Bild: Pixabay

Der CRA legt strenge Anforderungen an Hersteller, Importeure und Händler fest.

Findet DORA

Mit der fortschreitenden Entwicklung in der IT kommen nicht nur neue Chancen, sondern auch erhöhte Risiken, insbesondere im Bereich der IT-Sicherheit und operativen Resilienz. Um diesen Herausforderungen zu begegnen, hat die Europäische Union die Digital Operational Resilience Act (DORA) verabschiedet.

Dieses Regelwerk zielt darauf ab, die operative Widerstandsfähigkeit von Finanzunternehmen zu stärken und die Risiken von IT-Störungen und Cyberangriffen systematisch zu reduzieren. Doch was genau steckt hinter DORA, und was bedeutet das für Unternehmen?

Was ist DORA?

Die Digital Operational Resilience Act (DORA) ist ein EU-Gesetz, das im Jahr 2022 verabschiedet wurde und ab dem 17. Januar 2025 in Kraft tritt. Es richtet sich an alle Finanzdienstleister in der Europäischen Union und zielt darauf ab, ihre operative Resilienz in einer zunehmend digitalen Welt zu stärken. Dabei adressiert DORA insbesondere Risiken, die aus der Abhängigkeit von Technologie und Drittanbietern resultieren.

Mit DORA wird erstmals ein einheitlicher, sektorübergreifender Ansatz geschaffen, der Unternehmen verpflichtet, robuste Standards in der IT-Sicherheit, im Risikomanagement und bei der Zusammenarbeit mit Drittanbietern einzuhalten.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Warum wurde DORA eingeführt?

Die Einführung von DORA wurde durch mehrere Faktoren notwendig:

1. Zunahme von Cyberangriffen

Die Zahl und Komplexität von Cyberangriffen auf Finanzunternehmen haben in den letzten Jahren stark zugenommen. Ein erfolgreicher Angriff kann nicht nur für das betroffene Unternehmen verheerende Folgen haben, sondern auch das Vertrauen in das gesamte Finanzsystem untergraben.

2. Technologische Abhängigkeiten

Finanzdienstleister verlassen sich zunehmend auf Drittanbieter für IT-Dienste wie Cloud-Computing, Datenanalysen und Zahlungssysteme. Diese Abhängigkeit birgt Risiken, insbesondere wenn es bei den Dienstleistern zu Ausfällen oder Sicherheitsvorfällen kommt.

3. Fragmentierte Regulierungslandschaft

Vor DORA existierten in der EU keine einheitlichen Standards für die digitale Resilienz von Finanzunternehmen. Dies führte zu Unterschieden in der Umsetzung und erschwerte die Zusammenarbeit zwischen Unternehmen und Aufsichtsbehörden.

Mit DORA will die EU sicherstellen, dass die Finanzindustrie widerstandsfähiger gegen digitale Bedrohungen wird und ein stabiler Rahmen für die Bewältigung von IT- und Cyberrisiken geschaffen wird.

Die fünf Hauptkomponenten von DORA

DORA ist ein umfassendes Regelwerk, das sich in fünf zentrale Bereiche gliedert:

1. Governance und Risikomanagement

Unternehmen müssen ein robustes Risikomanagement für ihre IT-Systeme und -Prozesse implementieren. Dies umfasst:

- Klare Verantwortlichkeiten für die IT-Sicherheit auf Managementebene.
- Regelmässige Bewertungen der IT-Risiken.
- Massnahmen zur Sicherstellung der Geschäftskontinuität im Falle von IT-Störungen.

2. IT-Risikomanagement

DORA fordert Unternehmen dazu auf, ihre IT-Risiken systematisch zu analysieren und zu minimieren. Dazu gehören:

- Sicherheitsmassnahmen wie Firewalls, Verschlüsselung und Multi-Faktor-Authentifizierung.
- Regelmässige Updates und Patches, um Schwachstellen zu schliessen.
- Frühwarnsysteme zur Identifikation von Bedrohungen.

3. Operative Resilienz und Tests

Finanzdienstleister müssen ihre operative Resilienz regelmässig testen. Dazu zählen:

- Penetrationstests, um Schwachstellen in IT-Systemen zu identifizieren.
- Krisenübungen, um die Reaktion auf IT-Ausfälle zu simulieren.
- Stresstests für verschiedene Szenarien, wie Cyberangriffe oder Naturkatastrophen.

4. Drittanbieter-Management

DORA legt grossen Wert auf die Kontrolle von Drittanbietern, da viele Unternehmen für ihre IT-Infrastruktur auf externe Dienstleister angewiesen sind. Die Anforderungen umfassen:

- Vertragsklauseln, die Sicherheitsstandards und Audit-Rechte garantieren.

– Überwachung der Dienstleister durch regelmässige Bewertungen.
– Ein Risikomanagementplan für den Fall, dass ein Drittanbieter ausfällt.

5. Berichterstattung und Aufsicht

Im Rahmen von DORA müssen Unternehmen Vorfälle und Schwachstellen dokumentieren und der zuständigen Aufsichtsbehörde melden. Ziel ist es, Transparenz zu schaffen und frühzeitig auf Bedrohungen reagieren zu können.

Wer ist von DORA betroffen?

DORA richtet sich an eine breite Palette von Unternehmen in der Finanzindustrie, darunter:

– Banken und Kreditinstitute
– Versicherungen
– Wertpapier- und Investmentgesellschaften
– Zahlungsdienstleister
– Kryptowährungs-Dienstleister
– IT-Dienstleister, die kritische Infrastrukturen für Finanzdienstleister bereitstellen

Die Verpflichtungen variieren je nach Grösse, Geschäftsmodell und Rolle im Finanzsektor. Auch kleinere Finanzdienstleister müssen DORA-Anforderungen erfüllen, jedoch in einem angepassten Umfang.

Welche Strafen können von der EU verhängt werden?

Die Digital Operational Resilience Act der EU sieht empfindliche Sanktionen bei Verstössen vor, die von zuständigen nationalen Aufsichtsbehörden und den drei zentralen europäischen Aufsichtsbehörden (EBA, ESMA, EIOPA) durchgesetzt werden. Die möglichen Konsequenzen umfassen:

Verwaltungsstrafen

Dazu gehören Bussgelder, deren Höhe sich nach dem Schweregrad und der Häufigkeit der Verstösse richten. Diese können bei schwerwiegenden Verstössen gegen die Anforderungen an das IKT-Risikomanagement, die Meldepflicht von Vorfällen oder die Resilienztests verhängt werden.

Auflagen zur Abstellung von Mängeln

Unternehmen können verpflichtet werden, innerhalb eines vorgegebenen Zeitraums Korrekturmassnahmen zu ergreifen, um identifizierte Schwächen zu beheben. Dies kann beispielsweise die Anpassung von Verträgen mit Drittanbietern oder die Einführung zusätzlicher Sicherheitsmassnahmen umfassen.

Strafrechtliche Sanktionen

In einigen Fällen sind auch strafrechtliche Konsequenzen möglich, wenn etwa grob fahrlässig oder vorsätzlich gegen die Sicherheitsanforderungen verstossen wurde.

Die genauen Strafen können je nach nationaler Gesetzgebung und der Schwere des Verstosses variieren, aber die EU will durch DORA sicherstellen, dass Unternehmen hohe Standards der digitalen Resilienz einhalten, um den Finanzsektor vor zunehmenden Cyberrisiken zu schützen. Nationale Behörden haben dabei weitreichende Befugnisse zur Durchsetzung, einschliesslich Vor-Ort-Inspektionen und der Einforderung von Informationen von Unternehmen.

Herausforderungen bei der Umsetzung

Die Umsetzung von DORA bringt mehrere Herausforderungen mit sich, insbesondere für kleinere Unternehmen oder solche mit komplexen IT-Infrastrukturen:

Ressourcen und Know-how

Viele Unternehmen müssen in neue Technologien und Fachkräfte investieren, um die Anforderungen zu erfüllen.

Integration in bestehende Prozesse

DORA erfordert oft tiefgreifende Anpassungen in der IT- und Risikomanagementstrategie eines Unternehmens.

Überwachung von Drittanbietern

Die Einhaltung der DORA-Standards durch externe Dienstleister zu gewährleisten, ist ein komplexer Prozess, der rechtliche und organisatorische Herausforderungen mit sich bringt.

Hohe Meldeanforderungen

Die umfangreichen Berichts- und Dokumentationspflichten können zusätzlichen Verwaltungsaufwand verursachen.

Tipps zur erfolgreichen Umsetzung

Um die Anforderungen von DORA zu erfüllen, sollten Unternehmen folgende Massnahmen ergreifen:

Risikobewertung

Eine umfassende Analyse der bestehenden IT-Systeme und -Prozesse ist der erste Schritt, um Schwachstellen zu identifizieren.

Schulungen und Awareness

Mitarbeitende auf allen Ebenen sollten über die DORA-Anforderungen und die Bedeutung von IT-Sicherheit informiert werden.

Zusammenarbeit mit Drittanbietern

Unternehmen sollten eng mit ihren IT-Dienstleistern zusammenarbeiten, um sicherzustellen, dass diese die DORA-Standards einhalten.

Kontinuierliche Verbesserung

Die digitale Resilienz ist ein dynamischer Prozess. Regelmässige Tests und Anpassungen sind entscheidend, um auf neue Bedrohungen reagieren zu können.

Fazit

Die Digital Operational Resilience Act (DORA) ist ein wegweisendes Gesetz, das die digitale Widerstandsfähigkeit der europäischen Finanzindustrie stärken soll. Mit einheitlichen Standards für IT-Sicherheit, Risikomanagement und die Überwachung von Drittanbietern setzt DORA einen neuen Massstab für die operative Resilienz.

Für Unternehmen bedeutet dies jedoch auch eine erhebliche Verantwortung und die Notwendigkeit, in neue Technologien und Prozesse zu investieren. Wer sich frühzeitig auf die Anforderungen vorbereitet und die Umsetzung strategisch angeht, kann DORA jedoch auch als Chance nutzen, um die eigene Wettbewerbsfähigkeit zu steigern und das Vertrauen von Kunden und Investoren zu stärken.