

Marcelo Corrêa de Oliveira ist CEO von Covadis SA, die Lösungen für Authentifizierung, Identifikation und E-Banking anbietet.



Fordern Sie dringend mehr Sicherheit!

Die meisten Vermögensverwaltungsfirmen wickeln den Datenverkehr mit ihrer Depotbank inzwischen online ab. Wie sicher sind diese Datenverbindungen? Die beunruhigende Wahrheit lautet: niemand darf sich ganz sicher fühlen! Im Juni dieses Jahres fielen 3400 Citigroup-Kunden einem Cyberangriff zum Opfer, und die Hacker verschafften sich Zugang zu vertraulichen Daten von 360 069 weiteren Konteninhabern.

Der durch Kreditkartenbetrug verursachte Schaden beläuft sich laut Wall Street Journal in den USA auf 10 Milliarden Dollar; 15 Millionen Amerikaner sind Opfer solcher Online-Betrügereien geworden – vom Diebstahl von Kundenlisten durch Bankangestellte ganz zu schweigen...

Dabei gibt es probate Gegenmittel – etwa Kartenleser, mit denen sich der Kartenbenutzer im Interesse eines wirksam geschützten Datenaustauschs sicher identifizieren lässt. Die Leser mit Biodatenchip (Fingerabdruck) sind dank der proprietären Verschlüsselungstechnologie bisher nicht ein einziges Mal geknackt worden.

Schäden nicht hoch genug?

In Frankreich bietet BNP Paribas diese sicheren Kartenleser bereits für kleine und mittle-

re Unternehmen an. Die schweizerischen Banken zögern noch. «Die durch Betrug und Unterschlagung verursachten Schäden sind nicht hoch genug», urteilte kürzlich ein Vertreter.

Dabei sind die Schweizer das am höchsten versicherte Volk der Erde. Dieses Sicherheitsbedürfnis ist ein individueller und kollektiver Wesenszug der Schweizer Psyche. Sicherheit erwarten auch die ausländischen Kunden der schweizerischen Finanzinstitute. Dennoch fällt es den Banken schwer, diesen Erwartungen mit ihrer Online-Strategie Rechnung zu tragen – aus Kostengründen, wie es heisst. Erstaunlich ist auch, dass sich die Verbraucherverbände kaum für einen besseren Schutz der Öffentlichkeit engagieren.

Diese zögerliche Haltung ist desto verwunderlicher, als Gefahr ja nicht nur von aussen, sondern auch von innen droht. Wie stand es um die interne Sicherheit der Bank eines benachbarten Fürstentums, deren Angestellter Listen ausländischer Kunden erstellen und an die deutschen Steuerbehörden verkaufen konnte?

Dieser Angestellte hatte nicht nur Zugriff auf Daten, die ihm nicht hätten zugänglich sein dürfen – schlimmer noch: er konnte diese sogar auf einem Datenträger speichern! Wie werden die an die Steuerbehörden ihres Landes verratenen Kunden wohl auf diese Panne reagieren? Was wird diese Panne die Bank an Ansehen und Entschädigungszahlungen kosten? Dabei genügen heute zum Schutz von Computerarbeitsplätzen Chipkartenleser mit Fingerprint-Lesefunktion.

Der Bankensektor ist auf Informatik zunehmend angewiesen. Aber wenn seine Dienstleistungen heute mit einem Handy von überall auf der Welt abrufbar sind, dann muss das Sicherheitsniveau hier angepasst werden.

«Erstaunlich, dass sich die Verbraucherverbände kaum für einen besseren Schutz der Öffentlichkeit engagieren.»

Zumal die Kosten für die erforderlichen Systeme inzwischen erträglich sind. Viele Nutzer, nicht zuletzt die unabhängigen Vermögensverwalter, wären zweifelsohne bereit, diesen Preis zu zahlen.