Mobile Geräte – sicher, aber **effizient**

Von Thomas Laubrock

Besserverdiener lieben das mobile Surfen im Netz via Smartphone oder Tablet. Wer mit einer attraktiven Zielgruppe auf Augenhöhe kommunizieren will, so der Autor, tut gut daran, im Außendienst der Finanzberatung immer stärker auf mobile Geräte zu setzen. Das signalisiert Innovationsbereitschaft und einen flexiblen, schnellen Service vor Ort. Doch der effektive Einsatz von Tablets und Smartphones im Bankenwesen setzt einen sicheren Zugriff auf Kunden- und Finanzdaten voraus. Eine Herausforderung, für die TÜV Rheinland mit F5 eine Lösung bietet. Red.

Je höher das Nettoeinkommen, desto höher das Interesse am mobilen Internet. Das haben der Bundesverband Digitale Wirtschaft (BVDW) und das Marktforschungsinstitut Yougov Deutschland herausgefunden. Fast die Hälfte der besser verdienenden Nutzer mit einem Nettoeinkommen von über 4 000 Euro surft am liebsten mit mobilen Geräten durchs Internet. Bei Nettoeinkommen unter 2 500 Euro sinkt das Interesse am „Internet to go" auf nicht ganz ein Drittel.

Und noch ein Zusammenhang, der für Finanzexperten interessant sein dürfte: Je höher der monatliche Verdienst, desto höher auch die Aktivität in sozialen Netzwerken. Über 60 Prozent aller User, die mehr als 4 000 Euro monatlich verdienen, sind regelmäßig in Foren unterwegs. Bei Haushaltseinkommen unter 1 000 Euro sind es allerdings immer noch 50 Prozent. Der Besuch in Foren erfolgt häufig nicht nur zum Plaudern, sondern auch, um sich mit anderen Konsumenten über Leistungen und Produkte auszutauschen.

Verbraucher wie gewerbliche Kunden sind heute deutlich besser informiert und vergleichen Preis-Leistungs-Verhältnisse viel stärker als früher. Geldinstitute, die gegenüber der zunehmenden Konkurrenz auch aus der EU nicht den Anschluss verlieren wollen, werden nicht umhin kommen, beim Kunden vor Ort mit aktuellen Informationen, schnellem Service, Mobilität und Flexibilität aufzutrumpfen und sich stärker in den Informations- und Entscheidungsfindungsprozess ihrer Zielgruppe einzubringen.

Denn ob Eigenheimfinanzierung, Lebensversicherung, Investmentfonds, Firmenkredit oder Wertpapiere: Kunden sind heute zunehmend selbstbewusster und anspruchsvoller. Die Konsumentenmacht, die ihnen die Online-Interaktion in sozialen Netzwerken und die digitale Öffentlichkeit verleihen, spielen sie aus, auch Firmenkunden nutzen das Netz, um Konditionen und Angebote zu vergleichen.

Zugleich gibt es für Banken immer weniger Berührungspunkte, weil Kunden aufgrund des Online-Bankings immer seltener in die Filiale kommen. Umso wichtiger wird der effiziente Auftritt bei einem individuellen Kundengespräch, das immer häufiger in den eigenen vier Wänden oder im Büro des gewerblichen Kunden stattfindet.

Zum Autor

Thomas Laubrock, Head of Product Management der TÜV Rheinland i-sec GmbH, Köln.

Sicherheit hat Vorrang vor User-Komfort

Der Bankkunde hält es für selbstverständlich, dass der Berater mit Smartphone oder Tablet einen flexiblen, schnellen und vor allem sicheren Zugriff auf Kundendaten und auf relevante Anwendungen der Bank mitbringt. Bestenfalls kann der Berater während des Gesprächs gleich online den Kredit- oder Auto-Leasing-Antrag ausfüllen. Nur Minuten später erhält der Kunde bereits die Kreditzusage – abgeglichen und abgesichert durch eine aktuelle Bonitätsauskunft. Denkbar ist auch eine Beratung des Firmenkunden in Bezug auf kapitalmarktorientierte Finanzierungslösungen oder der Blick auf Historie und voraussichtliche Volatilität eines optimalen riskanten Portfolios.

Wie Mitarbeiter in anderen Branchen setzen auch Finanzberater immer häufiger Geräte

ein, die sie – genau wie ihre Kunden – auch privat zu schätzen gelernt haben: Ein Plus an Produktivität, Komfort und Kundenorientierung. So attraktiv der Einsatz mobiler Geräte im Finanzwesen auch ist, ihre Einbindung stellt gerade Geldinstitute vor große Herausforderungen in puncto Sicherheit. Denn der Finanzdienstleistungssektor zählt ohnehin zu den Hauptzielen von Cyberkriminellen. Sind Smartphones und Tablets nicht ausreichend abgesichert und werden sie durch Angreifer, Viren oder Schadsoftware kompromittiert, droht dem Geldinstitut nicht nur ein kaum zu beziffernder Imageschaden, sondern auch ein Verstoß gegen geltende Datenschutzgesetze und Compliance-Richtlinien.

Mobile Performance beeinflusst Mitarbeitermotivation

Grundsätzlich müssen mobile Finanzberater oder auch dritte Vertriebspartner heute sowohl auf externe Inhalte wie die Unternehmenshomepage als auch auf interne Verzeichnisse und Dienste zugreifen können, abhängig von der jeweils individuellen Rollendefinition. Die wichtigsten Fragen dabei sind: Welche mobilen Geräte verlangen Zugriff? Auf wen ist das Gerät registriert? Welche Anwendungen sind freigegeben und wie kann der User zwischen Unternehmenswebsite, Intranet, internen Datenbanken und externen Diensten wie etwa der Schufa-Auskunft sicher navigieren?

Das sind sicherheitsrelevante Faktoren, die in der Praxis zumeist eine komplexe Sicherheitsinfrastruktur nach sich ziehen. Die Datenübertragung erfolgt klassischerweise vom Server über gesicherte Verbindungen wie etwa einem Virtuellen Privaten Netz (VPN). Eine Zweifaktor-Authentisierung, zum Beispiel mit Einmal-Passwort (OTP), sowie Zugangskontrolle und Rechteverwaltung sorgen dafür, dass die Daten geschützt sind.

Das bedeutet allerdings auch, dass der User für jede einzelne Anwendung eigene Zugangsdaten eingeben muss. Eine Vielzahl an Benutzerkennungen und Passwörtern sowie langwierige Einwahlprozeduren sind die Folge. Die Eingabe auf der Mikro-Tastatur mobiler Geräte ist mühsam und kostet im Kundengespräch dazu noch kostbare Zeit. Kann der Finanzberater vor Ort nicht flexibel und in Echtzeit auf relevante Daten zugreifen, sind das produktive Potenzial mobiler Geräte und der gute Eindruck beim Kunden schnell dahin.

Übrigens: Der Einfluss der mobilen Performance auf die Motivation der Außendienstler ist nicht zu unterschätzen: Im i-Pass-Report 2012 gab über die Hälfte der Befragten an, frustriert zu sein, wenn sie über ihre Smartphones und Tablet-PCs aufs Firmennetzwerk zugreifen und dieses nicht für mobile Geräte optimiert ist.

Datensicherheit und Effizienz gleichermaßen wichtig

TÜV Rheinland ist der Ansicht: Sicherheit darf Effizienz und Business-Entwicklung nicht egalisieren, weil dies zulasten von Produktivität und Wertschöpfung geht. Die sichere und flexible Einbindung mobiler Geräte soll ein hohes Maß an Sicherheit gewährleisten, zentral alle notwendigen Funktionen bedienen können, automatisch zu konfigurieren sein, die unterschiedlichen Betriebssysteme der mobilen Geräte unterstützen und für den Zugang lediglich einen einzigen Login erfordern. Und natürlich muss die Technologie zuverlässig sein und eine hohe Skalierbarkeit ermöglichen.

Der TÜV Rheinland hat den Markt auf diese Anforderungen hin unter die Lupe genommen und verschiedene Ansätze sowie diverse Technologien rund um die sichere Einbindung von mobilen Geräten im Finanzwesen analysiert. Sehr flexibel erfüllt die Anforderungen die Portallösung von F5, ein global tätiger Hersteller für Application Delivery Networking aus München.

Bei der Entwicklung der Plattform zur Einbindung mobiler Geräte in die Unternehmensumgebung hat F5 nicht nur großen Wert auf Datensicherheit, sondern auch auf Anwenderfreundlichkeit und Performance außerhalb der Geschäftsräume des Geldinstituts gelegt. Gleichermaßen trägt die Technologie der Verfügbarkeit der Daten in Echtzeit angemessen Rechnung, was zu einer deutlichen Produktivitätssteigerung im mobilen Vertrieb führt. Darüber hinaus werden laufende Kosten und Einflüsse auf die Geschäftsvorgänge auf ein Minimum reduziert.

Einheitlicher Login

Strukturelle Voraussetzung für die Portallösung ist die Integration von Tablets und Smartphones über ein Mobile Device Management System (MDM), wie es etwa Mobile-Iron anbietet. Das MDM managt zentral die mobilen Geräte der Mitarbeiter und registriert bis hin zur Telefonnummer, wem welches Gerät gehört. Hier setzt die Portallösung an: Auf jedes so personalisierte mobile Gerät wird automatisiert ein Zertifikat aufgespielt, das Bestandteil der Hardware ist und nur nach Eingabe der Geräte-PIN zur Authentisierung zur Verfügung steht. Ähnlich dem Token werden Smartphone oder Tablet bei der Authentisierung mit dem lokal gespeicherten Zertifikat so neben der Geräte-PIN zum wesentlichen Faktor der Authentisierung. Fehlt einer der Faktoren – Zertifikat oder PIN – ist ein Zugriff nicht möglich.

Die Geräte-PIN der Smartphones und Tablets sichert neben dem Zertifikat auch die gespeicherten Daten, wie zum Beispiel E-Mails und Kontakte, daher sollte sie eine ausreichende Komplexität haben, etwa als sechs- bis achtstellige alphanummerische PIN. Die Benutzerakzeptanz ist aufgrund der Komplexität erfahrungsgemäß häufig zunächst nicht sehr hoch. Erkennt der User allerdings, dass im Anschluss daran alle Dienste und Apps ohne weiteren Login genutzt werden können, stellt sich die Akzeptanz beim Anwender schnell ein.