GVB Genossenschaftsverband Bayern

ARTIKEL

Interessenvertretung #Onepager 24.05.2024

Standpunkt: EU-Cybersicherheit (DORA)

Banken ausgewogen vor Cyber-Angriffen schützen

Kernforderungen

- Schutz vor Cyber-Angriffen proportional ausgestalten
- Systemisches Gefahrenpotential bei Auflagen berücksichtigen
- IT-Verbünde bei Mehranbieter-Strategie herausnehmen

Worum geht es?

Hintergrund

Der 2023 in Kraft getretene Digital Operational Resiliance Act (DORA) soll dazu dienen, den Finanzsektor in Europa besser vor Cyberrisiken zu schützen. Ab dem 17. Januar 2025 gelten für mehr als 3.600 Unternehmen des Finanzsektors in Deutschland und für über 20.000 Finanzunternehmen in Europa zusätzliche Meldepflichten und IT-Standards. Anlass für die Verordnung ist die wachsende Gefahr, dass unzureichende, bankenindividuell festgelegte IT-Standards im Finanzwesen verheerende Auswirkungen nicht nur auf den Bankensektor, sondern auch auf die Realwirtschaft und damit auf ganze Volkswirtschaften haben. Da es um die Grundlage des täglichen Wirtschaftens und Zusammenlebens geht, sind in einem so sensiblen Bereich besondere Vorsichtsmaßnahmen

geboten, die einen störungsfreien Geschäftsbetrieb garantieren.

Direkt von DORA betroffen sind vor allem Kreditinstitute und Versicherungsunternehmen, aber auch Versicherungsvermittler, Vermögensverwalter, Abschlussprüfer sowie Drittanbieter von Informations- und Kommunikationstechnologien (IKT). Die Beaufsichtigung erfolgt durch die europäischen Aufsichtsbehörden (ESA, European Supervisory Authorities).

Ausgangslage

Die EU plant für Finanzmarktakteure europaweit einheitliche IKT-Mindeststandards, vor allem in Bezug auf das Risikomanagement, einzuführen. Ziel ist es, dadurch die Widerstandsfähigkeit gegen Cyber-Angriffe zu erhöhen. Dies ist im Grundsatz zu begrüßen. Denn aktuell bestehen noch große Ungleichheiten bei den Sicherheitsstandards je nachdem in welchem Land sich ein Finanzunternehmen befindet. Nachdem 2023 die ESA-Konsultationen zu den technischen Standards abgeschlossen wurden, sollen im zweiten Halbjahr 2024 alle Konkretisierungen veröffentlicht werden.

Problem

Die IKT-Anforderungen berücksichtigen weder die Größe einer Bank noch ihr Geschäftsmodell. Diese Faktoren sind jedoch entscheidend, um das damit verbundene Gefahrenpotential für die Finanzstabilität und letztlich auch für die Resilienz ganzer Volkswirtschaften zu quantifizieren. Kleine und mittlere Banken wie Volks- und Raiffeisenbanken würden pauschale Anforderungen somit unverhältnismäßig treffen. Dadurch entstünden Kosten, die unbegründet sind und keinen verhältnismäßigen Mehrwert für die digitale Sicherheit der Banken und des Finanzsystems insgesamt bieten. In der Folge müssten die Kunden unter vermeidbaren Kostensteigerungen leiden. Im äußersten Fall droht die Streichung von Bankleistungen. Hinzu kommt die Verpflichtung, bei der IT-Auslagerung eine Mehranbieter-Strategie zu verfolgen. Dies verursacht vor allem bei Genossenschaftsbanken, die aus Effizienzgründen ihre IT in IT-Verbünde ausgelagert haben, enormen bürokratischen Aufwand. Denn sie müssen die Abhängigkeit von einem oder wenigen Dienstleistern offenlegen und deren Zusammensetzung erläutern.

Lösung

Nachdem DORA beschlossen worden ist sowie die Regulierungs- und Durchführungsstandards weitgehend feststehen, ist die Europäische Bankenaufsicht gefordert, die Vorschriften bürokratiearm und – wie explizit in Art. 4 DORA festgeschrieben – verhältnismäßig auszulegen. Sie müssen auf dem Prinzip der Proportionalität und dem Gefahrenpotential, das von einer Bank für die Finanzstabilität ausgeht, basieren. „One-size-fits-all“-Regulierungen können dementsprechend auf dem so vielfältigen Bankenmarkt grundsätzlich keine befriedigende Lösung darstellen. Es muss daher in der Praxis der Bankenaufsicht Berücksichtigung finden, dass das systemische Risiko von Genossenschaftsbanken erheblich geringer ist als das von international vernetzten Großbanken. Gleichzeitig geht es darum, Meldepflichten auf ein Mindestmaß zu reduzieren. Besonders ist darauf zu achten, dass es gegenüber den Meldestellen nicht zu Doppelabfragen kommt. Bestehende Meldeanforderungen sind deshalb mit neuen Auflagen zusammenzulegen. Zudem sollten diejenigen Banken, die ihre IT in Finanzverbünde ausgelagert haben, von der Mehranbieter-Strategie befreit werden.

Dr. Christian-Friedrich Hamann

Referent Interessenvertretung

Stab Vorstand

+49 (89) 2868-3159

Anlagen

EU-Cybersicherheit (DORA) (185.2 KB)