Digital Operational Resilience Act (DORA)

Von Ralf Hörnig, qSkills GmbH & Co. KG

Die EU-Verordnung gilt ab dem 17. Januar 2025 unmittelbar in allen Mitgliedsstaaten der EU – und sie betrifft weit mehr Akteure, als vielen bewusst ist.

In einer Welt, in der digitale Bedrohungen unsere finanzielle Stabilität fortwährend herausfordern, hat die Europäische Union mit der Verordnung 2022/2554, dem Digital Operational Resilience Act (DORA), einen entscheidenden Schritt unternommen. Diese Regelung fordert, dass alle Unternehmen des Finanzsektors umfassende Maßnahmen implementieren, um sich gegen Cyberangriffe und andere informations- und kommunikationstechnologische Risiken zu schützen. Die Verordnung trat am 17. Januar 2023 mit einer Umsetzungsfrist von 24 Monaten in Kraft. Als EU-Verordnung gilt DORA nach dieser Frist ab dem 17. Januar 2025 unmittelbar in allen Mitgliedsstaaten der EU, ohne dass sie zunächst – wie die NIS2-Richtlinie – in nationales Recht umgesetzt werden muss. Dies verdeutlicht die Dringlichkeit und die einheitliche Herangehensweise der EU, die digitale operationale Resilienz im Finanzsektor auf ein neues Level zu heben.

DORA gilt für alle Finanzunternehmen, darunter Banken, Versicherungsunternehmen, Zahlungsdienstleister, Ratingagenturen und Anbieter von Kryptodienstleistungen. Ausnahmen oder vereinfachte Regelungen gelten nur für einzelne Finanzunternehmen, beispielsweise für sehr kleine Firmen. Handeln ist auch für IKT-Drittdienstleister erforderlich. Diese Unternehmen stellen »digitale Dienste und Datendienste« bereit, die mittels IKT-Systemen Dienstleistungen wie die Bereitstellung, Eingabe, Speicherung und Verarbeitung von Daten sowie Berichterstattung, Datenüberwachung, datenbasierte Services und Entscheidungsunterstützung für interne oder externe Nutzer umfassen. Die breite Definition schließt Anbieter von Cloud-Diensten, Software, Datenanalyse und Rechenzentren ein, die von Finanzunternehmen genutzt werden. Die Finanzbranche unterliegt damit in Zukunft besonders strengen Regulierungen. Gegenüber dem Digital Operational Resilience Act (DORA) erscheinen die Vorgaben der NIS2-Richtlinie vergleichsweise mild.

Worum geht es im Kern eigentlich?

Es geht um die Betriebskontinuität (Business Continuity), also die Aufrechterhaltung und Wiederherstellung des Betriebs im Falle von Störungen sowie der Resilienz, also der Widerstandsfähigkeit gegenüber solchen Störungen. Kurz: Betriebskontinuität bringt uns dorthin zurück, wo wir vor einem Vorfall waren, aber eine widerstandsfähige Organisation entwickelt sich weiter und wächst an dem Vorfall.

Die DORA-Verordnung macht dazu in vier Kapiteln Vorgaben für:

- das Risikomanagement,
- den Umgang mit Sicherheitsvorfällen,
- das Testen der digitalen operationalen Resilienz sowie
- das Risikomanagement von IKT-Dienstleistern.

Die Abbildung gibt einen Überblick über die wesentlichen Elemente von DORA und wichtige Begriffe. >>

Überblick DORA

IKT-Risikomanagement (Kapitel II)	IKT-bezogene Vorfälle (Kapitel III)	Prüfung der digitalen Betriebsstabilität (Kapitel IV)	Steuerung des Risikos durch IKT-Drittanbieter (Kapitel V)
1 IKT-Governance & Risikomanagement-rahmen 2 Business Continuity Management und Notfallplan 3 Regelkreis Sicherheit 4 Lernprozesse und Weiterentwicklung	5 Vorgehensweise für die Bewältigung IKT-bezogener Vorfälle 6 Meldung und Zentralisierung schwerwiegender IKT-bezogener Vorfälle bei der Aufsichtsbehörde	7 Vorgaben zu regelmäßigen Tests zur Überprüfung kritischer Systeme auf Betriebsstabilität und Absicherung in Bezug auf IKT-Störungen	8 Aufsichtsrahmen für IKT-Drittanbieter 9 Minimale Vertragsinhalte 10 Befugnisse der Aufsichtsinstanz

Die Gesamtzahl der DORA-Anforderungen liegt in einem mittleren, dreistelligen Bereich

Abbildung oben verdeutlicht, dass DORA eine Vielzahl von Maßnahmen verlangt, um die operationale Resilienz im Finanzsektor zu verbessern. Dazu zählt das Management von Risiken in der Informations- und Kommunikationstechnologie (IKT), einschließlich der Bewertung und Minderung möglicher Schwachstellen und Bedrohungen. Unternehmen müssen zudem IKT-bezogene Vorfälle dokumentieren und melden, um schnell reagieren und Schäden begrenzen zu können.

Die Überprüfung der digitalen Betriebsstabilität erfolgt durch umfassende Tests, um sicherzustellen, dass kritische Systeme auch unter schwierigen Bedingungen funktionieren. Weiterhin wird das Risiko, das von IKT-Drittanbietern ausgeht, streng reguliert und erfordert eine sorgfältige Überwachung der externen IKT-Services. Diese Maßnahmen basieren auf der DORA-Strategie sowie den zugehörigen Leitlinien und Richtlinien.

Die Führungskräfte von Finanzunternehmen tragen eine zentrale Verantwortung gemäß DORA. Sie müssen nicht nur spezifische IKT-Aufgaben übernehmen oder initiieren, sondern auch die damit verbundenen Risiken verstehen und bewerten können. Bei Nichterfüllung dieser Verpflichtungen haften sie für die Folgen und sind gegenüber den Aufsichtsbehörden rechenschaftspflichtig. Verstöße gegen DORA können zu Sanktionen, finanziellen Strafen und Reputationsschäden führen.

So könnte ein effektives Vorgehen zur Umsetzung von DORA im Finanzsektor aussehen:

1. DORA verstehen: Zuerst sollten die Anforderungen und Richtlinien von DORA vollständig verstanden und analysiert werden, um sicherzustellen, dass alle relevanten Aspekte der Regulierung bekannt sind.
2. Gap-Analyse durchführen: Identifizieren Sie die Lücken zwischen den aktuellen operativen und digitalen Resilienzpraktiken und den Anforderungen von DORA. Dies hilft dabei, prioritäre Bereiche für Verbesserungen zu erkennen.
3. Budgetierung und Verantwortlichkeiten festlegen: Stellen Sie sicher, dass ein angemessenes Budget zur Verfügung steht und klare Verantwortlichkeiten definiert sind. Dies ist entscheidend für die effektive Durchführung und Überwachung der notwendigen Maßnahmen.
4. Implementierungsprojekt aufsetzen: Entwickeln Sie ein strukturiertes Projekt oder Programm zur Umsetzung der identifizierten Maßnahmen.
5. Schulungen und Trainings initiieren: Schulen Sie das Personal bezüglich der neuen Richtlinien und Verfahren, um die Compliance und das Bewusstsein für digitale Resilienz zu fördern.
6. Maßnahmen priorisiert umsetzen: Beginnen Sie mit der Umsetzung der wichtigsten Maßnahmen und gehen Sie systematisch vor, um die Anforderungen von DORA zu erfüllen.
7. Überwachung und kontinuierliche Verbesserung: Überwachen Sie die Umsetzung fortlaufend und passen Sie Maßnahmen bei Bedarf an, um auf dem neuesten Stand der Technik und Gesetzgebung zu bleiben.

Diese Schritte sollten in enger Zusammenarbeit mit allen Stakeholdern erfolgen, um eine umfassende und wirksame Umsetzung zu gewährleisten.

Aber wie den Wandel in unruhigen Zeiten angehen?

Großartige Aussicht statt brennender Plattform: eine inspirierende Antwort auf die Frage Warum. Die Richtigen statt alle: Eine begeisterte, fähige und konsistente Minderheit wird eine Mehrheit umstimmen und für den Wandel gewinnen. Neue Routinen statt ständiger Appelle: Ein Großteil unseres Denkens und Handelns ist unbewusst – ein neuer Rahmen führt zu neuem Verhalten. Ein guter erster Schritt sind erst Experimente und darauf aufbauend einen Masterplan zu entwickeln, denn Experimente zeigen, was wirkt und was nicht.

Fazit: DORA setzt einen der höchsten neuen Maßstäbe für die zukünftige Betriebsstabilität und Resilienz im Zeitalter der Digitalisierung und Cyberangriffe mit sehr umfangreichen und teilweise recht detaillierten Vorgaben und Anforderungen. Aus der Digitalisierung zurück gehen ist kein wirklich sinnvoller Weg. Erstmal abwarten und Tee trinken auch nicht. Starten Sie mit einer aktiven Auseinandersetzung mit dem Thema.

»If you think compliance is expensive, try noncompliance.«
– Paul McNulty

Der Autor Ralf Hörnig ist Experte und Trainer für Informationssicherheit, Cloud Security und DORA beim IT-Qualifizierungsexperten ***qSkills GmbH & Co. KG*** in Nürnberg. ❐