Stellungnahme

Die Bedeutung des Zusammenspiels von EUCS / NIS / DORA für den Finanzmarkt
29. November 2022

Zusammenfassung

Kevin Hackl
Bereichsleiter Digital Banking & Financial Services

T +49 30 27576-109
k.hackl@bitkom.org

Lukas Marschallek
Referent Digital Banking & Financial Services

T +49 30 27576-551
l.marschallek@bitkom.org

Albrechtstraße 10
10117 Berlin

Der Bitkom verfolgt bereits seit längerem aktiv die Entwicklung des European Cybersecurity Certification Scheme for Cloud Services (EUCS) durch die ENISA. Neben der horizontalen Perspektive haben sich die Mitglieder auch ausführlich zu möglichen Auswirkungen des EUCS auf den Finanzmarkt ausgetauscht. Hierbei ist insbesondere das Zusammenspiel zwischen EUCS, NIS und DORA in den Blick zu nehmen.

Bitkom hat Bedenken betreffend den Anwendungsbereich und insbesondere bezüglich der diskutierten sogenannten „Immunitäts- und Souveränitätsanforderungen“. Denn diese könnten Innovation im Finanzmarkt hemmen und die Ziele der Digital Finance Strategy der Europäischen Kommission vom 24. September 2020, die Digitalisierung im Finanzmarkt voranzutreiben, konterkarieren.[1]

Im September 2021 wurde im Rahmen der ENISA-Prozesse der Vorschlag eingebracht, „immunity to non-EU laws-Anforderungen“ in die Risikoklasse "high" des EUCS aufzunehmen. Der Prozess ist nicht transparent für die Industrie. Unserem Verständnis nach würden diese Anforderungen an die Risikoklasse „high“ des EUCS zwei besondere Bedingungen an das Erbringen von Cloud Diensten stellen: (a) Cloud Service Provider (CSPs) müssten ihre Hauptniederlassung innerhalb der EU haben und (b) das direkte Erbringen von Cloud Diensten durch CSPs würde untersagt werden, wenn deren Unternehmensanteile von Nicht-EU-Staaten kontrolliert werden. Aus finanzspezifischer Perspektive stellt dieser Zugang eine klare Abkehr von den Grundprinzipien von DORA dar: Der Digital Operational Resilience Act formuliert klare Standards und stellt ein „aufsichtliches Zugriffsrecht“ auf Dienstleister aus Nicht-EU-Staaten sicher, ohne Immunitäts- und Souveränitätsanforderungen herbeizuführen.

Artikel 21 der NIS-Richtlinie 2.0 sieht in Verbindung mit Artikel 18 eine mögliche Verpflichtung zur Verwendung von Zertifizierungsschematas wie dem EUCS für “essential entities” & “important entities” im Sinne der NIS 2.0-Richtlinie vor, was das

1 Digital Finance Strategy vom 24.9.2020 der Europäischen Kommission https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0591&from=DE

Prinzip der Freiwilligkeit im CSA aufheben würde. Das Europäische Parlament hat am 10. November dem Gesetzestext der NIS 2.0 Richtlinie zugestimmt. Am 28. November folgte die Zustimmung des EU Rats. Sobald die Richtlinie im Amtsblatt der Europäischen Union veröffentlicht wird, müssen die Mitgliedstaaten die Richtlinie binnen 21 Monate in nationales Recht überführen. In Deutschland wird es dazu zu Anpassungen am BSI Gesetz sowie der Kritis-Verordnung kommen müssen. Es ist außerdem zu erwarten, dass die NIS 2.0 durch ein IT-Sicherheitsgesetz 3.0 in nationales Recht umgesetzt wird.

Es versteht sich von selbst, dass im Falle einer breiten Anwendung des hohen Niveaus die Anforderungen an die vermeintliche Immunität und insbesondere die Anforderungen an die "Hauptniederlassung in der EU" und das "Verbot der Kontrolle ausländischer Beteiligungen" die Freiheit des Finanzmarkts in der EU, mit Lieferanten ihrer Wahl zusammenzuarbeiten, stark beeinträchtigen würden.

Zu diesem Ergebnis ist man bereits in den Verhandlungen rund um DORA gekommen. Hier hat man bewusst wieder Abstand von etwaigen „Immunitäts- oder Souveränitätsanforderungen“ für kritische IKT-Drittanbieter genommen. Ein möglicher Verweis darauf, dass EUCS für den Finanzmarkt keine Rolle spiele, weil DORA im Verhältnis zu NIS lex specialis sei, greift zu kurz. Die Wertschöpfungsketten des Finanzmarkts sind komplex. Es ist bis heute nicht abzusehen wie viel Teile dieser Wertschöpfungskette von DORA abgedeckt sind. Teile, die nicht von DORA abgedeckt werden würden, könnten damit weiterhin in den Anwendungsbereich von NIS und damit dem EUCS unterfallen. Zusätzlich ist nicht ausgeschlossen, dass die Nutzung zertifizierter Clouddienste über zukünftige Regularien (sowohl horizontal als auch sektorspezifisch) verpflichtend wird.

Das Finance-Vertical des Bitkom würde daher einen Austausch in einem geeigneten Format zum Zusammenspiel von insbesondere EUCS, NIS sowie DORA begrüßen.

Perspektive Finanzen: Zusammenspiel von EUCS / NIS / DORA

Grundsätzlich begrüßt der Bitkom im Sinne des Abbaus einer Markt-Fragmentierung EU-einheitliche Zertifizierungs-Scheme. Das von der ENISA auszuarbeitende EUCS enthält jedoch in seiner derzeitig Form Immunitäts- und Souveränitätsanforderungen durch die (potenzielle) Risiken für die Digital- und Finanzwirtschaft entstehen.

Die Auswirkungen von Lokalisierungsanforderungen (Haupt-)Standorts von CSPs und ihrer Anteilseigner sowie des Ortes, an dem ihre Daten gespeichert oder verarbeitet werden als verpflichtende Grundvoraussetzung einer Zertifizierung für die Risikoklasse „high“ sind derzeit außerordentlich unklar. Dazu trägt insbesondere bei, dass noch unklar ist, welche Anwendungsfelder im Rahmen von (regulatorischen) Anforderungen

unter welche Sicherheitssniveaus/-levels fallen und wie dieser Prozess der Klassifizierung und Einordnung konkret gestaltet werden soll. Es ist lediglich eindeutig, dass die Aufnahme solcher Anforderungen bedeuten würde, dass bestimmte CSPs keine Zertifizierung für die Sicherheitsstufe "hoch" erhalten könnten.

Für den Finanzsektor gilt mit der DORA eine Ausnahmesituation: Durch DORA wurde eine sektorspezifische Lösung für Cyber-Resilienz und IT-Sicherheit innerhalb Europas geschaffen. Ein möglicher Verweis darauf, dass EUCS für den Finanzmarkt keine Rolle spiele, weil DORA im Verhältnis zu NIS lex specialis sei, greift jedoch zu kurz. Es ist bis heute nicht abzusehen wie viel Teile dieser Wertschöpfungskette von DORA abgedeckt sind. Teile, die nicht von DORA abgedeckt werden würden, könnten damit weiterhin in den Anwendungsbereich von NIS und damit dem EUCS unterfallen.

Unklar bleibt also inwiefern EUCS für den Finanzbereich greifen würde, entweder über (a) gesetzliche Regelungen oder (b) Marktrealitäten: Tritt horizontal ein EUCS in Kraft, ist die Wahrscheinlichkeit nicht gering, dass dieses auch für Finanzdienstleister herangezogen wird (selbst wenn DORA dies nicht fordert).

Der Bitkom sieht unter anderem folgende Risiken:

- Reduzierung des Cloud-Dienste-Angebots (durch reduzierte Zahl an CSPs)
- Steigende Kosten (Angebot und Nachfrage)
- Potenzielles Konzentrationsrisiko durch vermindertes Angebot
- Gemindertes technisches Sicherheitsniveau

Grundsätzlich besteht der Eindruck, dass die Anforderungen nicht ausschließlich technische Sicherheit verbessern, sondern auch durch das politische Ziel der „Digitalen Souveränität“ getrieben sind. Mit einer solchen Vermischung der technischen und politischen Ebene gehen für den Bitkom grundsätzlich große Unwägbarkeiten einher, die dem Ziel einer schnellen Digitalisierung und Cloudifizierung von Infrastrukturen, Produkten und Services zuwiderlaufen.

Während das politische Ziel gesteigerter Souveränität grundsätzlich zu begrüßen ist[2], gilt es sicherzustellen, dass nicht das Gegenteil bewirkt wird. Eine Verknappung von Cloud-Diensten durch Immunitäts-Anforderungen könnte sektorale Anwender (wie Finanzdienstleister) und damit den Standort in Summe schwächen. Dies hängt unter andrem damit zusammen, dass der Zugang zu den besten Technologien erschwert wäre und damit die operative und Cyber-Resilienz der EU-Kooperationspartner, aber auch die Wettbewerbsfähigkeit unserer Tätigkeiten in der EU untergraben werden könnte.

Auf Basis des bisherigen Entstehungsprozesses der Zertifizierungs-Schemes und des unklaren Zusammenspiels von EUCS / NIS / DORA kann die Finanzindustrie die Auswirkungen des EUCS derzeit nicht klar bewerten, weil sie bezüglich der möglichen

2 Bereits im Jahr 2015 hat der Bitkom eine Position zur Digitalen Souveränität veröffentlicht, die in weiten Teilen noch heute Relevanz hat: https://www.bitkom.org/sites/main/files/2020-01/200116_stellungnahme_digitale-souveranitat.pdf

Immunitäts-/Souveränitäts-anforderungen nicht konkret eingebunden ist und den aktuellen Sachstand der Debatte kaum nachvollziehen kann. Insbesondere Sektoren mit hoher Clouddurchdringung, z.B. Finanzbereich, brauchen Klarheit und Planungssicherheit. Viele der im Bitkom organisierten Unternehmen haben mittlerweile ihre Bedenken geäußert. Entsprechend gilt es die Entscheidungsprozesse innerhalb der ECCG transparenter zu machen und Stakeholder aus relevanten Verticals miteinzubeziehen. Ein strukturierter Dialog mit potenziell betroffenen Anbietern von Cloud-Diensten und potenziell betroffenen Kunden oder eine Risikofolgeabschätzung hat unseres Wissens nach bisher nicht stattgefunden.

Das Finance-Vertical des Bitkom würde es daher begrüßen, wenn ein geeignetes Format gefunden wird, dass eine wirtschaftspolitische Diskussion dieser Aspekte für die digitale Finanzwirtschaft zulässt, die der strategischen Relevanz dieser miteinander verknüpften Fragestellungen gerecht wird. Dabei sollte die weitere Entwicklung eines Zertifizierungs-Scheme unter Einbezug relevanter Stakeholder aus dem Finanzbereich (Ministerien, inbes. BMF, NCAs (Bundesbank & BaFin) & Markteilnehmern) stattfinden. Im Zentrum sollten dabei folgende Punkte diskutiert werden:

- Potenzielle Risiken für Nutzer und Anbieter von Cloud-Diensten und damit verbunden mögliche sektorale und gesamtwirtschaftliche Auswirkungen.
- Das Zusammenspiel und potenzielle Wechselwirkungen des EUCS, der NIS-Richtline 2.0, DORA und der Critical Entities Regulation, insbesondere im Rahmen der nationalen Umsetzung der NIS-Richtlinie 2.0 mit ihrer höchstwahrscheinlich großflächigen Ausweitung des Geltungsbereichs und Zertifizierungspflicht.

Die Ziele eines solchen Austausches sollten dabei sein:

- Transparenz darüber, welche Anwendungsfelder im Rahmen von (regulatorischen) Anforderungen unter welche Sicherheitsniveaus/-levels fallen.
- Klärung potenzieller Standortnachteile: Die potenzielle Schwächung des deutschen und europäischen Standortes, die Gefahr eines Kapazitäten-Engpasses an Cloud-Dienstleistern.
- Die Klärung von Souveränitätsfragen im Rahmen der jetzigen Marktrealitäten, bzw. die Schaffung von Anreizen zur Förderung der EU als Investitions- und Innovationsstandort.