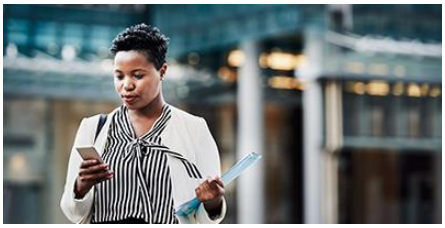
DORA

Nieuw kader in de maak voor digitale weerbaarheid in de financiële sector



Digitalisering en innovatie leidt tot meer cyberrisico's, ook in de financiële sector. De Europese Commissie (EC) heeft daarom een voorstel gedaan voor een verordening om de digitale weerbaarheid van de sector te vergroten: de Digital Operational Resilience Act (DORA). De Autoriteit Financiële Markten (AFM) verwacht dat DORA eind 2022 in werking treedt. Het is belangrijk voor financiële ondernemingen om zich hier tijdig op voor te bereiden.

De afhankelijkheid van digitale processen in de financiële sector neemt toe, net als het aantal gerichte cyberaanvallen op financiële organisaties. De gevolgen voor organisaties en hun klanten kunnen groot zijn. In het ergste geval treft het zelfs het financiële systeem als geheel. Digitale weerbaarheid staat daarom hoog op de Europese én nationale agenda's.

Met DORA heeft de EC drie hoofddoelen voor ogen:

1. De versnipperde regels ten aanzien van digitale weerbaarheid in de EU harmoniseren
2. Een basiskader scheppen voor financiële organisaties waarvoor nog geen regelgeving is
3. Het beter mitigeren van risico's van uitbesteding door de financiële sector aan kritieke digitale derde dienstverleners

DORA stelt eisen aan financiële organisaties ten aanzien van: IT-risicomanagement, IT-incidenten, periodieke testen van digitale weerbaarheid, de beheersing van risico's bij uitbesteding aan (kritieke) derden. Daarbij wordt rekening gehouden met de grootte, het risicoprofiel en het systeembelang van individuele organisaties.

Eén uniform wetgevend kader

Er gelden nu al (Europese) regels op het gebied van cyberrisico's, maar deze zijn beperkt en versnipperd. Voor sommige financiële organisaties zijn er alleen regels op landelijk niveau of zijn er zelfs helemaal geen regels. Dat leidt tot inconsistenties in wet- en regelgeving tussen lidstaten en zorgt voor onnodige kosten voor de financiële sector. Met DORA wil de EC één uniform wetgevend kader implementeren. Bestaande wetgeving voor de digitale weerbaarheid blijft overigens gelden.

Nieuwe wetgeving: de Digital Operational Resilience Act verordening (DORA)

Het risico op cyberaanvallen in de financiële sector wordt steeds groter. Om dit risico te beperken heeft de Europese Commissie in 2021 een voorstel gedaan voor een verordening om de digitale weerbaarheid van de financiële sector te vergroten: de Digital Operational Resilience Act (DORA). De verordening, die in mei 2022 een voorlopig akkoord heeft bereikt, moet ervoor zorgen dat de financiële sector in Europa bij ernstige operationele verstoringen veerkrachtig kan blijven. De nieuwe verordening zal de huidige wetgeving niet vervangen, maar een aanvulling zijn door een kader te bieden voor het beheer van operationele risico´s in een digitale omgeving. Het doel van de nieuwe wetgeving is om ervoor te zorgen dat financiële instellingen cyberaanvallen kunnen weerstaan door best practices te implementeren, zoals gegevensbescherming en incident response planning.

Inhoud DORA verordening

In de DORA verordening komen vereisten voor de beveiliging van netwerk- en informatiesystemen van bedrijven en organisaties, die actief zijn in de financiële sector en van cruciale derde partijen die

hen ICT-gerelateerde diensten verlenen, zoals Cloud platforms en/of gegevensanalyses. De verordening zal belangrijke veranderingen in het leven roepen in de manier waarop financiële dienstverleners omgaan met hun gegevensbeveiliging.

Alle financiële instellingen zullen op grond van de DORA een cyberbeveiligingsprogramma implementeren dat beleidslijnen, procedures en risicobeheersactiviteiten omvat. Het beleid dient jaarlijks gecontroleerd te worden door een externe financiële toezichthouder.

In de DORA verordening zijn de volgende primaire eisen beschreven:

Bedrijven moeten een plan hebben voor de reactie op incidenten, met een gedetailleerde beschrijving van wat een cyberaanval inhoudt, hoe werknemers moeten reageren en hoe de activiteiten worden hersteld als er een inbreuk is;

Bedrijven moeten een cyberbeveiligingsprogramma bijhouden dat een beoordeling omvat van de risico´s van cyberaanvallen en een actieplan om die risico´s te beperken;

Bedrijven moeten hun digitale infrastructuur aan passende beveiligingscontroles onderwerpen. Deze controles omvatten encryptie, authenticatie, toegangscontroles, audit trails, monitoringssystemen, eventmanagement systemen en incident response plannen;

Bedrijven moeten incidenten melden als zij zich voordoen, zodat regelgevers hun kwetsbaarheden kunnen beoordelen en aanbevelingen kunnen doen om hun beveiliging te verbeteren;

Bedrijven moeten een plan hebben om de continuïteit van de dienstverlening te waarborgen bij eventuele onderbrekingen.

DORA is een eenduidig wettelijk kader voor digitale weerbaarheid van de financiële sector in alle EU-landen. Daarmee zorgt het voor uniformering van wetgeving en een gelijk speelveld voor financiële dienstverleners binnen de Europese Unie. DORA stelt eisen aan de risico´s van uitbesteding aan kritieke derde dienstverleners, om deze beter te beheersen. DORA heeft ook als doel om een veel duidelijkere basis te leggen voor Europese financiële toezichthouders.