Lochkarte trifft auf App

Banken Finanzkonzerne leiden unter einer Serie von IT-Pannen und Cyberattacken. Schützen müssen sich die Verbraucher selbst.

Der Twitter-Nutzer Sir Rant-A-Lot (@Revolvermann) teilt sein halbes Leben über den Kurznachrichtendienst mit, so auch sein Entsetzen am vergangenen Montag, als er sich auf seinem Comdirect-Konto einloggen wollte. „HOLY SHIT! Bei jedem neuen Login lande ich in einem anderen @comdirect account ... aber nicht in meinem." Auch weitere Nutzer warnten: „Sehe gerade Kontostände fremder Leute."

Der Grund für die Aufregung war offensichtlich: Seit Stunden landeten die Kunden auf den Konten fremder Nutzer, wenn sie sich online einloggten. Sie konnten dabei Gehaltseingänge sehen, Miet- und Kreditzahlungen, Wertpapierbuchungen und etliche andere Daten wildfremder Menschen, die so mancher Bankkunde nicht einmal seinem Ehepartner anvertrauen würde.

Es ist die wahrscheinlich peinlichste Datenpanne der jüngsten Zeit bei Banken: So gab es bei der Deutschen Bank kürzlich Millionen Doppelbuchungen, die Konten teils tief ins Minus rissen. Im Herbst konnten Sparkassenkunden aufgrund einer Fehlfunktion im Netzwerk in halb Deutschland kein Geld mehr abheben. Und im Juni kamen einer Fintech-Firma für Crowdfunding durch einen Hackerangriff 53 Millionen Dollar abhanden.

Je mehr sich das Geldgeschäft ins Internet und auf das Smartphone verlagert, desto gefährlicher scheint es für die Verbraucher zu werden. „In den letzten Jahren ist Onlinebanking immer mehr Ziel von Kriminellen geworden", sagt Konrad Rieck, Professor für Informatik an der Technischen Universität Braunschweig. Aber auch verheerende Pannen ohne Fremdeinwirkung nehmen zu.

Selbst hochrangige Banker erwarten, dass es in den nächsten Jahren häufiger zu Zwischenfällen kommt. Denn die IT-Systeme deutscher Banken stammen teils gefühlt noch aus der Lochkartenära des Computerzeitalters, es sind Programmiersprachen im Einsatz, die heute kaum noch jemand beherrscht, die Systeme gleichen großen Flickenteppichen.

Die Banken aber sind getrieben, müssen sich dem technischen Fortschritt anpassen, der eigentlich zu schnell für sie ist. Sie gehen deshalb mit technisch unausgereiften Produkten auf den Markt, die erst dann weiterentwickelt werden.

„Der Druck auf die IT-Abteilungen ist enorm, sie müssen verschärfte regulatorische Vorschriften in ihren Systemen umsetzen und gleichzeitig ihren Kunden ständig neue Features bieten", sagt der IT-Experte und Bankenberater Bernd Richter. Verbraucher wollen Geld per Smartphone überweisen, Kontostände jederzeit abfragen, selbst Kreditanträge oder Geldanlagen mobil erledigen. Wer das nicht schnell bietet, droht den Kampf um das Bankgeschäft der Zukunft zu verlieren.

Früher dauerte es bis zu 18 Monate, bis ein Bankprodukt entwickelt, die Umsetzbarkeit von der IT geprüft, das Angebot nachgebessert und schließlich auf den Markt gebracht wurde. Die Banken sammelten Neuerungen und spielten nur ein bis zweimal im Jahr neue Software auf, die dann aber umfassend getestet war.

Heute werden Produkte binnen zwei Wochen entwickelt und mehrmals wöchentlich Software-Updates durchgeführt. Die niederländische Großbank ING etwa hat ihre Organisation komplett umgekrempelt. Hunderte Programmierer arbeiten jetzt in kleinen Teams direkt mit den Produktentwicklern zusammen, um schneller mit neuen Angeboten am Markt zu sein.

Mit der Häufigkeit der Updates steigt das Risiko von Fehlern. Banken verfolgen außerdem in der Regel eine Strategie der zwei Geschwindigkeiten: Sie experimentieren einerseits mit schnell entwickelter, neuer IT, arbeiten aber im Kern mit den alten Systemen weiter – was an den Schnittstellen zusätzlich Fehler befördert.

Doch die internen Schwachstellen sind nur die eine Front, an der die Finanzbranche kämpft. Denn gleichzeitig werden die Verbrecher, die Banken und ihre Kunden angreifen, immer professioneller.

Wie jede andere Industrie setzt auch die Hacking-Branche mittlerweile auf Arbeitsteilung und effizienten Einsatz von Ressourcen. „Spezialisten hacken massenweise schlecht geschützte Privat-PC und vermieten diese im Internet an andere Kriminelle, für 5, 10 oder 20 Dollar das Stück", sagt IT-Professor Rieck.

Ein unangreifbares System zum Schutz vor solchen Angriffen gibt es nicht. Egal, welches Gerät und welche Identifizierung genutzt wird: Jedes Sicherheitssystem ist bislang irgendwann überwunden worden. Weder TAN und PIN noch Identifizierung per Fingerabdruck bieten 100-prozentigen Schutz.

Die gute Nachricht für Verbraucher ist: Wer regelmäßig Virenschutz, Betriebssystem und Anwendungsprogramme auf den neuesten Stand bringt, hat gute Chancen, verschont zu werden. „Viele Hacker konzentrieren sich auf die leicht zu knackenden PC, weil sie damit am Ende einfach mehr Geld machen", sagt Rieck.

Die Aufsichtsbehörden haben die Cybersicherheit zwar längst als große neue Schwachstelle bei den Banken erkannt. Die EZB hat die Kontrolle von IT-Risiken dieses Jahr zu einer Schwerpunktaufgabe gemacht und begonnen, eine Datenbank aufzubauen, an die Banken der Eurozone systematisch größere Zwischenfälle in ihren Systemen melden.

Doch erst im kommenden Jahr werden alle 130 von der EZB beaufsichtigten Banken an das Frühwarnsystem angeschlossen sein. Den Aufsehern fehlt es wie den Banken an gutem Personal, um mit den Cyberherausforderungen fertig zu werden.

Sanktioniert werden IT-Pannen von den Behörden bislang kaum, auch im Fall der Comdirect gilt eine Strafe wegen des blamablen Vorfalls als unwahrscheinlich. Experten halten das für fahrlässig. „Die Aufsichtsbehörden sollten klare Richtlinien für den Umgang mit Cyberrisiken, zur IT-Entwicklung und für Tests vorgeben und Manager persönlich für fehlerhafte Releases haftbar machen", findet Richter.

Martin Hesse, Anne Seith
Mail: martin.hesse@spiegel.de, anne.seith@spiegel.de