



Neue aufsichtsrechtliche Anforderungen für Cybersicherheit bei Kredit- und Finanzdienstleistungsinstituten

Cybersicherheits-Vorfälle in der Finanzbranche im Fokus der Aufsicht

Die Aufsichtsbehörden für Kredit- und Finanzdienstleistungsinstitute und die EU Kommission verstärken ihre Bemühungen gegen die Cyberkriminalität.

Die neuen Maßnahmen kommen zu einem Zeitpunkt, zu dem das Thema Cybersicherheit Unternehmen der Finanzindustrie, Politik und Medien bewegt. Anfang September ist bekannt geworden, dass sich Hacker bei der Wirtschaftsauskunftei Equifax Zugriff auf sensible Daten wie Sozialversicherungsnummern, Geburtsdaten und Kreditkartennummern von 143 Millionen Kunden aus den USA, Kanada und UK verschafft haben. Am 20.09. hat die U.S. Börsenaufsicht SEC nunmehr bekannt gemacht, Angriff eines schwerwiegenden Hackerangriffs auf eine sensible Datenbank geworden zu sein ([SEC Statement vom 20.09.2017](#)). Dieser Vorfall hat sich bereits vergangenes Jahr ereignet, die SEC habe jedoch erst im August dieses Jahres erfahren, dass der Angriff illegale Börsengeschäfte wie Insiderhandel ermöglicht haben kann.

Die Bankaufsichtsbehörden in Deutschland und die EU Kommission haben das Thema Cybersicherheit seit letzter Woche verstärkt im Fokus (siehe zu Maßnahmen von Bundesbank, EZB und US-Banken auch unseren [Newsletter vom 23.06.2017](#)).

Maßnahmen von Aufsicht und EU Kommission

Die EZB hatte bereits am 19.06 verkündet, in diesem Sommer für von der EZB beaufsichtigte Kreditinstitute eine Berichtspflicht über Cybersicherheits-Vorfälle einzuführen ([EZB Statement vom 19.06.2017](#)).

Nunmehr hat die BaFin hat am 14./15.09 zwei unterschiedlichen Maßnahmen verkündet:

- Meldepflicht und neues Meldeverfahren bei Sicherheitsvorfällen: Am 14.09. hat die BaFin angekündigt, für Zahlungsdienstleister ein elektronisches Meldeverfahren für schwerwiegende Betriebs- und Sicherheitsvorfälle einzuführen. Das neue Meldeverfahren ersetzt den bisherigen Meldeweg über E-Mail. Es beruht auf der Melde- und Veröffentlichungsplattform (MVP) der BaFin und soll zeitgleich mit dem neuen Zahlungsdiensteaufsichtsgesetz zum 13.01.2018 in Betrieb gehen. Um Zahlungssicherheitsvorfälle an die BaFin melden zu können, müssen Zahlungsdienstleister oder vom Zahlungsdienstleister beauftragte Dienstleister (1) sich als Nutzer am MVP-Portal der BaFin registrieren und (2) die Freischaltung für das Meldeverfahren „PSD2-Zahlungssicherheitsvorfälle“ beantragen (siehe [BaFin Informationen vom 14.09.2017](#)).
- Zulässigkeit von Lösegeldversicherungen mit Cyberversicherungen: Die BaFin hat angesichts der zunehmenden Cyberkriminalität zudem eine wichtige Entscheidung zu Cyberversicherungen getroffen. Am 15.09. hat die BaFin entschieden, die Bündelung von Lösegeldversicherungen mit Cyberversicherungen in einem Vertrag zu akzeptieren. Solche Versicherungen durften Versicherungsunternehmen bisher nicht anbieten (siehe [BaFin Meldung vom 15.09.2017](#)). Finanzunternehmen dürften damit bald weitere Optionen für die Absicherung gegen Cyberrisiken zur Verfügung stehen.

Die EU Kommission hat ebenfalls am 19.09. Maßnahmen zur Stärkung der Abwehrfähigkeit und Reaktion der EU bei Cyberattacken verkündet. Geplant ist,

- die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) zu stärken,
- einen EU-weiten Rahmen für die Cybersicherheitszertifizierung einzuführen und
- ein Europäisches Forschungs- und Kompetenzzentrum für Cybersicherheit zu gründen.

Zu diesem Zweck plant die EU Kommission auch die Einführung neuer Rechtsvorschriften, u.a. eine neue Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln, um eine effizientere strafrechtliche Verfolgung bei Cyberangriffen zu ermöglichen. Der Vorschlag der Kommission ist bereits bekannt. Änderungen des Richtlinien-Entwurfs im Gesetzgebungsverfahren und durch die Umsetzung in den Mitgliedsstaaten bleiben abzuwarten.

Fazit

Cyber-Security bleibt international das Top-Thema für die Finanzbranche. Aufsichtsbehörden und Gesetzgeber ergreifen stetig neue Maßnahmen zur Stärkung der Cybersicherheit, die Kredit- und Finanzdienstleistungsinstituten adressieren und die von diesen zu implementieren sind.

Bei Fragen stehen wir Ihnen gerne jederzeit zur Verfügung.

Dr. Lars Lensdorf

Tel: +49 (69) 768063-30

Mobile: +49 (160) 90704902

E-Mail: l.lensdorf@heylaw.de

Dr. Moritz Hüsch, LL.M.

Tel: +49 (69) 768063-453

Mobile: +49 (151) 12577724

E-Mail: m.huesch@heylaw.de