Positionspapier

Juni 2025

Für praxisnahe IT-Anforderungen an Sicherheit und Resilienz!

Anpassungen regulatorischer Rahmenbedingungen für IT-Resilienz sind notwendig.

Am 17. Januar 2025 trat der Digital Operational Resilience Act (DORA) in Kraft – ein Meilenstein für die Cybersicherheit im Finanzsektor. Gemeinsam mit dem Cyber Resilience Act (CRA) und der Network and Information Systems Directive (NIS 2) soll DORA einen regulatorischen Rahmen für Finanzinstitute bilden, um die digitale Resilienz aufzubauen und Cyberbedrohungen effektiv zu begegnen. CRA, DORA und NIS 2 greifen dabei im besten Fall ineinander und fordern von Banken ein hohes Maß an Anpassungsfähigkeit und Voraussicht, allerdings auch viele formale Aktivitäten, die erhebliche Ressourcen in den Instituten binden. Obgleich der generelle Ansatz gut ist, sind wichtige Anpassungen notwendig, um sich auf die wirklich notwendigen Elemente zu konzentrieren und Raum für Innovationen zu lassen. Letztlich ist dies auch im weltweiten Wettbewerb in der Finanzwirtschaft sowie auch zwischen Standorten und Märkten notwendig.

Die gleichzeitige Umsetzung von CRA, DORA und NIS 2 stellt Banken zusätzlich auch vor die Aufgabe, ihre internen Prozesse, IT-Infrastrukturen und Risikomanagementsysteme grundlegend zu überarbeiten. Neben vielen wichtigen Notwendigkeiten wird das Ziel bei einigen Anforderungen überschritten. Für viele Institute ist es zudem herausfordernd, die neuen Vorgaben proportional umzusetzen, ohne ihre Ressourcen zu überlasten und das eigentliche Bankgeschäft in den Mittelpunkt zu stellen.
Eine Verschlankung der regulatorischen Anforderungen ist offensichtlich notwendig! Wir regen daher an, die geltenden Regelwerke auf den generellen Prüfstand zu stellen und bis zum Abschluss der Überprüfung keine neuen Regelwerke hinzuzufügen. Vielmehr sollten wir uns in dieser Übergangsphase unter dem Aspekt „less is more“ gesetzlich und aufsichtlich auf das Nötigste beschränken und so Vertrauen zurückgeben und echte Entlastung herbeiführen.

Neben den regulatorischen Anforderungen sind weiteren Rahmenbedingungen entscheidend. Dazu zählt nicht zuletzt die mögliche unkomplizierte und so wenig wie möglich reglementierte Nutzung von Cloud- und KI-Innovationen im operativen Geschäft.

Darüber hinaus sehen wir die Notwendigkeit allgemeiner Verbesserungen von Gesetzgebungsverfahren direkt durch den Gesetzgeber sowie auch in Bezug auf delegierte Rechtsakte. Die wichtigsten Aspekte haben wir den fachlichen Positionen in diesem Dokument vorangestellt.

Bundesverband Öffentlicher Banken Deutschlands, VÖB, e.V.
Lennéstraße 11, 10785 Berlin
www.voeb.de

A. Generelle Änderungsnotwendigkeiten

1. „Grundanforderungen an Rechtsakte: Eindeutigkeit, rechtzeitige Finalisierung, Mandatswahrung“

→ Überprüfung aller IT-bezogenen Gesetze und bestehenden delegierten Rechtsakte auf Notwendigkeit und für die konkrete Praxis und Aufsicht tatsächlich erforderliche Aspekte sowie Parallelregelungen – auch unter Berücksichtigung einer Aufwand-Nutzen-Betrachtung für die betroffenen Finanzinstitute. Streichung nicht notwendiger Elemente in einem Omnibus-Gesetz. Differenzierung der Anforderungen nach systemisch wichtigen Instituten und anderen mit deutlichen Entlastungen für letztere.

→ Aussetzung ergänzender Regulierung und Fokussierung auf die Harmonisierung zwischen den bestehenden Gesetzen und Rechtsakten und Review der bestehenden Gesetze nach Durchführung von Effizienzanpassungen (siehe Punkt zuvor).

→ Primärrechtsakte: Wenige, dafür klare, eindeutige und konkrete Vorgaben, die eine zielgerichtete Umsetzung ermöglichen, einschließlich etwaiger, konkreter Erwartungen und Beschreibung des Rahmens für delegierte Rechtsakte. Benennung einer konkreten Umsetzungsfrist bereits im jeweiligen Gesetz, wieviel Zeit für die Umsetzung den Marktbeteiligten nach Fertigstellung der delegierten Rechtsake eingeräumt wird. Das zumeist praktizierte Vorgehen einer Umsetzungsfristnennung inklusive der Erarbeitung der delegierten Rechtsakte verkürzt defacto die Umsetzungszeit für den Markt, da die finale Freigabe von delegierten Rechtsakten der ESAs (EBA, ESAM EIOPA) bspw. durch die Europäische Kommission teilweise zeitlich erheblich später nach der Entwurfsfertigstellung erfolgt. Teilweise verzögert sich diese dann noch weiter, wenn weitere Änderungen vorgeschlagen werden.

→ Sekundärrechtsakte: Rechtzeitige, mandatsgetreue Finalisierung zur Erfüllung der Gesetzesvorgaben unbedingt notwendiger Regelungen. Kopplung des Inkrafttretens wie zuvor erwähnt an ihre vollständige Fertigstellung sowie Start der Umsetzungszeit für den Markt ab diesem Zeitpunkt und formaler Freigabe des jeweiligen Rechtsaktes (bspw. durch die Kommission über die Veröffentlichung im EU-Amtsblatt).

2. Kommunikative Blackboxes eindämmen

→ Bidirektionale Kommunikation: Standardisiert, idealerweise über eine gemeinsame EU-weite Plattform zur aggregierten Auswertung, d. h. Rückmeldungen und Auswertungen bspw. aus Meldeverpflichtungen, die Mehrwerte für den Markt bieten können, und

→ Transparente Rückkopplung der individuellen Analyseergebnisse an die Verpflichteten, um gezielte Verbesserungen und Anpassungen zu ermöglichen (einschließlich der Details bei der Prüfung, sofern Drittdienstleister durch die Aufsicht direkt adressiert werden)

3. Dokumentation nicht als Selbstzweck: Wirkung statt Nachweiskultur

→ Dokumentation und die Anforderungen an die schriftlich fixierte Ordnung (sfO) darf generell kein Selbstzweck sein – entscheidend ist, dass sie die Wirkung und Wirksamkeit der Maßnahmen nachvollziehbar macht, nicht bloß deren Vollständigkeit.

→ Das gilt insbesondere für DORA, aber auch für andere Regelwerke, in denen durch hohe Dokumentationsanforderung ein Scheinwirkweise transportiert wird.

B. Fachliche Positionen

1. Harmonisierung und Abbau von Mehrfachregulierung

→ Vermeidung von Mehrfachregulierung von Finanzdienstleistern in der IT-Regulierung durch Harmonisierung von DORA, NIS2 und CRA

→ Vereinheitlichung und Vereinfachung der Auslagerungs- und Informationsregister auf kritische oder wichtige Funktionen (Harmonisierung EBA-Leitlinien mit DORA)

→ Perspektivische, zielgerichtete Umstellung des bankenaufsichtlichen Berichts- und Meldewesens auf Basis von Datenabrufen der Aufsicht und standardisierter Datenbereitstellung durch Banken in geeigneten Intervallen (beispielhaft, aber nicht beschränkt auf) iReF-Einführung über anzupassendes BiRD-Datenmodell– Details noch zu klären)

2. Verhältnismäßigkeit als gelebte Praxis

→ Dezidierte und praxisnahe Anwendung der Verhältnismäßigkeit bei Berücksichtigung von Größe und Geschäftstätigkeit im Rahmen des umfassenden IKT-Risikomanagements, Gestaltungsraum für die Institute und Vermeidung eines Pauschalansatzes. Herleitung, Nachvollziehbarkeit und Niederlegung in der schriftlich fixierten Ordnung sind dabei Grundlage.

→ Ausklammern von kleineren Instituten vom vollen DORA-Rahmen (keine Kleinstunternehmen). Berücksichtigung des in DORA angelegten vereinfachten IKT-Risikomanagementrahmens (Art. 26 Abs 1 DORA) für den Großteil kleinerer Finanzinstitute ohne Retail-Geschäft und wesentlicher Bedeutung für die Finanzwirtschaft insgesamt. Zudem ist die Durchführung eines verpflichtenden Threat-led Penetration Testings (TLPT) außer für die signifikanten Geschäftsbanken für andere als genereller Standard entbehrlich. Auch DORA sieht ohnehin umfassende interne Prüf- und Kontrollsysteme vor, inkl. der Durchführung von PEN-Tests etc. Bei großen Verbundrechenzentren wären zudem regelmäßige Standard-TLPT mit einem oder wenigen Beispielinstituten ausreichend.

→ Verhältnismäßigkeit des zu erstellenden internen Testregimes, angepasst auf die Finanzdienstleistungen und das Risikoprofil.

→ Entbindung von Instituten mit geringem Sicherheitsrisiko, z.B. solche, die kein Retailgeschäft betreiben, von Meldeverpflichtungen an Wochenenden und Feiertagen, die letztlich auch nicht an Wochenenden ausgewertet werden.

3. Effizienz im IKT-Drittparteienmanagement

→ Erleichterte Audits von IKT-Drittdienstleistern und Hyperscalern durch die Interne Revision. Reine Durchführung durch Dritte ohne direkte Einbindung von Institutsvertretern nach den Anforderungen der Institute, auch in Pools, generell ermöglichen – enges Reporting vorausgesetzt.

→ Verzicht auf die verpflichtende Durchführung von Audits für Standarddienstleistungen wie Office 365/Azure, Standard Cloud Storage etc. Ausschließliche Nutzung von Informationen und Bestätigungen der europäischen Aufsichtsbehörden im Rahmen der Oversight-Prozesse für kritische Dienstleister i. S. von DORA (CTPP – Critical Third-Party Providers) oder von SOC2-Zertifikaten (o.ä.) der Anbieter durch Finanzinstitute; Bereitstellung bzw. Ermöglichen der Referenz auf die durchgeführten Überwachungsmaßnahmen.

→ Angemessene Berücksichtigung von Zertifikaten, wo sie zielführend sind, bzw. mangelnde Verpflichtung von Zertifikaten für sicherheitskritische Hard- und Softwarekomponenten

4. Praktikable Sicherheitsstandards und Technologieanforderungen

- → Realistische Umsetzungsstandards bei neuen Sicherheitsarchitekturen wie Cloud-Diensten und Verschlüsselungstechnologien, d.h. Berücksichtigung internationaler Standards wie ISO 27001, Cobit oder für kleinere Häuser auch IT-Grundschutz gemäß BSI. Vollständige Anerkennung bei externer, autorisierter und regelmäßiger Re-Zertifizierung in geeigneten Intervallen unter Einbeziehung von wesentlichen IKT-Drittdienstleistern in Ergänzung zu deren Berichten (insbesondere SOC 2).
- → Schrittweise, langfristig fokussierte, praxisnahe Einführung einer ZeroTrust-Infrastruktur bei Finanzdienstleistern nach dem tatsächlichen Notwendigkeitsprinzip. Schriftliche Fixierung von anderem Vorgehen, wie bspw. bestimmten Segmentierungsmodellen oder der Einführung von Alternativmaßnahmen nur für kritische oder wichtige Funktionen (DORA). Generell müssen längere Übergangsfristen gewährt werden. Die derzeitige Anforderung der Verschlüsselung von „data in use“ ist eher noch ein akademischer Ansatz. Perspektivisch wird anerkannt, dass die Sicherheit an den nutzenden Identitäten hängen muss und Infrastruktur nicht frei zugänglich nach Login ins Netzwerk erfolgen darf; konkreter Proportionalitätsbezug notwendig, um immensen Aufwand in der Breite zu vermeiden; über neue Bedrohungsszenarien und Anpassungen an Sicherheitsmechanismen kommen diese Sicherheitsstandards („by design“) ohnehin bei den Instituten zum Tragen
- → Etablierung einheitlicher Zertifizierungen für Standarddienstleistungen großer IKT-Dienstleister zur Verbesserung der IT-Resilienz
- → Zertifizierung von Cloudanbietern nach EUCS als Freistellung von Auditpflichten für Standardleistungen
- → Erleichterter Zugang zu Sicherheitsdienstleistern ohne verpflichtende Zertifizierungen i.S.d. CSA insbesondere für Institute mit geringem Sicherheitsrisiko

5. Erleichterung interner Prüf- und Kontrollmechanismen

- → Erleichterte interne Prüf- und Kontrollmechanismen, z.B. PEN-Tests für Eigen- und Drittsoftware, Akzeptanz alternativer Prüfverfahren z.B. bei Quellcode-Analysen
- → Reduzierter risikoorientierter Testrahmen, z.B. nach Kritikalität der Systeme abgestufte Testtiefe unter Flexibilisierung der Testhäufigkeit unter Verknüpfung an Ereignisse wie wesentliche Änderungen, schwerwiegender Vorfälle oder externe Bedrohungslage

Zu A. Generelle Änderungsnotwendigkeiten

Status / Hintergrund

Obwohl DORA eine angemessene Umsetzungsfrist vorsah, wurde die Umsetzung durch die Institute erheblich erschwert. Dies lag insbesondere an den weit gefassten und offenen Formulierungen, etwa im Bereich des IKT-Risikomanagementrahmens, den Vertragsanpassungen, den Meldepflichten und den Tests. Diese erforderten zwingend eine Konkretisierung durch 2nd-Level-Rechtsakte. Die Fertigstellung dieser Rechtsakte verzögerte sich in einigen Fällen – wie beispielsweise beim RTS-SUB und beim ITS/RTS für das Informationsregister – bis über das Inkrafttreten von DORA hinaus. Infolgedessen mussten die Institute ihre Implementierung auf Grundlage der vorläufigen Entwürfe erneut anpassen, was zusätzliche Ressourcen in Anspruch nahm. Die Korrektur von Mandatsüberschreitungen, wie sie beim RTS-SUB durch die Europäische Kommission erfolgte, wurde grundsätzlich positiv aufgenommen. Sie verdeutlicht jedoch das zugrunde liegende Problem: Der Primärrechtsakt war nicht ausreichend präzise formuliert, sodass die für die Konkretisierung zuständigen Behörden keine klaren Mandatsgrenzen hatten und vermutlich personell mit der Vielzahl an erforderlichen Rechtsakten an ihre Kapazitätsgrenzen stießen.

Dieses Phänomen lässt sich auch in anderen komplexen Regelwerken beobachten. Häufig setzt sich das Problem auch auf die Aufsichtsebene fort, da Prüfungen zusätzliche subjektive, anwendungsbezogene Aspekte einbeziehen, die gegebenenfalls zu einer Verschärfung der Vorgaben führen. In der Regel fehlt eine übergreifende, transparente Kommunikation der Prüfungsergebnisse, sodass sich die Institute nicht auf eine standardisierte Prüfungspraxis einstellen und vorbereiten können.

Zusätzlich stellte DORA hohe Berichtsanforderungen an verschiedene Behörden. Die Informationswege unterscheiden sich von Mitgliedstaat zu Mitgliedstaat, und es existiert keine übergreifende digitale Plattform. Zudem bleibt unklar, ob und welche Analysen durchgeführt wurden. Aggregierte Auswertungen sowie eine transparente Rückkopplung der Ergebnisse an die Verpflichteten sind nicht durchgehend bekannt.

Hinzu kommen sehr hohe Dokumentenanforderungen an sich mit dem Ziel des Nachweises der Resilienz, die häufig aber nur auf einer formalen Ebene existieren (u.a. Durchführung von Tests, rechtzeitige Meldung von Vorfällen, Vorhandensein eines IKT-Risikomanagementrahmens).

Forderung / Änderungsnotwendigkeit

Unter dem Eindruck von DORA und anderen großen Regelwerken fordern wir klare Primärrechtsakte, die praxisnah die Mindestanforderungen für eine rechtssichere Implementierung darlegen, sodass die Umsetzung unmittelbar auf Grundlage dieser Primärrechtsakte beginnen kann. Darüber hinaus regen wir an, dass die voraussichtlich zu reduzierenden 2nd-Level-Rechtsakte rechtzeitig finalisiert werden, damit sie vor Inkrafttreten des Primärrechtsaktes zur verfeinerten Umsetzung genutzt werden können. Alternativ sollte das Inkrafttreten des Primärrechtsaktes an die Fertigstellung der 2nd-Level-Rechtsakte angepasst werden.

Im Rahmen der aufsichtlichen Prüfung erwarten wir, dass übergeordnete Ergebnisse im Sinne einer transparenten und planbaren Prüfungspraxis übermittelt werden.

Mit Blick auf die bidirektionale Kommunikation zwischen Behörden und Verpflichteten wünschen wir uns eine digitale, standardisierte Austauschplattform. Diese sollte es ermöglichen, dass Informationen von den Finanzinstituten über einen einzigen Kanal bereitgestellt, ausgewertet und aggregiert zurückgespielt werden. Auf diese Weise kann dem Eindruck eines Blackbox-Effekts entgegengewirkt werden, dass nur einseitig Informationen gesammelt werden.

Daher ist es uns wichtig, dass Dokumentation nicht zum Selbstzweck verkommt, sondern vielmehr tatsächliche Wirkung dokumentiert, um nicht zur bloßen „Papierresilienz“ zu verkümmern, die keine Aussagekraft über den tatsächlichen Stand des Resilienzgrades eines Instituts hat.

Fazit

Zusammenfassend fordern wir klare und praxisnahe Primärrechtsakte sowie rechtzeitig finalisierte 2nd-Level-Rechtsakte, um eine rechtssichere Umsetzung und eine transparente, planbare Prüfungspraxis zu gewährleisten. Zudem sollte eine digitale, standardisierte Austauschplattform etabliert werden, um einen bidirektionalen Informationsfluss zwischen Behörden und Verpflichteten und gegenseitige Verbesserungen zu fördern. Der Informationsfluss sollte sich auf Wirksamkeit von Maßnahmen fokussieren und nicht auf bloße Tätigkeitsnachweise.

Zu B. Fachliche Positionen

1. Vermeidung von Mehrfachregulierung von Finanzdienstleistern in der IT-Regulierung

Status / Hintergrund

Die Digital Operational Resilience Act (DORA) trat am 17. Januar 2025 in Kraft und gilt als sektorspezifischer Rechtsakt für Finanzunternehmen, wodurch er Vorrang vor der NIS2-Richtlinie hat. Der Cyber Resilience Act (CRA) ist am 10. Dezember 2024 in Kraft getreten und wird ab dem 11. Dezember 2027 vollumfänglich verbindlich angewendet. Obwohl DORA, NIS2 und CRA unterschiedliche Schwerpunkte haben, gibt es Überschneidungen, die zu Mehrfachregulierungen führen können. Diese betreffen vor allem Anforderungen an das IKT-Risikomanagement, Meldepflichten für Sicherheitsvorfälle und Vorgaben zur Resilienz von IT-Systemen. Während DORA spezifische Anforderungen für Finanzinstitute regelt, adressiert NIS2 branchenübergreifend kritische Infrastrukturen, was zu parallelen Berichtspflichten und Sicherheitsvorgaben führen kann. In Deutschland beispielsweise werden durch zusätzliche Registrierung sowie Benennung einer Kontaktstelle ggü. dem BSI weitergehende Anforderungen gestellt, die den integrierten Ansatz teilweise aushebeln.

Der CRA ergänzt diese Regelwerke, indem er Produkt- und Softwaresicherheitsanforderungen entlang der gesamten Lieferkette festlegt, wodurch Doppelprüfungen bei der Bewertung von IT-Dienstleistern und Technologien entstehen können.

Diese Gemengelage setzt sich auch administrativ, dass es allein in der Finanzindustrie mit dem Auslagerungsregister und dem Informationsregister verschiedene Register gibt, die auch vor dem Hintergrund der IT-Resilienz jeweils dasselbe Ziel verfolgen, nämlich ein verbessertes Risikomanagement und die Erhöhung der Transparenz auch über IKT-Dienstleister. Daher fordern wir eine Vereinheitlichung nach dem Prinzip des minimalsten Aufwands unter Berücksichtigung der wirklich notwendigen Informationen. Es ist uns wichtig, dass keine Maximaldatenforderung bei der Zusammenführung der beiden Register im Zuge der Überarbeitung der EBA-Leitlinien für Auslagerungen umgesetzt werden.

Überlagert werden diese Anforderungen von der Cloud-Regulierung, die aktuell auch im geopolitischen Spannungsfeld zu betrachten ist. Wir werden daher aktiv an einer europäischen Cloud-Regulierung mitarbeiten, die auch die Bedürfnisse der Finanzindustrie nach Flexibilität, Effizienz und Sicherheit abbildet. Im Rahmen der anstehenden Anpassung der EBA-Cloud-Leitlinie werden wir uns für einheitliche und harmonisierte Anforderungen für die Nutzung von Cloud-Diensten einsetzen. Eine zentrale Position ist daher, dass Harmonisierung nicht zu einer Überregulierung führen darf, die Innovation behindert oder den Zugang zu marktüblichen Cloud-Diensten einschränkt. Vor dem Hintergrund bedarf es standardisierter Zulassungsverfahren für Cloud-Anbieter.

Dies hat auch Folgen unter dem Aspekt Zertifizierung. Mit dem CSA wurde ursprünglich die Rolle der Europäischen Cybersicherheitsagentur ENISA gestärkt, indem ihr ein dauerhaftes Mandat und zentrale Aufgaben zur Unterstützung der Mitgliedstaaten bei Cybersicherheitsfragen übertragen wurden. Die Verordnung schaffte zudem einen europäischen Rahmen für die freiwillige Zertifizierung der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen, um Fragmentierung zu

vermeiden. Dadurch soll das Vertrauen in digitale Produkte und Dienstleistungen gestärkt und der europäische Binnenmarkt unterstützt werden.

Forderung / Änderungsnotwendigkeit

Eine wirksame IT-Regulierung für Finanzdienstleister erfordert die Vermeidung von Doppelbelastungen durch parallele Vorgaben aus unterschiedlichen Regelwerken. Die Harmonisierung von DORA, NIS2 und CRA ist entscheidend, um Mehrfachregulierungen zu verhindern und klare, konsistente Anforderungen zu schaffen. Finanzdienstleister, die bereits durch DORA umfassenden Vorgaben zur IT-Resilienz unterliegen, sollten nicht zusätzlich durch die Regelungen der NIS2 oder CRA belastet werden. DORA, NIS2, CRA und FinmadiG verlangen z.B. jeweils die Meldung schwerwiegender IKT-Vorfälle – teils mit unterschiedlichen Fristen, Formaten und Empfängern (z. B. EZB/EBA, BSI, Landesaufsicht). Bei NIS2 betrifft dies vor allem die zusätzliche Registrierung und Benennung einer Kontaktstelle. Hier setzen wir uns dafür ein, dass in Deutschland kein Goldplating in der nationalen Umsetzung erfolgt und die zusätzliche Registrierung und Benennung einer Kontaktstelle abgeschafft werden. Beim CRA streben wir an, dass Finanzunternehmen gemäß Art. 2 Abs. 5 b) über die Vergleichbarkeit der Regelung in DORA aus dem Regelwerk herausgenommen werden, da mit DORA als sektorspezifischer Vorschrift dasselbe Schutzniveau erreicht wird.

Vor dem Hintergrund sind auch in einem ersten Schritt das Informations- und das Auslagerungsregister zügig zu vereinheitlichen. Einheitliche Register könnten die Meldestrukturen deutlich vereinfachen, indem sie redundante Berichterstattungen an verschiedene Stellen vermeiden und somit den administrativen Aufwand reduzieren. Wir sehen hier erste gute Ansätze, um Doppelungen und damit überbordende Bürokratie zu vermeiden. Hier wünschen wir uns eine sehr kurzfristige Klärung, wie sich über ein gemeinsames Register der eigentlichen Zielsetzung eines transparenten Überblicks über Konzentrationsrisiken nachkommen lässt.

Perspektivisch streben wir eine zielgerichtete Umstellung des bankenaufsichtlichen Berichts- und Meldewesens auch für Anforderungen aus DORA oder aufsichtliche EZB- bzw. BaFin Anforderungen auf Basis von Datenabrufen der Aufsicht und standardisierter Datenbereitstellung durch Banken (bspw. nach iReF-Einführung über anzupassendes BIRD-Datenmodell) an.

Die Europäische Cloud-Industrie ist derzeit nicht global wettbewerbsfähig. Die bisherigen Lösungsinitiativen (AI Factories, IPCEI Cloud – bedeutende Projekte von gesamteuropäischen Interesse, Data Act, Energy Efficiency Initiative) tragen aus unserer Sicht nur bedingt zum Hochlauf europäischer Lösungen bei.

Um sicherzustellen, dass hochkritische Anwendungsfälle in einer europäischen Cloud betrieben werden können, müssen die europäischen Cloud-Anbieter deutliche und zeitnahe Sprünge bei Leistung, Diensten und fertigen SaaS- und PaaS-Produkten vollziehen. Solange die globalen Hyperscaler deutlich vorne liegen, werden tendenziell auch die Use Cases bei ihnen betrieben.

Es ist entscheidend, europäische Public Cloud-Anbieter gezielt zu fördern und Schulungen entlang der gesamten Lieferkette durchzuführen. Dazu müssen Cloud- und KI-Themen in Schulungsorganisationen wie Universitäten deutlich hervorgehoben werden. Dies umfasst die Infrastruktur

für Cloud, Sicherheit der Cloud, Virtualisierungsdienste und die Entwicklung neuer Dienste und Produkte. Weiterhin müssen globale Fachkräfte angelockt werden.

Keinesfalls sollte die Nutzung von globalen Hyperscalern beschränkt werden, solange keine EU-eigenen Lösungen verfügbar sind. Dadurch würde per heutigem Stand eher die Gefahr bestehen, dass die EU noch stärker ins Hintertreffen gerät. Es ist zudem zu unterstreichen, dass praktisch alle für den Wirtschafstandort relevanten KI-Lösungen in der Cloud Betrieben werden. Investitionen in die Cloud sind folglich Bedingung für Innovationen durch KI und die Weiterentwicklung von KI.

Vor dem Hintergrund ist es essentiell, dass im Rahmen des Reviews des Cyber Security Act (CSA) das Spannungsfeld zwischen Sicherheit und Innovation angemessen und risikoorientiert gelöst wird. So ist es wichtig, dass es keine europäische Zertifizierungspflicht gerade für sicher für sicherheitskritische Hard- und Softwarekomponenten gibt. Diese könnte dazu führen, dass die marktführenden Produkte – in der Regel nicht aus Europa – schwerlich oder nicht mehr eingesetzt werden könnten. Teilweise gebe es auch überhaupt keine europäischen Alternativprodukte. Ein weiterer von den Instituten geäußerter kritischer Aspekt ist der Umgang mit Updates im Rahmen von Zertifizierung und der bestehenden Gefahr, auf veraltete Produkte zurückgreifen zu müssen, da entsprechende Zertifizierungen nicht zügig erteilt würden.

Fazit

Aufeinander abgestimmte harmonisierte Regelwerke unter Anerkennung der bestehenden Schutzmechanismen stärken am Ende nicht nur die Resilienz der Branche, sondern vermeiden auch unnötige bürokratische Hürden und ermöglichen eine zielgerichtete Umsetzung der regulatorischen Vorgaben.

2. Verhältnismäßigkeit als gelebte Praxis – Proportionalität in Bezug auf das tatsächliche Geschäft

Status / Hintergrund

Die Verhältnismäßigkeit ist ein zentrales Prinzip unter DORA. Das in DORA verankerte differenzierte Vorgehen soll sicherstellen, dass regulatorische Anforderungen effizient und verhältnismäßig angewendet werden, ohne die Resilienz zu gefährden. DORA passt daher die Anforderungen an das IKT-Risikomanagement, die Governance und die Sicherheitsmaßnahmen an die Größe, Art, Komplexität und das Risikoprofil der betroffenen Finanzinstitute an. Besonders kleinere Institute können von vereinfachten Risikomanagementrahmen profitieren, z.B. bei der Umsetzung von IKT-Kontrollen für die Ausnahmeregelungen vorgesehen sind. Die Bewertung nach Verhältnismäßigkeit lässt sich auch dem jüngst veröffentlichten RTS zum TLPT entnehmen. Zusätzlich zu den in Art. 26 Abs. 8 DORA genannten Kriterien, gibt dieser zusätzliche Schwellenwerte zur Auswahl von Unternehmen, die den TLPT durchführen müssen vor.

In Deutschland wurde von diesem vereinfachten Risikomanagementrahmen im FinmadiG gerade für die unter die CRR/CRD-Ausnahme fallenden Institute nicht Gebrauch gemacht.

Zudem ermöglicht DORA grundsätzlich eine flexiblere Ausgestaltung interner Prozesse für Institute, die weniger komplexe IKT-Strukturen oder geringere operationelle Risiken aufweisen. Aller-

dings wurde bei den Testprogrammen keine Wesentlichkeitsschwelle eingefügt. Das bedeutet, dass alle Finanzinstitute verpflichtet sind, angemessene interne Tests durchzuführen, unabhängig von der Größe oder Komplexität ihrer IKT-Systeme.

Forderung / Änderungsnotwendigkeit

Hier ist unser Anliegen, zur Vereinfachung die Standardregelungen des EU-Gesetzgebers aktiv zu nutzen und nicht – wie mit dem FinmadiG geschehen – über den bereits gesetzten Rahmen deutlich hinauszugehen. Insbesondere könnten mindestens die in der CRR/CRD benannten Ausnahmeinstitute wie Förderbanken dem vereinfachten IKT-Risikomanagementrahmen unterfallen. Dies ist nicht im Gleichklang mit anderen vergleichbaren Instituten in Europa und verursacht erhebliche Kosten. Für eine stärkere Konkretisierung können wir uns eine Abstufung nach Standard-Services bei kleineren Häusern mit einfachen, konkreten Anforderungen und mehr Flexibilität und dafür höhere Anforderungen für große Institute bzw. Geschäftsbanken mit breitem Geschäft vorstellen, den diese nach ihren Bedürfnissen methodisch gestalten können.

Beispielhaft sei folgendes genannt: Kleine und mittelständische Institute stehen vor der Herausforderung, die umfassenden Anforderungen an das IKT-Risikomanagement und nach Benennung durch die Behörde oder der Erfüllung eines der in Art. 2 RTS TLPT iVm. Art. 26 DORA benannten Kriterien verpflichtende Penetrationstests (TLPT) mit begrenzten Ressourcen umzusetzen. Eine dezidierte Anwendung der Verhältnismäßigkeit erfordert klare Leitlinien und praxisnahe Kriterien, um sicherzustellen, dass regulatorische Anforderungen an die individuelle Risikostruktur angepasst werden. Dazu könnten vereinfachte Berichtsformate, und risikobasierte Ansätze bei der Durchführung von Penetrationstests (TLPT)beitragen. Die Herausforderung liegt in der Balance zwischen regulatorischer Sicherheit und operativer Umsetzbarkeit, die durch enge Zusammenarbeit zwischen Aufsichtsbehörden und Finanzinstituten überwunden werden kann. Ein Dialog, der frühzeitig auf die spezifischen Bedürfnisse gerade kleinerer Banken eingeht, ist essenziell. Wie werden uns weiter auch im Dialog mit Aufsichtsbehörden dafür einsetzen, dass diese Verhältnismäßigkeit auch gelebt und umgesetzt wird.

Dazu gehört nach unserem Verständnis, dass insbesondere kleinere Institute, die der CRR/CRD-Ausnahme unterliegen, aus den Anforderungen zur Durchführung von verpflichtenden TLPT herausgenommen werden, wenn nachgewiesen wird, dass sie keine kritischen Funktionen im Sinne von DORA Art. 26(1) selbst erbringen bzw. nicht bedeutend iSd. RTS – TLPT sind bzw. gleichwertige Alternativen wie ISO/IEC 27001-Audits oder BSI-Grundschutzprüfungen nutzen. Dies sollte das FinmadiG auch explizit klarstellen. Derartige kleinere Institute verfügen in der Regel über weniger komplexe IT-Infrastrukturen und ein geringeres systemisches Risiko für den Finanzsektor. Wenn sie bereits auf robuste Standard-Sicherheitsmaßnahmen wie regelmäßige Penetrationstests, Vulnerability Assessments und Business-Continuity-Tests im Rahmen des internen Testregimes setzen, ist ein angemessenes Sicherheitsniveau ohne die zusätzliche Komplexität von TLPT gewährleistet. Überdies stellt TLPT für kleinere Institute mit begrenzten Ressourcen durch die Komplexität des Tests und den Einsatz spezialisierter externer Dienstleister eine unverhältnismäßige finanzielle Belastung dar, ohne dass der Sicherheitsgewinn im gleichen Maße steigt. Diese Argumente greifen auch für ein machbarkeitsorientiertes internes Testregime, wenn bereits anderweitige Prüf- und Kontrollmechanismen eine ausreichende Resilienz bestätigen.

Diese Grundgedanken der mangelnden Systemrelevanz und der Verhältnismäßigkeit des Ressourceneinsatzes setzen sich insbesondere für die Wochenend- und Feiertagsmeldungen von schwerwiegenden Vorfällen fort, wofür separat Personal aufgebaut werden müsste. Die Abwendung von Wochenendmeldungen bedeutet nicht, dass Banken Sicherheitsvorfälle nicht ernst nehmen oder keine Maßnahmen ergreifen. Die technische Reaktion auf Vorfälle erfolgt weiterhin in Echtzeit – lediglich die aufsichtliche Meldung kann auf den nächsten Werktag verschoben werden, ohne dass dies die IT-Resilienz gefährdet. Hinzu kommt, dass auch für die Aufsichtsbehörden die sofortige Meldung von Vorfällen am Wochenende bei kleinen, nicht systemrelevanten Instituten oft operativ nicht erforderlich ist, da keine unmittelbaren Interventionsmaßnahmen zu erwarten sind. Dies würde auch den Aufsichtsressourcen zugutekommen. Generell sind die Schwellenwerte für Meldungen zu überprüfen, da die Meldepflichten insbesondere auf viele Häuser mit speziellen Geschäftsmodellen nicht passen. Hier wäre eine Ausweitung der Systemausfallzeiten z.B. für zentrale Fördersysteme von mehr als vier Stunden, bei nicht kritischen Systemen von mehr als 24 Stunden, ebenso wünschenswert wie die Beurteilung der Anzahl der betroffenen Kunden bzw. der finanziellen Auswirkungen auf Basis der gefährdungsrelevanten Grundmenge, d.h. betroffene Förderkunden bzw. z.B. 1% des Anteils jährlicher Förderzusagen.

Im Sinne einer weitergehenden Simplifizierung wäre ein abgestuftes Verhältnismäßigkeitskonzept in der Anwendung von DORA wünschenswert, um Proportionalität noch besser zu leben und zu prüfen. So ließe sich der vollumfängliche DORA-Rahmen beispielsweise auf Institute beschränken, die nach DORA und dem RTS-TLPT TLPT-pflichtig sind, d.h. Bilanzsumme > 15 Mrd., O-SII/G-SII, zentrale Marktrolle, digitale Vernetzung. Eine nächste Schwelle würde dann der vereinfachte IKT-Risikomanagementrahmen bis einschließlich der Größe von CRR/ CRD-Instituten gelten. Für noch kleinere Institute sollten lokal weitere Erleichterungen angestrebt werden.

Fazit

Die wirksame Umsetzung von DORA erfordert mehr als formale Compliance – sie lebt von der praktischen Anwendung des Verhältnismäßigkeitsprinzips. Regulatorische Anforderungen müssen nicht nur das Risiko adressieren, sondern auch die operative Realität der Institute berücksichtigen. Ein risikobasierter, praxisnaher Ansatz stärkt nicht nur die Resilienz, sondern sorgt auch für eine effiziente Nutzung von Ressourcen – sowohl auf Seiten der Institute als auch der Aufsicht.

3. Effizienz im IKT-Drittparteienmanagement

Status / Hintergrund

Auch das IKT-Drittparteienmanagement ist vom Prinzip der Verhältnismäßigkeit geprägt und strebt durch eine zentralisierte Aufsicht über kritische IKT-Drittdienstleister, standardisierte Vertragsanforderungen und die erleichterte Nutzung von Standard-Cloud-Dienstleistungen eine industrieweite Effizienz an, indem eine Differenzierung nach Kritikalität der Drittparteien zugrunde gelegt wird.

So ist absehbar, dass durch die zentrale Aufsicht der ESAs über als kritisch eingestufte IKT-Dienstleister der Prüfungsaufwand für die Institute erheblich reduziert und Doppelprüfungen vermieden werden können.

Auch durch die Definition klarer Mindestanforderungen für Verträge mit IKT-Dienstleistern sollen Vertragsverhandlungen effizienter gemacht werden, indem sich Institute an diesen Vorgaben orientieren können, anstatt individuelle vertragliche Risikoanalysen von Grund auf zu erstellen.

Für Standard-Cloud-Dienstleistungen oder häufig genutzte IT-Services sieht DORA die Möglichkeit vor, sich als Teil eines umfassenden Überwachungsansatzes auf bestehende Zertifizierungen und Prüfberichte zu stützen, ohne die Institute von der eigenen Prüfung zu entbinden.

Gemäß DORA dürfen Finanzinstitute darüber hinaus gemeinsame Prüfungen durchführen. Dies soll den Prüfaufwand für einzelne Institute reduzieren und zu einer besseren Ressourcennutzung führen.

Forderung / Änderungsnotwendigkeit

In der aufsichtlichen Praxis wird dieser Spielraum oft durch Leitlinien der EBA oder europäische bzw. nationale Auslegungen konkretisiert.

Eines unserer Petita, nämlich die Herausnahme von regulierten Finanzdienstleistern aus dem IKT-Drittparteienmanagement von DORA, insbesondere im Konzernverbund oder bei Zentralbankfunktionen, wurde von den ESAs mittlerweile bestätigt. Allein bleibt es nun weiter daran zu arbeiten, dass mit dieser als Erleichterung gedachten Grundweiche nun keine sonstigen Anforderungen aus DORA zwischen den beteiligten regulierten Finanzunternehmen oder anderweitigem Handlungsbedarf im leistungsbeziehenden Unternehmen führt. Beispielhaft seien hier vertragliche Grundlagen oder Meldungen bei Vorfällen genannt.

In DORA gibt es keine explizite Regelung, die pauschal festlegt, dass für Standarddienste (wie Office 365, Standard-Cloud-Speicher etc.) auf bestehende Zertifizierungen und Prüfberichte zurückgegriffen werden kann, um vollständig von eigenen Prüfpflichten entbunden zu werden. Allerdings gibt es Bestimmungen, die implizit auf diesen Ansatz hindeuten und den Rückgriff auf externe Nachweise erleichtern, wie z.B. der indirekte Verweis auf den Cyber Security Act (CSA), unter dessen Rahmen das EUCS entwickelt wird. Zertifizierte Cloud-Dienste nach EUCS könnten perspektivisch von individuellen Auditpflichten befreit werden, wenn die Zertifizierung bestimmte Sicherheitsanforderungen nach DORA abdeckt. Dies gilt jedoch nur für kritische Anbieter, nicht pauschal für alle Standarddienste. Diese Ausweitung auf alle Standarddienste ist weiter unsere Zielsetzung.

In dem Zusammenhang verweisen wir auch auf die obigen Ausführungen zur Zertifizierung im Rahmen des Abschnitts zu Harmonisierung.

Auch darüber hinaus streben wir eine Erleichterung in der Prüfung von kritischen IKT-Dienstleistern auch jenseits der zentralisierten Aufsicht an. Gerade bei kleineren Häusern ist die Dokumentation der Leistungserbringung insbesondere bei standardisierten oder öffentlichen IT-Dienstleistern zu komplex. Hier würde eine Zusammenfassung in einem konsolidierten Jahresbericht bzw. eine „IKT-Outsourcing-Übersicht“ mit Fokus auf SLA-Einhaltung und nicht auf alle Verträge statt vieler Einzelberichte eine erhebliche Erleichterung darstellen. Dazu gehören insbesondere für kleinere Häuser praktische Erleichterung in der Prüfungsdurchführung z.B. gemeinschaftliche

Prüfungen. Dies erfordert auch eine umsetzbare Handhabung auch des Datenschutzes. Derzeit erarbeiten wir ein Leistungsangebot mit dem GDV für ausgewählte IKT-Dienstleister. Es wäre wünschenswert, wenn dieser Ansatz noch weiter standardisiert Kosten und Aufwand reduzieren könnte.

Umgekehrt ist wichtig, dass die Stimmen der Banken Gehör finden und entsprechende Rückkopplungen von den IKT-Dienstleistern entsprechend übermittelt und Anpassungen vorgenommen werden.

In dem Zusammenhang verweisen wir auch auf die obigen Ausführungen zur Zertifizierung im Rahmen des Abschnitts zu Harmonisierung.

Fazit

DORA lässt im IKT-Drittparteienmanagement bereits spürbare Effizienzgewinne durch die zentrale Aufsicht der ESAs über kritische IKT-Dienstleister, standardisierte Vertragsanforderungen und die erleichterte Nutzung bestehender Zertifizierungen erwarten. Dennoch bleibt es wichtig, dass diese Erleichterungen in der Praxis nicht durch zusätzliche aufsichtliche Anforderungen konterkariert werden. Unser Ziel bleibt es daher, den Spielraum für pragmatische Prüfansätze weiter auszubauen, um Institute gezielt zu entlasten und Standarddienste effizienter zu integrieren.

4. Praktikable Sicherheitsstandards und Technologieanforderungen

Status / Hintergrund

Die IT-Regulierungen wie DORA, NIS2 und der Cyber Resilience Act (CRA) formulieren Sicherheitsstandards und Technologieanforderungen, die einerseits ein hohes Maß an IT-Resilienz sicherstellen sollen, andererseits aber auch auf Praktikabilität ausgerichtet sein sollen. Allen drei Regulierungen merkt man das Bemühen an, auf eine Kombination aus Mindestanforderungen, proportionalen Maßnahmen und Risikoorientierung zu setzen, wobei Sicherheitsstandards nicht als starre Vorgaben verstanden werden, sondern flexibel an unterschiedliche Unternehmensgrößen und -risiken angepasst werden können sollen. Insbesondere gibt es an sich keine verpflichtenden Vorgaben für spezifische Technologien, sondern Anforderungen an das Sicherheitsniveau. Demnach sollen Finanzinstitute ihre IKT-Systeme auf dem neusten Stand der Technik („state of the art“) halten. Die Formulierung „neuster Stand der Technik“ umfasst nicht nur technische Anforderungen an die Sicherheit sondern auch das Sicherstellen aktuellen Know-Hows über neue Technologien und damit Einschätzung der Veränderung der Bedrohungslage in einem Finanzinstitut.

Allerdings sehen wir de facto ein regulatorisches Go für den Weg zu einer vollständigen Zero-Trust-Architektur in allen Bereichen, da implizit die Empfehlung ausgesprochen wird, diese Architektur gezielt und schrittweise für besonders kritische oder risikobehaftete Bereiche zu implementieren. Gleiches gilt für die Verschlüsselung von „Data in Use“. Der daraus resultierende enorme Mehraufwand wird nicht mit dem Verhältnismäßigkeitsprinzip in Einklang gebracht.

Forderung / Änderungsnotwendigkeit

Auch hier wird die Prüfpraxis und weitere Auslegung über verschiedene nachgelagerte Rechtsakte zeigen, wie diese offenen Aspekte dann tatsächlich gehandhabt werden.

Um die Belastungen der Finanzindustrie wissend, sehen wir, dass die Umsetzung von Technologien nach dem Stand der Technik häufig erwartet wird (s. z.B. Konsultation EZB-Leitfaden Cloud Outsourcing). Dies stellt Banken vor erhebliche Herausforderungen, was durch die bisher nicht harmonisierten Anforderungen für die Nutzung von Cloud-Diensten noch erschwert wird.

Besonders deutlich zeigt sich dies bei den Anforderungen an die digitale operationelle Resilienz von Finanzinstituten und ihren IT-Dienstleistern, die sich klar mit den Prinzipien eines Zero-Trust-Ansatzes in Verbindung bringen lassen. Dabei sollte berücksichtigt werden, dass nicht jede Bank ein vollumfängliches Zero-Trust-Modell braucht. Vielmehr sollten die kritischen Geschäftsprozesse mit angemessenen Umsetzungsfristen im Mittelpunkt stehen und die individuellen Risikoprofilen Berücksichtigung finden, ohne unnötige Komplexität zu erzeugen. Standard-IT-Dienste wie Office-Anwendungen oder Marketing-Websites sollten im Sinne der Verhältnismäßigkeit reduzierten Anforderungen unterliegen. Gerade kleineren Instituten muss es generell ermöglicht werden, z.B. über Automatisierung und Managed Security Services verhältnismäßige Sicherheitsniveaus zu erreichen.

Ein weiteres Beispiel stellen die komplexen, teils kostspieligen und technisch nicht gelösten Anforderungen an Verschlüsselungstechnologien wie „Data in Use“ dar. Die schnelle Weiterentwicklung von Technologien erschwert zusätzlich die Definition von Standards, die langfristig praktikabel sind und regulatorische Klarheit schaffen. Daher setzen wir uns bei allem Verständnis für schnelllebige Technologien auch vor dem Hintergrund von zunehmenden Sicherheitslücken dafür ein, dass der neuste Stand der Technik realistisch zum Risikoprofil des Hauses im Sinne der Verhältnismäßigkeit passen muss, solange das Haus dem dahinterstehenden grundsätzlichen Zweck der Regelung gerecht wird.

Banken benötigen flexible, risikobasierte Ansätze, die den tatsächlichen Sicherheitsanforderungen Rechnung tragen und gleichzeitig wirtschaftlich tragbar sind. Standards sollten technologieoffen formuliert werden, um Raum für Weiterentwicklungen zu lassen, und eng mit Branchenakteuren abgestimmt werden, um die Praxisrelevanz sicherzustellen. Dies könnte durch die Einrichtung von Testumgebungen für neue Technologien wie KI, Cloud Computing, Quanten Computing und einen verstärkten Austausch mit der Aufsicht unterstützt werden. Ein wesentlicher Punkt ist dabei auch eine zukunftsorientierte Datenpolitik, denn die Nutzung von Daten ist der Schlüssel für Innovationen, aber gerade auch für Resilienz in einer vernetzten Welt.

Daher sind uns, insbesondere wenn es einer grundsätzlichen Architekturumstellung bedarf, realistische Umsetzungsstandards wichtig, um z.B. bei Cloud-Diensten und Verschlüsselungstechnologien auch die Skalierbarkeit von Sicherheitsmaßnahmen zu gewährleisten. Gleiches gilt für die faktische ZeroTrust-Modell-Einführung. Auch wenn sie nur auf kritische Funktionen beschränkt wird, fordern wir deutlich längere Übergangsfristen, um eine Stärkung der Cybersicherheit in der Umsetzung wirtschaftlich vertretbar zu gestalten.

Auf das Thema Zertifizierung sind wir bereits im Abschnitt zum IKT-Drittparteienmanagement eingegangen. Es hat hier aufgrund seines Technologiebezugs ebenfalls seine Berechtigung.

Darüber hinaus setzen wir uns gerade mit Blick auf die Vielzahl technologischer Möglichkeiten dafür ein, dass bei aller Relevanz eines transparenten Sicherheitsniveaus gleichzeitig zur Abwendung unnötiger Konzentrationsrisiken ein erleichterter Zugang zu Sicherheitsdienstleistern ohne verpflichtende Zertifizierungen i.S.d. CSA insbesondere für Institute mit geringem Sicherheitsrisiko möglich sein muss. Dazu gehören auch Leitfäden und Guidance, um Anforderungen an Rechenzentren besser verstehen zu können.

Fazit

Die Umsetzung technischer Vorgaben ist für die Finanzinstitute herausfordernd, da der „neuste Stand der Technik“ in u.a. Art. 7 DORA unklar definiert und damit eine revisionsresistente Umsetzung z.B. bei Cloud-Diensten oder Verschlüsselungstechnologien erschwert.
Deshalb fordern wir realistische Umsetzungsstandards, die die wirtschaftliche Tragbarkeit gemessen an der Größe und Risiko Affinität verschiedener Finanzinstitute und die Skalierbarkeit von Sicherheitsmaßnahmen berücksichtigen. Dies gilt besonders für komplexe Themen wie Zero-Trust-Modelle und „Data in Use“-Verschlüsselung. Eine enge Abstimmung mit der Aufsicht, längere Übergangsfristen und technologieoffene Standards sind dabei entscheidend, um Innovation zu fördern und zugleich die Cybersicherheit effektiv zu stärken.

5. Erleichterung interner Prüf- und Kontrollmechanismen

Status / Hintergrund

DORA legt großen Wert auf die Etablierung robuster interner Prüf- und Kontrollmechanismen, um die digitale operationelle Resilienz von Finanzinstituten sicherzustellen. Finanzinstitute müssen ein umfassendes IKT-Risikomanagement einrichten, das neben der Identifikation, Bewertung und Steuerung von Risiken auch interne Kontroll- und Prüfmechanismen umfasst. Dazu gehören regelmäßige Bewertungen von IKT-Risiken, die kontinuierliche Überwachung von IKT-Systemen sowie die Implementierung von Kontrollverfahren zur frühzeitigen Erkennung und Minderung von Risiken. Ein konsolidierter Bericht über das IKT-Risikomanagement ist mindestens einmal jährlich zu erstellen und vom Leitungsorgan zu genehmigen.

Darüber hinaus sind Testprogramme zur Überprüfung der Resilienz von IKT-Systemen verpflichtend. Diese umfassen kontrollierte Schwachstellenbewertungen, Penetrationstests (PEN-Tests) und andere Formen von Resilienztests, die in Abhängigkeit von der Kritikalität der Systeme sowohl intern als auch von unabhängigen Dritten durchgeführt werden können.

Für kritische Systeme und Anwendungen wird erwartet, dass regelmäßige Sicherheitsüberprüfungen, einschließlich PEN-Tests, durchgeführt werden, um Schwachstellen frühzeitig zu identifizieren. Dies gilt sowohl für Eigenentwicklungen als auch für Drittsoftware. Hinsichtlich der Quellcode-Prüfung gibt es derzeit keine klar definierten Wesentlichkeitsschwellen, was insbesondere bei weniger kritischen Anwendungen zu einem unverhältnismäßigen Prüfaufwand führen kann.

Forderung / Änderungsnotwendigkeit

Im Rahmen der praktischen Ausgestaltung und aufsichtlichen Prüfung setzen wir uns dafür ein, den Aufwand insbesondere für unter die CRR/CRD-Ausnahme fallenden Institute und weniger kritische Bereiche risikoadäquat zu reduzieren, ohne die Sicherheitsziele von DORA zu gefähr-

den. Das betrifft diverse interne Berichte, die sich sinnvoll für eine derartige Institutsgruppe verschlanken ließen bzw. seltener oder zusammengeführt berichtet werden sollten: Dazu zählen u.a. der Bericht über das IKT-Risikomanagement, bei dem bereits heute das Risiko besteht, dass der Bericht symptomatisch für eine regulatorische Bürokratie wird – mit wenig Impact auf echte Resilienz. Er ist vielmehr der Versuch eines zentralen Steuerungselement, der aber aufgrund der Dynamik der digitalen Risiken, zwingend erforderlicher begleitender KPIs (z.T. in Echtzeit) und der Notwendigkeit der Einbettung in ein kontinuierliches IKT-Risikomanagementsystem Gefahr läuft, statisch zu bleiben. Statt einer detaillierten Risikoanalyse auf granularer Prozessebene könnte eine Konzentration auf Kernprozesse mit digitaler Kritikalität (z. B. Antrag, Bewilligung, Auszahlung) bzw. ein aggregierter IKT-Risikobericht auf Funktionsebene, halbjährlich statt quartalsweise, sinnvoll sein. Gleiches gilt für die vollständigen, jährlichen Berichte zu allen BCM-Plänen, statt sich auf Systeme mit Relevanz z.B. für Fördermittelabruf, Mittelverwendung und Förderkundenkommunikation zu konzentrieren bzw. wie in einem Rotationsprinzip jedes Jahr nur Teilbereiche im Detail zu dokumentieren und die übrigen nur in Stichprobe. Auch der Cybersicherheitslagebericht bietet bei stabiler Lage monatlich oder quartärlich geringen Erkenntnisgewinn – bei signifikanten Bedrohungsänderungen z.B. in Kombination mit dem IKT-Risikobericht sähe dies anders aus.

Wir fordern insbesondere eine stärkere risikobasierte Differenzierung, sodass Institute mit geringerem IKT-Risiko weniger komplexe Risikobewertungen durchführen müssen. Anstelle detaillierter Szenarioanalysen sollte für solche Institute ein vereinfachtes Risikoinventar ausreichen.
Bei den erwarteten PEN-Tests sollte der Spielraum für alternative Sicherheitsmaßnahmen erweitert werden. Für weniger kritische Systeme könnten regelmäßige Schwachstellen-Scans in einem verhältnismäßigen Turnus je nach Besonderheit des Instituts oder automatisierte Sicherheitsüberprüfungen ausreichen, sofern diese ein gleichwertiges Sicherheitsniveau gewährleisten. Im Bereich der Quellcode-Analysen sollten Schwellenwerte je nach Kritikalität zum Ansatz gebracht werden, um den Prüfaufwand zu reduzieren, ohne die Sicherheitsziele zu gefährden.

Zudem sollte die Häufigkeit von Tests risikobasiert angepasst werden. Für nicht-kritische Systeme könnten längere Testintervalle (z.B. alle 2–3 Jahre statt jährlich) zulässig sein. Gemeinsame Testprogramme für mehrere Institute, insbesondere im Rahmen von Verbundstrukturen oder Brancheninitiativen, könnten ebenfalls zu einer effizienteren Ressourcennutzung beitragen, ohne die Wirksamkeit der Sicherheitsmaßnahmen zu beeinträchtigen. Es kann sinnvoll sein, den Testrahmen zeitlich in Abhängigkeit von bestimmten Anlässen zu flexibilisieren.

Fazit

DORA fordert nachvollziehbar robuste interne Prüf- und Kontrollmechanismen, um die digitale Resilienz von Finanzinstituten sicherzustellen. Während für kritische Systeme umfangreiche Tests wie PEN-Tests verpflichtend sind, besteht bei weniger kritischen Systemen und kleineren Instituten Spielraum für risikobasierte Vereinfachungen.

Wir setzen uns dafür ein, den Prüfaufwand durch differenzierte, risikobasierte Ansätze zu reduzieren. Dazu gehören alternative Sicherheitsmaßnahmen, verlängerte Testintervalle für nicht-kritische Systeme sowie gemeinsame Testprogramme zur effizienten Ressourcennutzung – ohne die grundlegenden Sicherheitsziele von DORA zu gefährden.

Der Bundesverband Öffentlicher Banken Deutschlands, VÖB, ist ein Spitzenverband der deutschen Kreditwirtschaft. Er vertritt die Interessen von 64 Mitgliedern, darunter die Landesbanken sowie die Förderbanken des Bundes und der Länder. Die Mitgliedsinstitute des VÖB haben eine Bilanzsumme von rund 3.029 Milliarden Euro und bilden damit etwa ein Viertel des deutschen Bankenmarktes ab. Die öffentlichen Banken nehmen ihre Verantwortung für Mittelstand, Unternehmen, die öffentliche Hand und Privatkunden wahr und sind in allen Teilen Deutschlands fest in ihren Heimatregionen verwurzelt. Mit 57 Prozent sind die ordentlichen VÖB-Mitgliedsbanken Marktführer bei der Kommunalfinanzierung und stellen zudem rund 22 Prozent aller Unternehmenskredite in Deutschland zur Verfügung. Die Förderbanken im VÖB haben im Jahr 2024 Förderdarlehen in Höhe von knapp 60 Milliarden Euro bereitgestellt. Als einziger kreditwirtschaftlicher Verband übt der VÖB die Funktion eines Arbeitgeberverbandes für seine Mitgliedsinstitute aus. Die tarifrechtlichen Aufgaben, insbesondere der Abschluss von Tarifverträgen, werden von der Tarifgemeinschaft Öffentlicher Banken wahrgenommen. Ihr gehören rund 60.000 Beschäftigte der VÖB-Mitgliedsinstitute an.

Weitere Informationen unter www.voeb.de