Felix Hufeld

Cyberrisiken – ein Thema für deutsche Banken?

Als ich mein neues Amt als Präsident der BaFin im März übernahm, wurde mir schnell bewusst, dass die BaFin als Allfinanzaufsicht auch Verantwortung für die Cybersicherheit der beaufsichtigten Unternehmen trägt. Nahezu täglich fand ich Meldungen über Hackingaktivitäten, die insbesondere auch den Finanzsektor zum Ziel hatten. Cyberrisiken sind ohne Zweifel eine Bedrohung für jedermann. Sind diese Risiken aber auch eine Bedrohung für deutsche Banken, die bislang im Vergleich zu anderen Staaten noch relativ unbehelligt dastehen? Sind ihre IT-Systeme so widerstandsfähig, dass sie gelassen in die Zukunft schauen können? Diesen zentralen Fragen wird im Folgenden nachgespürt.

Risiken und Chancen des Cyberraums

Zum Auftakt möchte ich etwas zum Begriff Cyberrisiken sagen und dabei eine vorsichtige Einschätzung zur Cyberrisikolage wagen. Diese Einschätzung möchte ich anschließend mit drei in der Finanzwelt bekannten Beispielen zur Cyberkriminalität untermauern. Last, but not least will ich die zukünftigen und durchaus positiven Aspekte des Cyberraums nicht ausblenden, nennen wir sie Cyberchancen.

Worüber reden wir, wenn wir den Begriff Cyberrisiko verwenden? Die Wortkomposition Cyberrisiko bringt zum Ausdruck, dass Ereignisse aus dem Cyberraum Schäden zunächst in IT-Systemen verursachen können, mit negativen Konsequenzen für die Geschäftsabläufe und letztlich die Kunden von Finanzinstituten. Das Internet ermöglicht Menschen, unberechtigt auf IT-Systeme anderer zuzugreifen und diese zu schädigen. Der Schaden kann darin liegen, dass die IT-Systeme nicht mehr verfügbar sind oder dass gespeicherte Daten gestohlen oder verfälscht werden.

Mit dem Siegeszug des Internets wächst bei den Nutzern auch das Bewusstsein der damit verbundenen Gefahren. Immer mehr Menschen nutzen immer häufiger und immer professioneller die Möglichkeiten des Internets, um andere zu schädigen. Die European Union Agency for Network and Information Security (ENISA) hat für das Jahr 2014 fünfzehn Top-Bedrohungsvektoren ausgemacht. Diese reichen von Phishing, Würmern, Trojanern über webbasierte Attacken, Botnetze, Identitätsdiebstahl bis hin zur Spionage. ENISA hat festgestellt, dass zwölf dieser Bedrohungsvektoren im Vergleich zum Vorjahr zugenommen haben.

Wer sind die Menschen, die sich hinter diesen Bedrohungsvektoren verbergen? Das Spektrum umfasst einzelne Hacker, Aktivisten, aber auch international organisierte Cybergangs und staatliche Institutionen wie Nachrichtendienste. Es überrascht nicht, dass gerade der Finanzsektor besonders im Fokus der Angreifer steht, da hier das schnelle Geld winkt. Dies möchte ich mit einigen Fällen, die durch die Presse gegangen sind, illustrieren.

DDoS-Angriffe gegen Banken

Starten möchte ich mit fast schon Alltäglichem, den Distributed Denial of Service (DDoS)-Angriffen. Bei einem DDoS-Angriff werden IT-Systeme absichtlich überlastet, um die bereitgestellten Dienste wie zum Beispiel Online-Banking in ihrer Funktionsfähigkeit zu stören. Eine solche DDoS-Attacke geschah an Heilig Abend vergangenen Jahres in Finnland. Betroffen war die größte Finnische Bank OP Pohjola financial services group. Der Angriff dauerte sechs Tage. Das Online-Banking und die Geldautomaten fielen aus. Bitter für eine Bank, die rund vier Millionen Kunden zählt in einem Land, das etwa 5,4 Millionen Einwohner hat. DDoS-Angriffe gegen Banken finden vor allem in den USA statt, sie können mehrere Wochen andauern. Aber auch deutsche Institute waren bereits betroffen.

Es ist zu befürchten, dass DDoS-Angriffe weiter zunehmen werden. Es soll im „Darknet" spezialisierte Dienstleister geben, die entsprechende Dienste bereits ab vier Dollar anbieten. Botnetze, die DDoS-Attacken ermöglichen, können sehr umfangreich sein. 2012 wurde ein Botnetz mit dem Namen Zeus ausgehoben, das 13 Millionen Rechner verteilt über mehrere Staaten umfasste. Das heißt, auf 13 Millionen Rechner wurde unbemerkt entsprechende Malware aufgespielt und stand für DDoS-Angriffe zur Verfügung. Das Risiko, solchen Angriffen ausgesetzt zu sein, ist also

Felix Hufeld, Präsident, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Bonn und Frankfurt am Main

Heftige Cyberattacken können im Zeitalter der Digitalisierung gravierende Auswirkungen haben und selbst die staatliche Ordnung empfindlich stören. In Extremfällen können sie die öffentliche Verwaltung und Versorgung bedrohen, wirtschaftliche Abläufe aus den gewohnten Bahnen bringen und wichtige Schutzmechanismen außer Kraft setzen. Vor diesem Hintergrund muss sich auch die Finanzdienstleistungsaufsicht mit den Szenarien rund um die Cybersicherheit beschäftigen. Der Autor schärft das Bewusstsein der Branche mit drei markanten Praxisbeispielen und mahnt die betroffenen Unternehmen, die Sicherheitsstandards ihrer IT-Infrastruktur auf ein angemessenes Niveau zu bringen. Allerdings will er auch die Chancen einer digitalisierten Welt keineswegs ausblenden und plädiert für eine konstruktive Offenheit gegenüber den Ideen neuer Fintech-Unternehmen. (Red.)

sehr ernst zu nehmen. Die Bankenaufsicht geht davon aus, dass die Institute dieses hohe Cyberrisiko entsprechend den Anforderungen nach KWG (§ 25a Abs. 1 KWG) in ihr Risikomanagement einbeziehen und sich auf diese Angriffe vorbereiten.

Das zweite Beispiel betrifft einen modernen, international organisierten Cyberdiebstahl, der eine arabische Bank[1)] getroffen hat. Im Februar 2013 hoben Kriminelle innerhalb von zehn Stunden in 36000 Transaktionen zirka 40 Millionen Dollar weltweit in 24 Staaten[2)] an Geldautomaten ab. Auch in Deutschland. Wie konnte das geschehen? Zunächst drangen die Kriminellen in das IT-System eines Kreditkartenabwicklers ein und erhöhten dort die Verfügungslimite von zwölf Kreditkartenkonten. Dann kopierten sie die Magnetstreifenkarten und verteilten diese weltweit an ihre Handlanger. In einer konzertierten Aktion hoben anschließend hunderte von Helfern Geld ab.

International organisierter Cyberdiebstahl

Was sind die Lehren aus diesem Cyberdiebstahl? Erstens: Sicherheitsstandards sind nicht nur von Instituten, sondern auch von ihren Dienstleistern konsequent einzuhalten. Banken wiederum haben die Einhaltung der Anforderungen bei ihren IT-Dienstleistern konsequent zu überwachen. Das erwartet auch die BaFin. Zweitens: Cyberrisiken werden nicht nur von Einzelnen oder kleinen Gruppen von Hackern verursacht. Wir haben es teils mit arbeitsteilig organisierten Strukturen zu tun, die bis zu 50000 Kriminelle umfassen sollen. Drittens: Magnetstreifenkarten sind unsicher.

Beim letzten Beispiel soll sich der verursachte Schaden über einen Zeitraum von zwei Jahren auf insgesamt eine Milliarde Dollar summiert haben. Es geht um die Carbanak-Gang, die hochprofessionell agierte. Seit 2013 soll diese Gang laut Kaspersky bis zu 100 Banken in nahezu 30 Staaten, darunter auch Deutschland, geschädigt haben. Zunächst erhielten Mitarbeiter dieser Banken eine Mitteilung per Mail. Die Mail war so Vertrauen einflößend gestaltet, dass die Empfänger eine angehängte Worddatei öffneten, wodurch im Hintergrund das Herunterladen einer angehängten Malware auf den PC des Mitarbeiters aktiviert wurde. Die Hacker installierten eine Hintertür und erlangten die Kontrolle über den PC. Von diesem PC verbreiteten sie die Malware auf die PCs anderer Mitarbeiter.

Das eigentliche Ziel war der PC des Administrators. Nachdem auch dieser übernommen war, schalteten sich die Hacker auf die PCs der Mitarbeiter der Bank und studierten zunächst über längere Zeit deren Arbeitsweise, insbesondere den Umgang mit den Zahlungssystemen. Dann agierten sie wie Bankmitarbeiter. Sie veranlassten beispielsweise Swift-Überweisungen von bestehenden Konten oder legten neue Konten mit Guthaben an, von denen sie wiederum Überweisungen tätigten.

Ein alarmierendes Niveau

Die Vorgehensweise der Carbanak-Gang wird im Fachjargon als Advanced Persistent Threat (APT) bezeichnet, was für einen komplexen, zielgerichteten und effektiven Angriff steht, bei dem mehrere Angriffsvektoren verknüpft werden. Bezeichnend ist, dass die Kriminellen zunächst in Ruhe ihre Opfer studierten und damit – bis zu vier Monate lang – Bankwissen aufbauten, bevor sie mit ihren Transaktionen loslegten. Diese waren im IT-System nicht als schädlich erkennbar, da die Täter die Berechtigung der Bankmitarbeiter auf den vorgesehenen Anwendungen nutzten und die Bankprozesse einhielten. Ein perfektes Verbrechen also? Nicht ganz. Die Carbanak-Gang flog auf, als ein manipulierter Geldautomat „verrückt" spielte und über diese Anomalität die Untersuchung des Falles ausgelöst worden war.

Die Qualität der Cyberrisiken im Finanzsektor hat ein alarmierendes Niveau erreicht. Ob und welche technischen Gegenmaßnahmen im Einzelnen möglich sind, bleibt den Spezialisten überlassen. Wichtig ist jedenfalls, dass wir uns der Risiken bewusst sind, die mit Cyberangriffen verbunden sind. Banken müssen aus diesen Angriffsmustern lernen und ihre Gegenmaßnahmen entsprechend ausrichten. Und sollten sie betroffen sein, gilt es, eng mit den zuständigen Strafverfolgungsbehörden (Bundeskriminalamt und Landeskriminalämter) und dem Bundesamt für Sicherheit in der Informationstechnik zusammenzuarbeiten.

Auch die Aufsicht lernt aus dieser Entwicklung. So wurde inzwischen bei der Europäischen Bankenaufsichtsbehörde (EBA) eine Task-Force zu IT-Risiken gegründet, die neue Anforderungen an die IT-Organisation der Banken in Europa aufstellen wird und damit die Basis für eine einheitliche IT-Aufsicht legt. In Deutschland hat die BaFin in Zusammenarbeit mit der Bundesbank in den vergangenen zwei Jahren Prüfungsmodule zu IT-Prüfungen erarbeitet und wird dieses Know-how sowohl bei den Arbeiten der EBA als auch in den Single Supervisory Mechanism (SSM) einbringen.

Die EZB beschäftigt sich derzeit besonders mit der Widerstandsfähigkeit der bedeutenden Banken gegen Cyberattacken (sogenannte Cyber Resilience) und wird nach Auswertung der Erhebungen über weitere Maßnahmen entscheiden. Aber wie gesagt: Auch für die Aufsichtsbehörden – wir befinden uns gerade in einer gewaltigen Lernkurve – ist dieses Thema nur im Zusammenspiel von aufsichtlichem, technischem und kriminalistischem Know-how zu bewältigen.

Angesichts der Risikolage im Cyberraum ist es nur konsequent, dass der deutsche Gesetzgeber im Kontext der deutschen Cybersicherheitsstrategie am 12. Juni 2015 das IT-Sicherheitsgesetz verabschiedet hat. Danach soll die Cybersicherheit in Deutschland in sogenannten kritischen Infrastrukturen auf einem hohen Niveau aufrechterhalten werden. Und das Finanz- und Versicherungswesen ist eine solche kritische Infrastruktur. Die BaFin wird das Bundesamt für Sicherheit in der Informationstechnik bei der weiteren Ausgestaltung des Gesetzes beziehungsweise der danach zu erlassenden Verordnung unterstützen.

Cyberchancen

Von den Cyberrisiken – die es sozusagen aus der Defensive zu beherrschen gilt – nun zur offensiven Seite, den Cyberchancen. Der Cyberraum ist ein virtueller Begegnungsraum und damit zugleich ein potenzieller Marktplatz. Jeder kann seine Produkte und Dienstleistungen über einen Webauftritt ins Netz stellen und hat damit im Grunde die Chance, weltweit digital Geschäfte zu tätigen. Kein Wunder also, dass die Digitale Agenda der Europäischen Union die Schaffung eines digitalen europäischen Binnenmarkts als eine der wichtigsten strategischen Maßnahmen der EU benannt hat. Dies soll zur Wirtschaftsbelebung in den Mitgliedsstaaten beitragen.

Aber dieses Ziel kann nur dann erreicht werden, wenn eine Grundbedingung erfüllt ist, und diese heißt Vertrauen. Nur wenn der Konsument davon ausgehen kann, dass er bei der Nutzung der Internetangebote nicht betrogen wird und seine Daten sicher sind, wird er sich auf dem digitalen Marktplatz bewegen.

Deshalb zählt die Gewährleistung der Netz- und Informationssicherheit zu den strategischen Zielen der digitalen Agenda 2020. Hier wird nochmals deutlich, dass die Gewährleistung der Cyber- und IT-Sicherheit kein isolierter und nur kostenverursachender Selbstschutz ist. Cybersicherheit ist die unabdingbare Basis dafür, dass Finanzinstitute auch die Chancen des digitalen Binnenmarktes ausschöpfen können.

Es stellt sich die Frage, ob es sich für Banken überhaupt lohnt, in den digitalen Binnenmarkt zu investieren. Reicht es nicht aus, die Kunden über ein dichtes Filialnetz und allgemein über Werbung zu erreichen? Die Antwort hierauf ist natürlich ein klares Nein. Der Fortschritt in der Informationstechnologie hat die Lebensgewohnheiten der Menschen stark verändert. Heute hat fast jeder einen PC mit Internetzugang. Das Smartphone setzt seinen Siegeszug unbeirrt fort und schon wartet mit der digitalen Uhr der nächste Innovationsschub. Das reale Leben verlagert sich immer mehr ins Internet, wo inzwischen fast alles erledigt werden kann. Die Cloud erscheint als der Ort für Innovationen. Kleine und große Unternehmen der Internetbranche treiben dies erfolgreich voran und mischen ganze Branchen auf, etwa die Musikindustrie und das Verlagswesen. Vielleicht wird das selbstfahrende Auto künftig nicht mehr von traditionellen Autokonzernen produziert, sondern von einem Internetunternehmen.

Erfolgsgeschichten der Internetbranche

Haben Internetkonzerne und junge Startups den Finanzsektor vergessen? Nein, ganz und gar nicht. Sie sind seit Jahren dabei, auch in diesem Bereich die Chancen des digitalen Marktes konsequent zu nutzen, und nehmen dabei eine Vorreiterrolle ein. Diese Unternehmen, die gerne als Fintechs bezeichnet werden, zeigen eindrucksvoll, welche Möglichkeiten das Internet hergibt. Sie reichen von Crowdfunding über Peer-to-Peer-Lending und Finanzforen bis hin zu völlig neuen Zahlungsdiensten.

Gerade im Zahlungsverkehr sehen vor allem die etablierten Internet-, Software- und Hardwareschmieden große Chancen. Egal von welchem Geschäftsmodell sie ursprünglich herkommen, alle arbeiten an technisch neuen Lösungswegen. Inzwischen verfügen mehrere dieser Unternehmen über eine Lizenz für Zahlungsdienstleistungen (zum Beispiel: Google – E-Geldlizenz in London; Facebook – E-Geldlizenz in Irland) oder eine Vollbanklizenz (Paypal in Luxemburg).

Ein Beispiel, wie erfolgreich die Chancen des digitalen Marktes genutzt werden können, ist das chinesische Unternehmen Alibaba. Das Unternehmen startete ursprünglich wie Ebay als Online-Handelsplattform, erweiterte sein Geschäftsmodell dann mit einer Tochter im Zahlungsverkehr. Inzwischen hat die Alibaba-Gruppe auch das Einlagengeschäft sowie die Vergabe von Händlerkrediten im Angebot. Die Alibaba-Gruppe ist nun auch in den USA aktiv und machte 2014 mit dem bislang größten Börsengang von sich reden, der 21,8 Milliarden Dollar in die Firmenkasse brachte – das Fundament für weitere Expansionen. Alibaba unterhält auch eine deutsche Website.

Diese und noch weitere Erfolgsgeschichten der Internetbranche sprechen dafür, dass es sich auch für deutsche Institute lohnt, in den digitalen Binnenmarkt zu investieren. Hinzu kommt der zunehmende Wettbewerbsdruck, daneben das regulatorische Umfeld. Die europäische Zahlungsdienste-Richtlinie dient dem Zweck, den digitalen Binnenmarkt mit einem einheitlichen Zahlungsverkehrsraum zu flankieren. Im vergangenen Jahr wurde Sepa (die Single European Payments Area) umgesetzt, und dieses Jahr soll die überarbeitete Zahlungsdienste-Richtlinie (ZDR II) verabschiedet werden.

Die neue Zahlungsdienste-Richtlinie wird sogenannte Dritte Zahlungsdienstleister einer Aufsicht zuführen und damit gleichen Anforderungen wie traditionelle Zahlungsdienstleister unterwerfen. Traditionelle Zahlungsdienstleister hingegen müssen dann den Zugriff der Dritten Zahlungsdienstleister auf die Konten ihrer Kunden zulassen. Wettbewerbspolitisch betrachtet bezwecken die neuen Regelungen deshalb eine Marktöffnung und die Förderung des digitalen Wettbewerbs. So werden alle Banken Europas durch die Europäische Kommission

auf die digitalen Chancen oder – je nach Perspektive – auch Bedrohungen aufmerksam gemacht.

Fehlentwicklungen identifizieren und Chancen aufzeigen

Warum interessiert sich die deutsche Aufsicht für diese Entwicklung? Weil wir potenzielle Fehlentwicklungen der Institute identifizieren müssen. Dazu gehört auch, Veränderungen beziehungsweise Chancen aufzuzeigen, deren Missachtung letztlich zum Verlust von Marktanteilen, sinkender Rentabilität und Wettbewerbsfähigkeit führen kann. Die Banken sind heute mehr denn je gehalten, nachhaltige Geschäftsstrategien aufzuweisen. Und die Aufsicht beschäftigt sich intensiv mit den Geschäftsstrategien. Der digitale Wandel erfordert eine Antwort der Banken auf diese Entwicklung. Er erfordert eine Digitalisierungsstrategie. Diese ist also auch ein Aufsichtsthema.

Natürlich weiß ich, dass viele Finanzdienstleister auf diesem Gebiet bereits aktiv sind. Dem Privatkunden werden zahlreiche Finanzdienste und -produkte über das Internet angeboten. Auch über neue Zahlungsdienste wird nachgedacht oder sie sind bereits im Aufbau. Der Bankathon 2015[3] hat gezeigt, dass Banken und Fintechs gemeinsam neue Ideen entwickeln können. Problematisch wäre es daher, gewissermaßen aus traditioneller Sicht die IT noch immer vor allem als Kostenfaktor zu sehen und nicht als ein strategisches Instrument. Genauer beobachtet werden muss auch der Trend, dass immer mehr IT-Prozesse in die Cloud gegeben werden, wodurch neue Risiken geschaffen und IT-Expertise und mögliche Innovationsressourcen verloren gehen könnten.

Selbstverständlich können auch Banken den digitalen Wandel für sich und ihre Kunden nutzen. Die Herausforderung besteht darin, alle Geschäftsbereiche und Prozesse im Lichte digitaler Ökosysteme und Walled-Garden-Strategien zu prüfen und damit einen Strukturwandel anzustoßen. Die neuen Vertriebs- und Kommunikationskanäle müssen konsequent den Bedürfnisse der Retail-Kunden und der Internethändler angepasst werden. Das Silodenken der einzelnen Geschäftsbereiche sollte der Vergangenheit angehören. Der digitale Wandel bietet Banken die Gelegenheit, neue Geschäftsmodelle sofort unter Berücksichtigung der unabdingbaren IT-Sicherheit und des Datenschutzes zu entwerfen.

IT-Sicherheit einfordern und kontrollieren

Die Beherrschung von Cyber- und IT-Risiken ist eine Grundbedingung dafür, dass Banken die Chancen des digitalen Wandels ausschöpfen können. Dafür bedarf es einer Digitalisierungsstrategie, auch angesichts des Eintritts von Fintechs in die Geschäftsfelder der traditionellen Banken. In Europa treibt die Digitale Agenda diese Entwicklung voran. Die Richtlinie zur Netz- und Informationssicherheit und die Zahlungsdienste-Richtlinie II zielen darauf ab, Sicherheit und Fortschritt miteinander zu verbinden.

Cyberrisiken werden weiter zunehmen. Sie gehören zu den Toprisiken eines jeden Unternehmens. Banken werden nur dann wettbewerbsfähig bleiben, wenn sie die IT-Sicherheit entlang der gesamten Wertschöpfungskette auf allen IT-Ebenen gewährleisten können. Deswegen ist die IT-Sicherheit von den Banken konsequent bei ihren IT-Dienstleistern und IT-Zulieferern einzufordern und zu kontrollieren. Auch die EZB sieht die zunehmenden Cyberrisiken an oberster Stelle der IT-Risiken der Banken und verlangt entsprechende Vorkehrungen. In die gleiche Richtung geht das gerade verabschiedete deutsche IT-Sicherheitsgesetz.

Keine digitale Demenz

Die BaFin wird sich deshalb dafür einsetzen, dass die operative IT-Aufsicht im Rahmen des SSM weiter verstärkt wird und die EBA einen europäischen Rechtsrahmen für die IT-Aufsicht entwickelt. Die aufsichtlichen Anforderungen müssen der steigenden Bedrohungslage und dem digitalen Wandel konsequent angepasst werden. Es könnte auch erforderlich werden, die Einhaltung dieser Anforderungen öfter und intensiver vor Ort zu überprüfen. Die Banken selbst sollten ihre Widerstandfähigkeit durch regelmäßige Penetrationstests auf die Probe stellen.

Zum Schluss noch ein Wort der Hoffnung, dass die weltweite Digitalisierung nicht in die von Prof. Manfred Spitzer vorausgesagte digitale Demenz führen wird. Auch deshalb hat das vitale Leben und der direkte Kontakt zwischen den Menschen für mich immer noch Vorrang. Live und direkt.

Fußnoten

1) Bank of Muscat in Oman. Zwei Monate zuvor (12/2012) war eine andere Bank, die Rakbank in den Vereinigten Arabischen Emiraten, auf gleiche Weise geschädigt worden. Der Schaden belief sich hier auf 5 Millionen Dollar.
2) Einschließlich USA, Japan, Russland, Rumänien, Ägypten, Kolumbien, England, Sri Lanka und Kanada.
3) 15 Banken und 15 Fintechs trafen sich am 6. Mai 2015 auf der Fintech-Konferenz Exec I/0 in Frankfurt und entwickelten innerhalb von 30 Stunden 27 neue Ideen für Bankingservices.

Der Beitrag basiert auf einer Rede des Autors auf dem Bundesbank Symposium „Bankenaufsicht im Dialog" am 8. Juli 2015 in Frankfurt am Main. Zwischenüberschriften sind von der Redaktion eingefügt.