Die Zahl der „klassischen“ Raubüberfälle auf Geldinstitute und Poststellen ist in Deutschland von 1.049 im Jahr 2000 kontinuierlich auf 409 im Jahr 2009 zurückgegangen.

Gefahrenpotenzial verringern

Die Sicherheit von Banken, deren Mitarbeiter und Kunden war Schwerpunkt bei einem Simedia-Forum am 9. und 10. November 2010 in Frankfurt/Main.

Nicht zuletzt auch aus Gründen der Risikoverringerung sind Banken dazu übergegangen, Geschäftsprozesse wie etwa das Bargeldhandling an unbemannte Selbstbedienungsstellen auszulagern. Dadurch haben sich neue Tatgelegenheiten für Straftäter ergeben“, sagte Kriminalhauptkommissarin Mechthild Schlitz vom Landeskriminalamt (LKA) Hessen beim Simedia-Forum „Banken-Sicherheitstage“. Die Zahl der „klassischen“ Raubüberfälle auf Geldinstitute und Poststellen ist in Deutschland von 1.049 im Jahr 2000 kontinuierlich auf 409 im Jahr 2009 zurückgegangen. In diesem Zeitraum ist die Zahl der Raubdelikte von 59.414 auf 49.317 gesunken.

Die Zahl der Einbrüche in Banken/Sparkassen, Poststellen und dergleichen ist in diesen Jahren mit etwa 1.300 pro Jahr konstant geblieben.

Stark angestiegen ist hingegen das Ausspähen von Daten, von 1.743 Fällen im Jahr 2004 auf 11.491 Fälle im Jahr 2009. Darunter sind auch Skimming-Fälle zu verstehen, bei denen das Ausspähen von Daten die Vorstufe ist.

Da Skimming-Angriffe Anbauten an der Vorderseite von Geldautomaten erfordern, wurden durch ein Unternehmen der Kreditwirtschaft und der Zentralen Geschäftsstelle der Kriminalprävention der Länder und des Bundes (ZGS) für Polizisten 130.000 Exemplare einer Taschenfaltkarte als Fahndungshilfsmittel aufgelegt. Auf Fotos werden Skimming-Anbauten und typische Veränderungen dargestellt.

Der Betrug mittels Daten von Zahlungskarten hat in Deutschland um das Vierfache in vier Jahren zugenommen, nämlich von 3.646 Fällen im Jahr 2006 auf 17.072 im Jahr 2009. Zuvor waren die Zahlen ab 2002 annähernd gleich geblieben. 2003 waren nur 2.424 Fälle registriert worden. Bei dieser Betrugsart werden überwiegend Daten von Zahlungskarten missbraucht, die zuvor durch zumeist durch Spam-Mails oder durch Phishing im Online-Banking ausgespäht wurden. Ebenfalls stark zugenommen hat in Deutschland die Zahl der Skimming-Angriffe auf Geldautomaten. Im Jahr 2009 wurden hier bundesweit 964 Geldautomaten manipuliert, teilweise mehrfach. Dadurch erfolgten 2.058 missbräuchliche Angriffe im Jahr 2009.

Gassprengungen. Zum Problem geworden sind Angriffe auf Geldautomaten durch Gassprengungen. 2005 wurden in Deutschland 27 Fälle registriert – inklusive Versuche. 2009 waren es bereits 57 Fälle. Für das Jahr 2010 haben sich nach Angaben des BKAs Wiesbaden 64 Fälle (einschließlich Versuche) ergeben.

Die Versicherungen schlagen Alarm, weil zumeist auch beträchtliche Ge-

FOTO: ARCHIV

bäudeschäden entstehen. In manchen Fällen mussten Bankfilialen abgetragen werden. Laut Mechthild Schlitz ist es nur glücklichen Umständen zuzuschreiben, dass es in Deutschland, zum Unterschied von anderen Ländern, durch diese Sprengungen bisher noch zu keinen Personenschäden oder Tötungen gekommen ist.

Da Geldautomaten auch in Einkaufs- und Baumärkten, Möbelhäusern und Tankstellen aufgestellt werden, können sich auch dort Angriffe auf Geldautomaten ereignen. Diese Standorte gehören daher in die Präventionskonzepte einbezogen. Ein weiteres Problem könnte die Aufstellung von Automaten werden, die Gold ausgeben und rechtlich wie Warenautomaten behandelt werden. Ursprünglich als Werbegag gedacht, gibt es in Hessen und Baden-Württemberg bereits fünf solcher Goldautomaten, etwa 500 sollen es insgesamt werden.

Mechthild Schlitz: „Stark angestiegen ist das Ausspähen von Daten."

Skimming. „Das Problem bei Debitkarten ist, dass sie aus Gründen der Abwärtskompatibilität immer noch mit einem Magnetstreifen versehen sind, obwohl beispielsweise in Deutschland mit Beginn des Jahres 2011 bereits alle Geldausgabeautomaten für den Einsatz von Chipkarten ausgerüstet sind", führte Wolfgang Hamann, Senior Produktmanager Sicherheit von *Wincor Nixdorf,* aus. „Der Umstand, dass noch nicht alle Länder, vor allem außereuropäische, auf dieses technische Niveau nachgezogen haben, macht Skimming nach wie vor möglich und zur Angriffsart mit der größten Schadenssumme bei Geldausgabeautomaten."

Im Gegensatz zur Chipkarte, die bei einem Geldausgabevorgang mit dem Bankomaten in einen Dialog tritt, bei dem die Berechtigung überprüft wird, sind die Daten auf dem Magnetstreifen statisch abgespeichert und können auch von Unberechtigten ausgelesen werden. Beim Skimming werden während eines normalen Transaktionsvorgangs mit speziellen Vorbauten, die vor dem Kartenleser montiert sind und täuschend ähnlich nachgebaut sind, vom Magnetstreifen die Kartendaten ausgelesen, ohne dass der Kunde davon etwas bemerkt. Ferner wird entweder optisch über eine versteckte Minikamera oder mit einer über die Tastatur gelegten, gefälschten PIN-Tastatur die Eingabe der PIN mitverfolgt und gespeichert oder weitergeleitet.

Die Daten werden in weiterer Folge auf „White Plastics" übertragen, Karten mit Magnetstreifen, die in einigen Ländern (Nordamerika, Brasilien) noch an Geldautomaten verwendet werden können. In der Folge wird das Konto des Geschädigten bis zum Limit ausgeschöpft, einschließlich des verfügbaren Zahlungsrahmens.

Erfolgt die Weitergabe der Daten über Funk an ein Notebook, wurde festgestellt, dass bereits zwei Stunden später mit Dubletten Umsätze generiert wurden. „Skimming bedeutet international organisierte Kriminalität"; das Zentrum in

Foto: Kurt Hickisch

Europa wird in Rumänien vermutet. Maßnahmen zur Verhinderung von Skimming bestehen in einer mechanischen Verstärkung des Vorbauschutzes, sodass dieser nicht abgeschnitten und ersetzt werden kann, im Einsatz einer speziellen, kapazitiven oder induktiven Sensorik, die das Anbringen von Skimming-Geräten erkennt, oder in einer optischen Überwachung mit Bildanalyse (Optical Security- Guard), die Veränderungen am Bedienfeld oder beim Karteneingabeschlitz erkennen lässt. Gegen das Mitlesen der PIN bei der Eingabe helfen spezielle Sichtschutzblenden oder ein Abdecken der Tastatur.

Gefährdungsbeurteilung. Über Gesichtspunkte, die für oder gegen die Wahrscheinlichkeit eines Überfalls auf ein Geldinstitut sprechen und die Basis für eine Gefährdungsbeurteilung bilden könnten, berichteten Christian König vom Sparkassenverband Bayern und Oliver Klempa vom Sparkassenverband Baden-Württemberg. Eine solche Beurteilung ist in Deutschland nach arbeitnehmerschutzrechtlichen Bestimmungen (Arbeitsschutzgesetz – ArbSchG) erforderlich.

Gefährdungspotenziale ergeben sich

• aus der Lage der Bankfiliale (Nähe zur Autobahn, zu öffentlichen Verkehrsmitteln, ampelgeregelte Kreuzungen im Umfeld, Möglichkeit, in der Menge unterzutauchen, Abgeschiedenheit, verbunden mit langen Anfahrtszeiten für die Polizei, Parkmöglichkeiten vor der Straße, sodass dort allenfalls ein Komplize in einem Kfz mit laufendem Motor warten könnte);

• aus der Bewaffnung der Täter (Schusswaffen, Hieb- und Stichwaffen, Reizstoffe wie z. B. Pfefferspray, Explosivstoffe oder leicht entzündliche Stoffe, wobei von Bedeutung ist, ob sich das potenzielle Opfer in einem gesicherten Bereich wie etwa einer Kassenbox befindet oder dem Täter ohne Abtrennung gegenübersteht);

• durch unzureichende mechanische Abtrennungen (nicht ausreichende Beschusshemmung, unzureichende Stabilität der Konstruktion, Splitterabgang, Querschläger);

• durch die Außerkraftsetzung von mechanischen oder elektronischen Sicherungseinrichtungen oder optischen Raumüberwachungseinrichtungen;

• durch psychische Belastungen (kann durch bauliche, technische oder organisatorische Maßnahmen das Sicherheitsgefühl der Mitarbeiter verbessert werden?);

• durch die Gestaltung der Ein- und Ausgänge für Publikumsverkehr und Personal (Können sich Kunden nach Geschäftsschluss in der Filiale aufhalten oder Täter sich in Geschäftsräumen oder Toiletten verstecken? Können Not-/Lieferantenausgänge manipuliert werden, sodass sie offen bleiben? Bestehen nicht einsehbare Eingänge durch Hinterhöfe, Gärten, Treppenhäuser? Können Mitarbeiter beim Betreten oder Verlassen abgefangen werden);

• durch schlecht oder nicht gesicherte Öffnungen in der Außenhaut des Gebäudes (Fenster, Decken-/Dachluken, Lichtschächte);

• durch die Bearbeitung und Verwahrung von Banknoten (Einsehbarkeit auf Vorgänge des Sortierens, Zählens, Bündelns. Wo und durch wen erfolgt die Übergabe und Übernahme Bargeld, die Geldversorgung von Automaten – durch eigene Mitarbeiter oder externe Dienstleister; in einem gesicherten Bereich an der Rück- oder an der Vorderseite?);

• durch das Verhalten von Mitarbeitern (Schulungen, Betreuung) und Tätern.

Deutschland: Stark zugenommen hat die Zahl der Sprengungen von Geldautomaten mit Gas.

Einige Geldinstitute in Österreich haben ihre Bankomaten vor Gassprengung geschützt.

In der Folge sind die Gefährdungen nach der Eintrittswahrscheinlichkeit eines Überfalls und dem Ausmaß des Schadens zu gewichten. Das Risiko ergibt sich aus dem Produkt dieser beiden Größen. Hohe Eintrittswahrscheinlichkeit und großes Schadensausmaß (schwere körperliche Schäden, Tod eines Mitarbeiters) erfordern sofortiges Handeln.

Das Sicherungskonzept sollte so ausgelegt sein, dass es für einen Täter uninteressant ist, gerade diese Bankfiliale zu überfallen.

Traumatisierung. „Ein Banküberfall ist ein potenziell traumatisches Ereignis. Cirka 20 Prozent der Betroffenen entwickeln ohne rechtzeitige und angemessene Hilfe bleibende Beschwerden“, erläuterte Joachim Schottmann von der *Humanprotect Consulting GmbH, Köln (www.humanprotect.de)*.

Als Notfallsreaktion vorgegebene Verhaltensmuster sind Flucht, Kampf oder Erstarren. Dem Opfer eines Banküberfalls bleibt zumeist nur die Möglichkeit des Erstarrens. Typische Begleiterscheinungen dabei sind Tunnelblick, Verlust des Zeitgefühls, Gedächtnislücken, und Übererinnerung einzelner Sequenzen. Beschrieben wird das in diesem Zustand Erlebte mit Worten wie „Wie ein schlechter Film; wie in Zeitlupe; fühlte mich wie betäubt; habe wie ferngesteuert gehandelt; konnte alles tun, weiß aber auch nicht mehr wie; es kam mir so unendlich lang vor“.

In der Schockphase, die eine Stunde bis mehrere Tage nach dem Überfall dauern kann, ist das Opfer noch nicht in der Lage, das Geschehen zu vergegenwärtigen. Es kann zu paradoxem Verhalten kommen, Weinen, Schreien, Lachen, Aktionismus, aber auch zum inneren Rückzug, „Funktionieren nach Autopilot“.

In dieser Phase geht es um eine „psychologische Erste Hilfe“. Es soll – auch bei polizeiliche Einvernahmen – vom Tatort und vom inneren Geschehen Abstand hergestellt werden. Informieren und normalisieren, beruhigen, begleiten, nicht allein lassen; signalisieren, dass man sich kümmern wird, sind die wichtigsten Maßnahmen, die auch von Kollegen durchgeführt werden können. In diesem Stadium kann eine erste unaufdringliche Kontaktaufnahme

Fotos: Archiv

Skimming: Mit speziellen Vorbauten werden die Kartendaten vom Magnetstreifen ausgelesen.

durch den Psychologen erfolgen – als Zeichen, dass es jemanden gibt, an den man sich wenden kann.

In der anschließenden, etwa zwei bis vier Wochen dauernden Einwirkungsphase versucht der Betroffene, sich dem Ereignis zu stellen. Sinneseindrücke, Gefühle und Verhaltensimpulse werden als Ausfluss eines Heilungsprozesses nacherlebt. Es können Zustände einer Übererregung auftreten (psychisch etwa Schreckhaftigkeit, Angst, exzessive Wachsamkeit; körperlich: Schlafstörungen, Kopfschmerzen, Erschöpfungszustände), Erinnerungsattacken (man spürt die Pistole im Nacken – Flashback), Vermeidungsreaktionen (Vermeidung von Menschen, Orten, Situationen; Teilnahmslosigkeit gegenüber der Umwelt, Rückzug), Depression (Schuldgefühle, Selbstzweifel – „Hätte ich doch …“).

In der Erholungsphase, etwa acht bis zwölf Wochen nach dem Ereignis, gelingt es dem Betroffenen entweder, das Ereignis zu bewältigen („die Wunde vernarbt“) oder es kommt zu einer Chronifizierung mit Traumafolgestörungen, die sich gesundheitlich unter anderem als Phobien, Zwangsstörungen, Substanzmissbrauch oder psychosomatischen Erkrankungen äußern. Psychosozial kann es zum Verlust von Lebensqualität, Arbeitsausfällen, Verlust des Arbeitsplatzes und Berufsunfähigkeit kommen.

Eine Psychotherapie, die etwa zwei bis drei Wochen nach dem Überfall einsetzt, ist geeignet, das Risiko solcher Folgeschäden zu vermeiden.

Durch Reaktionen der Umwelt kann es zu zusätzlichen Belastungen kommen, etwa durch neugieriges Fragen und unbedachte Äußerungen von Kollegen („Ich hätte ihm nicht so viel gegeben“). Dem Betroffenen gegenüber sollte Mitgefühl gezeigt, aber ein Sich-Aufdrängen vermieden werden. In einen Zwangsurlaub sollte er nicht geschickt werden – das könnte das Gefühl aufkommen lassen, als „gestört“ angesehen zu werden. Besser ist es, in der Arbeit Freiheiten hinsichtlich Arbeitszeit und ausgeübter Tätigkeit zu gewähren; anzubieten, in einer anderen Filiale zu arbeiten; oder auch, mit einem Blumenstrauß Anerkennung zu zeigen. Jedenfalls zu vermeidende Verhaltenssünden sind bagatellisierende Floskeln, Vorwürfe, Lügen, Hektik, Witze.

Kurt Hickisch

Foto: Archiv