

# Die digitale Anatomie der genossenschaftlichen Finanzgruppe

Von Carsten Pfläging



**Die Rechenzentren der Fiducia & GAD IT sind das „digitale Herz“ der genossenschaftlichen Finanzgruppe, so Carsten Pfläging. Und die Rolle der IT wird mit den veränderten Kundenerwartungen immer wichtiger. Herausforderung Nummer eins ist dabei die Sicherheit. Denn die Cybergefahren nehmen rasant zu. Eine Sicherheitsstrategie kann daher niemals abgeschlossen sein. Sondern sie ist ein dynamischer Prozess, der auch die Zusammenarbeit mit Experten außerhalb des Verbundes erfordert.** Red.

Mit rund 1 000 Volks- und Raiffeisenbanken, einer Zentralbank sowie diversen Verbundunternehmen und Sonderinstituten ist die genossenschaftliche Finanzgruppe einer der bedeutendsten Player in der Deutschen Kreditwirtschaft. Das digitale Herz der Gruppe schlägt in vier Hochleistungsrechenzentren in Münster und Karlsruhe: Hier sorgt die Fiducia & GAD IT AG mit modernster Technik und permanenten Innovationen für einen rund um die Uhr verfügbaren Bankenservice, dessen Qualität und Zuverlässigkeit das Fundament für die Wettbewerbsfähigkeit der betreuten Banken ist.

Eine der größten Herausforderungen, vor der IT-Dienstleister aktuell steht: Maxima-

le IT-Sicherheit angesichts rasant zunehmender Cybergefahren. Denn nur unter dieser Bedingung können die Volks- und Raiffeisenbanken dem gewachsenen Vertrauen ihrer Kunden auch in Zeiten der Digitalisierung umfassend gerecht werden.

Pro Minute wickeln deutsche Genossenschaftsbanken gut 1 500 Überweisungen ab. Im gleichen Zeitraum werden an SB-Automaten mehr als 1 200 Kontoauszüge gedruckt und etwa 1 000 Bargeldauszahlungen vorgenommen. 550-mal wird in diesen 60 Sekunden die VR-Banking-App aufgerufen; 2 600-mal wählen sich Kunden in das genossenschaftliche Online-Banking ein. Über das Jahr gerechnet, summieren sich sämtliche Kontobewegungen für die rund 18,4 Millionen Mitglieder aller betreuten Institute auf insgesamt 6,8 Milliarden Buchungsposten.

## Täglich 3,1 Petabyte Netzwerk-Traffic

Dieser imposanten Zahl steht eine hochentwickelte IT-Landschaft gegenüber, deren Dimensionen nicht weniger eindrucks-

voll sind: In den vier Rechenzentren der Fiducia & GAD verarbeiten neun ultraschnelle Großrechner täglich rund 44,2 Milliarden Hosttransaktionen. Zirka 16 500 Netzwerk-Switches bewältigen ein Datenvolumen von durchschnittlich 3,1 Petabyte pro Tag – weit mehr, als das Fassungsvermögen von einer halben Million handelsüblicher DVDs. Nebeneinandergelegt, ergäbe sich auf den Autobahnen A5 und A6 eine lückenlose Kette aus Silberscheiben, die von Mannheim bis Karlsruhe reicht.

Die Rechenzentren der Fiducia & GAD versorgen in ganz Deutschland rund 173 000 Bankarbeitsplätze in den betreuten Instituten. Außerdem erbringt der genossenschaftliche IT-Provider unterschiedlichste Druck- und Versanddienstleistungen – wobei jährlich etwa 1 Milliarde Druckseiten beziehungsweise 250 Millionen kuvertierte Sendungen die insgesamt 45 Hochleistungsdruck- und Kuvertierstraßen verlassen. Nicht zuletzt sorgt die Fiducia & GAD für den zuverlässigen Betrieb von bundesweit gut 36 000 genossenschaftlichen SB-Geräten, an denen sich Kunden rund 540 Millionen Mal im Jahr Bargeld auszahlen lassen.

### Zum Autor

**Carsten Pfläging**, Mitglied des Vorstands, Fiducia & GAD IT AG, Karlsruhe/Münster

### Gewandelte Kundenerwartungen

Warum ist die Leistungsfähigkeit der IT heute wichtiger denn je? Weil sich die Rolle des Kunden in der digitalen Ära grund-

legend verändert hat. Und dies nicht nur im Finanzdienstleistungsmarkt: Das Internet stärkt das Selbstbewusstsein der Verbraucher. Immer weniger Bankkunden wollen ausschließlich passive Konsumenten von Dienstleistungen wie der konventionellen Kontoführung sein.

Stattdessen wächst die Zahl derjenigen Kunden, für die der Online-Kontozugang so etwas wie ein Single-Point-of-Service ist, um die eigenen Finanzangelegenheiten in unterschiedlichen Lebenssituationen aktiv zu gestalten. Solche Kunden brauchen eine moderne Bank, die als Partner auf Augenhöhe jederzeit zur Verfügung steht. Moderne Banken wiederum sind auf eine sichere, leistungsfähige und hochverfügbare IT-Unterstützung angewiesen.

Die veränderten Erwartungen der digitalen Kundengeneration betreffen nicht zuletzt auch den Zahlungsverkehr: Private Geldtransfers – etwa bei einem Restaurantbesuch mit Freunden, die sich die Rechnung teilen wollen – sollen ohne komplizierte Überweisungsmasken am besten mit dem Smartphone möglich sein.

Die Fiducia & GAD hat diesen Kundenbedarf bereits Ende letzten Jahres durch einen zusätzlichen Menüpunkt für die VR-Banking-App erfüllt: Mit dem neuen Feature „Geld senden & anfordern“ funktioniert der Geldtransfer an Freunde und Verwandte ohne langwieriges IBAN-Tippen genauso einfach wie ein Whatsapp-Chat. Bei Summen unter 30 Euro ist dafür nicht einmal die sonst obligatorische TAN-Eingabe notwendig.

Anders als bei vergleichbaren Transferofferten aus der Fintech-Szene brauchen mobile Kunden der Volks- und Raiffeisenbanken für das Feature „Geld senden & anfordern“ keine separate App. Die Fiducia & GAD bündelt bewusst sämtliche Mobile-Banking-Funktionen unter dem Dach der VR-Banking-App. Denn dies erleichtert die Nutzung im Alltag und festigt zudem die Bindung mobiler Kunden an die genossenschaftliche Marke der

VR-Banken. Die Banking-App wird auf diese Weise gleichsam zur Hausbank in der Hosentasche – zu einem Lebensbegleiter rund um die Uhr.

### **Das wichtigste Kapital im digitalen Bankgeschäft heißt Vertrauen**

Der digitale Lebensstil hat einen Werte- und Verhaltenswandel ausgelöst, der vor allem am zunehmenden Trend zur gemeinschaftlichen Nutzung materieller Güter sichtbar wird. Der Eigentumsgedanke tritt in den Hintergrund: Carsharing oder online vermittelte Unterkünfte sind zwei Beispiele für kollektiven Ko-Konsum, den insbesondere junge Leute als eine nachhaltige Alternative zu individuellem Besitz empfinden. Via App teilen Menschen heute nicht nur Meinungen und Fotos, sondern auch Wohnungen und Autos oder tauschen Bücher und zu klein gewordene Kinderkleidung aus.

Anders als bei rein kommerziell ausgerichteten Giganten wie Airbnb und Uber befinden sich viele neue Plattformen aus der digitalen Ökonomie im Besitz derjenigen, die sie auch tatsächlich nutzen. Ein Beispiel dafür ist Fairmondo – ein digitaler Marktplatz, der Online-Riesen wie Ebay und Amazon die Stirn bieten will.

Im gemeinschaftlichen Partizipationsmodell solcher digitalen Ökosysteme erlebt die ursprüngliche Genossenschaftsidee derzeit eine Renaissance. Im Unterschied jedoch zu traditionellen Genossenschaften etwa im Wohnungsbau oder der Landwirtschaft, wo praktisch jeder jeden kennt, sind persönliche Bekanntschaften in einer überregionalen Online-Genossenschaft ein seltener Ausnahmefall – weshalb das notwendige Vertrauen auf andere Art entstehen muss.

Hier könnten die Volks- und Raiffeisenbanken quasi als Vertrauensbroker einspringen, denn sie kennen ihre Mitglieder durch persönliche Legitimation. Daraus ergibt sich die Chance, die in der deut-

schen Bankenlandschaft einzigartige Reputation der Genossenschaftsbanken in einen zusätzlichen Wettbewerbsvorteil zu verwandeln – und dies ist nur eines von vielen Argumenten, warum das Vertrauen der Kunden im Wettbewerb der Kreditwirtschaft immer wichtiger wird.

### **Kein Vertrauen ohne Sicherheit**

Massiv gefährdet ist das Kundenvertrauen heute allerdings durch Cyberkriminalität: Weltweit nehmen Phishing-Angriffe und Hackerangriffe in besorgniserregendem Ausmaß zu. Im Gegenzug sind „klassische“ Bankraub- und Überfallsdelikte in der Bundesrepublik seit Jahren rückläufig – wohl auch deshalb, weil in den Filialen immer weniger Bargeld vorgehalten wird.

In die Schlagzeilen schaffen es meist nur spektakuläre Fälle – wie im vorigen Jahr ein großangelegter Cyberangriff auf die Nationalbank von Bangladesch, bei dem eine organisierte Gang rund 81 Millionen US-Dollar erbeutete. Security-Spezialisten fanden im Nachhinein heraus, dass die Täter gezielt Schwachstellen in den IT-Systemen der Bank ausgespäht hatten, über die sie im Anschluss manipulierte Swift-Aufträge in die Systeme einschleusen.

Solche Tätergruppen gehen meist hochprofessionell vor und agieren nicht selten international – was die Ermittlungstätigkeit der Strafverfolgungsbehörden erschwert. In manchen Fällen öffnet mangelndes Problembewusstsein und die Arglosigkeit vieler Anwender den Kriminellen Tür und Tor.

### **Die Öffentlichkeit ist sensibilisiert**

Aufsehenerregende Meldungen in den Medien haben zumindest ein Gutes: Sie sensibilisieren eine breite Öffentlichkeit für die wachsenden Gefahren im digitalen Raum.

■ Aktuell sind zum Beispiel erneut Phishing-Mails im Umlauf, die den Adressaten dazu verleiten, seine Login-Daten auf einer gefälschten Website der Volks- und Raiffeisenbanken einzugeben. Auch das Vorgehen, via Social Engineering fremde Rechner zu infiltrieren, ist weiter auf dem Vormarsch. Bei beiden Vorgehensweisen täuschen Kriminelle oft einen vertrauenswürdigen Kontext vor – zum Beispiel, indem sie seriöse Namen von Behörden, Banken oder Hilfsorganisationen als fingierten Absender für Phishing-Mails missbrauchen.

■ Beim alltäglichen Surfen unterschätzen viele Anwender zudem die Gefahr einer sogenannten Drive-by-Infektion, bei der ein Schadprogramm sogar ohne das Zutun des Nutzers über eine Schwachstelle im Browser oder Browser-Plug-ins in den Computer eindringen kann. Die regelmäßige Überprüfung und Optimierung der Anwendungen ist daher enorm wichtig.

Was in Presseberichten über Millionen-Coups wie dem bei der Bangladescher Nationalbank nicht so ohne weiteres deutlich wird, ist die Tatsache, dass es für Finanzdienstleister beim Thema IT-Sicherheit eben nicht nur um die Abwehr monetärer Schäden geht: Viel schwerer wiegt unter Umständen der Reputations- und Vertrauensverlust – etwa, wenn in der Presse über den Abfluss personenbezogener Kundeninformationen durch einen Diebstahl von Kreditkartendaten berichtet wird.

### Wie eine digitale Festung

Aus Sicht der Fiducia & GAD können isolierte Schutzmaßnahmen sowohl im Herzen der Rechenzentren als auch am anderen Ende auf den Clientgeräten draußen in den Bankfilialen den komplexen Security-Herausforderungen allein nicht gerecht werden. Worauf es vielmehr ankommt, ist das nahtlose Zusammenspiel unterschiedlicher Präventions-, Detektions- und Abwehransätze, die in einer

ganzheitlichen Sicherheitsstrategie vergleichbar einer digitalen Festung zusammenfließen müssen.

So schützen Virens Scanner und Firewalls vor Cyberangriffen, permanent wird der gesamte Netzwerkverkehr sowie jeder einzelne Anwendungs- und Systemzugriff überwacht. Bei Anzeichen für ein ungewöhnliches Traffic- oder Zugriffsmuster läuten sofort die Alarmglocken.

Zudem sind Systeme, Verfahren und IT-Anwendungen des Unternehmens gemäß ISO 27001 zertifiziert und nach den Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) umgesetzt.

### Informationssicherheit – ein laufender Prozess

Hervorzuheben ist, dass die Informationssicherheits-Strategie des genossenschaftlichen IT-Dienstleisters alles andere als starr in Stein gemeißelt ist: Sie hat im Gegenteil eine hochflexible Struktur, die auf eine stete Anpassung an neue Gefahrensituationen ausgelegt ist. Was auch immer der Entwickler-Stab für das Bankverfahren agree21 oder eine Kundensoftware wie der VR-Banking-App an Verbesserungen plant – IT-Sicherheit ist vom ersten Entwicklungsschritt an ein unabdingbares Designkriterium.

Außerdem handelt das Security-Team, dem mehr als ein Dutzend hochqualifizierter Sicherheitsexperten angehören, nicht nur reaktiv – also erst dann, wenn ein hauseigenes System angegriffen wird. Vielmehr untersuchen sie neu auftauchende Angriffsmuster mit forensischer Akribie, sobald sie davon Kenntnis erhalten.

Wichtig ist dabei der Dialog mit Sicherheitsfachleuten anderer Organisationen innerhalb und außerhalb der genossenschaftlichen Finanzgruppe, darunter auch die Bundes- und Landeskriminalämter. Zuweilen ahmen die Security-Mitarbeiter bei der Fiducia & GAD sogar die Metho-

den von Cyberkriminellen nach, um anhand von Scheinattacken bislang unentdeckte Sicherheitslücken zu erkennen und zu schließen – bevor ein echter Hacker sie für einen realen Angriff ausnutzen kann.

Gleichwohl: Hundertprozentige Sicherheit gibt es selbst bei noch so großer Anstrengung nicht. IT Security ist kein jemals erreichbarer Zustand, sondern ein fortwährender Prozess, der die Schutz- und Abwehrmaßnahmen permanent optimiert. Das jedenfalls ist der Anspruch der Fiducia & GAD.

Dies ist im Übrigen nicht nur eine Frage der Technik, vielmehr steht häufig der „Security-Faktor“ Mensch im Vordergrund: Aufklärung und Sensibilisierung sind eine bleibende Aufgabe – sowohl im Hinblick auf die eigenen Mitarbeiter und Bankangestellten als auch, was die Kunden der Volks- und Raiffeisenbanken betrifft.

### Maximaler Ausfallschutz

Zusammenfassend lässt sich festhalten: In der genossenschaftlichen Finanzgruppe stützen sich klassische IT-Verfahren genauso wie innovative Service-Angebote, die sich an eine zunehmend mobile Kundengeneration richten, auf eine extrem leistungsfähige digitale Infrastruktur.

Mit einer Verfügbarkeit von 99,98 Prozent in den Rechenzentren und einem adaptiven Sicherheitskonzept, das auf State-of-the-Art-Technologien basiert, sorgt die Fiducia & GAD für maximalen Ausfallschutz und verlässliche Servicequalität – von der alltäglichen Kontobewegung bis hin zur softwaregestützten Kundenberatung in der Filiale oder per Video-Chat.

Der hohe Innovationsgrad der genossenschaftlichen IT-Infrastruktur schafft hierbei die Grundvoraussetzung dafür, dass die Digitalisierung der Banken mit hohem Tempo weiter voranschreiten kann. ■■■