

## Zielgenaue Ansprache

Umsetzung  
bis Ende 2007

■ Fortsetzung von Seite 1.

In der laufenden Pilotierungsphase setzen die Projektinstitute die konzipierten Maßnahmen bis Ende 2007 um. Die daraus resultierenden validen Erfolgsbeispiele werden einen breiten Einsatz von wirkungsvollen Online-Kommunikations- sowie Vertriebsmaßnahmen in der Sparkassen-Finanzgruppe fördern. Neben der Überleitung in die Filiale setzt der effektive Vertriebsauftrag aber auch den flächendeckenden Einsatz von wettbewerbsfähigen Produkt- und Abschlussmodulen für Leuchtturm- und weitere Standardprodukte voraus. Die neuen Internet-Rahmenauftritte werden in dieser Hinsicht wie auch im Hinblick auf einen integrierten Online-Vertrieb mit zielgenauer Kundenansprache neue Maßstäbe setzen. Durch die Umsetzung der von den DSGVO-Gremien mit Nachdruck unterstützten Projektergebnisse und Handlungsempfehlungen insbesondere bei Leuchtturmprodukten, kann der Online-Vertrieb zum Erfolg der Vertriebsoffensive sowie Steigerung des Produktabsatzes der Sparkassen einen maßgeblichen Beitrag leisten. Das große Potenzial des Online-Vertriebs innerhalb unserer Multikanalstrategie gilt es jetzt zu nutzen. Die Realisierung eines vollständigen Multikanalansatzes mit flächendeckendem Filialsystem und kundenorientierten medialen bzw. Online-Kanälen wird der Sparkassen-Finanzgruppe wieder zu deutlichen Markterfolgen gegenüber den Direktbanken und online-aktiven Multikanalbanken verhelfen.

■ **Ansprechpartner beim DSGVO:** Dr. Axel Grote, Telefon: 030 20225-5715, E-Mail: axel.grote@dsgv.de.



Großes Potenzial: Der DSGVO forciert den Online-Vertrieb. Foto dpa

## Kombinationslösung aus Software, Chipkarte und Chipkartenleser verhindert Manipulationen von Daten durch Trojaner

## Sicherheit für mobile Lösungen

Die Angriffe auf Online Banking-Systeme nehmen zu. So wurden von Januar bis August 2006 mehr als 3000 neue Trojaner in Online Banking-Anwendungen registriert. Dies entspricht einer Zunahme um 25 Prozent gegenüber dem Vorjahreszeitraum.

Die Trojaner machen leichte Beute: Derzeit verfügen die Sicherheitsverfahren PIN (Persönliche Identifikationsnummer) und TAN (Transaktionsnummer) sowie iTAN (indizierte Transaktionsnummer) über einen Marktanteil von mehr als 80 Prozent. Diese Verfahren sind jedoch nicht trojanersicher. Dennoch setzen gemäß einer Studie von Fittkau und Maaß drei Viertel der Online Banking-Nutzer diese Verfahren ein und nur fünf Prozent verwenden Chipkarten. Trojanersicher sind jedoch nur Verfahren, bei denen die Signaturverarbeitung in ein nicht öffentlich zugängliches Betriebssystem ausgelagert ist.

Trojaner sind deshalb so tückisch, weil sie ohne das Wissen des Kunden Programme auf dessen PC installieren, die die Anzeige bewusst verändern und damit dem Kunden korrekte Daten vorgaukeln. Möglich ist auch, dass so genannte Keylogger Tastatureingaben des Kunden in Dateien speichern und dann von Betrügern eingesehen werden können.

Ein von der PPI AG und dem Chipkartenhersteller Reiner SCT entwickeltes System soll helfen, den Datenmissbrauch durch Trojaner zu verhindern. Die Internet-Banking-Lösung basiert auf dem Produkt Travic-Sign von PPI. Dabei werden die elektronischen Unterschriften von Kunde und Kreditinstitut abgeglichen. Über das im Browser installierte Travic-Sign kann der Kunde am heimischen Rechner einen Chipkartenleser nutzen, um die bankseitig signierten Auftragsdaten seinerseits zu signieren und per HTML an sein Kreditinstitut zu schicken. Dort werden die kundenseitig signierten Auftragsdaten geprüft und verarbeitet, zum Beispiel über das System Travic-Retail oder eigene Anwendungen des Kreditinstituts. Jede Information wird dabei auf die korrekte Signatur geprüft – Manipulationen können so von Kunde und Kreditinstitut aufgedeckt und die Auftragsausführungen können abgelehnt werden.

Um zusätzlich Trojanerangriffe auszuschließen, werden die verschiedenen Prüf- und Ansteuerungsformen,



Wirksamer Schutz vor Trojanern: Für Transaktionen übers Internet bietet eine Kombination aus Software, Chipkarte und Kartenlesegerät das höchste Maß an Sicherheit. Foto DSV-Gruppe

die bislang Bestandteil der Kundensoftware waren, in die Hardware des Chipkartenlesers von Reiner SCT verlagert. Dadurch soll gewährleistet werden, dass wichtige Sicherheitssoftware nicht mehr durch ungewollte Trojaner-Programme manipuliert werden kann. Sowohl der Kunde als auch das Kreditinstitut können nach Herstellerangaben dadurch sicher sein, dass die vorhandenen Ein- und Ausgabedaten tatsächlich authentisch sind.

Damit Angriffe von Trojanern und Viren weiterhin abgewehrt werden können, müssen die Sicherheitsverfahren immer wieder an die aktuelle technische Entwicklung angepasst werden. Travic-Sign ist vollständig in die vor-

handenen Prozessabläufe der jeweiligen Internet-Banking-Lösung des Kreditinstituts integrierbar. Dadurch wird nicht nur das Sicherheitsniveau des Systems erhöht, sondern auch die Wettbewerbsfähigkeit des Kreditinstituts gestärkt, ohne dass hohe Investitionen nötig sind. Denn Systeme, die ein hohes Maß an Sicherheit bieten, tragen dazu bei, das Kundenvertrauen in ein Kreditinstitut nachhaltig zu verbessern.

Auch hinsichtlich der vielfach geforderten Mobilität von Online Banking-Lösungen bietet Travic-Sign eine Möglichkeit. Zusammen mit dem Smartcard-Terminal mIDenty der Firma Kobil kann eine komplette Ablaufumgebung – Internet Browser,

Travic-Sign, Treiber und Chipkartenleser – für sicheres Internet Banking auf der Größe eines USB-Sticks platziert werden. Ohne Treiber installieren zu müssen, kann das Terminal einfach in einen PC mit Internet-Anschluss und USB-Schnittstelle gesteckt werden. Es stellt eine komplette Ablaufumgebung mit allen Einstellungen zur Verfügung. Die Anwendung startet automatisch vom Terminal und nutzt nur die dort hinterlegten Programmteile. Diese Lösung soll die Mobilität erhöhen und den nicht stationären Betrieb ergänzen. Sie ist allerdings nicht trojanersicher, da hierbei ein Klasse-1-Kartenleser ohne Tastatur und Display eingesetzt wird. DSV