Andreas Abel / Jochen Dinger

# **Informationssicherheit**: Basis für das genossenschaftliche Bankgeschäft

Es war schon eine kleine Sensation, als Edward Snowden am 22. November per Videokonferenz auf der JBFOne, dem IT-Kongress der Fiducia & GAD IT AG in München, das Wort ergriff. Der Whistleblower sprach eine halbe Stunde zu IT-Sicherheitsthemen wie Hackerangriffe auf Geldströme, das Outsourcing von Daten oder die Nutzung vermeintlich sicherer persönlicher Assistenten. „Bequemlichkeit ist ein Risiko", sagte Snowden. „Was dem Nutzer den Alltag zunehmend erleichtern soll, ist für die Privatsphäre eine Gefahr."

**Betrugsversuche schwerpunktmäßig im Bereich Konto und Karte**

Warum das Thema Informationssicherheit gerade auch in der genossenschaftlichen Finanzgruppe stetig an Bedeutung gewinnt, verdeutlichte der diesjährige IT-Kongress des genossenschaftlichen IT-Dienstleisters gleich mit mehreren hochkarätigen Security-Beiträgen. Deutlich wurde dabei unter anderem, welche konkreten Cybergefahren für einen potenziellen Schaden in mehrstelliger Millionenhöhe bei den Volks- und Raiffeisenbanken verantwortlich sind. Im aktuellen Lagebild zeichnet sich ab, dass sich Betrugsversuche schwerpunktmäßig auf den Bereich Konto und Karte konzentrieren. Eine Antwort auf diese Entwicklung: Erfolgreiche Abwehr derartiger Betrugsversuche durch ein tief verankertes Anti-Fraud-Management für den Zahlungsverkehr in den Bankverfahren agree-21 und bank-21.

Während physische Angriffe auf Geldautomaten durch Sprengung zunehmen und weiterhin technische und organisatorische Gegenmaßnahmen erfordern, weisen manche Deliktsbereiche demgegenüber rückläufige Tendenzen auf. So sanken die Schäden durch sogenanntes Skimming an Geldautomaten zwischen 2010 und 2015 um insgesamt 94 Prozent in Deutschland. Der starke Rückgang beweist, dass sich die bisherigen Investitionen zum Beispiel in robuste Authentifizierungs- und Legitimationsmechanismen (EMV-Chip) für Genossenschaftsbanken durch ein steigendes Sicherheitslevel für die Bankkunden und die Banken auszahlen.

**Cyberkriminelle weiter auf dem Vormarsch**

Solche Erfolge dürfen aber nicht zu der Annahme verleiten, dass Cybergefahren im Bankensektor weitgehend gebannt wären. Im Gegenteil: Der aktuelle Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik BSI spricht sogar von einer rasanten Professionalisierung und Globalisierung innerhalb der organisierten Internetkriminalität. Nach Schätzungen von Europol im jährlichen Cybercrime-Bericht 2016 wird Cyberkriminalität – auch als „crime as a service" bezeichnet – künftig ein größeres Volumen aufweisen als traditionelle Delikte. Die Finanzbranche ist immer wieder Ziel solcher Angriffe. Dies zeigt sich auch darin, dass Ransomware und Banking-Trojaner laut Europol einen wesentlichen Teil der Cybercrime ausmachen.

Dies bestätigen auch mehrere spektakuläre Cyberangriffe auf Kreditinstitute in aller Welt. So erbeutete zum Beispiel eine internationale Hackerbande im Mai vorigen Jahres mithilfe gestohlener Kreditkartendaten rund 19 Millionen US-Dollar von Konten einer südafrikanischen Bank. Der Coup gelang mit etwa 14000 illegalen Transaktionen an japanischen Geldautomaten. Erst drei Monate zuvor hatte ein digitaler Überfall auf die Nationalbank von Bangladesch für Schlagzeilen gesorgt: Hier stahlen die Täter gut 80 Millionen US-Dollar durch manipulierte SWIFT-Aufträge – vermutlich hatten sie es jedoch auf mehr als das Zehnfache abgesehen. Die tatsächlich ergaunerte Summe wuschen sie schließlich in philippinischen Spielcasinos.

**Angriffe nach dem Muster der „Kill-Chain"**

Den Analysen von IT-Sicherheitsfirmen zufolge nutzten Cyberkriminelle für ihre Verbrechen unterschiedliche Schwachstellen in der IT-Infrastruktur der angegriffenen Banken aus. Die Angriffsmuster und Angriffsketten (Kill-Chain) sind sich dabei oft sehr ähnlich: Ein argloser Klick auf den infektiösen Anhang einer Mail oder auf einen integrierten Link, der zu einer kom-

*Dr. Andreas Abel, Leiter Risiko-, Compliance-, Sicherheitsmanagement und Recht, und Dr. Jochen Dinger, Leiter Sicherheitsmanagement bei der Fiducia & GAD IT AG, Münster und Karlsruhe*

*Ein verlässlicher Schutz vor Hacker- und Phishing-Attacken im Bankensektor beugt aus Sicht der Autoren nicht nur finanziellen Schäden in den bekannt werdenden Einzelfällen vor, sondern bewahrt vor allen Dingen auch das so enorm wichtige langfristig gewachsene Vertrauen vieler Millionen Kunden in die gesamte deutsche Kreditwirtschaft. Sie plädieren für eine ganzheitliche Cyber-Security-Strategie, die über die notwendige Prävention hinaus auch auf detektive und reaktive Fähigkeiten setzt, um nach einer erfolgreichen Infiltration die eingedrungenen Softwareschädlinge im System umgehend erkennen und isolieren sowie im Idealfall den Angriff stoppen zu können, bevor es zu Manipulationen oder dem Abfluss vertraulicher Informationen gekommen ist. Auch wenn das Team proaktiv neu auftauchende Angriffsmuster rechtzeitig zu erkennen und zu analysieren sucht, stufen die Experten ihre Arbeit als Daueraufgabe ein. (Red.)*

promittierten Webseite führt, löst unbemerkt die Installation eines Trojaners aus. Von dem infizierten Rechner hangeln sich die Angreifer weiter über das Netzwerk und versuchen, andere Systeme unter ihre Kontrolle zu bringen.

Auf infizierten Geräten schneiden solche Trojaner beispielsweise Screenshots und Tastatureingaben mit und richten heimlich einen Fernzugriff auf dem gekaperten Computer ein. Auf diese Weise können Hacker auch typische Nutzungsmuster zunächst eingehend studieren, um sie später desto täuschender zu imitieren. Wenn ein Cyberangriff im Geschäftsalltag von Banken nicht rechtzeitig detektiert wird, bleibt den Tätern genügend Zeit, um über die manipulierten Systeme erhebliche Beträge über Strohmannkonten ins Ausland abzuzweigen.

Außer technischen Schwachstellen in Software- oder Hardwaresystemen spielen aber auch Arglosigkeit und mangelndes Bewusstsein aufseiten der Anwender solchen kriminellen Machenschaften in die Hände. Insofern haben die Schlagzeilen über spektakuläre Cybercoups im Bankensektor zweifellos auch ihr Gutes: Sie lenken die Aufmerksamkeit einer breiten Öffentlichkeit auf die wachsenden Gefahren im digitalen Raum. Und das ist auch notwendig, denn die Versuche unterschiedlich motivierter Tätergruppen, fremde Rechner via Social Engineering anzugreifen, ist eine wachsende Bedrohung. Hierbei gaukeln Kriminelle nicht selten Vertrauenswürdigkeit vor, indem sie seriös klingende Namen von Behörden, Hilfsorganisationen oder Banken als fingierte Absender für Phishing-Mails missbrauchen.

## Dreiklang aus Prävention, Detektion und Reaktion

Angesichts der Vielfalt und Komplexität der heutigen Bedrohungslage bieten präventive Sicherheitsvorkehrungen wie der klassische Virenscanner allein keinen ausreichenden Schutz mehr. Weil Schadprogramme von Scannern anhand charakteristischer Bitmuster oder „einfacher" Heuristiken ausgefiltert werden, funktionieren viele Erkennungsmechanismen nur bei bekannten Schadprogrammen. Die Hackerszene hat allerdings längst gelernt, die Virenscanner mit polymorphem Schadcode auszutricksen. Auch Patches schließen nur bekannte Schwachstellen. Sie verkürzen somit die Zeitspanne, innerhalb derer die betreffende Sicherheitslücke für einen Angriff ausgenutzt werden kann. Gegen sogenannte Zero-Day-Exploits – also gegen Angriffe, die auf noch unentdeckte Schwachstellen zielen – gibt es keinen Sicherheitspatch.

Aus alldem ergibt sich die klare Konsequenz: Eine ganzheitliche Sicherheitsstrategie darf nicht mehr einseitig auf Maßnahmen zur Prävention ausgerichtet sein. Darüber hinaus kommt es heute verstärkt auch auf detektive und reaktive Fähigkeiten an. Denn nur damit lassen sich nach einer erfolgreichen Infiltration die eingedrungenen Softwareschädlinge im System umgehend erkennen und isolieren, um letztlich den Angriff zu stoppen – am besten noch bevor es zu Manipulationen oder dem Abfluss vertraulicher Informationen kommt.

## Digitaler Fels in der Brandung

Dem reibungslosen Zusammenspiel unterschiedlicher Präventions-, Detektions- und reaktiver Abwehransätze auf der Basis einer ganzheitlichen Sicherheitsstrategie kommt eine besondere Bedeutung zu. Dabei geht es um eine Strategie, die sich vom Kern der Hochsicherheitsrechenzentren des genossenschaftlichen IT-Dienstleisters über sämtliche Bankfilialen der betreuten Institute hinweg bis auf alle stationären und mobilen Anwendungen der Bankmitarbeiter und der Kunden erstreckt. Überdies wird der Netzwerkverkehr mithilfe hochentwickelter Sensorikmechanismen kontinuierlich überwacht, sodass ungewöhnliche Traffic- oder Zugriffsmuster sofort auffallen.

Als Orientierung für ihr durchgängiges Sicherheitsframework vom Rechenzentrum bis zur mobilen App stützt sich die Fiducia & GAD auf den NIST Cybersecurity Framework – eine international anerkannte Methodik, die auch von der European Banking Authority EBA zur Bewertung von IT-Security-Bestrebungen in bedeutenden Instituten verwendet wird. Ziel dieser Methodik ist es, eine hohe Widerstandsfähigkeit gegen Cyberangriffe (auch Cyber-Resilience genannt) zu erreichen. Dazu gehört neben der erwähnten Reaktions- beziehungsweise Response-Fähigkeit bei geglückten Angriffsversuchen auch eine sogenannte Recover-Komponente: Anhand definierter Maßnahmen und Prozesse kann damit eine schnelle Wiederherstellung des Normalzustandes gewährleistet werden.

Allerdings agiert das Sicherheitsteam, dem mehr als ein Dutzend hochqualifizierte Sicherheitsexperten angehören, nicht nur reaktiv – also erst dann, wenn ein hauseigenes System angegriffen wird. Vielmehr untersucht das Team proaktiv neu auftauchende Angriffsmuster mit analytischer Akribie, sobald es davon Kenntnis erhält. Wichtig ist dabei der Dialog mit Sicherheitsfachleuten anderer Organisationen innerhalb und außerhalb der genossenschaftlichen Finanzgruppe, darunter auch nationale und internationale Polizeibehörden. Dabei ahmt das Team sogar Methoden von Cyberkriminellen nach, um durch Scheinattacken bislang unentdeckte Sicherheitslücken zu erkennen und zu schließen – bevor ein echter Hacker sie für einen realen Angriff ausnutzen kann.

Angesichts einer ständig veränderten Bedrohungslage, die auch in Zukunft nichts von ihrer Dynamik verlieren wird, ist das Sicherheitsmanagement einem ebenso dynamischen Wandel unterworfen. Hohe Agilität im Sinne schneller Anpassung an neue Cybergefahren gilt daher zu Recht als ein wichtiges Effektivitätskriterium für jedes IT-Sicherheits-Framework, um auf neue Angriffsmuster zu reagieren. Die Cyber-Security-Strategie des genossenschaftlichen IT-Dienstleisters ist folglich nicht in Stein gemeißelt. Sie hat im Gegenteil eine hochflexible Struktur, die ihre Agilität und Adaptionsfähigkeit in neuen Gefahrensituationen schon mehrfach unter Beweis gestellt hat.

## Work in Progress: Security als Designprinzip

Die maximale Effektivität muss auch mit einem Maximum an Effizienz, insbesondere Kosteneffizienz verbunden werden. Deshalb hat das Thema Risikoorientierung eine hohe Bedeutung für die Sicherheitsstrategie. Dies schließt eine gründliche Risikoevaluierung der Geschäftsprozesse der Fiducia & GAD als auch der Banken ein. Denn nur so lässt sich der konkrete Schutzbedarf für die einzelnen Prozesse und Bankanwendungen ermitteln. Davon ausgehend folgt dann die Festlegung der individuell notwendigen Schutzmaßnahmen, die dem jeweiligen Schadenspotenzial bei einem möglichen Cyberangriff tatsächlich entsprechen. Diese konsequente

Prozessperspektive wird der Vorgehensweise der Täter gerecht: Denn diese attackieren schließlich nicht zwingend die IT, wenn beispielsweise der Prozess durch Social Engineering leichter auszuhebeln ist. Daher ist eine ganzheitliche Denkweise nötig, die über die IT und IT-Sicherheit hinausgeht und den gesamten Geschäftsprozess vor Augen hat.

Diese Denkweise wird nicht nur auf bestehende Geschäftsprozesse angewendet, sondern ist auch eine Leitlinie bei der Entwicklung neuer Anwendungen: Was auch immer der Entwicklerstab an Verbesserungen für das Bankverfahren oder eine Kundensoftware wie dem Onlinebanking plant: Informationssicherheit ist schon während der ersten Konzeptionsschritte ein unabdingbares Designkriterium. Auf diese Weise entsteht ein Anlaufgefüge, das sich durch ein hohes Maß an Cyber-Resilience auszeichnet.

**Vertrauensbildende Maßnahme: IT-Sicherheit im Dialog mit den Kunden**

Jenseits der Firewalls ihrer abgesicherten Rechenzentren und Zugangsnetzwerke sorgt der genossenschaftliche IT-Dienstleister durch eine Vielzahl unterschiedlicher Maßnahmen für den Schutz der Kunden von Volks- und Raiffeisenbanken vor kriminellen Cyberattacken. Für Überweisungen per Onlinebanking kommen beispielsweise ausschließlich Zwei-Kanal-Verfahren wie mobile TAN, Sm@rt-TAN-plus oder Sm@rt-TAN-optic zum Einsatz. Speziell für Firmenkunden gehört auch die Lösung Profi cash in Verbindung mit einem Chipkartenleser (dem Secoder) und einer passenden Chipkarte (der VR-Net-World Card) zum Security-Portfolio der Fiducia & GAD. Einen weitgehenden Schutz bietet auch der gehärtete Browser VR-Protect, weil er nur Banking-Webseiten darstellt.

Wie eingangs erwähnt, öffnen nicht nur technische Schwachstellen Tür und Tor für Cyberkriminelle, sondern auch Arglosigkeit und das mangelnde Wissen von Anwendern. Aufklärung ist daher laufend notwendig. Denn jede noch so ausgefeilte Präventionsmaßnahme bleibt im Zweifelsfall wirkungslos, wenn sich die Anwender keiner Gefahr bewusst sind. In puncto Aufklärung und Information leisten die Genossenschaftsbanken mit Unterstützung ihres IT-Dienstleisters bereits hervorragende Arbeit. Sie positionieren sich im Wettbewerb als moderner IT-Sicherheitspartner, wobei die offensive Darstellung der eigenen Security-Anstrengungen das Vertrauen der Kunden stärkt.

**Ein fortwährender Prozess der permanenten Optimierung**

Bei der Entwicklung neuer Anwendungen stehen alle IT-Dienstleister grundsätzlich vor zwei Herausforderungen: Zum einen die Lösung so aufzusetzen, dass eine komfortable und produktive Nutzung gewährleistet ist, aber gleichzeitig auch die Sicherheitsrisiken, denen die mobilen Devices ausgesetzt sind, minimiert werden. Dabei sollte aber nicht verschwiegen werden, dass es hundertprozentige Sicherheit niemals geben kann.

Cyber-Security ist kein endgültig erreichbarer Zustand, sondern ein fortwährender Prozess der permanenten Optimierung aller bisherigen Schutz- und Abwehrmaßnahmen. Obwohl es also keine hundertprozentige Sicherheit geben kann, gibt es dennoch den hundertprozentigen Einsatz dafür. Und mit dieser Anstrengung vermehren die Volks- und Raiffeisenbanken eines der wertvollsten immateriellen Assets – nämlich das gewachsene Kundenvertrauen.