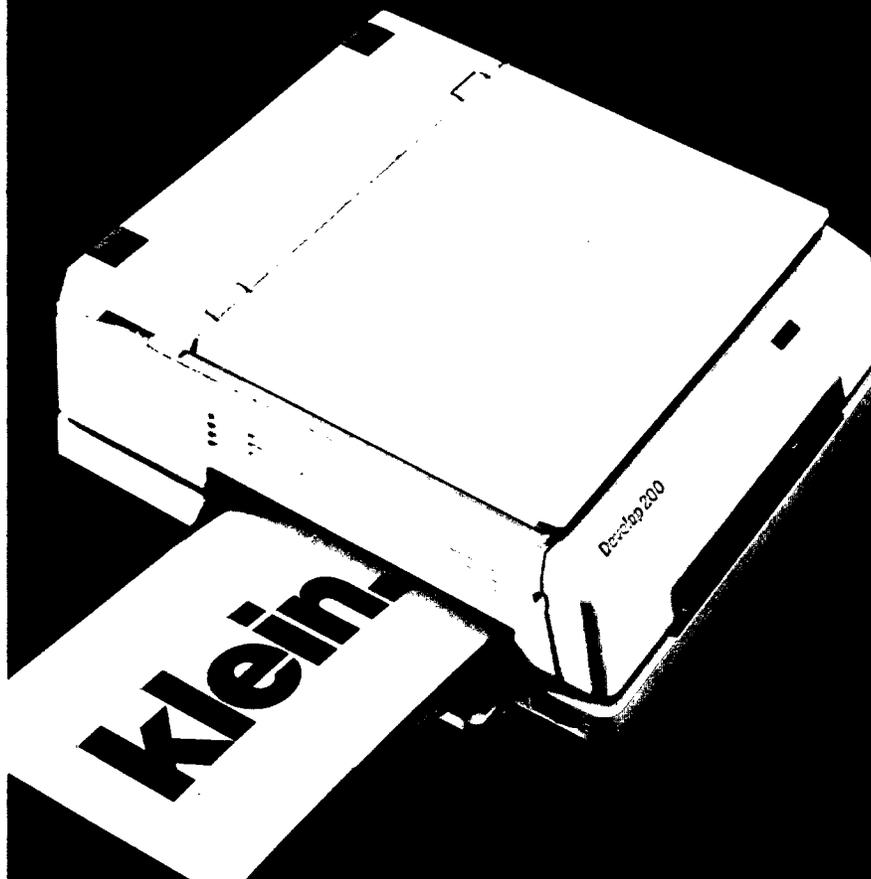
Denn so können Sie da kopieren (lassen), wo die Kopien auch anfallen – am Arbeitsplatz. Zu geringsten Kosten. In bester Qualität, gestochen scharf. Auf Normalpapier, auf Folie, auf Postkartenkarton usw.

Und in Farbe: in Rot, Blau, Braun oder Grün. Und schnell: 10 Kopien A4 in der Minute. Und vollautomatisch.

Develop 200 heißt diese kleine Sensation. Vielleicht merken Sie sich den Namen. Es könnte sich lohnen.

### Develop

Develop Dr. Eisbein GmbH & Co.  
Dieselstraße 8, D-7016 Gerlingen 1  
Telefon (0 71 56) 208-0  
Telefax (0 71 56) 208-180



win Wildgruber von der Hamburger Sparkasse weiß.

Viele tragen sogar das Computerbriefchen mit sich herum, das ihnen von ihrer Bank verschlossen und mit dem dringenden Hinweis anvertraut worden war, es nach Studium der Nummer sofort zu vernichten. Manche, die ihrem Gedächtnis nicht trauen, notieren sich die Nummer auf einem Zettel oder, für Diebe praktisch, einfach auf der Scheckkarte. „Die können“, meint ein Bankexperte, „ihr Geld auch gleich wegwerfen.“

Wer die Sicherheitsempfehlungen der Banken befolgt, ist gleichwohl nicht unbedingt vor Schaden geschützt. Das belegt der Fall der Arztfrau Sigrid Achner aus Haar bei München.

Die Bankkundin zerriß das PIN-Briefchen nach Lektüre „in ganz winzige

### *Traut die Bank selber nicht der Perfektion des Systems?*

Stücke“, die Papierschnipsel warf sie in den Müll. Aufschreiben mußte sie sich die vier Ziffern auch nicht, denn „die konnte ich mir gut merken“.

Als ihr, an einem Samstag, im Gewühl eines Kaufhauses die Handtasche entrisen wurde, machte sie sich deshalb keine Sorgen, daß der Dieb mit ihrer Eurocheque-Karte Schindluder treiben könnte. Am Montag meldete sie den Vorfall bei der örtlichen Filiale der Bayerischen Hypotheken- und Wechsel-Bank.

Acht Tage später, als Sigrid Achner Kontoauszüge abholte, stellte sie mit Schrecken fest, daß dem Unbekannten auf die gestohlene Karte am Automaten wider Erwarten doch Bares ausgezahlt worden war, insgesamt 10 000 Mark.

Wie das, ohne Kenntnis der Geheimnummer, zugehen konnte, bleibt ein Rätsel. Die PIN befand sich jedenfalls, wie Sigrid Achner glaubhaft versichert, „weder im Original noch als Notiz, auch nicht verschlüsselt“, in der geraubten Handtasche. Ebenso wenig kann jemand die Arztfrau bei einer Abhebung am Automaten beobachtet haben – sie hat ein solches Gerät nachweislich niemals benutzt.

Auch die Bank weiß keine Erklärung. Und weil an der Schilderung der Betroffenen nicht zu deuteln ist, ersetzte sie immerhin neunzig Prozent des Schadens, „obwohl wir . . . dazu nicht verpflichtet sind“.

Ist die Kulanz der Bank womöglich ein Indiz, daß das Geldinstitut der behaupteten Perfektion des Systems selber nicht ganz traut? Läßt sich die Geheimzahl, wie Computerfreaks seit einiger Zeit munkeln, doch aus den Daten auf dem Magnetstreifen errechnen?

Die Antworten auf diese Fragen sind für die Banken von dramatischer Bedeutung: Wenn die Geheimzahl keine Geheimzahl mehr ist, bricht das EC-System zusammen.

Daß die PIN aus den Karten-Daten entschlüsselt werden könne, sei „ausgeschlossen“, beteuert Johannes Hergersberg, Referent für Zahlungsverkehrsa-  
 -utomation beim Sparkassen- und Giro-  
 -verband in Bonn: Die PIN stehe „im  
 -Klartext schon mal gar nicht und auch  
 -nicht in verschlüsselter Form drauf“.  
 -Vielmehr werde die Geheimzahl „bei  
 -der Transaktion im Automaten selbst  
 -neu gerechnet“.

Die Banken verwenden dazu ein inter-  
 -national gebräuchliches Verschlüsse-  
 -lungsverfahren, den „Data Encryption  
 -Standard“ (DES). Bankleitzahl, Konto-  
 -nummer und Kartenfolgenummer – bei  
 -mehreren Scheckkarten zum selben  
 -Konto müssen sich die PIN-Zahlen auch  
 -unterscheiden – werden mit einem  
 -16stelligen geheimen „Institutsschlüssel“  
 -in 16 Rechenschritten chiffriert.

Heraus kommt, wie Hergersberg sagt,  
 -ein „kryptographischer Wert“ aus 16  
 -Ziffern. Vier davon ergeben die PIN, die  
 -der Automatenkunde eintippt, die aber  
 -nicht auf der Karte steht. Feld 13 des  
 -Magnetstreifens enthält aber einen  
 -„Kontrollparameter für die persönliche  
 -Geheimzahl“: Dieser ebenfalls vierstellige  
 -„Ergänzungswert“ wird von den Ban-  
 -ken als „die Zahl“ definiert, „die, wenn  
 -diese auf das Ergebnis der Algorithmus-  
 -rechnung angewandt wird, die persön-  
 -liche Geheimzahl ergibt“.

Jeder Geldautomat enthält, in seinem  
 -gepanzerten Gehäuse, einen Verschlüs-  
 -selungschip, der in Sekundenschnelle  
 -jedemal die DES-Chiffrierung nach-  
 -vollzieht, wenn ein Kunde seine Scheck-  
 -karte in das Gerät schiebt. Passen  
 -PIN und Ergänzungswert zusammen,  
 -gibt der Automat die Geldausgabe-  
 -Taste frei.

Bisher, behauptet Hergersberg, sei es  
 -noch keinem gelungen, den Code zu  
 -knacken.

Doch es steht dahin, wie lange der  
 -Bankmanager recht behält. Unter Beru-  
 -fung auf die westdeutsche „Hacker-Sze-  
 -ne“ berichtet jedenfalls der Freibur-

### **Läßt sich die Verschlüsselung mathematisch ermitteln?**

ger Rechtswissenschaftler Ulrich Sieber  
 -in einem soeben in Großbritannien er-  
 -schienenen Handbuch über Computer-  
 -Verbrechen, „mehrere Computer-  
 -Freaks“ seien „gegenwärtig dabei, den  
 -DES-Algorithmus zu entziffern“\*.

Ein süddeutscher EDV-Fachmann  
 -versicherte dem SPIEGEL sogar, er  
 -könne aus nur drei Scheckkarten, deren  
 -PIN-Zahlen er kennt, innerhalb einer  
 -Stunde zu einer vierten, ihm fremden  
 -Karte zwei alternativ mögliche Geheim-  
 -nummern ausrechnen. Welche davon  
 -paßt, müßte sich dann im Praxistest

\* Ulrich Sieber: „The International Handbook on  
 -Computer Crime“. Verlag John Wiley & Sons.  
 -Chichester; 288 Seiten; 24,95 £.

## CELLVITAL®-Therapie

# Medizinische Revitalisation durch aktive Gewebetransplantate.



**D**ie CELLVITAL-Therapie ist  
 eine biologische Behandlungsweise  
 auf der Basis von aktiven Gewebe-  
 transplantaten.

Die zahlreichen Funktionsstö-  
 -rungen, durch die moderne Lebens-  
 -art hervorgerufen, stellen den  
 -Anwendungsbereich dieser Therapie  
 -dar. Die physischen und psychi-  
 -schen Belastungen sind für den Men-  
 -schen der Ursprung von Müdigkeit  
 -und Überbeanspruchung (Stress)  
 -oder sie bedeuten selbst ein vorzeiti-  
 -ges Altwerden. Das Resultat ist ein  
 -mehr oder weniger stark ausgepräg-  
 -tes Nachlassen der Lebensorgane.  
 -Der CELLVITAL-Behandlungsvorgang  
 -strebt eine Stärkung des Organismus  
 -an, und sein Ziel besteht darin, die  
 -geschwächten Organe durch das  
 -Eingreifen der aktiven Eigenschaf-  
 -ten, die sich im Kern der Transplan-  
 -tate befinden, neu zu revitalisieren.  
 -Die CELLVITAL-Behandlung wird seit  
 -30 Jahren angewendet. Sie profitiert  
 -von Erkenntnissen, die nur die

Klinik Lémana dank ihrer strengen  
 -Kontrollen, welche am Material  
 -nach der Entnahme durchgeführt  
 -werden, offerieren kann. Eine Kur  
 -unter ärztlicher Aufsicht dauert  
 -eine Woche.

Für alle Auskünfte:

**CLINIQUE LEMANA**  
 21, Av. Bosquets-de-Julie  
 CH-1815 Clarens s/Montreux 665  
 Schweiz

Name \_\_\_\_\_

Vorname \_\_\_\_\_

Strasse \_\_\_\_\_

PLZ/Ort \_\_\_\_\_

Tel. (004121) 641 641. Telex: 453 160 cdrl.

erweisen. Da die Geldautomaten zwei Fehlversuche tolerieren, würde der elektronische Bankraub allemal gelingen.

Auch Guido Maria Rossi, Generaldirektor einer italienischen Firma für Sicherheitssysteme, der an einer Studie des Verbandes italienischer Banken über Automaten-sicherheit mitgewirkt hat, ist überzeugt, daß der Algorithmus „mathematisch ermittelt“ werden kann – „wenn man eine bestimmte Anzahl an Geheimzahlen kennt und die entsprechenden Scheckkarten besitzt“.

Dann, schreibt Rossi in der Zeitschrift „Banca Oggi“, wären Betrüger sogar in der Lage, total gefälschte Karten zu produzieren und sich selbst die zu den Kartendaten passenden Geheimzahlen zuzuteilen. In großen Mengen hergestellte Fälschungen ließen sich nacheinander am selben Automaten einsetzen, „bis er vollständig geleert ist“ – jeder hält „im allgemeinen viele Dutzend Millionen Lire“ vorrätig, umgerechnet um die 100 000 Mark.

In der Bundesrepublik könnten Karten-Mafiosi, wenn sie das Sicherungssystem überwinden, noch mehr ergattern: Westdeutsche Bankautomaten haben das Doppelte bis Dreifache in Reserve. Allerdings beteuern deutsche Ban-

### **Der Kode wird unter Infrarotlicht sichtbar**

ker, hier sei jene Art der Automaten-leerung, die Rossi beschreibt, undenkbar; durch eine maschinelle Echtheitsprüfung würden Fälschkarten aussortiert – Blanketten sowieso, aber auch echte Karten, die auf Phantasiekonten lauten oder deren Magnetstreifen-Daten verändert worden sind.

Tatsächlich hat jede westdeutsche Eurocheque-Karte ein individuelles „Moduliertes Merkmal“ (MM), das Mißbrauch unmöglich machen soll: Bei der Herstellung wird im blauen Namensfeld auf der Vorderseite eine fünfstellige Schlüsselzahl eingedruckt, die mit bloßem Auge nicht sichtbar ist. Als Druck-„Farbe“ werde, wispert Eingeweihte, eine „seltene chemische Substanz“ verwendet.

Zudem wird der „MM-Schlüssel“ mit bestimmten Kartendaten verknüpft und als „Kartensicherungskode“ im Magnetstreifen chiffriert. Verändert ein Fälscher auch nur eine Ziffer der Kontonummer, ergibt sich ein völlig anderer Kode. Daher ist es auch unmöglich, das Verfalldatum einer abgelaufenen Scheckkarte durch einen elektronischen Eingriff in die Zukunft zu verlegen.

Eine „MM-Box“ in den Geldautomaten kontrolliert den Kode, ein Sensor tastet die Karten nach dem mysteriösen Merkmal ab. DSGV-Referent Hergersberg hält es für „ausgeschlossen, daß jemand die Beschaffenheit des Merk-



**Sparkassen-Referent Hergersberg**  
Geheime Berechnung im Automaten

mals in Erfahrung bringen könnte“. Denn es beruhe auf einer „geheimen Rezeptur“, die nur der „lizenzierte Hersteller“ fertigen könne – Giesecke & Devrient.

„Selbst mit hochwertigen Laboreinrichtungen“, behauptet Firmenpatriarch Otto, seien „Analyse und Reproduktion“ für Fälscher „schwer oder überhaupt nicht möglich“ – dank der „physikalisch-technischen Ausstattung des MM-Schlüssels“ und der „Anwendung gewerbeunüblicher Techniken und Materialien, die am freien Markt nicht erhältlich sind“.



**Rechtsexperte Sieber**  
Anekdoten aus der Hacker-Szene

Doch experimentierfreudige Automatenutzer wissen, daß noch längst nicht alle Bankomaten mit der MM-Box ausgerüstet sind. Und wo das Prüfgerät installiert ist, schaffen es erfinderische Bastler, den elektronischen Kartentest wirkungslos zu machen.

Denn der auf der Scheckkarten-Frontseite verborgene MM-Kode läßt sich unter Infrarotlicht mit bestimmten optischen Filtern sichtbar machen. Ein Fälscher kann eine echte Eurocheque-Karte beliebig oft reproduzieren, indem er die MM-Felder alter Scheckkarten zerschneidet und die Segmente in der richtigen Ziffernfolge neu zusammensetzt – sie paßt folgerichtig auch zum Kartensicherungskode auf dem kopierten Magnetstreifen.

Geldautomaten können derlei Fälschungen nicht von den Originalen unterscheiden, wie ein unter Aufsicht vorgenommener Versuch in Baden-Württemberg belegt: Die Villingener Volksbank hat schriftlich bestätigt, daß an ihrem Automaten, einem „NCR 5080 mit MM-Box“, am 5. Dezember vergangenen Jahres „mit einer improvisierten Karte“ Geld abgehoben wurde. „Bei der Verfügung . . . mit der rekonstruierten Karte“, so der Organisationsleiter der Bank, „wurde die MM-Prüfung nicht beanstandet.“

Was dem Tüftler gelang, ist gewiß auch Kriminellen möglich. Und wenn der Fälscher eine zeitweilig entwendete Karte dem rechtmäßigen Besitzer klammheimlich zurückgibt, merkt der erst an seinen Kontoauszügen, daß er geklaut worden ist.

Vielleicht läßt sich auf diese Weise erklären, was Ralf Steynen widerfuhr. Jedenfalls ist nicht auszuschließen, daß im Fall Steynen jemand mit einer nachgemachten Karte abkassiert hat.

Ein mögliches Beweismittel, das Zweifel beseitigen könnte, hat die Stadtparkasse Köln nicht genutzt. Nach den gemeinsamen Richtlinien der Banken müßte auf dem Magnetstreifen von Steynens Karte der Tag der letzten (umstrittenen) Abhebung notiert sein. Doch die Kasse verzichtet, wie viele Geldinstitute, auf eine solche Notierung, weil das Rechenzentrum die Transaktion festhält.

So gelingt es bestohlenen Kunden in der Regel nicht, falschen Verdacht auszusräumen. Dabei wäre die Beweissicherung ganz einfach: Wenn auf dem Magnetstreifen der Originalkarte kein Datum notiert ist, an dem eine strittige Auszahlung erfolgte, kann die echte Karte jedenfalls nicht im Automaten gesteckt haben. Folglich muß ein falsches Doppel im Spiel gewesen sein.

Die Banken verweigern ihren Kunden nicht nur ein Beweismittel, sie leugnen – trotz gegenteili-

**JB**  
1735  
**BLANCPAIN**



Schon über 250 Jahre...  
und trotzdem machen wir immer noch keine Quarzuhren.  
Es wird auch nie eine bei Blancpain geben.

Denn die acht Uhren, die das Atelier jeden Tag verlassen,  
werden nach wie vor von Hand zusammengesetzt,  
poliert und jede mit einer eigenen Nummer versehen.

Katalog und Information durch **BLANCPAIN SA CH-1348 Le Brassus**  
Tx 459 420 Tél. 021 85 40 92

AACHEN Lückert AUGSBURG Hirt BADEN-BADEN Friedrich BERLIN Hüls BONN Toussaint BREMEN Brinckmann & Lange,  
Wempe DARMSTADT Teichel DORTMUND Rüschenbeck DUISBURG Rüschenbeck, Jansen DÜSSELDORF Blome, Wempe ESSEN  
Deiter FRANKFURT Friedrich, Wempe, Christ GLADBECK Exner GÜTERSLOH Lübke HAGEN Rüschenbeck HAMBURG Becker,  
Wempe HANNOVER Brinckmann & Lange, Wempe HEIDELBERG Rieth HEILBRONN Luthke KARLSRUHE Kamphus KOBLENZ  
Hofacker KÖLN Höltscher, Wempe LANDSHUT Schneider LÜBECK Meyer LÜDENSCHIED Hohage MANNHEIM Braun, Friedo  
Frier MÖNCHENGLADBACH Simon MÜNCHEN Hemmerle, Huber, Weissberg, Wempe MÜNSTER Freisfeld NÜRNBERG Wempe,  
Wallner OSNABRÜCK Bretschneider, Franke & Middelberg REUTLINGEN Depperich STUTTGART Wempe, Friedo Frier TIMMENDORFER-  
STRAND Lindner TRIER Press WÜRZBURG Fischer.

ger Erfahrung – auch die Möglichkeit technischer Manipulationen.

Zweifel an der Sicherheit des Systems empfinden die Geldinstitute als ungeschicklich. Daß Mißtrauen angebracht ist, beweisen indes die Vorwürfe von Banken-Sprechern, der „ARD-Ratgeber Technik“ habe „Verbrecher- statt Verbraucher-Aufklärung“ geleistet – wenn es die Systemmängel nicht gäbe, wäre die ganze Aufregung überflüssig.

Zudem können die Banken nicht ausschließen, daß ungetreue Kassen-Angestellte an Automatenräubereien beteiligt

**„Banken sind nicht nur von Engeln besetzt“**

sind. „Die Banken“, sagt der Hamburger Rechtswissenschaftler Udo Reifner, „sind nicht nur von Engeln besetzt.“

Möglich ist beispielsweise, daß ein Kontoführer, bevor er dem Kunden das PIN-Briefchen aushändigt, die Perforationsheftung auf Schraubenzieher-Breite öffnet. Da läßt sich dann ein Strohhalm einführen, an dessen Enden winzige Spiegel angebracht sind. Die minimale Beschädigung fällt, wie ein automatenbeschädigter Bankkunde nachgewiesen hat, kaum auf.

Oder: Entgegen der Beteuerung der Banken kann die Geheimzahl im verschlossenen Umschlag „unter dem schleifenförmigen Überdruck mit gerichteten Scheinwerfern sichtbar gemacht werden“ – der Hamburger Polizeihauptkommissar Heerdts hat es selber ausprobiert.

Und: Auch durch Rubbeln ist die Geheimzahl zu ermitteln. Die Umschläge der PIN-Briefchen, die oftmals nach dem Öffnen achtlos in der Schalterhalle weggeworfen werden, „funktionieren wie normale Selbstdurchschreibesätze“: Im leeren Kuvert, enthüllte die ARD, seien zwar keine Abdrücke zu sehen, aber „um die verdeckte Zahl wieder sichtbar zu machen, genügt ein Quitungsblock“ – die beschichteten Papiere reagieren auf Druck.

Obwohl der Umgang mit den Automatenkarten also „ganz offensichtlich risikoreich“ ist, wie Rechtsprofessor Reifner von der Hamburger Hochschule für Wirtschaft und Politik bemängelt, weisen die Geschäftsbedingungen der Banken „das Risiko einseitig den Kunden zu“ – ein rechtspolitischer Skandal.

„Der Kontoinhaber“, heißt es schlichtweg in den Benutzungsbedingungen für Geldautomaten, „trägt . . . alle Schäden, die durch eine unsachgemäße oder mißbräuchliche Verwendung oder durch Verfälschung einer auf sein Konto ausgegebenen Eurocheque-Karte mit Magnetstreifen entstehen.“

Verantwortlich gemacht wird der Kunde ebenso für Schäden aus einer „mißbräuchlichen Verwendung der per-

sönlichen Geheimzahl“ – die Banken sparen keinen Eventualfall aus, um sich aus der Verantwortung zu stehlen.

Selbst wenn der Kontoinhaber, vertragsgemäß, sofort meldet, daß seine Scheckkarte verlorengegangen ist oder daß er den „begründeten Verdacht“ hat, ein „Unbefugter“ habe „Kenntnis von der persönlichen Geheimzahl erlangt“, bleibt die Hauptlast an ihm hängen.

Für Schäden, die „nach einer derartigen Benachrichtigung des ausgebenden Kreditinstituts eingetreten sind“, muß der Kunde „nur bis zu einem Betrage von DM 800,-“ aufkommen – eine euphemistische Formulierung: Die zuvor aufgelaufenen Summen hat er allein zu tragen.

Wenn der Kunde erst nach Tagen oder Wochen merkt, daß seine Scheckkarte verschwunden ist, kann ein Dieb ganze Jahresgehälter einsacken, ohne daß die Bank zur Rückzahlung auch nur eines Pfennigs verpflichtet wäre: Nach den Geschäftsbedingungen ist sie „berechtigt“, das Konto „auch bei mangelndem Guthaben zu belasten“.

Als sich Ralf Steynen bei der Stadtsparkasse Köln beschwerte, daß er aufgrund der von ihm bestrittenen Abhebungen mit mehr als 10 000 Mark in die Miesen gerutscht sei, obwohl das ihm eingeräumte Dispositionslimit nur 3500 Mark betrage, verwies ihn die Kasse kühl auf ein Urteil des Landgerichts Lüneburg: Die Geldinstitute bräuchten ihre Automaten „nicht so zu programmieren, daß eine Kontoüberziehung gar nicht oder je nach Kreditwürdigkeit des Kunden nur bis zu einer bestimmten Höhe möglich ist“.

Daß die Automaten großzügig Minus-Salden ignorieren und Kreditlimits auf den Magnetstreifen nicht vermerkt sind, verführt nicht nur rechtmäßige Karteninhaber, sich über Gebühr selbst zu bedie-

### **Alarmwege sind umständlich und zeitraubend**

nen. Die fehlende Summenbeschränkung verhilft auch Kartendieben zu unbegrenztem Geldsegen.

Kaum ein Kunde, der sich das Kärtchen mit Geheimzahl als bequemes Mittel zur Bargeldbeschaffung hat aufschwätzen lassen, ahnte bislang, worauf er sich da einließ.

Zwar versprechen die Banken in der Regel, Betrugsopfer würden kulant entschädigt. Doch mit der versprochenen Großzügigkeit ist es in der Praxis nicht weit her.

Beteuerungen von Betrogenen, sie hätten ihre Geheimzahl nirgendwo oder nur an gut gesicherter Stelle notiert, tun die Banken regelmäßig als Schutzbehauptung ab. Nur wenn, wie bei dem Kölner Coup, die Täter überführt sind oder, wie in Braunschweig, der Tathergang eindeutig geklärt ist, springen der

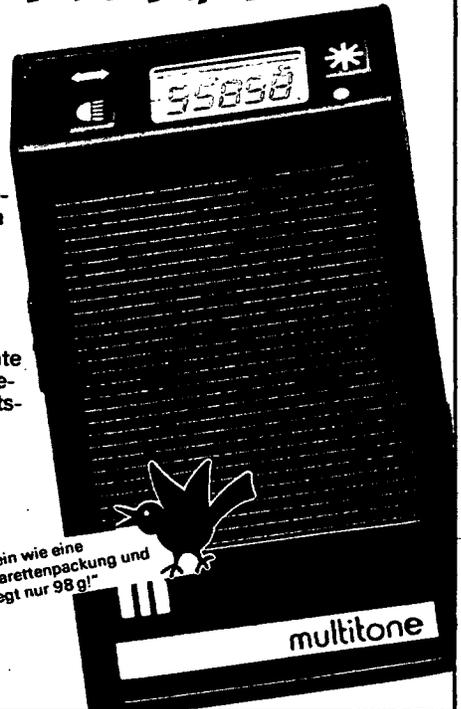
# PIEPSER und WARNT

## Modell access

ist die findige Personensuchanlage von Multitone, mit der Sie mehr machen können als nur piepsen:

**z. B. bis zu 8 unterschiedliche Rufsignale wie Alarm, Notruf, Gruppenruf, Sammelruf, Selektivruf, Telefon etc. akustisch und optisch übermitteln!**

Machen auch Sie den Schritt vom Piepser zum fortschrittlichen Informationssystem. Das Modell access bietet ausgeklügelte Technik und kinderleichte Handhabung. Der modulare Aufbau gewährleistet maßgeschneiderte zukunfts-sichere Lösungen.



☎ 0211 / 48 44 01

**multitone**

Die bessere Verständigung

Multiton Elektronik GmbH  
Roßstraße 11, 4000 Düsseldorf 30

„Klein wie eine Zigarettenpackung und wiegt nur 98 g!“



Kein Grund zur Panik. In der Normandie ist alles beim alten. Hamsterkäufe von Calvados und Gläschen horten sind völlig unangebracht.

*Calvados ist etwas Feines.*

*(Offizielle Meinung des Bureau National Interprofessionnel des Calvados.)*

Haftungsfonds der Sparkassen oder die Automatenmißbrauchversicherung der Banken ein.

Wo es dagegen wirklich um Kulanz ginge, wird das Ansinnen schnöde zurückgewiesen.

Beispiel Heike Gerdener: Die Chemielaborantin aus Spenge bei Bielefeld hatte, wie die Kreissparkasse Herford bestätigt, noch niemals zuvor ihre Eurocheque-Karte an einem Geldautomaten verwendet, als sie ihr aus dem Umkleide-raum einer Turnhalle gestohlen wurde. Innerhalb von zwölf Stunden hob der unbekannte Dieb 4000 Mark ab. Doch die Sparkasse beschied die Geschädigte schroff, „daß ein Kulanzantrag aussichts-

les Risiko einzugehen. Aber nur wenige Banken sind zum Umtausch bereit, wenn Kunden eine neue Karte verlangen, die nur für Schecks gültig ist. Es gibt jedoch, so der Jurist Reifner, „keine Verpflichtung des Kunden, die gefährlichen Karten zu behalten“.

Die „ins Gerede gekommene Scheckkarte“, prophezeien die jugendlichen Computer-Piraten von der „Bayrischen Hackerpost“ bereits, werde „ja wohl in der nächsten Zeit zu Grabe getragen“ – eine Prognose, die keineswegs voreilig anmutet.

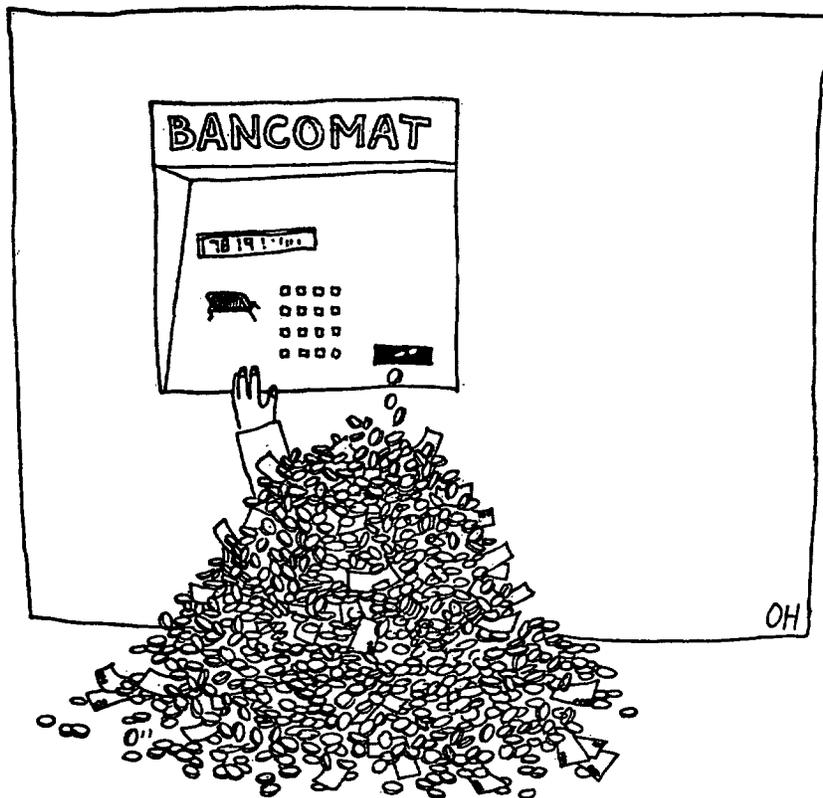
Denn es gibt nur geringe Möglichkeiten, das EC-System kurzfristig besser gegen Mißbrauch zu sichern. So sind die

außerhalb der Schalterstunden entgegen- nimmt.

Neuerdings erst, nach den jüngsten Automatenraubzügen, sieht sich die Branche zu hektischem Handeln veranlaßt. Denn wenn die verschreckte Kundenschaft vollends das Vertrauen in die Geldroboter verliert, ginge die Rechnung der Banken nicht mehr auf, für die sich der Service bislang bezahlt gemacht hat: Die „Stückkosten“ einer Barabhebung am Kassentresen betragen, wegen des Personal- und Papieraufwands, etwa 2,50 Mark, derselbe Vorgang am Automaten kostet die Banken gerade einen Groschen.

Deshalb ist das Kreditgewerbe bestrebt, die bloßgelegten Schwächen des Systems eilends zuzudecken. Bis Mitte nächsten Jahres, kündigen die Verbände an, sollen alle westdeutschen Geldautomaten durch direkte Datenfernleitungen („on line“) elektronisch miteinander verknüpft werden. Die von zentralen Rechnern ferngesteuerten EDV-Kassen würden die Auszahlungen selbsttätig verweigern, sobald Plastik-Falschgeld untergeschoben wird.

Bislang existiert ein solcher Datenverbund nur regional zwischen Automaten, die zum selben Kreditinstitut gehören. Doch auch die künftige Ausbauplanung sieht nur Inselnetze vor, jeweils getrennt



Süddeutsche Zeitung

los ist und eine Erstattung durch uns entfällt“.

Heike Gerdeners Fehler war ihre Ehrlichkeit. Arglos erzählte sie dem Filialleiter, als sie den Verlust der Karte anzeigte, sie habe ihr PIN-Briefchen aufgehoben und in ihrer Dokumentenmappe wohlverwahrt. Dies verstoße „gegen die vertraglichen Bestimmungen“, argumentiert die Sparkasse: „Die Möglichkeit, daß Dritte diese Geheimzahl – bei welcher Gelegenheit auch immer – ausgespäht oder erfahren haben, ist so nicht auszuschließen.“ Unter Hinweis auf eine formale Vertragsverletzung ziehen sich die Banker aus der Affäre, zur Tataufklärung brauchen sie so nichts beizutragen.

Viele Karteninhaber wollen denn auch lieber auf die Automatenberechtigung verzichten, als ein unwägbares finanziel-

Alarmwege umständlich und zeitraubend: Die Nummern verlorener oder gestohlener Eurocheque-Karten, die gesperrt werden sollen, müssen von den Banken per Datenfernleitung oder Telex einer „Evidenzzentrale“ in Frankfurt mitgeteilt werden, die dann alle anderen Automatenbetreiber benachrichtigt.

„Natürlich gibt es da ein zeitliches Loch“, räumt Sparkassen-Referent Hergersberg ein. In der Regel vergehen, wenn ein Kunde den Verlust seiner Karte mitteilt, mehrere Tage, ehe sie gesperrt wird.

Daran ändert nichts, daß die Evidenzzentrale, wie Hergersberg berichtet, „jetzt auch an Wochenenden arbeitet“. Denn nur ganz wenige Banken haben bislang einen Bereitschaftsdienst organisiert, der Schadensmeldungen auch

### *Kleine Fingerzeige für Ganoven*

für Sparkassen, Privatbanken, Genossenschaftsbanken und Post. Auch dann wird etwa ein Volksbank-Automat keine Karte zurückweisen, die am selben Tag anderswo schon im Einsatz war.

Später erst sollen die Computer-Inseln über Zwischenrechner zusammenschaltet werden. Über Ausbaustand und zeitliche Perspektiven schweigen sich die Organisationen aus – angeblich, um Ganoven keine Fingerzeige zu geben.

Doch die Geheimniskrämerei belastet eher das Verhältnis zu den ehrbaren Kunden. Wo Aufklärung geboten wäre, setzen die Banken ihre Desinformationspolitik fort. Und sie täuschen Sicherheit vor, obschon die Angriffsflächen, die das System bietet, offenkundig sind.

Schwachstellen werden geleugnet, bis sie in der Praxis nachgewiesen sind. Bisweilen bequemen sich die Banken nicht einmal dann zur Wahrheit.

So behauptete der Rheinische Sparkassen- und Giroverband, zur Zeit der rätselhaften Abbuchungen von Steynens Konto sei in ganz Köln „lediglich ein Automat nach einer Neuinstallation noch nicht mit der MM-Box versehen“ gewesen, die falsche Karten hätte erkennen müssen.

Allein Jonas und sein Komplize hatten zur selben Zeit vier solcher Geldspender aufgespürt. ◆