DORA
Whitepaper

Welche Cybersecurity-Herausforderungen kommen auf den Finanzsektor zu?

Abstract

Die Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA) ist eine EU-Regulierung, die darauf abzielt, die digitale Sicherheit und Widerstandsfähigkeit von Finanzunternehmen zu stärken. Sie soll sicherstellen, dass Finanzinstitute angemessene Vorkehrungen treffen, um sich gegen Cyberangriffe und andere IT-bezogene Risiken zu schützen. DORA legt Anforderungen an das Risikomanagement, die Überwachung und das Melden von IT-Störungen fest. Zudem fordert sie von Finanzunternehmen, Drittanbieter von IT-Dienstleistungen sorgfältig zu überwachen und zu kontrollieren. Ziel ist es, die Stabilität und Integrität des europäischen Finanzsystems in der zunehmend digitalen Welt zu gewährleisten.

Einleitung

Am 17. November hat der europäische Rat die Verordnung des Europäischen Parlaments und des Rates über die digitale operationale Resilienz im Finanzsektor (kurz "DORA") beschlossen und sie tritt 20 Tage nach Veröffentlichung im Amtsblatt der EU in Kraft. 24 Monate später und somit ab 17. Januar 2025 gilt die Verordnung dann unmittelbar und verbindlich in jedem Mitgliedsstaat. Da es sich um eine Verordnung handelt ist keine gesonderte nationale Umsetzung erforderlich, der Text gilt in allen Mitgliedsstaaten gleichermaßen. Die Verordnung ist Teil des Aktionsplans der Europäischen Kommission aus dem Jahr 2018 mit der Zielsetzung der Schaffung eines wettbewerbsfähigen und innovativen europäischen Finanzsektors. Primäre Ziele des Aktionsplans sind die Verbesserung der Cyber-Resilienz der Finanzunternehmen und die Harmonisierung hinsichtlich konkreter Anforderungen an die Sicherheit der Informations- und Kommunikationstechnik (IKT) der Finanzunternehmen.

Geltungsbereich

Aufgrund der Zielsetzung der Schaffung eines kohärenten Ansatzes für das Management von IKT-Risiken im Finanzbereich in der EU - mit dem Ziel der Stärkung der digitalen operationale Resilienz der Finanzdienstleistungsbranche - hat man sich für einen sehr breiten Geltungsbereich entschieden, welcher neben klassischen Kreditinstituten, Zahlungsinstituten und Einrichtungen der Finanzmarktinfrastruktur wie Zentralverwahrern, zentralen Gegenparteien und Handelsplätzen auch alle Finanzdienstleister im weiteren Sinne umfasst, wie Wertpapierfirmen, Investmentfonds, Anbieter von Krypto-Dienstleistungen, Kontoinformationsdienstleistern, Versicherungs- und Rückversicherungs-unternehmen, Versicherungsvermittlern, Ratingagenturen sowie all deren Datenbereitstellungsdiensten und IKT-Drittdienstleistern. Artikel 2 sieht einige (wenige) Ausnahmen von der Verordnung vor sowie gewisse Erleichterungen (z.B. einen vereinfachten IKT-Risikomanagementrahmen) für Finanzdienstleister, die als „Kleinstunternehmen“ gelten (weniger als 10 Mitarbeiter und ein Jahresumsatz bzw. eine Jahresbilanz von unter 2 Mio. EUR). Bei allen Regelungen wird auf den Grundsatz der Verhältnismäßigkeit verwiesen, bei welchem der Größe, dem Gesamtrisikoprofil sowie Art, Umfang und Komplexität der Dienstleistungen und Geschäfte des Finanzdienstleisters Rechnung zu tragen ist. DORA gilt als Lex Specialis für die zeitgleich beschlossene NIS 2-

Richtlinie und ersetzt daher diese für alle betroffenen Unternehmen. Gleichzeitig ist DORA in einigen Punkten (z.B. Anforderungen an den IKT-Risikomanagementrahmen bzw. umzusetzender Schutzmaßnahmen) deutlich umfassender und tiefgreifender ausgeführt als die ähnlich ausgelegte NIS 2 Richtlinie, wodurch davon auszugehen ist, dass die nationalen Aufsichtsbehörden sich bei den Umsetzungsstandards an den detaillierteren Vorgaben von DORA orientieren werden.

Risikomanagementanforderungen

In Artikel 5 Governance und Organisation wird gefordert, dass Finanzunternehmen über einen internen Governance- und Kontrollrahmen verfügen, der ein *wirksames und umsichtiges Management von IKT-Risiken* gewährleistet, um ein *hohes Niveau an digitaler operationaler Resilienz* zu erreichen. Das Leitungsorgan des Finanzunternehmens verantwortet hierbei die Umsetzung aller Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen. Dies inkludiert die Zuweisung *angemessener Budgetmittel*, beschränkt sich aber nicht darauf. Das Leitungsorgan hat auch dafür zu sorgen, bezüglicher alle risikorelevanten Themen am Laufenden gehalten zu werden, einschließlich der Vereinbarungen über die Nutzung von IKT-Dienstleistungen. Weiters fordert DORA, dass die Mitglieder des Leitungsorgans des Finanzunternehmens ausreichende Kenntnisse und Fähigkeiten zu IKT-Risiken *auf dem neuesten Stand* haben – dies bedeutet, dass sie regelmäßig spezielle Schulungen absolvieren müssen. Es ist davon auszugehen, dass dies in einen erweiterten Anforderungskatalog der Fit & Proper Prüfungen Eingang finden wird.

Der Abschnitt 2 von DORA umfasst dann genaue Vorgaben an den IKT-Risikomanagementrahmen, der Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools umfassen muss, um alle IKT-Assets *ordnungsgemäß und angemessen* zu schützen, ebenso wie alle relevanten physischen Komponenten und Infrastrukturen, zB. Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche. Dieser IKT-Risikomanagementrahmen muss dokumentiert sein und gemäß dem Modell der drei Verteidigungslinien von einer unabhängigen Kontrollfunktion gemanagt und zumindest einmal jährlich überprüft werden. Der IKT-Risikomanagementrahmen muss die Risikotoleranzschwelle beschreiben, wesentliche Leistungsindikatoren und Risikokennzahlen festlegen und die Wirksamkeit mittels Tests und Monitoring laufend überprüfen. Weiters muss eine IKT-Referenzarchitektur definiert sein und die davon umfassten Systeme *stets auf dem neuesten Stand* gehalten werden. Die folgenden Artikel beschreiben entlang des Security Lifecycles „Identifikation“, „Prävention“, „Erkennung“, „Reaktion“ und „Wiederherstellung“ alle Mindestanforderungen, die der IKT-Risikomanagementrahmen zur Erfüllung der Sicherheitsziele enthalten muss. Dies betrifft alle wesentlichen Themen, die von gängigen Sicherheitsstandards wie ISO 27001 oder NIST 800-53 beschrieben werden: Szenarioanalyse, Business Impact Analyse, Asset Management, Veränderungsmanagement, Schutz der Verfügbarkeit, Authentizität und Integrität von Daten, Berechtigungsmanagement und Authentifizierung bis hin zu Geschäftsfortführungsleitlinien und Notfallplanung. Auch technische Maßnahmen werden konkret beschrieben wie beispielsweise die Fähigkeit, Anomalien zu erkennen und im Bedarfsfall Netzwerkverbindung sofort zu trennen oder zu segmentieren. Indem konkrete technische Fähigkeiten auf Verordnungsebene festgeschrieben werden, geht DORA weiter als jeder bisher vorliegende Gesetzestext auf EU-Ebene. Auch bezüglich Disaster Recovery & BCM spezifiziert DORA sehr konkrete Anforderungen, Vorgaben für Wiederherstellungszeiten und Wiederherstellungspunkte, welche die potenziellen Gesamtauswirkungen auf die

Markteffizienz berücksichtigen, ebenso wie redundante IKT-Kapazitäten mit ausreichenden Ressourcen und eigenem Risikoprofil, welche überdies regelmäßig umfassend getestet werden müssen, inklusive der von IT-Abteilungen oft gefürchteten Full-Failover-Tests. DORA fordert explizit, dass die vereinbarte Dienstleistungsgüte auch *in Extremszenarien* erreicht wird.

Behandlung kritischer Vorfälle und Meldepflichten

Kapitel 3 befasst sich mit der Behandlung IKT-bezogener Vorfälle, welche auch „*erhebliche Cyberbedrohungen*“ umfassen. Für diese sind Frühwarnindikatoren einzusetzen und geeignete Klassifikations-, Reaktions- und Kommunikationsmaßnahmen vorzusehen. Weiters sieht DORA – analog NIS – eine Meldepflicht für schwerwiegende Sicherheitsvorfälle vor, mit Erstmeldung, Zwischenmeldungen und einer Abschlussmeldung. Die genauen Fristen und Formate der Meldungen werden von der ESA im Rahmen technischer Regulierungsstandards innerhalb von 18 Monaten festgelegt. Finanzdienstleister bekommen das Recht, Meldepflichten nach diesem Artikel an einen Drittdienstleister auslagern, wobei sie immer die volle Verantwortung für die Erfüllung der Anforderungen behalten. Weiters soll die ESA prüfen, inwiefern eine weitere Zentralisierung der Meldungen möglich ist und was die Voraussetzungen für die Einrichtung einer einheitlichen EU-Meldeplattform sind. Dies würde eine Erleichterung der Finanzunternehmen im Hinblick auf aktuelle Mehrfachmeldeverpflichtungen bedeuten.

Testen der Resilienz

Ein weiterer Schwerpunkt von DORA sind Anforderungen für das Testen der digitalen Resilienz, welcher ein eigenes Kapitel gewidmet ist. Zentraler Punkt ist, dass bei allen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, mindestens einmal jährlich angemessene Tests durchgeführt werden müssen. Tests sind hierbei sehr breit gefasst und umfassen Schwachstellenbewertungen und -scans, Open-Source-Analysen, Netzwerksicherheitsanalysen, Überprüfungen der physischen Sicherheit, Scans von Softwarelösungen, Quellcodeprüfungen, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests. Durchgeführt werden müssen diese Tests von unabhängigen, internen oder externen Testern, wobei zumindest jeder dritte Test von Externen durchgeführt werden muss. Finanzunternehmen, die als bedeutend eingestuft wurden werden darüber hinaus verpflichtet, mindestens alle drei Jahre einen bedrohungsorientierten Penetrationstest („Threat Led Penetration Test“, TLPT) durchzuführen, welcher mehrere oder alle kritischen oder wichtigen Funktionen eines Finanzunternehmens einschließt und an Live-Produktionssystemen durchgeführt werden muss. In diese Tests sind ggf. auch IKT-Drittdienstleister einzubinden. Nach Abschluss der Tests sind der Behörde eine Zusammenfassung der maßgeblichen Ergebnisse, die Pläne mit Abhilfemaßnahmen und die Unterlagen vorzulegen, mit denen belegt wird, dass der Test anforderungsgemäß durchgeführt wurden. Auch bezüglich der TLPTs wird die ESA innerhalb von 18 Monaten technische Regulierungsstandards erarbeiten, welche Umfang und Testmethodik genauer spezifizieren.

Management des IKT-Drittparteienrisikos

Ein weiterer zentraler Punkt von DORA ist das Management des IKT-Drittparteienrisikos, mit welchem sich das Kapitel 5 befasst. Finanzunternehmen werden verpflichtet, das IKT-

Drittparteienrisiko als integralen Bestandteil des IKT-Risikos zu managen und dafür eine Strategie und zugehörige Leitlinie zu erstellen. Unternehmen werden verpflichtet, ein Informationsregister aller vertraglichen Vereinbarungen mit IKT-Drittdienstleistern zu führen und dieses aktuell zu halten. Das Leitungsorgan wird verpflichtet, regelmäßig die Risiken im Zusammenhang mit den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zu überwachen und zu überprüfen; zur Überwachung der Nutzung von IKT-Dienstleistungen ist eine eigene Funktion einzurichten. Vor Abschluss jeglicher vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen müssen Finanzunternehmen sicherstellen, dass diese Dienstleister *angemessene Standards für Informationssicherheit* einhalten, im Fall von kritischen oder wichtigen Funktionen, sogar die *aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit*. Dies ist während des gesamten Auswahl- und Bewertungsprozesses sicherzustellen und wird als Teil der Sorgfaltspflicht gesehen. Finanzunternehmen müssen sicherstellen, dass IKT-Drittdienstleister ihre Anforderungen in Bezug auf Informationssicherheit und Resilienz erfüllen und integrieren sie dazu bei Bedarf auch in ihre einschlägigen Schulungsprogramme. Finanzunternehmen müssen darüber hinaus sicherstellen, dass vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen gekündigt werden können, wenn nachweisliche Schwächen des IKT-Drittdienstleisters in Bezug auf sein allgemeines IKT-Risikomanagement bekannt werden, insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet. Dazu sind auch geeignete *Ausstiegsstrategien* festzulegen, welche es dem Finanzunternehmen erlauben, ohne Unterbrechung seiner Geschäftstätigkeit und ohne Beeinträchtigung der Kontinuität und Qualität seiner für Kunden erbrachten Dienstleistungen, aus vertraglichen Vereinbarungen ausscheiden zu können.

Regulatorische & Technische Standards

Obwohl die Anforderungen schon im Verordnungstext relativ konkret sind, wurden die drei ESAs (EBA, EIOPA und ESMA) beauftragt, im Rahmen technischer Regulierungsstandards die Anforderungen zu vielen Anforderungsbereichen noch deutlich konkreter zu spezifizieren. Die Europäische Kommission hat die **erste Tranche** der Entwürfe der drei ESAs (EBA, EIOPA und ESMA) am 13. März 2024 angenommen und sie befinden sich aktuell in der 3-monatigen Prüfungsphase, bevor sie veröffentlicht werden. Die erste Tranche der technischen Regulierungs- und Durchführungsstandards umfasst:

- RTS zum IKT-Risikomanagementrahmen (Art. 15) und zum vereinfachten IKT-Risikomanagementrahmen (Art. 16 Abs. 3)
- RTS zu Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen (Art. 18 Abs. 3)
- RTS zur Leitlinie in Bezug auf die Nutzung von IKT-Dienstleistungen von kritischen oder wichtigen Funktionen (Art. 28 Abs. 10)
- ITS zur Erstellung einer Standardvorlage für das Informationsregister (Art. 28 Abs. 9).

Die Konsultationsphase der zweiten Tranche der RTS- und ITS-Entwürfe ist bereits erfolgreich beendet. Diese umfassen:

- Threat Led Penetration Testing (Art. 26 Abs.11)
- Spezifizierung von Elementen bei der Untervergabe von kritischen oder wichtigen Funktionen (Art. 30 Abs. 5)
- Festlegung der Meldung schwerwiegender IKT-Vorfälle (Art. 20.a)

- Festlegung der Einzelheiten der Berichterstattung über größere IKT-bezogene Vorfälle (Art. 20.b)
- Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten (Art. 41)

Die Rückmeldungen zu den Entwürfen werden nun von den europäischen Arbeitsgruppen ausgewertet, mit dem Ziel bis zum 17. Juli 2024 die finalen Entwürfe ebenfalls an die europäische Kommission zu senden.

Überwachungsrahmen kritischer IKT-Drittdienstleister

Um Konzentrationsrisiken zu mitigieren, sieht DORA auch einen eigenen *Überwachungsrahmen kritischer IKT-Drittdienstleister* vor. In diesen sollen IKT-Drittdienstleister fallen, die systemische Auswirkungen auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen haben bzw. eine (noch zu bestimmende) Anzahl global systemrelevanter Institute (G-SRI) oder anderer systemrelevanter Institute (A-SRI) servicieren. Dies soll auch den Grad der Substituierbarkeit des IKT-Drittdienstleisters berücksichtigen. Gruppeninterne IKT-Dienstleister sollen nicht in den Überwachungsrahmen kritischer IKT-Drittdienstleister fallen. Die ESA wird die Liste kritischer IKT-Drittdienstleister erstellen, veröffentlichen und aktualisieren. Für diese wird eine eigene Überwachungsbehörde eingerichtet, welche bewertet, ob jeder kritische IKT-Drittdienstleister über umfassende, fundierte und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen für das Management der IKT-Risiken verfügt, welche in Artikel 33 aufgelistet sind und den Anforderungen an die Finanzunternehmen entspricht. Dazu wird für jeden kritischen IKT-Drittdienstleister ein individueller Überwachungsplan erstellt, in dem die vorgesehenen jährlichen Überwachungsziele und wichtigsten Überwachungsmaßnahmen beschrieben sind. Die Überwachungsbehörde erhält hierzu umfassende Befugnisse und Sanktionsmöglichkeiten, die von der Verhängung von Zwangsgeldern in der Höhe von 1% des durchschnittlichen weltweiten Tagesumsatzes über die Einschränkung von Unterauftragsvergaben bis hin zur Möglichkeit reicht, Finanzunternehmen zu verpflichten, die mit diesem kritischen IKT-Drittdienstleister geschlossenen vertraglichen Vereinbarungen zu kündigen. Die Ausgaben der Überwachungsbehörde für die Durchführung von Überwachungsaufgaben werden den kritischen IKT-Drittdienstleistern vollständig in Rechnung gestellt.

Aufsichtsrahmen und Sanktionen

Auch gegenüber den Finanzunternehmen selbst stellt die Verordnung *angemessene verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen für Verstöße* gegen die Verordnung fest, welche wirksam, verhältnismäßig und abschreckend sein sollen.
Mit DORA wird erstmals ein strenger Aufsichtsrahmen operationaler Risiken gesteckt, der europaweit einheitlich ist. Neben der strikten Maßnahmen, die DORA definiert und die zu einer weiteren Verbesserung der Widerstandsfähigkeit europäischer Finanzdienstleister führen soll, bringt dies gerade für international tätige Finanzdienstleister eine Harmonisierung mit sich, welche zu verbesserter Rechtssicherheit im europäischen Rahmen führt.

Der vollständige Rechtstext ist zu finden unter:
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554