Die Illusion von Sicherheit schwindet

Barbara Hummel

Das Thema IT-Sicherheit genießt dieser Tage hohe Aufmerksamkeit. Die Meldungen über Attacken auf Unternehmen der verschiedensten Branchen, aber auch auf öffentliche Institutionen mehren sich geradezu rasant. Auch Banken waren in den vergangenen Monaten immer wieder betroffen: Zuletzt wurde im Januar 2016 das Online-Banking der britischen HSBC einen Tag lang durch einen DDoS-Angriff (Distributed Denial of Service) lahmgelegt. Der Zeitpunkt war so gewählt, dass er größtmöglichen Schaden für die Bank und deren Kunden verursachte: An dem Freitag war nicht nur Zahltag für einen Großteil der britischen Bevölkerung, es war auch der Stichtag, an dem für viele Gewerbetreibende die Abgabe ihrer Steuererklärung anstand. Die Liste der geglückten DDoS-Attacken lässt sich beliebig fortsetzen: auch mit drei griechischen Banken, die zum Jahresende 2015 betroffen waren und von denen ein Lösegeld erpresst werden sollte. Mindestens ebenso spektakulär war der Fall eines Hackerangriffs auf die amerikanische Bank J. P. Morgan Chase & Co im Sommer 2014. Eine in die Bank eingeschleuste Schadsoftware wurde erst zwei Monate später überhaupt entdeckt. Hacker konnten in der Zwischenzeit Namen, Adressen und Mailadressen von über 76 Millionen Privatkunden und von 7 Millionen Firmenkunden stehlen.

Offenbar werden sich die Unternehmen der Gefährdung zunehmend bewusst: Im Risk Barometer 2015 des Versicherers Allianz rückten Cybervorfälle mit 28 Prozent der Antworten erstmals unter die drei größten Unternehmensrisiken auf – weltweit und in Deutschland. Noch drei Jahre zuvor im Risk Barometer 2012 nannte nur ein Prozent der Befragten Cybervorfälle als potenzielles Risiko. Als Hauptgrund für wirtschaftliche Schäden in der Folge eines Cyberangriffs wird der Reputationsverlust aufgeführt, gefolgt von Betriebsunterbrechungen und Haftungsansprüchen aufgrund einer Datenschutzverletzung. Jedes Jahr entstehen nach Schätzungen der Allianz Global Corporate & Specialty der Weltwirtschaft Schäden durch Cybercrime in Höhe von 445 Milliarden US-Dollar. Alleine in Deutschland werden diese von dem Versicherer auf jährlich rund 59 Milliarden US-Dollar (etwa 54 Milliarden Euro) beziffert. Das Bundesministerium für Wirtschaft und Energie schätzt die Schäden in Deutschland ähnlich auf rund 50 Milliarden Euro pro Jahr ein.

Aufseiten der Industrie wächst die Bereitschaft, sich (gemeinsam) gegen entsprechende Angriffe zu wappnen. Im Januar dieses Jahres haben die Firmen Airbus, Ericsson, BMW, Infineon und Deutsche Telekom dem EU-Kommissar für den digitalen Binnenmarkt Günter Oettinger das Konzept einer gemeinsamen IT-Sicherheitsstrategie vorgelegt. Initiativen für den beständigen Austausch, aber auch für eine angemessen schnelle Kommunikation bei aktuellen Bedrohungslagen gibt es auch in der deutschen Kreditwirtschaft. In Arbeitskreisen werden Informationen über aktuelle Vorfälle und deren Bekämpfung mit Aufsichtsbehörden, aber auch zwischen den Kreditinstituten ausgetauscht. In Frankfurt haben HVB, Commerzbank und ING-Diba den Verein German Competence Center against Cyber Crime (G4C) aus der Taufe gehoben. Die Einheit kooperiert mit dem Bundeskriminalamt. Auf deutscher Ebene ist zudem das UP Kritis aktiv, eine freiwillige öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (Kritis), deren Verbänden und den zuständigen staatlichen Stellen. Ihre Meldungen speisen sich unter anderem aus den Daten des BSI. Dazu kommt: die informellen Drähte glühen durchaus heiß, wenn Gefahr im Verzug ist.

Auf politischer Ebene ist dem Thema – spätestens nach dem Sicherheitsvorfall im Bundestag im Juni 2015 – ebenfalls Aufmerksamkeit sicher. Der rechtliche Rahmen in Sachen IT-Sicherheit ist in Deutschland – mindestens für die Kreditwirtschaft – seit geraumer Zeit eng gesteckt. Die Paragrafen 25 a und 25 b des KWG, die Paragrafen 23 ff. VAG, die Zahlungsdiensterichtlinie II, Guidelines der EBA, BaFin-Rundschreiben sowie MaRisk geben vor, wie sich die Institute im Sinne einer stabilen IT-Infrastruktur abzusichern haben. Gerade das MaRisk-Rundschreiben 10/2012 der BaFin, in dem die technisch-organisatorische Ausstattung der Banken geregelt ist, schreibt vor, dass die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen müssen. Um das zu erreichen, soll bei der Ausgestaltung der IT-Systeme und der -Prozesse auf gängige Standards abgestellt werden.

Mit dem IT-Sicherheitsgesetz hat die Bundesrepublik Deutschland seit dem Juli 2015 nun weitere neue Vorgaben unter anderem für die Betreiber kritischer Infrastrukturen geschaffen. Zu ihnen gehören Banken und Sparkassen. Auf welche Unternehmen der Branche das Gesetz jedoch genau angewendet werden soll, ist noch unklar. Für diese Einordnung sollen im zweiten Quartal des Jahres

2016 über eine Umsetzungsverordung noch maßgebliche Schwellen (das könnte beispielsweise die Zahl der von einem mutmaßlichen Ausfall betroffenen Kunden sein) definiert werden. Für die ganz großen Banken steht außer Frage, dass sie von den neuen Regeln betroffen sein werden. Für die beiden Finanzverbünde sind einige spannende Fragen aber noch offen, beispielsweise wie stark sie als Einheit gewertet werden. Das verdeutlicht auch folgendes Beispiel: Zu den zu schützenden Funktionen wird vom Gesetzgeber die Bargeldversorgung gerechnet. Fällt bei Sparkasse oder Volksbank XY das Geldautomatennetz aus, dann ist das kein für das Gesamtsystem signifikanter Vorfall. Fällt jedoch die Bargeldversorgung im gesamten jeweiligen Finanzverbund aus, dann ist das sehr wohl relevant. Ein kleiner Trost für die Branche: Einen guten Teil der neuen Vorgaben erfüllen Banken und Sparkassen ohnehin bereits, da sie ein hohes Eigeninteresse an stabilen IT-Infrastrukturen haben.

Der Bundestag hat zudem das IT-Sicherheitsgesetz zu einem Zeitpunkt beschlossen, als die Verhandlungen über gesamteuropäische Maßnahmen noch in vollem Gange waren. Unterhändler der zuständigen EU-Organe haben sich Mitte Dezember 2015 auf eine Fassung der sogenannten NIS-Richtlinie (Network and Information Security) geeinigt. Die formelle Verabschiedung der Richtlinie wird in Kürze erwartet. Das gerade in Kraft getretene IT-Sicherheitsgesetz wird daher binnen 21 Monaten nach Verabschiedung der NIS-Richtlinie nochmals leicht angepasst werden müssen.

Doch bedeutet das Erfüllen der rechtlichen Vorgaben dann auch gleichzeitig, dass die Systeme der Banken sicher sind? Eher nicht. Da es unmöglich erscheint, alle Angriffe komplett abzuwehren, muss in den Banken zukünftig noch stärker priorisiert werden, welche Daten und Systeme unbedingt schützenswert sind und welche man im Zweifelsfall vielleicht sogar verloren geben muss. Für den technischen Aufbau ist die Herausforderung daher das Anlegen einer Art von Labyrinth. Bildlich gesprochen soll sich der Angreifer darin verlaufen, da man ihm geöffnete Türen präsentiert ebenso wie Türen, die sich schwer öffnen lassen und Türen, die sicher verschlossen sind. Das Ziel: Jeden Angreifer oder Eindringling möglichst lange beschäftigen, ihn aber schnell bemerken, seine Vorgehensweise beobachten und ihn daraufhin wirkungsvoll bekämpfen. Die Stabilität und Sicherheit des IT-Systems ist aber nicht nur eine Frage der technischen Systeme – sondern auch der Menschen. Schon wenn sich zwei Mitarbeiter zusammentun, die mit entsprechenden Rechten im System ausgestattet sind, dann können sie eine Menge Schaden anrichten, der in einem komplexen System lange unentdeckt bleiben kann. Hier hilft nur kluges Personalmanagement. Neben dem ausgesprochenen Willen zu betrügen, kommt freilich noch die menschliche Natur als Sicherheitsrisiko hinzu. Genauso häufig wie Angriffe von außen sind Fehlverhalten oder Versagen von (ehemaligen) Mitarbeitern und Dienstleistern der Grund für Störungen in der Informationstechnik. Laut einer weltweiten Umfrage des Software-Unternehmens Palo Alto Networks gibt ein Viertel der Befragten zu, Sicherheitsbestimmungen im vollen Bewusstsein der Gefahren zu umgehen, weil sie den Zugang zu effizienteren Werkzeugen, Webseiten und Programmen verhindern. In Deutschland liegt deren Anteil mit 38 Prozent im europaweiten Vergleich sogar am höchsten.

Die Bankenaufsicht beschäftigt sich mit dem Thema der IT-Sicherheit intensiv. Im Jahr 2015 bezeichnete Felix Hufeld die „Qualität der Cyberrisiken im Finanzsektor" als „auf einem alarmierenden Niveau". Entsprechend aufmerksam wird das Thema behandelt. BaFin und Bundesbank thematisieren in Aufsichtsgesprächen und Sonderprüfungen immer wieder die IT-Sicherheit der Institute, zum Teil auch mit Fokus auf die Cybersicherheit. Aktuelles Thema ist dabei auch die Stellung des IT-Sicherheitsbeauftragten. In der Organisation Bank soll er möglichst unabhängig sein, darauf dringt auch die Bankenaufsicht in den vergangenen Monaten massiv. Das macht sich dann schon an der Frage deutlich, an welches Vorstandsmitglied der IT-Sicherheitsbeauftragte berichten soll: an den IT-Vorstand, wie es heute oftmals der Fall ist? Oder besser an den Risikovorstand beziehungsweise falls vorhanden an den Compliance-Vorstand? Im laufenden Jahr 2016 werden IT- und Cyberrisiken auch verstärkt im Fokus der EZB-Bankenaufsicht stehen. Bei der Europäischen Bankenaufsichtsbehörde (EBA) wurde eine Task-Force zu IT-Risiken gegründet, die daran arbeitet, neue Anforderungen an die IT-Organisation der Banken in Europa aufzustellen und damit die Basis auch für eine einheitliche IT-Aufsicht zu legen. Die EZB beschäftigt sich besonders mit der Widerstandsfähigkeit der bedeutenden Banken gegen Cyberattacken (Cyber-Resilience).

In der Bankstrategie und im Bankbetrieb stehen sich IT-Sicherheit und Innovationsfähigkeit oftmals diametral gegenüber; Big Data, Social Media und Cloud Computing sind große Chancen für die Branche, sie beinhalten jedoch auch neue Herausforderungen an die Banken-IT; denn mit jedem neuen Verfahren erhöht sich die Zahl der Schnittstellen und damit auch die Anfälligkeit für Fehler. Hundertprozentige Sicherheit gibt es im virtuellen Raum nicht und es wird sie auch in Zukunft nicht geben. Das Abwägen zwischen Chancen und Risiken neuer Technologien wird weitergehen – ebenso wie der uralte Wettlauf zwischen Verteidigern und Angreifern.