Reemt Matthiesen / Markus Kaulartz

Auswirkungen des **IT-Sicherheitsgesetzes** auf Banken und Versicherer

Das IT-Sicherheitsgesetz ist Teil der Cybersicherheitsstrategie der Bundesregierung und seit 25. Juli 2015 in Kraft. Es soll die Sicherheit von IT-Systemen in Deutschland durch Verbesserung ihrer Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität stärken. Doch was bedeutet das Gesetz für die ohnehin schon stark regulierte Banken- und Versicherungsbranche?

IT-Regulierung von Banken und Versicherungen

Der Banken- und Versicherungssektor wird von Jahr zu Jahr digitaler, die Mehrheit der Deutschen erledigt Bankgeschäfte online oder schließt Versicherungsverträge über das Internet ab. Auch intern ist die IT nicht wegzudenken, was jedoch wegen der Sensibilität der Geschäftsvorgänge erhöhter Sicherheitsvorkehrungen bedarf. Es verwundert daher nicht, dass die IT-Regulierung von Banken und Versicherungen seit Jahren stetig zunimmt: §§ 25a, 25b KWG, §§ 23 ff. VAG, Zahlungsdiensterichtlinie II, EBA Guidelines, BaFin-Rundschreiben, BAIT, MaRisk BA, MaRisk VA. Diese teils sehr allgemeinen und teils sehr speziellen Regelungen werden nun ergänzt durch branchenübergreifende Verpflichtungen zu technischen und organisatorischen Maßnahmen. Betroffen vom IT-Sicherheitsgesetz sind zum einen Betreiber kritischer Infrastrukturen und zum anderen Anbieter von Telemedien.

Unternehmen aus dem Finanz- und Versicherungswesen gehören dann zu den „kritischen Infrastrukturen", wenn sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Diese Definition ist in der Praxis wenig hilfreich. Daher werden die für die Beurteilung der kritischen Infrastrukturen maßgeblichen Schwellen abschließend und exakt durch eine Rechtsverordnung definiert, die noch im Laufe des Jahres 2016 erwartet wird. Für die meisten der neuen Regelungen haben die Unternehmen dann eine Umsetzungszeit von zwei Jahren.

Woran die Schwellenwerte anknüpfen, welche die kritischen Infrastrukturen beschreiben, also etwa an die Mitarbeiter- oder die Kundenzahl, ist noch nicht bekannt. Berücksichtigt man, dass branchenunabhängig insgesamt rund 2000 Unternehmen zu den kritischen Infrastrukturen zählen sollen, ist zu erwarten, dass nur die wenigsten Banken und Versicherungen hierunter fallen werden.

Das IT-Sicherheitsgesetz nennt aus dem Sektor Finanz- und Versicherungswesen beispielhaft den Zahlungsverkehr, die Bargeldversorgung, die Kreditvergabe, den Geld- und Devisenhandel, den Wertpapier- und Derivatehandel und die Versicherungsleistungen.

Dr. Reemt Matthiesen, Dr. Markus Kaulartz, Rechtsanwälte, CMS Hasche Sigle, München

Die IT-Regulierung von Banken und Versicherern nimmt seit Jahren zu. Mit dem im Juli 2015 in Kraft getretenen IT-Sicherheitsgesetz werden Betreiber kritischer Infrastrukturen und Anbieter von Telemedien stärker überwacht als bisher. Dies alleine wird voraussichtlich bei den Kreditinstituten nicht zu erheblichen Mehrbelastungen führen, da sie schon streng reguliert sind und auch per se bereits heute ein starkes Eigeninteresse an hoher IT-Sicherheit haben. Auch als Anbieter von Telemedien dürfte der Handlungsbedarf eher gering sein. Die Autoren schätzen es für die Banken und Versicherer nach wie vor als maßgeblich ein, sich eng mit dem Bundesamt für Sicherheit in der Informationstechnik, aber auch der BaFin abzustimmen. (Red.)

Angemessene technische und organisatorische Maßnahmen

Zu den umzusetzenden Maßnahmen gehört insbesondere die Durchführung angemessener technischer und organisatorischer Maßnahmen, wobei der Stand der Technik zu jeder Zeit zu berücksichtigen ist. Gerade Letzteres dürfte dort zu Herausforderungen führen, wo veraltete und vermeintlich bewährte Hard- und Software zum Einsatz kommt (zum Beispiel Betriebssysteme, für die keine Updates mehr bereitgehalten werden). Der in der IT beliebte Grundsatz „never change a running system", nach dem viele Betriebe ihre IT ausrichten, darf nicht die Maxime für die IT-Sicherheit sein.

Spezifische Sicherheitsvorschriften, die auf Banken und Versicherer zugeschnitten sind, werden dabei vom BSI (Bundesamt für Sicherheit in der Informationstechnik) in Abstimmung mit den Branchenverbänden erlassen. Dies sollte in der Praxis zu einer tauglichen Abgrenzung des Begriffs „Stand der Technik" beitragen.

Die umgesetzten Maßnahmen müssen dem BSI mindestens alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachgewiesen werden. Außerdem müssen Kontaktstellen eingerichtet und dem BSI benannt werden.

Erhebliche Störungen melden

Als bedeutende intraorganisatorische Änderung müssen dem BSI künftig erhebliche Störungen gemeldet werden, auch wenn sie nur zu einer Beeinträchtigung der

Funktionsfähigkeit führen können. Das BSI bündelt also branchenunabhängig alle Sicherheitsvorfälle und geht damit weit über die Funktion des bisher etwa genutzten LKRZV-Krisenreaktionszentrums für IT-Sicherheit der deutschen Versicherungswirtschaft hinaus. Die Branchenunabhängigkeit ist wichtig, da viele Angriffe branchenunabhängig ausgeübt werden. Das Gegenstück zur Meldepflicht ist die Aufgabe des BSI, Banken und Versicherungen die betreffende Informationen zur Gewährleistung einer IT-Sicherheit zur Verfügung zu stellen.

Anbieter von Telemedien

Unter den Begriff der Telemedien fallen etwa Webseiten und Banking-Apps. Auch hierfür sind umfangreiche technische Maßnahmen umzusetzen, wie etwa eine angemessene Verschlüsselung von Daten und der Verbindung. Die Maßnahmen müssen zwar „zumutbar" sein. Eine Erleichterung ist hiermit für Banken und Versicherungen mit Blick auf die Sensibilität der Daten allerdings kaum verbunden. Da betroffene Daten meist auch personenbezogene Daten sind und hierfür aufgrund des Bundesdatenschutzgesetzes oder der wohl 2018 in Kraft tretenden EU-Datenschutz-Grundverordnung ebenfalls schon Pflichten zur Umsetzung technischer und organisatorischer Maßnahmen bestehen, dürfte das Aktionspotenzial für Banken hier nur gering sein.

Die neuen Vorschriften geben dem BSI auch die Befugnis, von Herstellern von bei Banken und Versicherungen eingesetzten IT-Produkten und -Systemen, also auch Software, die Mitwirkung an der Beseitigung oder Vermeidung von Störungen zu verlangen. Überdies kann das BSI auch Sicherheitslücken veröffentlichen und IT-Produkte und -Systeme untersuchen, worunter nach der Gesetzesbegründung des IT-Sicherheitsgesetzes auch das Reverse Engineering von Software fallen soll. Die letztgenannte, europarechtlich nicht unumstrittene Möglichkeit des BSI wird in der Praxis bei kooperierenden IT-Herstellern kaum Bedeutung erlangen.

Durch die Verwendung des Begriffs „Stand der Technik" soll sichergestellt werden, dass auch neueren technischen Entwicklungen stets Rechnung getragen wird. Was konkret umgesetzt werden soll, kann sich grundsätzlich aus einschlägigen internationalen, europäischen und nationalen Normen und Standards ergeben. Auch spielen vergleichbare Verfahren, Einrichtungen und Betriebsweisen eine Rolle, die mit Erfolg in der Praxis erprobt wurden.

Schlichtes Befolgen der Richtlinien nicht ausreichend

Allerdings genügt eine schlichte Befolgung von etwa DIN- oder ISO-Normen oder Richtlinien des BSI nicht, was sich seit Jahren auch schon aus entsprechenden Mitteilungen der BaFin ergibt. Bei jeder Implementierung ist vielmehr zu hinterfragen, ob das umgesetzte Sicherheitsniveau angemessen ist. Maßgeblich für Banken und Versicherungen sind daher zuvorderst auch die spezifischen, zwischen den Bank- und Versicherungsverbänden und dem BSI abgestimmten Detailregelungen. Auch die BaFin wird hier eine bedeutende Rolle spielen.

Es findet eine Verschmelzung von Technik und Recht statt, die dazu führt, dass Rechtsabteilungen von handelnden Technikern eingebunden werden sollten, wenn es darum geht zu bestimmen, welche umzusetzenden Anforderungen im Detail für die konkreten Systeme erforderlich, aber auch angemessen sind und wann Ausnahmen zulässig sind.

Modifizierung durch europäische NIS-Richtlinie

Das IT-Sicherheitsgesetz ist Teil einer europaweiten Strategie zur Stärkung der Cybersicherheit. Der Bundestag beschloss das Gesetz zu einem Zeitpunkt, als die Verhandlungen über gesamteuropäische Maßnahmen noch in vollem Gange waren. Mitte Dezember 2015 einigten sich Unterhändler der zuständigen EU-Organe auf die sogenannte NIS-Richtlinie (Network and Information Security), die inhaltlich stark dem deutschen IT-Sicherheitsgesetz ähnelt. Die Richtlinie, deren formelle Verabschiedung in Kürze erwartet wird, entfaltet Rechtswirkungen allerdings nicht hinsichtlich einzelner Unternehmen, sondern verpflichtet die EU-Mitgliedsstaaten, die in ihr enthaltenen Grundsätze in nationales Recht zu gießen.

Das IT-Sicherheitsgesetz wird daher binnen 21 Monaten nach Verabschiedung der NIS-Richtlinie minimal angepasst werden müssen. Abgesehen von IT-Diensten, wo die Richtlinie kaum Gestaltungsspielraum lässt, ist es den Mitgliedsstaaten dabei überlassen, ob sie strengere Anforderungen normieren und damit über den in der Richtlinie vorgegebenen Schutzrahmen hinausgehen. Überdies steht es den Mitgliedsstaaten frei, die oben genannten kritischen Infrastrukturen in Grenzen frei zu definieren.

Zwar kann all dies zu einem europäischen Flickenteppich führen, welcher der Idee der Vereinheitlichung der Regelungen zur Cybersicherheit zuwiderläuft – es wird jedoch allgemein erwartet, dass die nationalen Regierungen eine einheitliche Lösung anstreben.

Bußgelder des BSI und Schadensersatzansprüche möglich

Für Banken und Versicherungen drohen aufgrund von Verstößen gegen Vorschriften des IT-Sicherheitsgesetzes Bußgelder des BSI in Höhe von bis zu 100 000 Euro, daneben spielen Schadensersatzansprüche von Betroffenen eine Rolle, etwa bei monetären Einbußen oder Datenverlusten durch Softwarefehler. Wichtig ist daher die vertragliche Absicherung: Die umzusetzenden Pflichten sollten vertraglich an die sachnäheren IT-Dienstleister weitergereicht werden, um im Schadensfall Regress nehmen zu können.

Formell gesehen sind Banken und Versicherer neuen Vorschriften ausgesetzt, die sie sowohl in ihrem täglichen Geschäftsbetrieb als auch beim Anbieten von Telemedien (zum Beispiel Webseiten und Apps) beachten müssen. Ob dies tatsächlich zu signifikanten Mehrbelastungen führt, ist zweifelhaft, denn Banken und Versicherungen haben ein starkes Eigeninteresse an hoher IT-Sicherheit. Im Übrigen müssen viele der neuen Plichten im Kern auch schon heute beachtet werden, wie aus den eingangs erwähnten Bestimmungen deutlich wird (etwa §§ 25a, 25b KWG).

Neu geregelt ist die enge Zusammenarbeit der Betreiber Kritischer Infrastrukturen mit dem BSI und – bedingt durch die NIS-Richtlinie – eine bessere Kooperation auf europäischer Ebene. Wichtig für Banken und Versicherungen ist nun, die notwendigen Änderungen ihrer technischen und organisatorischen Maßnahmen rasch zu identifizieren, um die Umsetzungsfrist nicht unerledigt verstreichen zu lassen.