Fact About

firstcloud

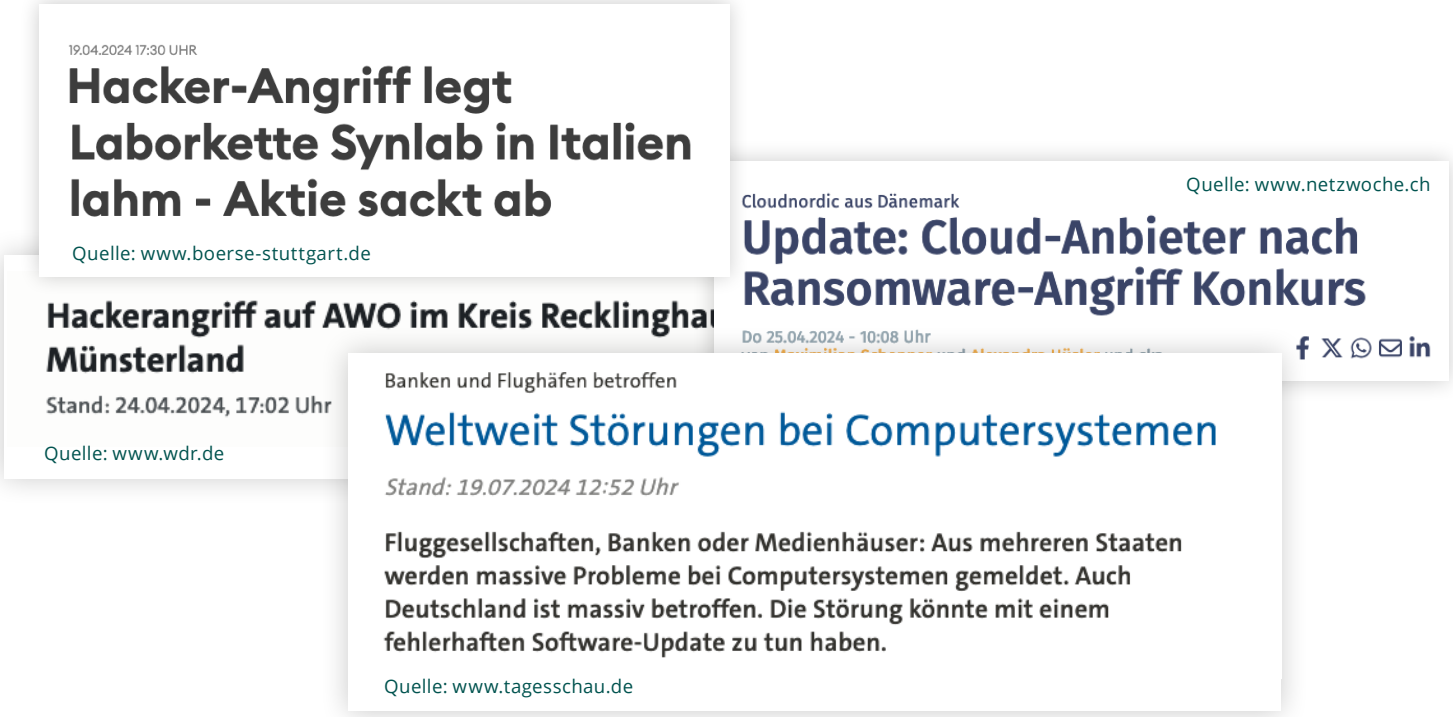
DORA – eine branchenweite Herausforderung und wie wir diese gemeinsam bewältigen werden

fact digital uncomplicators

DORA – Digital Operational Resilience Act

Ein Text von: **Aleksandar Ivezić**

Die Digitalisierung hat in den letzten Jahren insbesondere in der Finanzbranche einen beispiellosen Aufschwung erlebt. Mit dieser zunehmenden Digitalisierung geht jedoch auch ein erhöhtes Risiko einher, das durch Cyberangriffe, System-ausfälle und andere IT-bezogene Störungen verursacht wird.



Um diesen immer größer werdenden Risiken entgegenzuwirken, hat die Europäische Union den Digital Operational Resilience Act (DORA) eingeführt. Dieses Whitepaper bietet einen kurzen Überblick über DORA, die Zielsetzung, die Anwendungsbereiche, die Auswirkungen auf Informations- und Kommunikationstechnologiedienstleistungen (IKT-Dienstleistungen) sowie auf die vertraglichen Regelungen für IKT-Dienstleister.

Zusätzlich gehen wir in diesem Beitrag auf die Vorschläge und Maßnahmen der Fact ein und geben unseren Kunden einen Vorgehensplan an die Hand, wie wir gemeinsam diese Herausforderung meistern können.

Was ist DORA?

Der Digital Operational Resilience Act (DORA) ist eine Verordnung der Europäischen Union, die als Zielsetzung die Harmonisierung europäischer und nationaler Standards zur Stärkung der digitalen operativen Widerstandsfähigkeit im Finanzsektor hat. Die Verordnung zielt explizit darauf ab, die operationelle Widerstandsfähigkeit der Finanzbranche gegenüber IT-bezogenen Risiken zu stärken.

DORA legt Anforderungen fest, die sicherstellen sollen, dass Finanzinstitute und ihre Dienstleister in der Lage sind, Cyberbedrohungen und Systemausfällen standzuhalten und ihre Geschäftsabläufe auch unter extremen Bedingungen aufrechtzuerhalten und fortzuführen.

Wen betrifft DORA?

DORA betrifft eine Vielzahl von Akteuren innerhalb der Finanzbranche, wie bspw.:

- Banken
- Versicherungen
- Einrichtungen der betrieblichen Altersvorsorge
- Bausparkassen
- Wertpapierfirmen
- Kreditinstitute
- Zahlungsdienstleister
- IKT-Dienstleister, die wesentliche Dienstleistungen für diese Institutionen bereitstellen

Die Verordnung hat somit sowohl auf die Finanzinstitute und den Finanzsektor selbst als auch auf die ihnen zuarbeitenden Dienstleister erhebliche Auswirkungen.

Wie sieht der Zeitplan aus?

DORA wurde am 28. Dezember 2022 im Amtsblatt der EU veröffentlicht und trat 20 Tage später, am 17. Januar 2023, in Kraft. Die Verordnung ist ab dem **17. Januar 2025 in allen EU-Mitgliedstaaten direkt anwendbar**, wodurch Finanzinstitute und ihre IKT-Dienstleister aus heutiger Sicht nicht mehr so viel Zeit haben, um die erforderlichen Maßnahmen umzusetzen und die Einhaltung der neuen Vorschriften sicherzustellen.

Wie sehen die Regelungen aus? Was sind die Anwendungsbereiche? Welche Handlungsfelder gibt es?

DORA setzt auf ein umfassendes Regelwerk, das in verschiedenen Bereichen der IT-Sicherheit und des Risikomanagements greift:

Der DORA-Anwendungsbereich gilt für alle Finanzinstitute innerhalb der Europäischen Union sowie für deren IKT-Dienstleister. Dazu gehören bspw.

- die systematische Stabilität,
- die Gewährleistung, dass Finanzinstitute auch in Krisenzeiten funktionsfähig bleiben und
- die kritische Infrastruktur zum Schutz der Finanzbranche als Teil der kritischen Infrastruktur Europas.

DORA deckt mehrere zentrale Handlungsfelder ab. Beispielsweise:

- **das IKT-Risikomanagement**: Einführung robuster Risikomanagementverfahren für IT-Systeme und Daten,
- **das IKT-Incident-Management**: Etablierung von Prozessen für die Meldung und Bearbeitung von IT-Vorfällen,
- **die IKT-Sicherheitsvorkehrungen:** Implementierung von Maßnahmen zur Prävention und Abwehr von Cyberangriffen,
- **die IKT-Tests:** Durchführung von regelmäßigen Penetrationstests und Simulationen, um die Widerstandsfähigkeit zu prüfen,
- **die Abhängigkeit von Drittanbietern:** Management der Risiken, die durch externe Dienstleister entstehen, insbesondere bei kritischen Dienstleistungen.

Wie sind die Auswirkungen auf IKT-Dienstleistungen?

Die Einführung von DORA bedeutet, dass alle Finanzinstitute ihre IKT-Dienstleistungen auf den Prüfstand stellen müssen. Sie sind verpflichtet, sicherzustellen, dass ihre IT-Systeme und Datenmanagementprozesse robust und widerstandsfähig gegenüber Cyberbedrohungen sind. Dies könnte erhebliche Investitionen in IT-Infrastruktur, Sicherheitslösungen und Schulungen für Mitarbeiter erforderlich machen. IKT-Dienstleister, die wesentliche Dienste für Finanzinstitute bereitstellen, stehen vor der Herausforderung, ihre Dienstleistungen den neuen Anforderungen von DORA anzupassen. Dazu gehören bspw.

- verstärkte Sicherheitsmaßnahmen: Implementierung von erweiterten Sicherheits-standards und -protokollen,
- Risikomanagement: Einführung von Prozessen zur kontinuierlichen Überwachung und Bewertung von Risiken,
- vertragliche Verpflichtungen: Anpassung der Verträge mit Finanzinstituten, um die Einhaltung von DORA zu gewährleisten. Dies betrifft explizit auch bereits bestehende Verträge und somit alle Fact Kunden. Dabei unterscheidet DORA zwischen grund-legenden und kritischen IKT-Dienstleistungen, was sich in den vertraglichen Regelungen widerspiegeln muss.

Diese Einstufung ist durch das Finanzunternehmen zu treffen und erfolgt in

- grundsätzliche Einstufung (Anhang D1)
- kritische/wichtige Einstufung (Anhang D2)

Thema	grundsätzlich	kritisch/wichtig
Anforderungen an Form und Veränderung von Vereinbarungen	ja	erweitert
Beschreibung der Dienstleistung	ja	erweitert
Beschreibung der Dienstleistungsgüte	ja	erweitert
Unterauftragsvergabe	nein	ja
Standort	ja	ja
Datenschutz	ja	ja
Zugang zu Daten	ja	ja
IKT-Vorfallsunterstützung	ja	ja
Zusammenarbeit mit Aufsichtsbehörden	ja	ja
Prüfrechte / fortlaufende Überwachung	nein	ja
Kündigungsrechte und Fristen	ja	erweitert
Teilnahme an Schulungen des Finanzunternehmens	ja	ja
Berichtspflichten	nein	ja
Notfallpläne	nein	ja
Spezifische Maßnahmen zur IKT-Sicherheit	nein	ja
Beteiligung an TLPT	nein	ja
Ausstiegsstrategien	nein	ja

Anhang D1

Erfolgt die Einstufung nach Anhang D1 unterliegen IKT-Dienstleister, die grundlegende Dienste bereitstellen, standardmäßigen vertraglichen Verpflichtungen. Die vertraglichen Regeln beinhalten bspw.:

- eine regelmäßige Berichterstattung über die Sicherheitsmaßnahmen,
- die Erfüllung von Mindestanforderungen an Sicherheitsprotokolle,
- die Einhaltung der gesetzlichen Meldepflichten bei Sicherheitsvorfällen.

Anhang D2

Für IKT-Dienstleister, die als kritisch oder wichtig (Anhang D2) eingestuft werden, gelten strengere Anforderungen wie bspw.:

- erhöhte Berichtspflichten: umfassendere und häufigere Berichterstattung an die Finanzinstitute und Aufsichtsbehörden,
- erweiterte Sicherheitsanforderungen: zusätzliche Sicherheitsprotokolle und kontinuierliche Überwachung,
- Audits und Prüfungen: regelmäßige externe Prüfungen zur Bewertung der Sicherheitsmaßnahmen,
- Krisenmanagementpläne: Verpflichtung zur Erstellung und Pflege von Krisenmanagementplänen für den Fall schwerwiegender Störungen.

Wie geht die Fact mit den DORA-Herausforderungen um?

Die Fact beschäftigt sich schon seit langer Zeit mit den DORA Anforderungen und wir haben bereits ausführlich über die bei Fact eingeleiteten Maßnahmen berichtet. Sowohl in **digitalen Treffen**, über **Newsletter** sowie in größerem Umfang auf der **Fact Impulse Veranstaltung** in Düsseldorf. Aus dieser Kommunikation und den konstruktiven Gesprächen mit vielen unserer Kunden hat sich ein relativ standardisiertes Vorgehen entwickelt, welches im Nachfolgenden dargestellt wird:

1. Abstimmung des Vorgehens zwischen dem Finanzunternehmen und Fact
2. Prüfung der aktuellen Vertragslage durch Fact
3. Einstufung durch das Finanzunternehmen (Anhang D1 oder D2)
4. Erstellung eines Rahmenvertrags-Entwurfs für den Anhang D1 sowie D2 durch Fact
5. Versand des passenden Regelwerks durch Fact
6. Verhandlung des Regelwerks und des Preises
7. Umsetzung der im Vertrag vereinbarten Maßnahmen

Der Weg über einen neuen bzw. erweiterten Rahmenvertrag ermöglicht es uns als IKT-Dienstleister, die Regelungen in einen einzelnen Vertrag zu fassen. Somit können wir Finanzunternehmen – unabhängig davon welche und wieviele Produkte und Dienstleistungen von Fact verwendet werden – ein einziges globales Regelwerk bieten. Dieses Regelwerk orientiert sich dabei an den DORA-Vorschriften, wobei es auch bei diesen Regelungen Sachverhalte gibt, die für uns als IKT-Dienstleister nur schwer bzw. unmöglich umsetzbar sind.

Wir stellen diese kritischen Punkte in den Verhandlungen mit unseren Kunden deutlich dar und bieten Lösungen an, die für das Finanzunternehmen und die Fact umsetzbar und tragbar sind. Dies zeigt auch deutlich, dass DORA eine branchenweite Herausforderung ist und wir diese nur gemeinsam bewältigen können.

Fazit

Der Digital Operational Resilience Act (DORA) stellt eine bedeutende regulatorische Entwicklung dar, die die operationelle Resilienz der Finanzbranche in der EU stärken soll. Durch die Einführung strengerer Anforderungen an das IKT-Risikomanagement und die Zusammenarbeit mit IKT-Dienstleistern trägt DORA dazu bei, die Widerstandsfähigkeit gegenüber Cyberbedrohungen und Systemausfällen zu erhöhen.

Finanzunternehmen müssen bis 2025 umfangreiche Maßnahmen ergreifen, um die Anforderungen von DORA zu erfüllen und so ihre Geschäftskontinuität in einer zunehmend digitalisierten Welt zu gewährleisten.

Dazu gehört auch die Vertragsaktualisierung mit bestehenden IKT-Dienstleistern wie der Fact, mit dem Ziel, die zusätzlichen Maßnahmen nach gemeinsamer Verhandlung fest in das Vertragswerk zu integrieren.

Haben Sie Fragen oder möchten Sie sich zu diesen Themen austauschen? Lassen Sie uns darüber sprechen!

Aleksandar Ivezić
Senior Manager
Sales
+49 2131 777 238
a.ivezic@fact.de

fact digital uncomplicators

Fact Informationssysteme & Consulting GmbH

Hauptsitz Neuss
Hellersbergstraße 11 | 41460 Neuss | +49 2131 777-0 | info@fact.de

Standort Frankfurt am Main
Friedensstraße 6-10 | 60311 Frankfurt am Main | +49 69 8740313-121 | info@fact.de

Standort Erfurt
Erich-Kästner-Straße 1a | 99094 Erfurt | +49 2131 777-0 | info@fact.de

www.fact.de

Stand August 2024

Folgen Sie uns auf LinkedIn