DAS DHAKA-KOMPLOTT

Statt Kunden greifen Hacker inzwischen Banken an, sogar Zentralbanken. Sie erbeuten Millionen, zuletzt bei der Bank of Bangladesh. Behörden und Staaten sind hilflos

TEXT: JENS BRAMBUSCH
ILLUSTRATION: JAN STEINS

EIN BÜRO IRGENDWO AUF DER WELT. MONATELANG HABEN HACKER DEN GRÖSSTEN BANKRAUB DER GESCHICHTE VORBEREITET. SIE WOLLEN DIE ZENTRALBANK VON BANGLADESCH AUSRAUBEN. ES IST FREITAG, DER 5. FEBRUAR.

DIE HACKER WEISEN TRANSAKTIONEN IN HÖHE VON 951 MIO. DOLLAR AN. NIEMAND AHNT ETWAS. SWIFT GILT ALS ABSOLUT SICHER.

DAZU WOLLEN SIE DAS SWIFT-NETZWERK NUTZEN. ÜBER SWIFT MIT SITZ IN BELGIEN LAUFEN ÜBERWEISUNGEN ZWISCHEN 11 000 BANKEN WELTWEIT.

Der größte Bankraub der Welt scheitert am Ende an einem Tippfehler. Ein „a“ lässt die Hacker auffliegen. Doch es reicht für 81 Mio. Dollar.

Es ist Freitag, der 5. Februar 2016. Islamischer Feiertag. In Dhaka, der Hauptstadt von Bangladesch, ruht die Arbeit. Auch in dem grauen Betonklotz der Motijheel Commercial Area, ganz in der Nähe des Zentralbahnhofs des 17-Millionen-Molochs. Hier hat die Zentralbank ihren Sitz. Und so bekommt niemand mit, dass die Computer der Bank an diesem Tag wie von Geisterhand eine Transaktion nach der nächsten ausführen. 35 insgesamt. Immer hohe Millionenbeträge. Insgesamt 951 Mio. Dollar, eine knappe Milliarde.

Über das Netzwerk von Swift, der Society for Worldwide Financial Telecommunication mit Sitz in Belgien, wird die US-Notenbank Fed von Dhaka aus angewiesen, das Geld auf die Philippinen und nach Sri Lanka zu transferieren. Swift ist eine Art Genossenschaft der Finanzbranche. Sie regelt den Transaktions- und Nachrichtenverkehr von mehr als 11 000 Banken, Brokern und Börsen und gilt als absolut sicher. Jeden Tag werden über Swift mehr als 25 Millionen Geschäfte abgewickelt. Bei der Fed in New York wiederum lagern mehr als 250 staatsnahe Geldinstitute ihre Devisenreserven. So auch die Bank of Bangladesh: 27 Mrd. Dollar. Auf einen Teil davon haben es die Täter abgesehen.

Mit den ersten fünf Transaktionen fließen 81 Mio. Dollar auf Konten bei der philippinischen Bank RCBC, weitere 20 Mio. Dollar nach Sri Lanka. Alles läuft routinemäßig.

Doch plötzlich schlägt das System Alarm: Geldwäscheverdacht. Einer von vielen Parametern, die automatisch überprüft werden, passt nicht. Das muss noch nicht viel heißen, aber jetzt schaut sich ein Mitarbeiter der Fed den Vorgang genauer an. Und entdeckt einen winzigen Fehler. Der Empfänger der Überweisung nach Sri Lanka, eine kürzlich gegründete NGO, wird als „Fandation“ angegeben statt als „Foundation“. Ein Rechtschreibfehler, der stutzig macht. Das Misstrauen ist geweckt.

Jetzt bemerkt der US-Banker auch die ungewöhnlich hohe Anzahl der Transaktionen, die aus Dhaka angewiesen werden. Er will sich rückversichern, sucht den Kontakt zu seinen Kollegen in Bangladesch. Doch wegen des Feiertags erreicht er niemanden. Das kostet Zeit. Was also tun? Das Swift-System gilt als sicher. Noch nie ist es gehackt worden.

Trotzdem versendet die Fed an Dhaka und die Empfängerbanken eine sogenannte „MT 103“-Nachricht. Der Code besagt: Das Geld blocken! Vorsichtshalber. Doch als die Warnung auf den Philippinen eingeht, ist es schon zu spät. Zumindest für die ersten 81 Mio. Dollar. Die sind bereits von den Konten verschwunden. Die weiteren Überweisungen werden eingefroren – und so der größte Bankraub der Geschichte vereitelt.

EINE NEUE DIMENSION

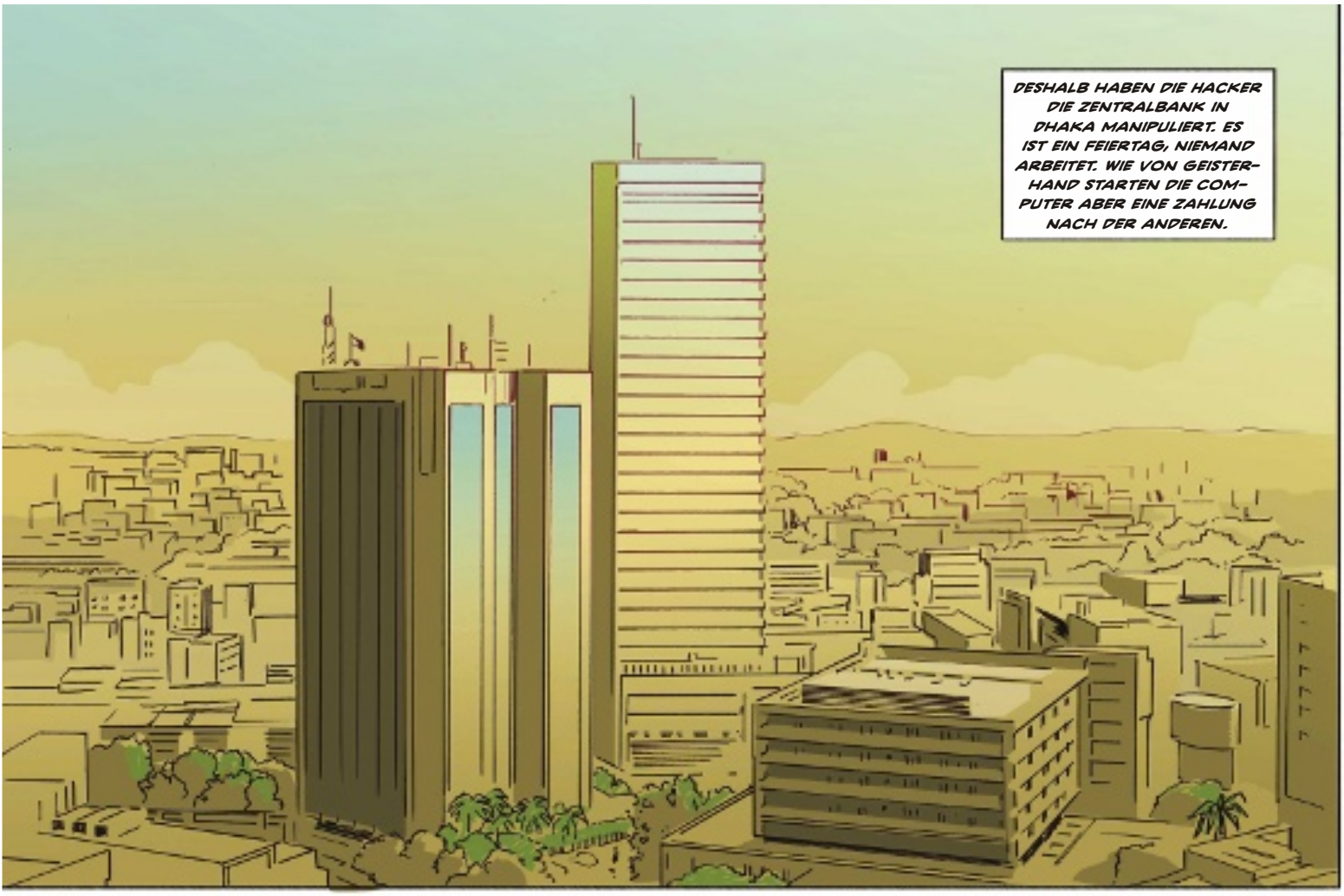
Dass Hacker versuchen, Geldtransfers zu manipulieren, ist nicht neu. Bislang sahen sie es aber meist auf das schwächste Glied in der Kette ab – den Endverbraucher. Ein leichtes Opfer für halbwegs erprobte Hacker. Doch auch die Beute ist gering. Der Cyberangriff auf die Zentralbank von Bangladesch in diesem Frühjahr markiert dagegen eine ganz neue Dimension.

Gottfried Leibbrandt spricht von einem „Wendepunkt“ in der Geschichte des Cybercrime. Der Niederländer ist Chef von Swift. „Offenbar handelt es sich um einen Teil einer größer angelegten und sehr anpassungsfähigen Kampagne“, sagt er. Und das besorgt ihn. Nach Wochen der Ermittlungen durch Behörden und IT-Forensiker scheint zwar festzustehen, dass die Täter nicht Swift direkt, sondern die Zentralbank in Dhaka gehackt haben. Dennoch wurde das Netzwerk als Werkzeug missbraucht. Und nicht nur einmal.

Bereits im Januar 2015 wurde die Banco del Austro in Ecuador nach dem gleichen Muster um 12 Mio. Dollar erleichtert. Ende des vergangenen Jahres bemerkte die vietnamesische Tien Phong Bank eine gefakte Überweisung über eine Million Dollar in letzter Minute. Auch hier hatten Cyberkriminelle Swift-Überweisungen manipuliert. Es habe mehrere Vorfälle gegeben, bei denen betrügerische Nachrichten über das Netzwerk gesendet wurden, bestätigt Swift, ohne Details zu nennen. Von bis zu zwölf Fällen ist die Rede, der letzte wurde erst vor wenigen Wochen aus Vietnam gemeldet.

Es gehe nicht mehr nur um die Gefahr eines Reputationsverlustes für Banken, mahnt Leibbrandt. „Es geht um die Existenz all derer, die darin versagt haben, sich vernünftig zu schützen.“ Er meint die Banken.

Die Europäische Zentralbank ist alarmiert. Noch im Februar rief sie eine Meldestelle für Cyberangriffe ins Leben. 18 der 130 Institute unter ihrer Aufsicht nehmen an dem Pilotprojekt teil. „Wir wollen eine Datenbank für Cyberstörfälle schaffen. Sie soll uns als Frühwarn- und Analysesystem dienen“, begründet François-Louis Michaud, stellvertretender Generaldirektor bei der EZB-Bankenaufsicht, den Schritt. Bereits seit 2011 hat die deutsche Bankenaufsicht Bafin ein eigenes Referat, das sich mit den IT-Infrastrukturen und der Cybersicherheit befasst. →



DIE ANWEISUNGEN AUS DHAKA LAUFEN ÜBER SWIFT BEI DER FED IN NEW YORK EIN. DORT LAGERT BANGLADESCH SEINE DEVISENRESERVEN. VON HIER SOLLEN DIE MILLIONEN TRANSFERIERT WERDEN.

ZUR SICHERHEIT VERSUCHT EIN BANKER DER FED, DIE KOLLEGEN IN DHAKA ZU ERREICHEN. ERFOLGLOS.

Aber reicht das? Sicherheitsexperten warnen: Im zweiten Halbjahr 2015 soll die Zahl der Cyberangriffe auf Banken im Vergleich zum ersten Halbjahr um 300 Prozent gestiegen sein. Das berichtet Fire Eye, ein weltweit tätiges, börsennotiertes US-Unternehmen, das sich auf Cybersicherheit spezialisiert hat. Fire Eye analysiert auch den Fall in Dhaka im Auftrag der Zentralbank.

Es ist ein Wettlauf zwischen Hackern und Banken, den die Geldhäuser nur allzu oft verlieren. Immer neue Schwachstellen entdecken die Angreifer und verschaffen sich Zugang zu den Finanzströmen dieser Welt. So infiltrierten Kriminelle im Jahr 2013 einen indischen IT-Dienstleister und manipulierten die Limits von Konten bei zwei arabischen Banken. Binnen Stunden wurden in mehreren Ländern rund 45 Mio. Dollar abgehoben. Im Sommer 2014 griffen Hacker die US-Bank JP Morgan Chase an und installierten eine Schadsoftware. Zwei Monate blieb die Attacke unentdeckt. Das Institut musste zugeben, dass die Diebe Daten von über 76 Millionen Privat- und sieben Millionen Firmenkunden gestohlen hatten. Was mit den Daten geschehen ist, ist unbekannt. Aber der Fall zeigt: Nicht nur Exotenbanken sind anfällig für Cyberangriffe. Auch die größten Institute der Welt sind nicht ausreichend geschützt.

KNAPPE MILLIARDE ERBEUTET

Vergangenes Jahr wurden Angriffe auf die türkischen Banken Isbank, Garanti und Ziraat Bank bekannt. Zudem wurden drei griechische Großbanken und die Zentralbank in Athen attackiert. Ziel waren auch die EZB, mehrere britische Banken, die Bank of China und die Bank of East Asia. Die russische IT-Sicherheitsfirma Kaspersky spricht von einem Schaden in Höhe von rund einer Milliarde Dollar, die Cyberkriminelle in zwei Jahren von weltweit etwa 100 Instituten ergaunert hätten – allein mittels eines Schadprogramms namens „Carbanak".

Die Hacker, die Banken angreifen, sind keine pubertierenden Nerds mit Hornbrille und Pickeln, wie man es aus Blockbustern kennt. Es sind hochprofessionelle Kriminelle. Manche Experten vermuten deshalb auch, dass Staaten wie Nordkorea oder China hinter den Attacken stecken könnten. Bewiesen ist das nicht. Auch weil die Täter es verstehen, ihre Spuren bis zur Unkenntlichkeit zu verwischen. Im Fall der Zentralbank in Dhaka wurde die Schadsoftware nach der Aktion bis zu sechsmal überschrieben.

„Die Täter wussten, dass die Büros in Dhaka am Freitag und Samstag geschlossen sind und dass in New York niemand am Wochenende arbeitet", sagt Subhankar Saha, ein Manager der Zentralbank in Dhaka. Die Gauner hätten darauf vertraut, dass es keine direkte Kommunikation an dem Wochenende gebe. Und genau so war es.

Panik brach erst aus, als am Montag danach die Zentralbank von Bangladesch die „MT 103“-Nachricht aus New York entdeckte. Sofort schickte Dhaka eine Mail über das Swift-System an die Philippinen: „Wir möchten Sie informieren, dass es sich um eine zweifelhafte Transaktion handeln könnte. Sie sind angehalten, die Auszahlung zu stoppen. Sollten Sie bereits ausgezahlt haben, frieren Sie bitte das Konto des Empfängers ein. Wir glauben, dass die Überweisung gegen die Geldwäscherichtlinie verstößt.“ Keine Antwort.

IMMER KOMPLEXERE ANGRIFFE

Die Kontaktaufnahme mit den Philippinen scheitert aus einem einfachen Grund. Jetzt ist dort Feiertag. Auch wenn nur etwa 1,5 Prozent der Philippiner Chinesen sind, ist das chinesische Neujahrsfest gesetzlicher Feiertag in dem Inselstaat.

Am Dienstag jagt Dhaka die nächste Nachricht nach Manila: „Top urgent!“ ist sie überschrieben. Äußerst dringend. „Es handelt sich um eine betrügerische Transaktion. Es gab einen unautorisierten Eingriff in unser Swift-System. Frieren Sie das Geld ein und senden es zurück an die Kontonummer 21 08 31 90.“

Als jemand auf den Philippinen auf die Nachrichten reagiert, hatten die Täter bereits vier Tage Zeit, das Geld in Ruhe weiterzuleiten und ihre Spuren zu verwischen. Sie hatten sich das perfekte Wochenende ausgesucht.

Harald Reisinger spricht von hochprofessionellen Hackergruppen, die auf das Eindringen in die IT von Banken spezialisiert sind. „Die Täter investieren viel Zeit und Ressourcen in die Angriffsvorbereitung und gestalten immer komplexere Angriffe. Die IT-Security-Teams von Banken werden in ein immer härteres Wettrennen verwickelt, welches nur die Fittesten gewinnen“, sagt der Geschäftsführer von Radar Services, einem Anbieter von IT-Security.

Wie fit die deutschen Banken sind, lässt sich nur schwer sagen. Immer noch gibt es keine Meldepflicht für Cyberattacken. Und die Institute geben nur ungern zu, wenn sie Opfer eines Angriffs geworden sind. Sie befürchten einen herben Imageschaden. Die Bundesbank forderte erst kürzlich die Kreditinstitute auf, „ihre IT- und Cyberrisiken genauso sorgsam zu managen wie die traditionellen Risiken des Bankgeschäfts.“

Vorfälle wie die Software-Panne der Deutschen Bank Anfang Juni, als 60 000 Kunden ihre EC-Karte nicht mehr nutzen konnten und diverse Abbuchungen doppelt erfasst wurden, lassen Schlimmes befürchten. Ähnliches war 2015 bereits vielen Sparkassenkunden widerfahren.

Schon kurz nach seinem Amtsantritt hatte Deutsche-Bank-Chef John Cryan von „lausigen Systemen“, „ineffektiven Prozessen“ und einer „veralteten IT“ gesprochen. 35 Prozent der verwendeten Hardware bei der Deutschen Bank würde sich dem Ende ihres Lebenszyklus nähern oder hätte es schon überschritten. Manche Programmiersprachen seien so alt, dass sie kaum noch einer beherrsche. Und 80 Prozent der 4 400 verwendeten Anwendungen würden von externen Anbietern bereitgestellt. Klare Worte. Und die Deutsche Bank scheint kein Einzelfall zu sein.

„ES GEHT UM DIE EXISTENZ ALL DERER, DIE VERSAGT HABEN“

GOTTFRIED LEIBBRANDT
Vorstandsvorsitzender von Swift

Die Beratungsgesellschaft Bain & Company hat vergangenen Herbst IT-Verantwortliche von Banken auf der ganzen Welt befragt. Das Ergebnis ist erschreckend: Mit dem rasanten Fortschritt könnten nur die wenigsten Banken mithalten, zahlreiche IT-Manager kämpften aufgrund knapper Budgets mit veralteten Systemen und Anwendungen, so das Fazit der Studie.

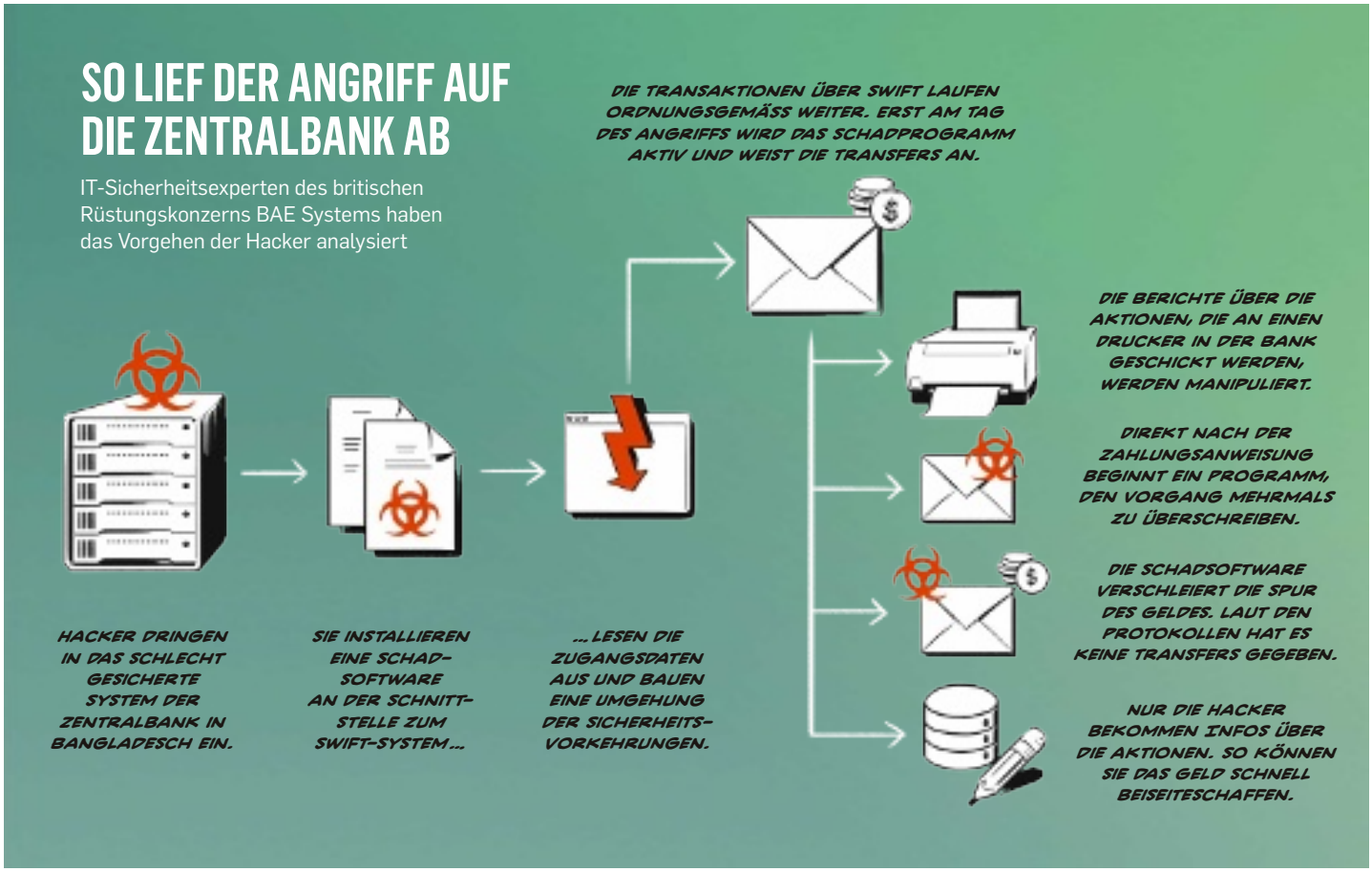
„Die Motivation von Hackern rund um den Globus ist dagegen extrem hoch“, sagt IT-Experte Reisinger. „Ohne eine allumfassende Überwachung der gesamten IT-Landschaft in Echtzeit an 24 Stunden am Tag und sieben Tagen in der Woche sollte jeder IT-Sicherheitsverantwortliche einer Bank schlaflose Nächte haben.“

ROUTER FÜR ZEHN DOLLAR

Wie professionell die Täter ihre digitalen Raubzüge planen, zeigt der Fall aus Bangladesch. Bereits am 15. Mai 2015, ein Dreivierteljahr vor dem großen Coup, werden bei der philippinischen Bank RCBC vier Konten eröffnet, mit jeweils 500 Dollar Einlage.

Die Namen der Privatkunden lauten Enrico Teodoro Vasquez, Alfred Santos Vergara, Michael Francisco Cruz und Jessie Christopher Lagrosas. Wahrscheinlich gibt es die Männer gar nicht. Die Bank schiebt der Filialleiterin die Schuld zu, sie habe die Identitäten nicht überprüft. Die Filialleiterin kontert, das Management habe angeordnet, die Konten einzurichten.

Wann das Netzwerk der Zentralbank in Dhaka gekapert wurde und wie, ist noch nicht bekannt. Allzu schwer hat die Bank es den Tätern aber nicht gemacht. Nicht →



einmal eine Firewall soll das Institut gehabt haben, berichten Ermittler. Auch seien Router für 10 Dollar das Stück eingesetzt worden, die selbst für den privaten Gebrauch als unsicher gelten. Zudem war das schlecht geschützte Firmennetzwerk nicht von dem Swift-Netzwerk getrennt – wie eigentlich vorgeschrieben.

Der Zutritt zur Bank war ein Kinderspiel, alles Weitere eine Meisterleistung. Selbst die Experten von Swift zollen Respekt: „Die Angreifer zeigen eindeutig ein tiefes Wissen von spezifischen operativen Vorgängen innerhalb der betroffenen Banken“, heißt es in einer Erklärung. Es handele sich um „Wissen, das von böswilligen Insidern oder von Cyberangriffen stammen könnte oder aus einer Kombination von beidem“.

Die Hacker haben nach Informationen des Rüstungskonzerns BAE Systems einen Trojaner in das Netzwerk der Zentralbank eingeschleust, der ihnen den Zugriff auf die Swift-Transaktionen und den normalen Geschäftsverkehr der Bank ermöglichte. Über Monate hatten sie so die Systeme überwacht, Informationen abgezogen und analysiert.

DRUCKER MANIPULIERT

Sie erbeuteten die Zugangsdaten für den internationalen Zahlungsverkehr, manipulierten lokale Dateien, verschleierten ihre Spuren und umgingen die Sicherheitsfunktionen. Swift sendet beispielsweise nach jeder Transaktion Daten an einen lokalen Drucker. Die wurden abgefangen und durch unverdächtige Versionen ersetzt. Wer die Zahlungsströme überprüfte, bekam nur die regulären Überweisungen angezeigt. Die manipulierten Transaktionen wurden von der Liste gelöscht. Ohne den Rechtschreibfehler hätte wahrscheinlich auch am Montag kein Mitarbeiter in Dhaka den Raubzug bemerkt.

Die 81 Mio. Dollar, die auf die Philippinen transferiert wurden, blieben dort nur wenige Minuten. Einige Stationen konnten die Ermittler nachverfolgen, ehe das Vermögen auf vielen verschiedenen Wegen in Südostasien versickerte. Zunächst wurde das Geld an den philippinischen Geldüberweisungsdienst Philrem weitergeleitet, eine Art asiatisches Western Union. Der tauschte die Dollars in philippinische Pesos. Die Chefin von Philrem steht deshalb nun wegen Geldwäsche vor Gericht.

Von dort ging das Geld zurück auf ein Konto bei der RCBC-Bank, allerdings auf das eines bekannten philippinischen Geschäftsmanns. Der behauptet, sein Konto sei gehackt und missbraucht worden – was durchaus denkbar ist. Von dessen Konto wiederum wurde das Geld an verschiedene Kasinos transferiert, dort in Jetons ausgezahlt und somit gewaschen. Von dort soll das Geld in kleinen Tranchen über Südostasien verteilt worden sein.

Die Millionen sind jetzt verschwunden. Und von den Tätern gibt es keine Spur. ◇