Maurits van den Heuvel en Rob Stout (CPI):

Digitale Operationele Veerkrachtwet (DORA), een nieuwe vorm van digitale veiligheid

In het tijdperk van digitalisering en technologie staat de veerkracht van digitale infrastructuren centraal. De Europese Unie (EU) heeft de groeiende noodzaak erkend om een uitgebreid kader te creëren dat de ononderbroken werking van vitale digitale systemen waarborgt. Als reactie op deze behoefte is de Digitale Operationele Veerkrachtwet (Digital Operational Resilience Act, oftewel DORA) ontwikkeld als een cruciale wetgeving. De specialisten van CPI Risk, Finance & Governance zien in de dagelijkse praktijk de issues die bedrijven hebben met het invoeren van cq. compliant worden aan DORA. In onderstaand artikel gaan de beide partners Maurits van den Heuvel en Rob Stout in op de achtergrond en ontwikkelingen die hebben geleid tot de invoering van DORA, de inhoud van de wet, status van de wet, technische standaarden en termijnen. Tevens geven ze een overzicht van de belangrijkste implicaties van de wet.

DORA is in essentie ontworpen om de operationele veerkracht van digitale dienstverleners te versterken, waaronder Cloud services, online marktplaatsen en financiële kerninfrastructuureenheden. De financiële kerninfrastructuur (FKI) is een groep van financiële instellingen en marktinfrastructuren die van essentieel belang zijn voor het Nederlandse betalings- en effectenverkeer. Te denken valt aan aanbieders van en deelnemers aan beurs- en handelsplatformen, *clearing* en *settlement* systemen. Of een instelling tot de FKI behoord wordt in Nederland vastgesteld door De Nederlandse Bank op basis van criteria, na afstemming met de AFM en het Ministerie van Financiën. De DORA wet belooft de manier waarop organisaties en dienstverleners hun digitale operaties beheren en beschermen te herdefiniëren.

REDENEN KOMST DORA

Ontwikkelingen die hebben geleid tot DORA

- **Toenemende Cyberdreigingen:** De stijging van cyberaanvallen, variërend van ransomware-incidenten tot grootschalige datalekken, benadrukt de urgentie van het versterken van cybersecurity-maatregelen. DORA heeft tot doel een uniforme aanpak van cybersecurity en incidentrapportage vast te stellen, waarbij samenwerking tussen relevante belanghebbenden wordt bevorderd.
- **Groeiende Digitale Verwevenheid:** De onderlinge verwevenheid van digitale systemen over landsgrenzen is enorm toegenomen. Dit heeft de noodzaak vergroot om tot een gecoördineerde inspanning te komen om de veerkracht van de financiële sector te waarborgen. DORA erkent de grensoverschrijdende aard van digitale diensten en benadrukt het belang van samenwerking tussen EU-lidstaten.
- **Realisatie na de pandemie:** De COVID-19-pandemie heeft kwetsbaarheden in digitale infrastructuur blootgelegd. Van thuiswerken tot remote doktersadvies, de afhankelijkheid van digitale diensten nam toe tijdens de crisis, waardoor veerkracht een cruciale zorg werd. De bepalingen van DORA streven ernaar deze kwetsbaarheden aan te pakken en voor te bereiden op toekomstige uitdagingen.
- **Harmonisatie van Regelgeving:** DORA streeft naar harmonisatie binnen de EU van verschillende bestaande voorschriften en richtlijnen met betrekking tot digitale diensten, waardoor een eenduidig kader voor operationele veerkracht wordt gecreëerd. Deze vereenvoudiging en consolidatie van regels moet de nalevingslast verminderen.

Maurits van den Heuvel

INHOUD VAN DE WET

De DORA wet is opgebouwd uit 5 belangrijke pijlers die ieder in een hoofdstuk zijn uitgeschreven:

Rob Stout

1. **ICT Risicomanagement:** Door middel van het risicomanagement proces houdt het management van de organisatie overzicht op ICT-risico's en worden risico's gemonitord en opgevolgd.
2. **Incident management:** Om de robuustheid van de gehele financiële sector te verhogen zijn er aanvullende eisen gesteld ten aanzien van het melden van incidenten met (potentieel) hoge impact. Organisaties moeten deze incidenten melden bij de nationale toezichthouder.
3. **Risicobeheer van derde aanbieders:** Vanwege langere ICT-ketens en de afhankelijkheid van deze leveranciers, zijn de eisen ten aanzien van derde aanbieders uitgebreid.
4. **Testen van veerkracht:** De Europese Commissie heeft eisen gesteld met betrekking tot continue testen van ICT-systemen en de aard van de uit te voeren testen. Organisaties moeten op basis van een gevarieerd palet van testen kunnen vaststellen dat hun kritische processen resilient zijn.
5. **Informatie-uitwisseling:** De wet bevat een aanmoediging om meer informatie te delen tussen organisaties om zodoende de reactiesnelheid van organisaties en kennis te vergroten. Dit is geen verplichting maar optioneel.

Los van deze indeling van vijf belangrijkste hoofdstukken zijn er een aantal essentiële elementen die extra benadrukt worden in deze wet. Laten we dieper ingaan op de essentiële elementen van de wet:

- **Risicobeheer:** legt een sterke nadruk op risicobeheer. Digitale dienstverleners zijn verplicht risico's te identificeren, te beoordelen en te beheersen die van invloed kunnen zijn op hun diensten. Bestuurders worden geacht actief betrokken te zijn bij risicobeheer. De wet beoogt de voorbereiding op onvoorziene gebeurtenissen te verbeteren.
- **Incidentrapportage:** Een belangrijk aspect van DORA is de verplichting voor digitale dienstverleners om aanzienlijke incidenten te melden aan bevoegde autoriteiten en getroffen klanten. Transparantie in rapportage is essentieel voor het beheer van risico's en een tijdige respons op verstoringen.
- **Grensoverschrijdende Samenwerking:** DORA erkent de onderlinge verbondenheid van digitale diensten en bevordert samenwerking tussen EU-lidstaten en relevante autoriteiten om grensoverschrijdende incidenten effectief aan te pakken.
- **Derden Dienstverleners:** De wet breidt haar toepassingsgebied uit naar derden dienstverleners die de kernactiviteiten van digitale dienstverleners ondersteunen. Van deze derden wordt verwacht dat zij aan bepaalde veerkrachteisen voldoen.
- **Testen en Evaluatie:** De wet schrijft regelmatige tests en evaluaties voor van de systemen van digitale dienstverleners om hun veerkracht te waarborgen. Deze tests kunnen verschillende ongunstige scenario's simuleren om de capaciteit van een entiteit om verstoringen te doorstaan te beoordelen. Testen heeft niet alleen betrekking op het uitvoeren van periodieke pen tests. Achterliggend doel is dat een organisatie een betrouwbaar beeld heeft van de veerkracht van haar digitale infrastructuur door middel van het analyseren van de (resultaten van de) verschillende testen. Hierbij kan men denken aan, onder andere, de volgende testen:
    - o Pen testing;
    - o Uitwijktesten; o Functionele testen na oplevering van nieuwe software;
    - o Performance testen.

- **Boetes voor Niet-Naleving:** DORA kan diverse sancties opleggen voor het niet nakomen van haar bepalingen, waaronder 1) boetes, 2) eisen om bepaalde gedragingen te stoppen en/of 3) publicatie van de aard van de overtreding en de identiteit van de organisatie of bestuurder. Deze sancties hebben tot doel de naleving van de wet te bevorderen.

Sancties die opgelegd kunnen worden, kunnen gebaseerd zijn op:

1) De materialiteit, de ernst en de duur van de inbreuk
2) De mate van verantwoordelijkheid van de voor de inbreuk verantwoordelijke natuurlijke of rechtspersoon;
3) De financiële draagkracht van de verantwoordelijke natuurlijke of rechtspersoon;
4) De omvang van de door de verantwoordelijke natuurlijke of rechtspersoon behaalde winsten of vermeden verliezen, voor zover deze kunnen worden bepaald;
5) De verliezen voor derde partijen ten gevolge van de inbreuk, voor zover deze kunnen worden vastgesteld;
6) De mate van medewerking van de verantwoordelijke natuurlijke of rechtspersoon met de bevoegde autoriteit, onverminderd de noodzaak om de terugbetaling van de door die persoon behaalde winsten of vermeden verliezen te garanderen;
7) Eerdere inbreuken van de verantwoordelijke natuurlijke of rechtspersoon

- **Gecoördineerde Respons op Incidenten:** DORA definieert een raamwerk voor een gecoördineerde respons op incidenten, waarbij wordt gezorgd dat getroffen partijen samenwerken om de impact van verstoringen te minimaliseren.
- **Toezicht en Controle:** Bevoegde autoriteiten in elke EU-lidstaat zullen verantwoordelijk zijn voor het toezicht en de controle op de naleving van DORA's bepalingen. Deze gedecentraliseerde aanpak beoogt een effectieve uitvoering te waarborgen.
- **Tijdige Melding aan het Publiek:** DORA vereist dat digitale dienstverleners het publiek tijdig informeren over incidenten die een aanzienlijke impact hebben op hun diensten. Deze transparantie stelt consumenten in staat geïnformeerde beslissingen te nemen.
- **Voortdurende Verbetering:** DORA moedigt voortdurende verbetering aan op het gebied van operationele veerkracht, waarbij wordt erkend dat het digitale landschap voortdurend evolueert en nieuwe bedreigingen kunnen ontstaan.

In aanvulling op de DORA wet worden er momenteel diverse RTS-en (Regulatory Technical Standards) en ITS-en (Implementing Technical Standards) ontwikkeld. RTS-en worden nu ontwikkelt met betrekking tot:

- ICT-risicomanagement raamwerk en een vereenvoudigd ICT-risicomanagement raamwerk;
- Criteria voor de classificatie van ICT gerelateerde incidenten;
- Het specificeren van het beleid met betrekking tot ICT-dienstverlening door derde partijen.

Een ITS wordt momenteel ontwikkeld die definieert hoe een register moet worden ingericht voor het bijhouden van contractuele regelingen over het gebruik van ICT-diensten van externe ICT-dienstverleners. Later in 2024 zullen nog een aantal RTS-en, ITS-en en richtlijnen gepubliceerd worden .

Tijdslijnen: DORA is gepubliceerd op 27 december 2022 en werd van kracht op 16 januari 2023. Op 17 januari 2025 is de DORA wet van toepassing op alle organisaties in de sector.

RELATIE MET ANDERE WETTEN EN RAAMWERKEN

De DORA wet is geen op zichzelf staande wet. De beheersmaatregelen waar DORA betrekking op heeft zijn ook in meer of mindere mate terug te vinden in andere raamwerken of regelgeving op het gebied van Risk Management en/of Informatiebeveiliging.

ISO27001, DNB Good Practice, NEN7510 (raamwerken), NIS, NIS2 en CER (wetten), ze hebben heel veel overlap. Afhankelijk van de sector waarin uw organisatie werkzaam is zal een specifiek raamwerk gangbaar zijn. DNB Good Practice voor Informatiebeveiliging is, net als DORA, van toepassing op de financiële sector, waarbij bijvoorbeeld het NEN7510 raamwerk wordt toegepast in de zorg.

Het is zeer waarschijnlijk dat veel organisaties al gedeeltelijk compliant zijn met DORA wanneer u één of meerdere van de genoemde regelgevingen en/of raamwerken in uw organisatie hanteert.

AANBEVELINGEN

Voor zowel organisaties als individuen is het essentieel om op de hoogte te blijven van de implicaties van de Digitale Operationele Veerkrachtwet (DORA). Digitale dienstverleners moeten de nodige maatregelen treffen om te voldoen aan de eisen van DORA, waaronder risicobeheer, incidentrapportage en het naleven van veerkrachteisen. Individuen moeten bewust zijn van de transparantie en rapportagevereisten die DORA met zich meebrengt, en ze moeten kritisch nadenken over de digitale dienstverleners waarmee ze in zee gaan.

Deze wet is een belangrijke stap in de richting van een meer veerkrachtige digitale toekomst, waarbij de nadruk wordt gelegd op cybersecurity en de bescherming van digitale diensten. Het is in het belang van ons allen om deze ontwikkelingen te volgen en te zorgen voor een veiliger digitale omgeving voor iedereen. Samen kunnen we bouwen aan een sterke digitale samenleving die bestand is tegen de uitdagingen van de moderne tijd.

Voor wie nog niet gestart is met een inventarisatie is het nu het moment om hier een begin mee te maken. Afhankelijk van het volwassenheidsniveau van uw organisatie ten aanzien van Risk Management en Cybersecurity heeft u meer of minder te doen. Gemiddeld genomen heeft een organisatie minimaal 1 jaar nodig om alle beheerdoelstellingen te bereiken.

Een aanpak die wij als CPI hanteren en reeds bij diverse klanten toepassen ziet er als volgt uit:

1. Gap-analyse van het huidige raamwerk voor ICT-risicobeheer
   a. DORA-vereisten versus geïmplementeerde beheermaatregelen
2. Projectplan a. Ontwerp & Implementatie b. Update van beheersmaatregelen/definiëren van nieuwe beheersmaatregelen
3. Opstellen van onderliggende documentatie, procedures, etc.
4. Testen
   a. 'Sample-of-1' b. 'Dry-runs'
5. Overgang en 'go live'
   a. Overdracht aan de staande organisatie ■

CPI helpt inmiddels diverse organisaties met het compliant worden met de DORA wetgeving: www.meetcpi.com.