Über Sicherheit sprechen

sb ▬ In der Kartenbranche galt früher der Grundsatz: „Wer über Sicherheit spricht, erweckt den Eindruck von Unsicherheit." Dem lag der Gedanke „Wer angibt, hat's nötig" zugrunde. Denn warum sollte die Anbieterseite die Sicherheit ihrer Lösungen betonen, wenn es gar keinen Grund gäbe, daran zu zweifeln? Seitdem hat sich viel geändert. Elektronische Bezahlverfahren sind weiter verbreitet, Online-Banking ist nahezu zum Normalfall geworden, und auch entsprechende mobile Anwendungen sind immer stärker auf dem Vormarsch. Das hat Bank- oder Payment-Systeme für die Hacker-Szene zu einem immer verlockenderen Ziel gemacht. Die Angriffe erfolgen häufiger und werden immer raffinierter. Datenpannen sind den Medien stets eine Schlagzeile wert, da man sich der Aufmerksamkeit einer breiten Öffentlichkeit sicher sein kann – schließlich betrifft das grundsätzliche Phänomen fast jeden. Wie viel über Sicherheit oder eben auch Unsicherheit gesprochen wird, hat die Anbieterseite damit längst nicht mehr in der Hand. Meldungen über das Ausspähen von Karten-Geheimnummern oder andere Datenabgriffe bei Banken haben früher bei manchem Empfänger noch eine Art wohliges Gruseln ausgelöst – es betraf ja nur die anderen. Auch das ist heute ganz anders. Denn natürlich fühlt sich der Nutzer vergleichbarer Anwendungen ungleich stärker davon berührt als die immer weiter sinkende Zahl der Nichtnutzer. Selbst wenn man persönlich von dem, worüber da berichtet wird, nicht betroffen ist, kommen die Einschläge gefühlt doch näher. Aus dem wohligen Gruseln kann Angst oder zumindest Unsicherheit werden.

Für die Banken bedeutet das zweierlei: Mehr denn je müssen sie sich dem Wettlauf mit der kriminellen Szene stellen und an der Sicherheit ihrer Systeme arbeiten. Und sie müssen darüber sprechen. Banken und Sparkassen tragen die Risiken und lassen ihre Kunden im Fall des Falles nicht im Regen stehen. Das ist eine ganz wichtige Botschaft, um das Vertrauen zu erhalten. Die andere lautet: Auch die Kunden stehen in der Verantwortung, das Ihre zur Sicherheit beizutragen, und sei es nur, ihr Mobiltelefon mit einem Kennwort zu sperren und für Banking-Dienste nicht das gleiche Passwort zu verwenden wie für soziale Netze und 50 Online-Shops. Die aktuelle Diskussion darüber, ob es sinnvoll ist, Virenschutzprogramme zu nutzen, oder ob damit nicht vielmehr die Wirksamkeit der in Betriebssysteme oder Browser eingebauten Sicherheitsfunktionen außer Kraft gesetzt wird, ist an dieser Stelle vielleicht nicht hilfreich. Dennoch kann der Nutzer gar nicht häufig genug an seine Eigenverantwortung erinnert werden. Denn die Finanzbranche kann die wachsende Verunsicherung durchaus zu ihren Gunsten ausnutzen – wenn es nämlich um die Akzeptanz immer neuer Sicherheitsverfahren geht. Wer um die Sicherheit seiner Daten fürchtet, der nimmt vermutlich auch etwas mehr Aufwand in Kauf, um dieselbe zu gewährleisten. Doch Obacht: Ein Freibrief für allzu komplexe Sicherheitslösungen ist das nicht. Schließlich machen die Fintechs vor, was Nutzerfreundlichkeit heißt.

Beim Thema Datenschutz und Datensicherheit geht es freilich nicht immer nur um unberechtigte Zugriffe von außen, sondern auch darum, was Banken und Versicherer selbst mit den verfügbaren Daten anfangen. Zu Recht hat die Branche hier immer noch Skrupel, Dinge zu tun, die etwa im Online-Handel längst eine Selbstverständlichkeit sind. Wer beispielsweise die Finanzströme seiner Kunden so weit analysiert, dass er ihm auf dieser Basis einen neuen Online-Shop oder einen günstigeren Stromtarif empfehlen kann, der muss genau wissen, ob die Kunden das goutieren. Sonst ist der Imageschaden weit höher als der Nutzen je sein könnte. Gerade im Payment sind „Bewegungsprofile" schließlich das Schreckgespenst aller Datenschützer. Big-Data-Abstinenz kann jedoch auch keine Lösung sein. Schließlich erwartet die Kundschaft zunehmend personalisierte Angebote. Die Assekuranz ist hier schon sehr viel weiter als Banken, die den Kunden den Mehrwert einer verstärkten Datennutzung noch nicht so plausibel gemacht haben. Aufgabe der Datenschutzbeauftragten darf es insofern nicht nur sein, neue Ansätze auszubremsen. Sondern sie müssen sie in die richtige Richtung steuern und für Transparenz sorgen. ▬