Sicherheit

Betrug im SB-Bereich: der **Anscheinsbeweis** wird **schwieriger**

Von Jörg Dettenbach und Felix Maria Rüther

Rund 60 Millionen Euro Schaden entstanden im vergangenen Jahr bei Betrugsfällen im SB-Bereich der Finanzdienstleister. Setzen Kreditinstitute veraltete Sicherungstechnik ein, so verletzten sie ihre Sorgfaltspflicht, erläutern die Autoren. Gleich ob der geschädigte Verbraucher den Anscheinsbeweis, der bisher meist für die Anbieter sprach, anficht oder nicht: So oder so tragen die Institute mit unwirksam gewordenen oder fehlenden Sicherungsmechanismen einen größeren Anteil der Schadenssummen. Red.

Der aufkeimende Optimismus aus dem vergangenen Jahr wich schnell neuer Sorge um die Sicherheit im SB-Bereich. Spätestens seit der Pressemitteilung des BKA vom 10. Mai dieses Jahres hat die Bankenbranche Gewissheit: „So wurden 2010 in Deutschland 3 183 Angriffe auf Geldautomaten registriert, was eine Steigerung von 55 Prozent gegenüber dem Vorjahr (2 058 Angriffe) bedeutet. Dabei waren 1 765 verschiedene Geldautomaten das Ziel von Manipulationen, auch hier ist eine Steigerung im Vergleich zu 2009 zu verzeichnen, und zwar um 83 Prozent (2009: 964 Automaten)."

Der finanzielle Schaden sei auf etwa 60 Millionen Euro zu schätzen, was im Vergleich zum Vorjahr immerhin eine Steigerung um 20 Millionen Euro bedeutet. Bankkunden und Verbraucherschützer fragen sich, ob und wann die Geldinstitute dieser Entwicklung nun endlich wirksam entgegentreten. Kein Institut möchte und kann sich – aus verschiedenen Gründen – weiteres Misstrauen in die Wirksamkeit ihrer Sicherheitslösungen und Präventionsansätze im SB-Bereich leisten. Zum einen ist der finanzielle Schaden (trotz Ausgleichsfonds) der Kostenreduktionstrategie in der Branche wenig zuträglich. Zum anderen wirft das Auftreten von Schadensfällen an den eigenen Automaten ein schlechtes Licht auf das Betreiberinstitut. Wie so oft sind die Folgen dieses Imageschadens nicht leicht zu messen.

Die massive Zunahme der Schadensfälle und die fehlende Ursachenbehebung ruft nun auch die Rechtsprechung auf den Plan. Laut einem Urteil des Kammergerichts Berlin vom 29. November 2010 heißt es: „In der Verwendung eines herkömmlichen TAN-Systems durch die Bank kann dann eine Sorgfaltspflichtverletzung gesehen werden, wenn dieses System bei der Mehrzahl der Kreditinstitute nicht mehr im Einsatz ist und hinter dem Sicherungsstand des neueren Systems zurückbleibt." Unter Bezugnahme auf das Urteil kann also allgemeiner gesagt werden, dass Kreditinstitute dann Sorgfaltspflichtverletzungen begehen, wenn sie überholte Sicherungstechnik einsetzen. Damit können auch die Bemühungen für eine wirksame SB-Betrugsprävention unter einem neuen Blickwinkel gesehen werden.

Zu den Autoren

Jörg Dettenbach ist Leiter Business & Sales der SARROS GmbH, Berlin, und **Felix-Maria Rüther** ist Rechtsanwalt für Bank- und Insolvenzrecht, Berlin.

Bestreitet nämlich der Kontoinhaber, die Auszahlung an einem Geldausgabeautomaten vorgenommen zu haben, trägt das Finanzinstitut zunächst die Beweislast für die Echtheit der Geldabhebung. Hierbei beruft es sich regelmäßig auf den Anscheinsbeweis, der dann zu seinen Gunsten greift, wenn die ec-Karte und die PIN bei ordnungsgemäßer Funktion des Geldautomaten verwendet wurden.

Deutliches Herausfallen einer Transaktion aus dem Nutzerprofil

In diesem Falle gehen die Gerichte davon aus, dass entweder der Kontoinhaber die Verfügung selbst vornahm oder ec-Karte und PIN an einen Dritten weitergegeben beziehungsweise dem Schädiger zugänglich gemacht wurden. Folglich sei nach der Lebenserfahrung zwar ein anderer Geschehensablauf nicht ausgeschlossen, aber als sehr unwahrscheinlich anzusehen. Allerdings stellt man sich bei der zwischenzeitlich aufgetretenen Fülle manipulierter Geld-

automaten zu Recht die Frage, ob derartige Manipulationen heute noch so unwahrscheinlich sind, dass der Anscheinsbeweis weiterhin bedenkenlos zugunsten der Finanzinstitute gelten kann.

Der Kontoinhaber hingegen kann den Anscheinsbeweis erschüttern, wenn es ihm gelingt, die Möglichkeit eines anderen als den typischen Geschehensablauf schlüssig darzutun und zu beweisen. Vor dem Hintergrund der Häufung der Manipulationsfälle und deren technischer Raffinessen dürfte dem Kontoinhaber heute die Erschütterung des Anscheinsbeweises daher zum Beispiel gelingen, wenn die von ihm bestrittene Transaktion aus seinem bisherigen gewohnten Nutzungsprofil in Bezug auf die Höhe der Verfügung, den Ort, die Uhrzeit, beispielsweise, deutlich herausfällt.

70 Prozent des Schadens trägt die Bank

Auch wenn der Anscheinsbeweis durch den Kontoinhaber nicht erschüttert wurde, trifft das Finanzinstitut ein erhebliches Mitverschulden an dem Schaden, also der bestrittenen Verfügung und es trägt deshalb auch einen ebenso erheblichen Anteil an dem Schaden, wenn es mit veralteter Technik operiert, weil es beispielsweise überholte oder gar keine Nutzerprofilsoftware verwendet, die atypische Verfügungen an Geldausgabeautomaten verhindert. Ein solches Finanzinstitut lässt nämlich diejenige Sorgfalt außer Acht, die jedem ordentlichen und verständigen Kaufmann obliegt, um sich und die berechtigten Nutzer von Geldautomaten vor Schäden zu schützen. Aus eben diesem Grunde hat das Kammergericht in dem Phishing-Urteil vom 29. November 2010 das Finanzinstitut verurteilt, 70 Prozent des entstandenen Schadens selbst zu tragen.

Die Devise für die Zukunft lautet folglich: Banken und Sparkassen müssen schnell in nachhaltige Präventionsmechanismen investieren. Doch wie können die Institute dem Anspruch der Sorgfaltspflicht wirklich gerecht werden? Verschiedene Lösungsansätze versprachen in der Vergangenheit mehr Sicherheit. Hardwareseitige Lösungsansätze beispielsweise bieten keinen Schutz, sobald die Kunden Automaten anderer Institute besuchen, die keine entsprechende Hardwareausstattung besitzen. Zudem weisen sie leider nur eine begrenzte Nutzendauer auf: Sind sie im Augenblick noch wirksam, stehen sie den Manipulationsideen von morgen schon wieder wehrlos gegenüber.

Auch EMV, der in Europa verbreitete chipgestützte Sicherheitsstandard, oder biometrische Authentifizierungswege sind Ansätze für einen Ausweg aus dem SB-Sicherheitsproblem. Tatsache ist jedoch, dass nicht alle Karten weltweit mit EMV-Chips ausgestattet sind. Zudem findet automatisch ein Fallback auf den Magnetstreifen statt, wenn der EMV-Chip oder biometrische Merkmale nicht vom Automaten gelesen werden können. Im Sinne der Interoperabilität dieser Verfahren wäre es ebenso erforderlich wie auch unwahrscheinlich, dass weltweit alle Institute auf diese Technik umstellen.

Deutschlands Kreditinstitute haben die Notwendigkeit zum Handeln erkannt und sich mit neuen Kartenstrategien auseinandergesetzt. So ist, beispielsweise, die Abschaffung des Magnetstreifens im Jahre 2011 ein Kernthema der Branche. Wie und in welcher Form Kunden im Ausland, wo der Magnetstreifen als Identifikationsmedium wohl noch Jahre gebraucht wird, zu Bargeld kommen, wird mal mehr, mal weniger kundenfreundlich gelöst werden. Die einen Institute wollen ihren Kunden Zweitkarten anbieten, die nur für den Einsatz im Ausland nutzbar sind. Die anderen konzentrieren sich eher auf die kundenindizierte Freischaltung der Karte für den Auslandseinsatz.

Ob eine neue Kartenstrategie die Lösung aller Probleme im Bereich SB-Betrug sein wird, ist fraglich. In Fachkreisen bestehen schon jetzt Zweifel ob ihrer nachhaltigen Wirksamkeit. Schlussendlich werden die kriminellen Energien nicht versiegen, sondern stets nach neuen Betrugswegen suchen. Genau darum sollten Banken und Sparkassen strategisch klug handeln und zusätzlich zu den bestehenden Aufgaben die softwareseitige Betrugsprävention auf die Agenda heben.

Sicherheit unabhängig vom Einsatzort

Der Markt hält geprüfte Lösungen für mehr Sicherheit im Bereich der kartengestützten Bargeldbeschaffung und Bezahlvorgänge bereit. Die Berliner Sarros GmbH zum Beispiel hat mit witFD ein Werkzeug entwickelt, das nachhaltig Manipulation verhindert. Mit Hilfe dieser Lösung werden sämtliche Transaktionen der institutseigenen Kunden, ob nun an den eigenen oder fremden SB-Geräten, auf Betrugsverdacht überprüft und bewertet. Mittels eines intelligenten Algorithmus werden unrechtmäßige Transaktionen erkannt.

Weltweit und unabhängig von der eingesetzten Sicherheitstechnologie der bargeldbereitstellenden Bank oder Sparkasse ließen sich Betrugsversuche eindämmen und das notwendige Vertrauen in die SB-Geräte erhalten. Mehr noch: Im Gegensatz zu anderen Präventionsansätzen erfordert die vergleichsweise einfache Integration der Lösung keine hohen Anfangsinvestitionen in Hardwarekomponenten und wird selbst höchsten Performanceanforderungen gerecht.

Immer mehr Sparkassen und Banken öffnen sich zukunftsorientierten Präventionsmaßnahmen. Nicht zuletzt mit Blick auf die Wahrung ihrer Sorgfaltspflichten sollten die Institute dabei genau prüfen, ob sie mit ihrer eingesetzten Lösung zeitgemäß aufgestellt sind. Sonst drohen möglicherweise auch rechtliche Konsequenzen. Die sicherste Strategie unerwünschter Folgen von Betrug im SB-Bereich zu vermeiden wäre, sich modernsten Präventionslösungen zu öffnen und sich stets mit den Neuerungen des Marktes auseinanderzusetzen. Vorteile hätte diese Vorgehensweise allemal – nicht nur aus rechtlicher Sicht.