FINBRIDGE

DORA-Verordnung verabschiedet

Niklas Nies

Steffen Jahr

Frank Kirr

Foto von Charlotte Venema auf Unsplash, Download-Datum: 08.02.2023

28.02.2023

Digitale Version

DORA-Verordnung verabschiedet

Am 16. Januar dieses Jahres haben der EU-Rat und das EU-Parlament nach längerer Diskussion den Digital Operational Resilience Act (DORA) verabschiedet. Diese Verordnung zielt darauf ab, über die Landesgrenzen der EU-Mitgliedsstaaten hinweg eine einheitliche Rechtsbasis für die Informations- und Kommunikationstechnik (IKT) der Finanzinstitutionen und Finanzunternehmen im EU-Raum aufzustellen. Ein wesentlicher Fokus liegt auf die zukünftig zu erfüllenden Regulatorischen Technischen Standards (RTS).

HINTERGRUND UND ZUSAMMENFASSUNG DER VERORDNUNG

Die infolge der 2008er Finanzkrise zusätzlich aufgestellten regulatorischen Anforderungen an die IKT des Finanzsektor der EU wurden in den einzelnen Mitgliedstaaten teilweise unterschiedlich interpretiert und führten somit lediglich zu einem Mindestmaß an Vergleichbarkeit und Harmonisierung.

DORA strebt an, diese Systeme nun durch einheitliche Standards zu modernisieren und die allgemeine Resilienz der europäischen Finanzinstitutionen gegenüber Cyber-Angriffen und anderen anomalen Vorfällen, wie dem Ausfall kritischer Infrastruktur, zu verstärken. Bisher sind die Standards für diesen Raum auf nationaler Ebene nicht geregelt. In Deutschland gelten für den Finanzsektor folgende Gesetzbücher und Rundschreiben:

- Finanzdienstleister:
    - *Kreditwesengesetz* (KWG)
    - *Mindestanforderungen an das Risikomanagement* (MaRisk)
    - *Bankaufsichtliche Anforderungen an die IT* (BAIT)
- Kapitalverwaltungsgesellschaften:
    - *Kapitalanlagegesetzbuch* (KAGB)
    - *Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften* (KaMaRisk)
    - *Kapitalverwaltungsaufsichtliche Anforderungen an die IT* (KAIT)

- Versicherungen:
    - *Versicherungsaufsichtsgesetz* (VAG)
    - *Mindestanforderungen an das Risikomanagement VA*
    - V*ersicherungsaufsichtliche Anforderungen an die IT* (VAIT)

Die Anforderungen der DORA betreffen darüber hinaus weitere Unternehmenstypen, wie E-Geld-Institute, Krypto-Dienstleister, Ratingagenturen, Handelsplätze, Transaktions- und Verbriefungsregister, Datenbereitstellungdienstleister und noch einige mehr, welche kollektiv unter den Sammelbegriff "Finanzunternehmen" fallen.

Die bisherigen Regelungen für den IKT-Bereich verschiedener Unternehmen sind auf unterschiedliche Rundschreiben verteilt. Das Ziel der DORA ist es, diese allgemeingültigen Regeln zur IKT in einer Quelle zu vereinen und innerhalb der EU zu vereinheitlichen. Wie die Integration von DORA in die nationalen Gesetzgebungen aussehen wird, steht bis dato noch nicht fest. Bei den folgenden zentralen Punkten unterscheidet sich DORA von den bisherigen Regelungen:

- **Sicherheitstests**: Spezifischere Anforderungen an die Tests der digitalen Betriebsstabilität im Rahmen verpflichtender vollständiger Tests aller IKT-Systeme mindestens einmal jährlich, sowie Threat-Lead Penetration Testing (TLPT) alle 3 Jahre bei Finanzunternehmen, welche von der EU als kritisch für den allgemeinen Finanzmarkt designiert werden. Konkrete Kriterien für das Testen werden bald veröffentlicht.

- **Risikobewertung**: Striktere Anforderungen bezüglich der Risiken von IKT-Drittanbietern, eingeschlossen sind hierbei präliminäre Untersuchungen der Drittanbieter, Überprüfung bestehender Verträge und das Führen eines Informationsregisters, welches auf Anfrage an die Behörden überstellt werden muss.

- **Risikomanagement**: Präzisierung der Inhalte eines IKT-Risikomanagementrahmens bzgl. geeigneter Methoden/Techniken, sowie Anforderungen für Anomalie-Entdeckungssysteme und Zugangsrechtsysteme, bis hin zur verpflichtenden Aufstellung von Kommunikationsplänen für Krisenzeiten.

- **Meldung**: Neue Pflichten hinsichtlich der erforderlichen Meldung von kritischen IKT-Vorfällen an die EU-Behörden, insbesondere durch die Pflicht, einen Vorfall noch am selben Werktag zu melden und die Behörden darüber hinaus mit Zwischenberichten und einer abschließenden Ursachenanalyse zu informieren. Hinzu kommen besondere Berichterstattungspflichten beim Aufbau neuer Geschäftsbeziehungen mit IKT-Drittanbietern und bei Auslagerung kritischer Betriebsfunktionen an Drittanbieter.

Es kommen somit einige Veränderungen auf die europäische Finanzbranche im Rahmen des IKT-Managements zu. Eine zusätzliche Herausforderung besteht darin, dass die RTS der DORA momentan noch nicht veröffentlicht sind. Diese Umsetzungsstandards sollen spätestens ein Jahr nach Inkrafttreten der Verordnung verfügbar sein. Hier zeichnet sich bereits ab, dass der Finanzbranche nur ein relativ kurzer Zeitraum für die Integration von neuen Compliance-Protokollen zur Verfügung stehen wird. Daher sollte bereits jetzt damit begonnen werden, sich mit den Auswirkungen der neuen Standards auseinandersetzen. Typische Fragestellungen in diesem Zusammenhang sind:

- Welche Lücken gibt es bezüglich der IKT-Sicherheit?

- Ist der Aufbau neuer Geschäftsbeziehungen mit anderen IKT-Drittanbietern notwendig?

Im folgenden Schaubild ist das Inkrafttreten der DORA, die Veröffentlichung der RTS und Ende der Umsetzungsfrist von DORA im Zeitablauf dargestellt:

KONKRETE INHALTE DER DORA

Insgesamt umfasst DORA sechs Themenblöcke im Rahmen der IKT des EU-Finanzsektors:

1. Anforderungen an die Governance

Dieser Teil der Verordnung stellt Anforderungen an die Führungsebene dar, speziell im Rahmen der Abstimmung von Geschäftsstrategien und des IKT-Risikomanagements. Zukünftig wird verlangt, dass Leitungsorgane IKT-Know-How aufweisen können, welches durch regelmäßige Fachschulungen kontinuierlich zu erwerben ist. Zudem wird von den Leitungsorgangen erwartet, eine aktive und damit entscheidende Rolle bei der Steuerung des IKT-Risikomanagements zu übernehmen. Demnach ist die Leitungsebene dafür zuständig, klare Aufgaben und Zuständigkeiten bezüglich der Funktionen der IKT festzulegen, wodurch die Leitung letztendlich die Endverantwortung für die Steuerung der IKT-Risiken übernimmt.

---

2. Anforderungen an das IKT-Risikomanagement

Die Anforderungen an das IKT-Risikomanagement stellen einen der größeren Teile der Verordnung dar. Diese orientieren sich in Teilen schon an internationalen und nationalen Normen, weswegen hier Überschneidungen mit bereits bestehenden Normen für Kreditinstitute, Versicherungen und Kapitalverwaltungsgesellschaften bestehen. Insgesamt wird hierbei von den Betroffenen verlangt, dass innerhalb der Unternehmung ein IKT-Risikomanagementrahmen aufgestellt wird, welcher Strategien, Richtlinien, Verfahren, IKT-Protokolle und Instrumente beinhaltet, um zum einen den physischen Standort von Daten (Rechenzentren) zu sichern, sowie den digitalen Aufbewahrungsort von Daten zu schützen. Dieser Rahmen ist mindestens einmal jährlich, sowie beim Auftreten von schweren IKT-Störungen, zu

überprüfen und kontinuierlich zu verbessern. Hierzu müssen die Systeme konstant überwacht und von den Unternehmen Schutz-/Desaster-Pläne aufgestellt werden. Diese Pläne müssen Gegenmaßnahmen enthalten, welche sich auf die Erhaltung der Funktionsfähigkeit von kritischer Infrastruktur beim Auftreten von Problemen konzentrieren und eine möglichst schnelle Wiederherstellung des Normalbetriebes gewährleisten. Damit solche Pläne sinnvoll gestaltet werden können, verlangt DORA nun ebenfalls eine Eigenanalyse des Betriebes bezüglich neuer Quellen von IKT-Risiken, Risikobewertungen bei einem IKT-Drittanbieterwechsel und das Führen von Verzeichnissen über diese Informationen. Zusätzlich hierzu müssen unternehmensinterne Mechanismen zur Erkennung und Bekämpfung anomaler Aktivitäten aufgebaut werden. Schlussendlich sind die Betriebe auch dazu verpflichtet, Kommunikationspläne für Zeiten der Krise zu erstellen, mittels derer sie ihre Kunden, andere Institutionen sowie die Öffentlichkeit im Allgemeinen informieren können.

Für das Risikomanagement werden folgende RTS definiert:

Festlegung weiterer Elemente, die in den genannten Strategien, Verfahren, Protokollen und Instrumenten für IKT-Sicherheit enthalten sein müssen und wie diese zu integrieren sind

Klarstellung geeigneter Techniken, Methoden und Protokolle

Standards für die Entwicklung von Systemkomponenten, welche die Erkennung anomaler Aktivitäten sowie die Verwaltung von Zugangsrechten ermöglichen

Präzisierung benötigter Komponenten eines IKT-Plans im Rahmen der Fortführung des Geschäftsbetriebes und der Wiederherstellung, sowie der Prüfung dieses Plans

3. Anforderungen an die Berichterstattung von IKT-Vorfällen

Die Anforderungen an die Berichterstattung orientieren sich an den Anforderungen für das Risikomanagement. Dies bedeutet konkret, dass die Betroffenen dazu aufgerufen werden, Verfahren zur Ermittlung, Verfolgung, Protokollierung, Kategorisierung und Klassifizierung von IKT-Vorfällen aufzustellen. Speziell werden in der nächsten Zeit von den spezifischen EU-Behörden RTS dafür aufgestellt, um IKT-Vorfälle bezüglich ihrer Schwere entsprechend klassifizieren zu können. Dies ist insofern wichtig, als dass DORA verlangt, dass kritische IKT-Vorfälle sofort den EU-Behörden gemeldet werden, eine Woche nach dem Vorfall ein Zwischenbericht gesendet wird und dass abschließend die fertige Ursachenanalyse bezüglich des Vorfalls ebenfalls weitergeleitet wird. Hierzu werden Unternehmen klare Richtlinien und Verhaltensprotokolle aufstellen müssen, um den reibungslosen Ablauf dieses Prozesses zu gewährleisten.

Für die Berichterstattung werden folgende RTS definiert:

Richtlinien bezüglich der genauen Klassifizierung von IKT-Vorfällen anhand verschiedener Merkmale

Einheitliche Formulare und Durchführungsstandards in Bezug auf die Berichterstattung von Vorfällen an die EU-Behörden

---

4. Anforderungen an die Tests der digitalen Widerstandsfähigkeit

DORA verpflichtet alle Finanzunternehmen zu Prüfungen der digitalen Betriebsfähigkeit bei Angriffen und anderen anomalen Aktivitäten. Diese Prüfungen müssen hierbei von unabhängigen Prüfern durchgeführt werden. Alle IKT-Systeme und Anwendungen müssen mindestens einmal jährlich überprüft werden. Dies beinhaltet ein vollständiges Spektrum angemessener Tests, darunter

Überprüfung und Bewertung der Anfälligkeit gegenüber anomalen Ereignissen, der Bewertung der Netzsicherheit und eine Analyse genutzter Open-Source-Software, Gap-Analysen bezüglich potenzieller Schwachstellen, Überprüfung und Analyse der physischen Arbeitsplätze und Datenzentren, Richtlinien bezüglich Scansoftware und Fragebögen, der Analyse von genutztem Quellcode, wobei hierbei nicht die vollständige Überprüfung verlangt wird, sondern nur in machbarem Rahmen. Zusätzlich zu all diesen Maßnahmen kommen noch Szenario-basierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests. Speziell haben EU-Behörden die Möglichkeit, für den Sektor besonders kritische Unternehmen zu designieren, was diese dazu verpflichtet, alle 3 Jahre ein Threat-Lead Penetration Testing durchzuführen. Hierbei wird sich innerhalb der EU meistens an den Standards von TIBER-EU orientiert und die RTS für diese Tests sind die Einzigen, welche bereits innerhalb der Kommission diskutiert werden.

Für die Tests werden bereits folgende RTS in der Kommission diskutiert:

Kriterien für die Prüfung kritischer IKT-Systeme

Standards hinsichtlich der TLPTs im Sinne des Umfangs, der Prüfmethodik und des Umgangs mit den Ergebnissen

---

5. Anforderungen bezüglich des Risikos durch IKT-Drittanbieter

Im Rahmen des Managements der Risiken durch IKT-Drittanbieter stellt DORA mehrere neue Standards auf. Unternehmen werden dazu angehalten, innerhalb ihres Risikomanagementrahmens einen genauen Blick auf ihre Geschäftsbeziehungen mit Drittanbietern zu werfen. Dies beinhaltet eine präliminäre Untersuchung aller IKT-Drittanbieter, mit besonderem Augenmaße auf die Etablierung eines Geschäftsverhältnisses mit einem Anbieter, welcher als besonders Markt-dominant angesehen wird und nicht einfach durch andere

Infrastruktur ersetzbar wäre. Weiterführend sollten Unternehmen bei der Etablierung eines Vertrags überprüfen, ob schon andere Verträge mit demselben Drittanbieter geschlossen wurden, da im Falle eines Ausfalls dieses Anbieters mehrere Aspekte der Firmeninfrastruktur betroffen sein könnten. Hierbei ist auch anzumerken, dass diese besonders dominanten Drittanbieter nach DORA der direkten Aufsicht durch die EU-Behörden unterstellt werden, womit Verhältnisse mit diesen Anbietern nach entsprechendem EU-Recht abgehandelt werden müssen. Abschließend werden Unternehmen dazu angehalten, einmal im Jahr Bericht über neue Verhältnisse mit Drittanbietern zu erstatten und auf Anfrage der Behörden eine komplette Kopie ihres Informationsregisters zu überstellen. Das Register muss dabei alle vertraglichen Vereinbarungen mit diesen Anbietern enthalten.

Bezüglich des Risikos durch Drittanbieter sollen folgende RTS definiert werden:

Die genauen Inhalte des über Drittanbieter zu führenden Informationsregisters sowie Vorgaben für Vereinbarungen mit Drittanbietern

Präzisierung der Aspekte, welche bei der Vergabe von kritischen oder wichtigen Funktionen an Drittanbieter bestimmt und bewertet werden müssen

Der Inhalt der Berichterstattung über kritische IKT-Anbieter, einschließlich der benötigten Informationen, des Berichtformats, wie der Bericht darzustellen ist sowie die Einzelheiten der Aktionen, welche auf Empfehlung der Behörden ergriffen wurden

---

6. Anforderungen bezüglich des Austauschs von Informationen

Schlussendlich beinhaltet DORA noch einen sehr kurzen Artikel über den Austausch von Informationen bezüglich IKT zwischen verschiedenen Unternehmen. Hierbei wird explizit erlaubt, dass Unternehmen sich über IKT-

Risiken, potenzielle Cyber-Risiken sowie Taktiken und Software austauschen dürfen, solange dieser Austausch dazu dient, Cyberbedrohungen besser abzuwehren und während des Austausches der persönliche Datenschutz, die Währung des Betriebsgeheimnisses sowie die Befolgung der Leitlinien zur Wettbewerbspolitik vollständig befolgt werden.

UNSER ANGEBOT ZU DORA

Aufgrund bereits bestehender regulatorischer Regelungen an die IT der betroffenen Unternehmen ist von einer guten Abdeckung der DORA-Anforderungen auszugehen. Nichtsdestotrotz sollte die relativ kurze Umsetzungsfrist von 2 Jahren genutzt werden, um die digitale Widerstandsfähigkeit und den Reifegrad des Unternehmens in Bezug auf IKT-Risiken zu prüfen. Hierbei kann Finbridge unterstützen.

Basierend auf den bisher veröffentlichten Materialien und unserem umfassenden Branchen Know-How unterstützen wir Sie bei der Gap-Analyse und leiten individuelle Handlungsempfehlungen ab, um Ihr Unternehmen auf den Umsetzungsbeginn optimal vorzubereiten.

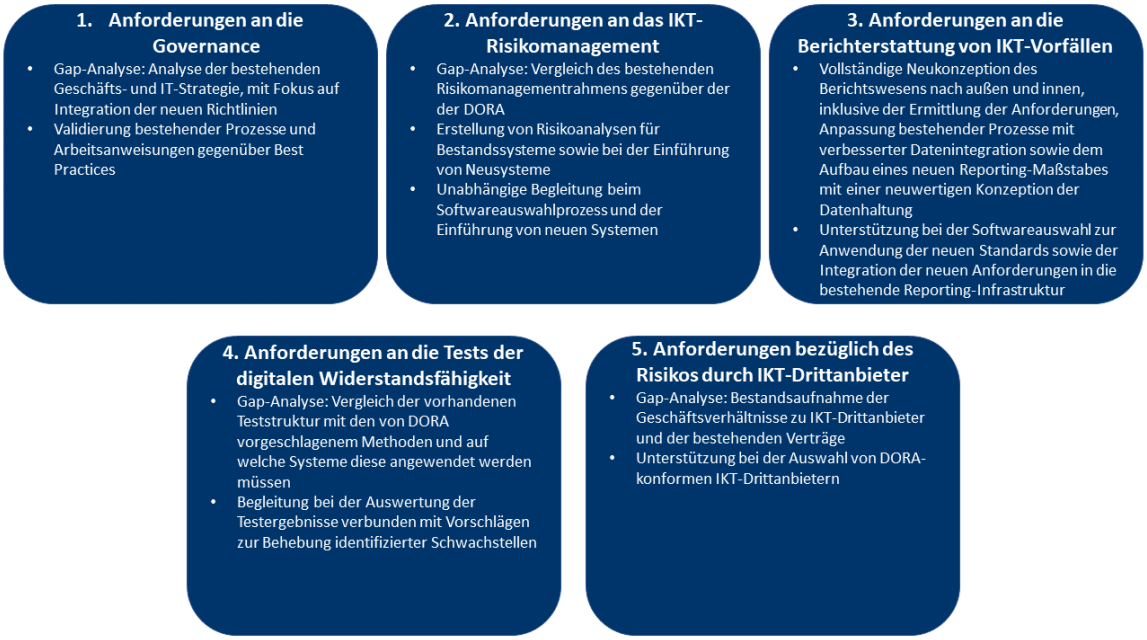

Abbildung 1: Eine Übersicht des Finbridge Angebots

Neben unserem Beratungsangebot zur Umsetzungsunterstützung der DORA-Anforderungen, unterstützen Sie unsere Berater auch bei der Softwareauswahl und Prüfung von IKT-Drittanbietern.

Haben Sie weitere Fragen bezüglich der DORA-Verordnung oder unserem Angebot?

Unsere Berater stehen Ihnen gerne mit ihrer fachlichen und technischen Expertise zur Seite und freuen sich auf ein Zusammenarbeiten mit Ihnen.

Sprechen Sie uns gerne an, wir freuen uns auf Ihre Anfrage!

Team

Niklas Nies
Consultant
Solutions
niklas.nies at
finbridge.de
LinkedIn | Xing

Steffen Jahr
Senior Manager
Solutions
steffen.jahr at
finbridge.de
LinkedIn | Xing

Frank Kirr
Senior Expert
Solutions
frank.kirr at
finbridge.de
LinkedIn | Xing

Quellen

DORA-Verordnung: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020PC0595

FINBRIDGE

Mehr Insights und Themen

Finbridge GmbH & Co. KG
Louisenstraße 100
61348 Bad Homburg v. d. H.
www.finbridge.de