Trust and Technology Blog

By PwC Deutschland | 19. Juli 2024

Erfolgreicher Abschluss der Konsultationsphase der zweiten Tranche der DORA RTS- und ITS-Entwürfe

Vom 8. Dezember 2023 bis zum 4. März 2024 führten die Europäischen Aufsichtsbehörden (EBA, ESMA und EIOPA) eine öffentliche Konsultation zur zweiten Tranche der RTS- und ITS-Entwürfe durch.

Diese Konsultation bezog sich konkret auf Entwürfe aus dem zweiten Batch, einem Satz von Standards. Diese Konsultationen ermöglichen es den Finanzinstituten, aktiv Feedback zu geben und damit die Regulatorik mitzubestimmen, wie es in der DORA allgemein festgelegt ist. Sie sind ein bedeutender Schritt in den fortlaufenden Bemühungen, die regulatorischen Rahmenbedingungen für Finanzdienstleistungen innerhalb der Europäischen Union zu verbessern und zu harmonisieren. Angesichts der zunehmenden Cyber-Bedrohungen und der rasanten technologischen Entwicklungen ist es entscheidend, dass Finanzinstitute nicht nur robust und widerstandsfähig sind, sondern auch effektiv überwacht und reguliert werden. Die während dieser Konsultationsphase geprüften Entwürfe betreffen verschiedene Aspekte der Cyber-Resilienz und der Überwachung im Finanzsektor. Sie umfassen eine Vielzahl von Themen, bei denen die aktive Beteiligung der Financial Entities besonders hervorzuheben ist. Diese Themen sind von großer Bedeutung für die Sicherheit und Stabilität des Finanzsystems.

RTS zu Threat Led Penetration Testing (Art. 26 Abs. 11):

Durch die Verpflichtung zur Durchführung von Threat Led Penetration Tests kann die Aufsicht die Resilienz der betroffenen Unternehmen verbessern, indem sie die Anforderungen und Verfahren für TLPTs spezifiziert. TLPTs sind wichtig für die Bewertung der Cyber-Resilienz von Finanzinstituten. Allerdings ist zu beachten, dass nicht alle Finanzinstitute verpflichtet sind, diese durchzuführen. Sie simulieren gezielte und realistische umfassende Angriffe, um Schwachstellen in den Systemen und Prozessen der Institute aufzudecken und zu beheben. Ein wichtiger Aspekt hierbei ist, dass die DORA ausgewählte Finanzunternehmen zur Durchführung von TLPTs nach festgelegten Kriterien bestimmen kann. Durch die Durchführung solcher Tests können sie besser auf tatsächliche Cyberbedrohungen vorbereitet werden und ihre Verteidigungsstrategien kontinuierlich verbessern. Die Ergebnisse dieser Tests liefern wertvolle Einblicke in potenzielle Sicherheitslücken und helfen dabei, geeignete Maßnahmen zur Risikominderung zu entwickeln.

RTS zur Festlegung der Meldung schwerwiegender IKT-Vorfälle (Art. 20.a):

Die Verfahren zur Meldung signifikanter Informationssicherheitsvorfälle im Bereich der Informations- und Kommunikationstechnologie werden in diesem Standard festgelegt. Ziel ist es, eine schnelle und effiziente Kommunikation solcher Vorfälle an die Aufsichtsbehörden zu gewährleisten, um potenzielle Risiken zu minimieren und die Auswirkungen auf die Resilienz im europäischen Finanzmarkt zu begrenzen. Durch die zeitnahe Meldung schwerwiegender IKT-Vorfälle innerhalb von 4 Stunden können die Aufsichtsbehörden rechtzeitig reagieren und gegebenenfalls koordinierte Maßnahmen zur Unterstützung der betroffenen Institute einleiten. Dabei werden Klassifikationskriterien wie beispielsweise ,,finanzieller Schaden'' angewendet, um die Dringlichkeit und den Umfang der Reaktionen zu bestimmen. Die Meldepflicht umfasst genaue Angaben über die Art des Vorfalls, die betroffenen Systeme und Daten sowie die ergriffenen oder geplanten Gegenmaßnahmen.

ITS zur Festlegung der Einzelheiten der Berichterstattung über größere IKT-Vorfälle (Art. 20.b):

Diese Implementierungstechnischen Standards spezifizieren die Detailanforderungen und das Format der

Berichterstattung über umfassende IKT-Vorfälle, um Konsistenz und Vergleichbarkeit der Meldungen sicherzustellen. Sie definieren die genauen Anforderungen an den Inhalt der Berichte, einschließlich der Beschreibung des Vorfalls, der betroffenen Systeme und Daten, der Folgen und der ergriffenen Gegenmaßnahmen. Ein standardisiertes Berichterstattungsformat erleichtert den Aufsichtsbehörden die Analyse und Bewertung der Vorfälle und trägt dazu bei, Trends und Muster zu erkennen, die auf systemische Schwachstellen hinweisen könnten. Durch diese detaillierte Berichterstattung können die Aufsichtsbehörden besser informiert Entscheidungen treffen und gezielte Maßnahmen zur Verbesserung der Cybersicherheit im Finanzsektor ergreifen.

Leitlinien für die Zusammenarbeit zwischen den Europäischen Aufsichtsbehörden und den nationalen Aufsichtsbehörden hinsichtlich der Struktur der Überwachung (Art. 32 Abs. 7):

Diese Leitlinien sollen die Kooperation und Koordination zwischen den Europäischen Aufsichtsbehörden und den nationalen Aufsichtsbehörden verbessern, um eine einheitliche und effektive Überwachung sicherzustellen. Sie definieren die Rollen und Verantwortlichkeiten der verschiedenen Behörden sowie die Verfahren für den Informationsaustausch und die Zusammenarbeit bei der Überwachung grenzüberschreitender Finanzinstitute. Durch die Verbesserung der Zusammenarbeit können Doppelarbeit vermieden und die Aufsichtstätigkeiten effizienter gestaltet werden. Eine harmonisierte Überwachungsstruktur trägt dazu bei, die Aufsichtspraxis in der gesamten EU zu vereinheitlichen und sicherzustellen, dass alle Mitgliedstaaten denselben hohen Standards folgen. Dies steht im Einklang mit den Zielen des Digital Operational Resilience Act, der eine einheitliche digitale Resilienz in der gesamten EU anstrebt. Wichtig zu betonen ist, dass für Finanzinstitute hierbei keine zusätzlichen Maßnahmen erforderlich sind.

RTS zur Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten (Art. 41):

Der RTS zur Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten gemäß Artikel 41 zielt darauf ab, einheitliche Standards für die Überwachung durch Aufsichtsbehörden im europäischen Finanzmarkt zu schaffen. Er legt spezifische Anforderungen fest, wie z.B. standardisierte Überwachungsverfahren, Mechanismen für den Informationsaustausch und die Zusammenarbeit zwischen den Mitgliedstaaten, technologische Anforderungen für die IT-Infrastruktur sowie Berichterstattungs- und Transparenzvorgaben. Diese Maßnahmen sollen die Effizienz und Kohärenz der Überwachung erhöhen, um Marktmissbrauch zu verhindern.

Die Konsultationsphase ermöglichte es den Interessengruppen, Kommentare und Anregungen zu den vorgeschlagenen Entwürfen abzugeben. Diese Rückmeldungen sind entscheidend, um sicherzustellen, dass die endgültigen verordneten RTS und ITS sowohl praktikabel als auch umsetzbar sind. Nach Abschluss der Konsultationsphase werden die eingegangenen Stellungnahmen von den Aufsichtsbehörden sorgfältig geprüft und gegebenenfalls in die endgültigen Entwürfe eingearbeitet. Die Verabschiedung und Inkraftsetzung der finalen Standards ist nun für Juli geplant. Angesichts des kurzen Umsetzungszeitraums bis zum 17. Januar 2025 ist es entscheidend, dass Finanzunternehmen sich zeitnah und aktiv mit den

Anforderungen vertraut machen, wie entsprechende Maßnahmen ergreifen. Es wird empfohlen, bereits bekannte Anforderungen jetzt zu berücksichtigen, da in der vorangegangenen Phase wenig Anpassungen vorgenommen wurden.

Die Strategie der internationalen Aufsichtsbehörden zeigt, dass der erfolgreiche Abschluss dieser Konsultationsphase einen wichtigen Schritt zur Stärkung der regulatorischen Rahmenbedingungen im Finanzsektor der EU markiert. Die präzise Definition und Harmonisierung der Anforderungen und Verfahren tragen dazu bei, die Sicherheit und Stabilität des Finanzsystems weiter zu festigen. Die Zusammenarbeit zwischen den europäischen und nationalen Aufsichtsbehörden spielt dabei eine zentrale Rolle, um den Herausforderungen in einer zunehmend digitalen und vernetzten Finanzwelt gerecht zu werden.

Haben Sie Fragen zu diesen regulatorischen Änderungen oder benötigen Sie Unterstützung bei der Umsetzung? Unser Team steht Ihnen gerne mit Fachwissen und einem erprobten Toolset beratend zur Seite!

Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie hier mehr über die Möglichkeiten und Angebote.

Zu weiteren PwC Blogs

Schlagwörter

Artificial Intelligence (AI), Digital Operational Resilience Act (DORA), Digitalisierung, Finanzmarkt, IT-Sicherheit, IT-Systeme, Informationstechnologie (IT)

Kontakt

Rüdiger Giebichenstein

Köln

ruediger.giebichenstein@pwc.com