D 7465

Zeitschrift für das gesamte
KREDITWESEN

73. Jahrgang · 1. September 2020

17-2020

Pflichtblatt der Frankfurter Wertpapierbörse
Fritz Knapp Verlag · ISSN 0341-4019

Digitaler Sonderdruck

ZAHLUNGS VERKEHR

Kampf gegen Cybercrime: Mehr globale Zusammenarbeit notwendig

Andreas Krautscheid / André Nash

Foto: zapp2photo

Andreas Krautscheid / André Nash

Kampf gegen **Cybercrime**: Mehr **globale Zusammenarbeit** notwendig

Als die Europäische Kommission Ende 2019 ihren Fahrplan für die kommenden Jahre präsentierte, lag das Augenmerk der breiten Öffentlichkeit vor allem auf dem prominent vorgestellten „European Green Deal". Dass die Kommission im Rahmen ihrer Digitalisierungsstrategie zugleich bekanntgab, einen weiteren Schwerpunkt ihrer Arbeit auf das Thema Cyber Security legen zu wollen, wurde hingegen weniger zur Kenntnis genommen. Überraschend aber ist die Wahl dieses Themas nicht – schließlich nimmt die Relevanz digitaler Themen und einer sicheren und funktionierenden digitalen Infrastruktur in allen gesellschaftlichen Bereichen ständig zu. Mit Blick auf den Finanzsektor ist die Cybersicherheit von existenzieller Bedeutung: Mittlerweile wird die Gefahr durch Cyberangriffe als eines der größten operationellen Risiken im Finanzsektor und auch als eine potenzielle Bedrohung für die Finanzstabilität eingeschätzt.

> „Eine gemeinsame langfristige Vision zur Absicherung des Finanzsektors muss noch entwickelt werden."

Technik und Regulatorik müssen sich weiterentwickeln

Banken müssen jederzeit mit deutlich raffinierteren und größeren Cyberangriffen rechnen als in der Vergangenheit. Die Angreifer haben sich in den letzten Jahren technologisch ständig weiterentwickelt und inzwischen in etwa das Niveau nationaler Sicherheitsbehörden erreicht. Insgesamt verändern neue Technologien die IT-Landschaft im Finanzsektor in rasendem Tempo. Künstliche Intelligenz wird sowohl bei Angriffen als auch bei der Abwehr von Cyberattacken in steigendem Maße eingesetzt. Anpassung und Innovation müssen deswegen immer schneller werden, um sich gegen künftige Angriffe erfolgreich wappnen zu können. Agilität und Flexibilität, schnelle Reaktions- und Wandlungsfähigkeit sind in den IT-Systemen und in den Köpfen der Verantwortlichen so notwendig wie noch nie.

Dementsprechend sind auch die Anforderungen an die Regulatorik hoch. Die rechtlichen Rahmenbedingungen und Vorgaben der Aufsichtsbehörden dürfen sich in diesem Wettlauf nicht abhängen lassen und müssen laufend weiterentwickelt werden, um auf der Höhe der Zeit zu sein. In den vergangenen Jahren ist diesbezüglich schon Einiges passiert: So wurden auf EU-Ebene unter anderem mit der Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie), mit der Zweiten Zahlungsdiensterichtlinie (PSD2) und auch mit dem Cyber Security Act wichtige Bausteine einer verbesserten Cybersicherheitsstruktur verabschiedet.

Die G7-Staaten haben parallel dazu verschiedene sogenannte Fundamental-Elements-Dokumente zum Thema „Cyber Security im Finanzsektor" entwickelt. Und im Auftrag der G20 war das Financial Stability Board aktiv – zuletzt mit einer Liste von Best Practices zu „Cyber Incident Response and Recovery".

Von Harmonisierung noch weit entfernt

Viele dieser und anderer Initiativen waren Reaktionen auf Cybervorfälle und Cyberentwicklungen der vergangenen Jahre. Häufig gelang es, Prozess- und Sicherheitslücken schnell zu schließen und die notwendigen Voraussetzungen dafür zu schaffen, dass der technologische Fortschritt nicht zu weit vorauseilt. Durch internationale Initiativen gibt es auch ein gemeinsames Verständnis und damit die Basis für ein einheitliches Sicherheitsniveau zur Stärkung der (grenzübergreifenden) Cyberwiderstandsfähigkeit im Finanzsektor.

Doch die Verordnungen und Richtlinien sowie die darauf aufsetzenden konkreten Regulierungsschritte der unterschiedlichen Aufsichtsbehörden sind nur teilweise miteinander verzahnt worden. Mit anderen Worten: Von einer wirklichen Harmonisierung und einer Konvergenz bei den Regulierungsvorhaben zur IT-Sicherheitsarchitektur sind wir noch weit entfernt. Auch eine gemeinsame langfristige Vision zur Absicherung des Finanzsektors muss noch entwickelt werden.

Immerhin, das Problem ist erkannt. Die EU-Kommission will mit einer aktuellen öffentlichen Konsultation[1)] den Finanzsektor in der EU „widerstandsfähiger und

Andreas Krautscheid

Hauptgeschäftsführer, Bundesverband deutscher Banken e.V., Berlin

André Nash

Associate Director, Themengruppe Banktechnologie und Sicherheit, Bundesverband deutscher Banken e.V., Berlin

In die deutsche Ratspräsidentschaft wird sehr viel Hoffnung gelegt. Aufgrund der Stellung Deutschlands erwarten sich die Protagonisten von den kommenden Monaten in vielen Bereichen spürbare Fortschritte. Ein wichtiges Thema dabei: Digitalisierung und IT-Sicherheit. Dabei spielt das Thema Cybersecurity auch für Finanzdienstleister inzwischen eine enorme Rolle. So wird die Bedrohung durch Cyberangriffe als eines der größten operationellen Risiken im Finanzsektor und auch als eine potenzielle Bedrohung für die Finanzstabilität eingeschätzt. Zwar sei in jüngerer Vergangenheit gerade auf Ebene der Regulatorik und Gesetzgebung schon sehr viel geschehen, loben die Autoren. Prozess- und Sicherheitslücken seien schnell geschlossen worden und es gebe ein auch international gemeinsames Verständnis. Allerdings gehen ihnen angesichts der Vielzahl an Initiativen die Koordination und Harmonisierung ein Stück weit verloren. Ihr Wunsch daher: Koordinierte Maßnahmen und gemeinsame Bemühungen von Politik, Aufsichtsbehörden, Zentralbanken und der Finanzindustrie, europaweit und global. (Red.)

sicherer gestalten“, indem sie die regulatorischen Anforderungen an die IT-Sicherheit im Finanzsektor harmonisiert. Solche international koordinierten und harmonisierten Anforderungen könnten Synergieeffekte und Effektivitätssteigerungen in den Sicherheitsarchitekturen der Banken schaffen und die Cyberresilienz in Europa stärken. Außerdem würden unverhältnismäßiger Aufwand, Doppelbelastungen und Unsicherheiten angesichts heute noch divergierender Anforderungen wegfallen. Die dadurch freigesetzten Ressourcen könnten die Banken wiederum in ihre eigenen Cyberabwehrmaßnahmen stecken.

Ineffizienzen auflösen

Konkrete Beispiele für bislang nicht koordinierte Regulierungsvorgaben gibt es viele: Dazu zählen umfangreiche Fragenkataloge und zu erbringende Nachweise, aber auch verschiedene Formulare für die Meldung von Sicherheitsvorfällen, die die Banken an unterschiedliche Behörden und Meldestellen verschicken müssen.

Dass dies nicht effizient ist, liegt auf der Hand: Die Vorgaben für die Meldungen und das Reporting von Cybervorfällen sollten deshalb vereinheitlicht werden – mit dem Ergebnis, dass sich die Transparenz und das Sicherheitslevel erhöhen, die Aufsichtsvorgaben einfacher werden und der Verwaltungsaufwand für die Institute sowie für die sich miteinander im Austausch befindlichen Behörden abnimmt.

Solche Harmonisierungs- beziehungsweise Koordinierungsschritte müssen auch in die aktuellen regulatorischen Arbeiten Eingang finden, zum Beispiel bei den Threat Intelligence-based Ethical Red Teamings, den sogenannten TIBER-Tests. Diese simulierten Hackerangriffe basieren auf einem Rahmenwerk der Europäischen Zentralbank (EZB). Während sich die EZB dabei auf die Finanzmarktinfrastrukturen fokussiert, setzen die nationalen Zentralbanken und Aufsichtsbehörden diesen Testansatz für die jeweiligen Banken in den einzelnen Mitgliedsstaaten um. Hier gibt es derzeit noch zahlreiche ungeklärte Aspekte: So wäre es wichtig, dass ein in einem Land durchgeführter Test auch von den anderen EU-Mitgliedsstaaten anerkannt wird, um doppelte Tests und unnötigen Mehraufwand zu vermeiden.

Was das Thema so komplex und teilweise unübersichtlich macht: Für die IT-Sicherheit sind eine Reihe von Vorgaben und Anforderungen relevant, die nicht nur auf den Finanzsektor zielen – zum Beispiel die Vorgaben zum Schutz der kritischen Infrastrukturen des IT-Sicherheitsgesetzes 2.0[2)] sowie die entsprechende BSI-Kritis-Verordnung, die die Kriterien für die kritischen Systeme und damit die kritischen Betreiber definiert.

IT-Sicherheit – sektorübergreifend und international koordiniert

Überarbeitet wird zurzeit die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie). Sie formuliert auf europäischer Ebene Vorgaben zur Absicherung der IT-Systeme im Zusammenhang mit den kritischen Dienstleistungen. Unter den adressierten Sektoren befinden sich der Finanzsektor, aber eben auch weitere Anbieter digitaler Dienste, wie zum Beispiel Online-Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze, deren Anforderungen sich ebenfalls auf die Dienstleistungen der Banken auswirken könnten.

> „Die Europäische Kommission muss mit ihrer Initiative über den Tellerrand hinausschauen.“

Darüber hinaus wird auch auf globaler Ebene intensiv an dem Thema gearbeitet, zum Beispiel durch das Financial Stability Board im Auftrag der G20, dem Board Of The International Organization Of Securities Commissions (IOSCO) oder der Bank for International Settlements, einem Zusammenschluss von über 70 Nationalbanken.

Die Europäische Kommission muss deshalb mit ihrer Initiative über den Tellerrand hinausschauen. Schließlich wird das

Finanzsystem von global agierenden Cyberkriminellen herausgefordert und bedarf Lösungen, die über die europäischen Grenzen hinaus wirksam sind. Wichtig in diesem Zusammenhang: Die Anforderungen außereuropäischer Regulatoren folgen dem gleichen Ziel und befinden sich in der Regel auf dem gleichen Maßnahmenniveau. Auf dem Weg, die Cyberwiderstandsfähigkeit des gesamten Finanzsektors global zu stärken, könnten wir deshalb einen deutlichen Schritt nach vorn machen, wenn die internationale Zusammenarbeit weiter intensiviert würde. Diese Chance sollte nicht verpasst werden.

Da Cyberattacken sektorübergreifend erfolgen, müssen in der Diskussion um mögliche Rahmenwerke diverse Interessen berücksichtigt werden – finanzmarktspezifische Themen sind hier nur ein Teil der relevanten Aspekte. Allerdings sollten alle Stakeholder gleichermaßen an der Sicherheit der Systeme interessiert sein, sodass alle am gleichen Strang ziehen und wir auf vernünftige, praxisnahe Lösungen hoffen können.

Die Bundesregierung hat bei verschiedenen Anlässen bestätigt, dass sie ihre EU-Ratspräsidentschaft dazu nutzen will, die Initiative der Kommission voranzutreiben und damit die Cyberwiderstandsfähigkeit Europas zu stärken. Auch wenn die Folgen von Corona und die Maßnahmen zur ökonomischen Wiederbelebung in den kommenden Wochen und Monaten die Agenda beherrschen werden, dürften Fragen der Cybersicherheit weiterhin eine große Aufmerksamkeit erfahren. Das politische Berlin hat vor einigen Jahren selbst schmerzhaft zu spüren bekommen, wie eine mutmaßlich russisch gesteuerte Hackerattacke auf das interne Netzwerk des Deutschen Bundestags zum Abfluss sensibler Daten geführt hat.

Europäisches und globales Handeln notwendig

Die europäische Marschrichtung wird zweifellos auch einen Einfluss darauf haben, wie Fragen der Cybersicherheit auf globaler Ebene adressiert werden. Am Ende bedarf es koordinierter Maßnahmen und der gemeinsamen Bemühungen von Politik, Aufsichtsbehörden, Zentralbanken und der Finanzindustrie.

Dabei sollten auch kollektive Maßnahmen von Regierungen zur Abschreckung böswilliger Cyberaktivitäten, die sich gegen Finanzinstitute richten, geprüft werden. Helfen könnten dabei internationale Normen und diplomatische Prozesse zur Erhöhung der Cyberstabilität, der internationale Aufbau von Kapazitäten für Regierungen und Finanzinstitutionen und die Entwicklung von Maßnahmen, um dem wachsenden Mangel an Arbeitskräften im Bereich der Cybersicherheit zu begegnen.

Fußnoten
1) „Öffentliche Konsultation zu einem Rahmen für die Betriebsstabilität digitaler Systeme im Finanzdienstleistungsbereich: Den Finanzsektor in der EU widerstandsfähiger und sicherer gestalten“: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-
2) Der aktuelle Entwurf erweitert die bisherigen Anforderungen des BSI-Gesetzes zum Schutz der IT-Systeme, die im Finanzsektor für die Zurverfügungstellung der kritischen Versorgungsdienstleistungen Bargeldversorgung und Zahlungsverkehr relevant sind.

Fotos Seite 3: Bankenverband