Sichere Banken

Wie Geldinstitute sich selbst, ihre Mitarbeiter und Kunden vor kriminellen Angriffen schützen können, wurde bei den 3. Bankensicherheitstagen in Frankfurt erörtert.

Im Jahr 2010 wurden in Deutschland 327 Raubüberfälle auf Geldinstitute und 106 auf Postfilialen und -agenturen verübt. Die Zahl der Überfälle auf Geldinstitute ist gegenüber dem Jahr davor fast gleich geblieben, die Aufklärungsquote stieg von 71 auf 82 Prozent. 2003 wurden noch 767 Raubüberfälle auf Banken verzeichnet. Seit 2001 war auch ein Rückgang der erbeuteten Beträge festzustellen. 2002 betrug die Schadensumme 27,5 Millionen Euro; in den Jahren 2009 und 2010 jeweils 9,8 Millionen Euro. Das sei darauf zurückzuführen, dass in den Instituten der Zugriff auf das Geld erschwert wurde, sagte Claus Opfermann vom LKA Hessen bei den 3. Bankensicherheitstagen am 15. und 16. November 2011 in Frankfurt/Main – organisiert von der *Simedia (www.simedia.de)*.

Zu rechnen sei laut Opfermann allerdings mit einer Verlagerung der Raubkriminalität auf Tankstellen, Spielhallen und Supermärkte. Bei diesen könnten die längeren Öffnungszeiten einen Tatanreiz bilden. Etwas mehr als die Hälfte der Täter sind bereits polizeilich in Erscheinung getreten, Frauen treten kaum als Bankräuberinnen auf. 2009 wurden 14 weibliche Tatverdächtige ermittelt, 2010 waren es 19. In den 433 Fällen von Raubüberfällen wurde 258-mal mit einer Schusswaffe gedroht, in fünf Fällen wurde geschossen. Gezielte Schüsse werden kaum abgegeben. „Der Täter ist ein Räuber, aber kein Mörder“, betonte Opfermann. Tote und Verletzte seien am ehesten bei Widerstand der Opfer zu befürchte, etwa bei Eingreifen eines Kunden.

Banküberfälle in Deutschland: steigende Aufklärungsquote.

FOTO: ARCHIV

Skimming. Zurückgegangen ist die Zahl der Skimming-Fälle. Dabei werden durch an Geldausgabeautomaten angebrachte technische Hilfsmittel (Kartenlesegeräte, Videokameras) der Code der Bankomatkarte und die PIN ausgespäht. Zu diesem Rückgang hat geführt, dass mit einem kopierten Magnetstreifen und der PIN im europäischen Raum kaum noch Geld abgehoben werden kann, weil hier nur mehr Chipkarten verwendet werden. Weiters sind die Spezialisten, die früher die technologischen Kenntnisse zum Herstellen der erforderlichen Gerätschaften hatten, in lukrativere „Geschäftszweige“ abgewandert.

Die derzeit noch mit dieser Methode auftretenden Täter werden relativ schnell gefasst. Zudem wurden auf Grund einer Initiative des LKAs Hessen und des deutschen Bundeskriminalamts im Dezember 2010 Polizeibeamte mit Foldern ausgestattet, die durch bildliche Darstellungen das Erkennen von Manipulationen an Geldautomaten erleichtern.

Straftaten gegen Geldinstitute hätten sich von den Kundenhallen (Raub, Einbruch) in den SB-Bereich verlagert, sagte Gerhard Reinhardt *(Commerzbank AG)*. Im SB-Bereich komme es zu Skimming, Aufbrüchen von Hartgeldeinzahlungsmodulen, Sprengungen oder Aufbrüchen von Geldautomaten, Überweisungsbetrug, Cash-Trapping (Banknoten werden bei der Ausgabe am Bankomaten durch Klebestreifen zurückgehalten), Vandalismus und Abhebebetrug. Die Videotechnik als die am universellsten einsetzbare Überwachungsmöglichkeit müsse sich daher verstärkt auf diesen Bereich konzentrieren.

Bauliche Gestaltung. Selbst wenn mehrere Mitarbeiter in einer Bankfiliale tätig sind, ist in vielen Fällen nur ein Mitarbeiter ständig im Service anwesend. Wie unter solchen Umständen durch bauliche und technische Rahmenbedingungen für einen sicheren Filialbetrieb gesorgt werden kann, wurde von Christian König und Oliver Klempa erörtert.

„Bauordnungen sind zum Großteil am Brandschutz orientiert sowie an Gesichtspunkten des Personenschutzes, des Schutzes der Nachbarschaft und der Umwelt, berücksichtigen aber nicht ausreichend die hohen Anforderungen, die, wie bei Banken, an Sicherheit und den Schutz von Werten zu stellen sind“, erläuterte Dr. Ing. Rüdiger Hass *(HHP Nord/Ost Beratende Ingenieure GmbH, Braunschweig – www.HHP-Nord-Ost.de)*.

Im Besonderen ergeben sich Konfliktsituationen zwischen Kundenfreundlichkeit und Bürokommunikation auf der einen und dem Abschottungsprinzip auf der anderen Seite oder der zeitnahen Personenrettung mit dem Schutz hoher Werte.

Rechenzentren. Das Herzstück von Banken sind die Rechenzentren. Brände in einem Rechenzentrum können mit automatischen Löschanlagen bekämpft und bei geringer Reaktionszeit sogar ausgeschlossen werden. Brände außerhalb eines Rechenzentrums haben in mehrfacher Hinsicht Auswirkungen auf dieses: Sie führen zu einer Erwärmung im Inneren des Rechenzentrums, zu einer Erhöhung der Luftfeuchtigkeit, weil im Mauerwerk/Beton gebundenes Wasser austritt, und Löschwasser eindringt, wenn ein Brand oberhalb des Rechenzentrums gelöscht werden muss. Rechenzentren sollten daher grundsätzlich nicht überbaut werden.

Gerd Otto-Rieke: „Ist jemand länger im Ausland tätig, fühlt sich für ihn kaum wer im Unternehmen mehr zuständig."

Rainer Hannich: „Leitende Angestellte von Kreditinstituten sollten für einen persönlichen Schutz sorgen."

Axel Romanus: „Zur Risikosteuerung ist es erforderlich, Risiken so weit wie möglich zu identifizieren."

Claus Opfermann: „Längere Öffnungszeiten von Tankstellen und Spielhallen können einen Tatanreiz bilden."

„Notfallplanung ist ein Non-Profit-Thema", betonte Peter Schwarz vom *Deutschen Sparkassenverband GmbH (www.dsv-gruppe.de)*. Man müsse auf den Fall der Fälle vorbereitet sein und ein *Business Continuity Management (BCM)* entwickeln. Anleitungen dazu bieten der BSI-Standard 100-4 (Bundesamt für Sicherheit in der Informationstechnik) sowie der prozessorientierte PDCA-Zyklus nach ISO 27001. Durch „Plan-Do-Check-Act" als sich ständig wiederholender Vorgang werde ein Höchstmaß an Ausfallsicherheit erreicht.

Wie Risiko methodisch analysiert werden kann, hat Dr. Axel Romanus *(IFS Umwelt und Sicherheit GmbH, Kiel)* dargestellt: Wie das Risiko gesehen wird, ob als Chance auf Gewinn oder als Gefahr eines Verlustes, hänge von Wertvorstellungen ab. Im Fall einer Gefahr sei das Risiko das mathematische Produkt von Schadenshöhe und Eintrittswahrscheinlichkeit. Zur Risikosteuerung sei erforderlich, Risiken so weit wie möglich zu identifizieren. Ein Teil dieser erkannten Risiken werde vermieden werden können. Nicht vermeidbare Risiken könnten durch personelle, technische und organisatorische Maßnahmen vermindert werden. Was nicht mehr vermindert werden könne, sollte versichert oder durch Vertragsklauseln abgedeckt werden. Das Restrisiko, zu dem die nicht identifizierten Risiken kommen, müsse man selbst tragen. Die Verantwortlichkeit treffe den Betreiber – denjenigen, der durch seine Tätigkeit Gefahren für andere schafft. Demgemäß habe er andere davor zu schützen. Nichterfüllung der Betreiberpflichten könne straf-, verwaltungs- und zivilrechtliche Konsequenzen nach sich ziehen. Durch den Umstand, dass im Zuge der Deregulierung Behörden und Überwachungsorganisationen Aufgaben vermehrt auf die Unternehmen übertragen, erhöhe sich diese Verantwortlichkeit.

„Wichtig ist, dass Unternehmen, über die vertraglichen Verpflichtungen mit dem Versicherer hinaus, nicht übersehen, welche Verpflichtungen ihnen von der Rechtsordnung auferlegt werden. Aus der Nichteinhaltung dieser Bestimmungen können sich ebenfalls Obliegenheitsverletzungen ergeben, die im Schadensfall versicherungsrechtlich relevant sein können", sagte Romanus.

Geschäftsreisen. „Geht jemand auf Geschäftsreise oder wird als Expat für längere Zeit ins Ausland entsendet, fühlt sich eigentlich kaum einer im Unternehmen mehr für ihn zuständig", sagte Gerd Otto-Rieke vom „Forum Sicherheit und Reisen", *(www.securityshow.de)*. In Deutschland wurden 2010 etwa 150 Millionen Geschäftsreisen unternommen, bei Gesamtkosten von etwa 43 Milliarden Euro. „In etwa 0,1 Prozent der Fälle passiert etwas."

Fürsorgepflichten des Arbeitgebers ergeben sich aus dem Arbeitsverhältnis, allgemeinen schuldrechtlichen Verpflichtungen, Regelungen über Schadenersatz, und letztlich ist die Reisesicherheit für Mitarbeiter wichtig.

Deren Nichteinhaltung kann zu Reputationsschäden führen. Dazu kommt, dass es in der EU Bestrebungen gibt, den in Großbritannien seit einigen Jahren bestehenden *Manslaughter Act* auf die EU auszudehnen. Nach diesem britischen Gesetz wird der Arbeitgeber verantwortlich, wenn er den Arbeitnehmer in eine gefahrgeneigte Situation gebracht hat und dieser dadurch körperliche Schäden erleidet.

„Bei Ausweitung dieser Regelung wird dem Thema Dienstreisen sicher mehr Aufmerksamkeit zugewendet werden", betonte Otto-Rieke. Risiken, die sich auf Geschäftsreisen ergeben können, seien zu identifizieren, zu bewerten und zu managen und können sich aus medizinischen Gründen sowie der Sicherheitslage im Zielland ergeben. Allenfalls seien Versicherungsverträge mit weltweiter medizinischer Betreuung abzuschließen sowie Verträge mit Sicherheitsassistenten vor Ort zur Betreuung, etwa zur Abholung am Flughafen und Begleitung zum Hotel. Nicht jeder Abholung dürfe vertraut werden – sie könnte in Lösegeldforderungen enden. Der Reisende muss die nötigen Länderinformationen erhalten *(z. B. www.checkmytrip.com)* sowie Schulungen zur Steigerung der Selbstverantwortung. Er muss im Besitz einer Notfallnummer sein und wissen, woher er Hilfe bekommen kann.

Der Arbeitgeber muss wissen, wo sich der Mitarbeiter aufhält, eventuell sogar, mit Zustimmung des Betriebsrats, über Handy-Ortung (Travel Tracking). Ferner muss im Unternehmen für Krisenfälle vorgesorgt sein, mit festgelegten Prozessen und Strukturen (Krisenstab, Krisenplan) zur schnellen Reaktion. Ein solcher entscheidet auch über Evakuierungen im Fall von Naturkatastrophen oder bei Ausbruch von Pandemien.

FOTOS: KURT HICKISCH

Bankfoyer: Für die Überwachung des SB-Bereichs einer Bankfiliale sollte verstärkt Videotechnik eingesetzt werden.

Foto: Archiv

Zu bedenken sind die Gefahr von Gepäcksverlust und Wirtschaftsspionage, Anschlägen und Entführungen. Juristischer Beistand für den Auslandsreisenden sollte ebenfalls gesichert werden.

Persönliche Sicherheit. Vorstände und Führungskräfte von Kreditinstituten sowie deren Familienangehörige können durch Geiselnahme, Entführung, Überfälle, Anschläge, gefährdet sein – wobei das Empfinden nicht unbedingt mit der Situation übereinstimmen muss. Realer kann die Gefährdung durch Raub oder Einbruch sein.

Es müsse eine individuelle Gefährdungsanalyse erstellt werden, unter Einbeziehung polizeilicher Erkenntnisse, Ereignisse in der Vergangenheit, dem Bekanntheitsgrad des Betreffenden, der Einschätzung in seinem Umfeld (Sekretärinnen, Fahrer) und seinen persönlichen Gewohnheiten, sagte Sicherheitsberater Rainer Hannich *(www.hannich-sicherheit-plus.de)*.

Der Sicherheitscheck umfasst zunächst das Privathaus, bei dem ein mechanischer Grundschutz für Türen und Fenster herzustellen sei. Dazu komme eine Außenbeleuchtung mit automatischer Ansteuerung bei allen Gebäudeseiten („Licht schreckt Täter ab“), eine Einbruch- und Überfallmeldeanlage (EMA, ÜMA) mit Weiterschaltung des Alarms zu einem Dienstleister. Von diesem erfolgen die Maßnahmen nach einem zuvor erarbeiteten Interventionsplan. Zu diesem gehören Lagepläne und Fotodokumentationen des Gebäudes sowie Wichtiges zur Person selbst (Fotos, benötigte Medikamente and andere).

Ferner müssten die Lebensumstände und Verhaltensweisen überprüft und gegebenenfalls verändert werden, etwa, was den Weg zur Arbeit betrifft (alternative Fahrstrecken, Fahrzeugwechsel).

Dazu kommen das Erkennen und Behandeln verdächtiger Sendungen, das Verhalten bei telefonischen Drohungen, der Aufenthalt im Haus selbst, der Umgang mit Besuchern und verdächtigen Wahrnehmungen, wobei die gesamte Familie einbezogen werden müsse. Es gehe dabei weniger um Investitionskosten als um die Änderung von Verhaltensweisen.

Kurt Hickisch