Datensicherheit wird trotz Kieber-Fall vielfach unterschätzt

Fragwürdige Schulungsprogramme mit echten Kundendaten in Banken

Datensicherheit ist ein Thema, das die oberste Unternehmensführung beschäftigen muss. Das scheint nicht überall mit genügend Verantwortungsbewusstsein beachtet zu werden, wie im Folgenden dargelegt wird.

Monika Roth

Heinrich Kieber, der zur Fahndung ausgeschriebene Dieb von Bankkundendaten, der unter einem deutschen Zeugenschutzprogramm an unbekanntem Ort mit neuer Identität lebt, hat Anfang August 2010 im «Stern» seinen Modus Operandi beschrieben. Wenn es so war, wie er sagt, handelte es sich beim Datendiebstahl um ein Kinderspiel. Es lässt sich sagen: Vertrauen wurde missbraucht auf übelste Weise, und von Datensicherheit kann nicht die Rede sein, wenn solches möglich ist:

Die Version des Diebes

«Ich habe die (gemeint sind die Daten) nicht kopiert, ich habe ein DLT mitgehen lassen, das ist ein Magnetband, ein sogenanntes Tages-Back-up-Band. Die Treuhand macht über Nacht eine Sicherungskopie auf einem handelsüblichen Magnetband. Das sieht aus wie so eine dicke, alte Kassette, ungefähr 12 mal 15 Zentimeter und 4 Zentimeter hoch. (. . .) Ich hab das Band nach dem Mittagessen eingesteckt, ein leeres Band auf den Tisch gelegt und weitergearbeitet. Es gab keine Kameras in den Büros. Das Band ist ja relativ klein und passt in die Jackentasche. Bei Feierabend hab ich es mitgenommen und bei mir zu Hause gut versteckt. Ich wusste, dass nichts passiert. Ich wusste, dass die verantwortliche Person das Band nicht ins Lesegerät steckt und nachschaut, ob da Daten drauf sind.»

Schulung ist immer wichtig

Der Fall Kieber (und weitere Diebstähle anderer Täter) gibt Anlass zu hinterfragen, wie die Sorgfaltspflichten im Umgang mit delikaten Daten im Alltag der Banken aussehen. Nachforschungen haben ergeben, dass noch heute von mangelnder Sensibilität und Vorsicht, von fehlender Verantwortung und bewusster Gefährdung der Datensicherheit gesprochen werden muss. Die nachfolgenden Schilderungen betreffen keinesfalls alle Banken, sie bilden aber keineswegs vereinzelte Ausnahmen. Ein Beispiel lässt viele Fragen aufkommen, beispielsweise diejenigen nach der Rolle der Bankleitung, des Internal Audit und der Compliance. Banken sind verpflichtet, ihre Mitarbeitenden zu schulen. Ein wichtiger Inhalt ist die Prävention von Geldwäscherei und Terrorismusfinanzierung.

Die diesbezüglichen Ausbildungen gehören in das Pflichtenheft der Geschäftsführung, die von der Compliance-Funktion oder von der ausdrücklich für Fragen der Geldwäscherei für verantwortlich bezeichneten Person unterstützt wird. Für diese Ausbildungen werden von einigen Banken, die zum Teil mit anderen zusammenarbeiten, gemeinsame Schulungen entwickelt und durchgeführt. Die daraus gewonnenen Daten sind – wie die Testdaten auch – teilweise oder grossmehrheitlich produktive Kundendaten, die ganz bewusst nicht anonymisiert werden.

Das heisst konkret: Die Datensicherheit wird verletzt, und echte Kundennamen und Kundendaten werden offen einer unbestimmten Vielzahl von internen und externen Mitarbeitenden unnötigerweise bekannt und unter Umständen auch Drittbanken zugänglich gemacht. Letzteres dann nämlich, wenn Kurse mit Teilnehmern verschiedener Banken stattfinden. Dazu kommt die Möglichkeit des Excel-Downloads, der bei einigen Instituten nicht deaktiviert ist. Das führt dazu, dass entgegen klaren Weisungen Entwickler die produktiven Daten auf ihr Notebook nehmen und unter Umständen damit ins Ausland in die Ferien verreisen können.

Ein Grund für dieses Vorgehen liegt in den Kosten. Es gibt zwar Tools, die Anonymisierungen gänzlich oder teilweise vornehmen können; diese Programme sind indessen unter Umständen mit grossem finanziellem, zeitlichem und personellem Aufwand verbunden. Man könnte es einfacher haben: Es befindet sich eine Vielzahl von Anbietern auf dem Markt, die neutrale, auf Phantasienamen beruhende IT-Schulungsprogramme verkaufen, was diese Risiken vermeiden würde.

Datensicherheit ist Chefsache

Für den Compliance Officer, der von solchen Praktiken erfährt, besteht die Pflicht, den zuständigen Organen die rechtliche Ausgangslage darzustellen und latente und konkrete Risiken zu thematisieren. Er muss transparent über Regeln und Verhaltenserwartungen sprechen, aber nicht selber über das konkrete Vorgehen entscheiden. Man kann sich hier fragen, ob ein Compliance Officer sich nicht weigern müsste, so wie dargestellt mit produktiven Kundendaten im beschriebenen Rahmen Schulungen durchzuführen oder zuzulassen.

Denn es genügt nicht, wenn nahestehende Banken (Vertragsbank) oder ihre an Schulungen teilnehmenden Angestellten eine Erklärung zur Wahrung von Bankgeheimnis und Vertraulichkeit unterzeichnen. Im Prinzip wäre es erforderlich, dass der Kunde auf den Schutz des Bankgeheimnisses verzichtet und ausdrücklich die Zustimmung dazu erteilt, dass sein Name und seine Daten bei einer Vertragsbank und weiteren Instituten für Schulungen verwendet werden dürfen. Daran fehlt es aber.

Die Vorfälle betreffend Datendiebstahl haben bestätigt, dass Mitarbeitende ein grosses operationelles Risiko darstellen. Allerdings zeigt es sich, dass die Gefahren nicht nur dort lauern: Sie sind vielmehr auch in der Führungsetage anzutreffen. Wenn in den Instituten Geschäftsleitung und Verwaltungsrat einen solchen Umgang mit Kundendaten beschliessen oder dulden, setzen sie nicht nur den Ruf ihres eigenen Instituts, sondern den des Finanzplatzes Schweiz aufs Spiel. Dass dieses Vorgehen sich mit der Gewähr für eine einwandfreie Geschäftsführung vereinbaren lässt, muss wohl verneint werden.

Prof. Dr. iur. **Monika Roth** ist Rechtsanwältin der Kanzlei Roth Schwarz Roth in Binningen und Studienleiterin des DAS Compliance Management am IFZ Zug (Hochschule Luzern).