CFA: met Dora klaar voor de storm

Can Yilmaz - 19 februari 2025

De Europese Digital Operational Resilience Act (Dora) markeert een nieuwe mijlpaal in de bescherming van onze digitale wereld. Het is een stevige reactie op een tijdperk waarin cyberdreigingen en IT-incidenten bijna vaste kost zijn. Met Dora zet de Europese Unie een heldere standaard: digitale weerbaarheid is een absolute noodzaak.

Wie de afgelopen jaren het nieuws heeft gevolgd, weet dat cyberaanvallen en IT-storingen onverminderd toenemen, zowel in frequentie als qua impact. Denk aan de corrupte CrowdStrike-update van afgelopen zomer, die chaotische gevolgen had voor talloze bedrijven en de financiële sector voor meer dan 1,4 miljard dollar aan schade berokkende. Of aan de groeiende dreiging van *ransomware*, die steeds geavanceerder wordt.

Ook datalekken blijven zorgen baren. Zo zijn in de afgelopen twee jaar onder andere bij ABN Amro, PFZW en PME mogelijk klantgegevens uitgelekt. Saillant detail: die lekken zijn telkens veroorzaakt door zwakke schakels bij derden. Bij ABN Amro door een *ransomware*-aanval bij haar leverancier van klantcommunicatietechnologie. Bij PFZW en PME vanwege een lek in de software die een klantonderzoeksbureau gebruikte. Zij hebben vooralsnog geen juridische procedures of boetes opgeleverd, maar komen het klantvertrouwen en de klanttevredenheid uiteraard niet ten goede.

Deze incidenten illustreren dat onze digitale infrastructuur kwetsbaar is. Voor de financiële sector kunnen deze kwetsbaarheden rampzalig zijn. Daarom introduceert Dora een breed pakket maatregelen dat niet alleen de symptomen bestrijdt, maar ook de oorzaken aanpakt.

Stevige fundering

Dora is geen administratieve formaliteit of een eenvoudig afvinklijstje. Het is een uitgebreid raamwerk dat financiële entiteiten verplicht om proactief hun digitale zwaktes aan te pakken. Van IT-risicobeheer en bedrijfscontinuïteitsplannen tot robuuste incidentresponse-procedures en het verplicht testen van systemen: de wet dwingt financiële entiteiten om de lat over de gehele linie hoger te leggen.

Een belangrijk onderdeel van Dora is de verplichting om een helder beeld te hebben welke bedrijfsfuncties welke IT-assets gebruiken. Dit lijkt op het eerste gezicht eenvoudig, maar in de praktijk blijkt het IT-landschap dikwijls een kluwen van complexe en sterk verweven systemen te zijn, vaak afhankelijk van derde partijen. Dat maakt naast identificatie ook de rest van de implementatie van Dora een forse uitdaging.

Gelukkig biedt de wet ruimte voor een risico-gebaseerde aanpak. Dit betekent dat financiële entiteiten vooral eerst prioriteit moeten geven aan de bescherming van hun kritieke functies, gebaseerd op hun specifieke IT-risico's. Entiteiten krijgen daarnaast de ruimte om implementatiekeuzes te maken die passen bij hun omvang, productaanbod en risicoprofiel. Voor grote entiteiten met complexe IT-landschappen zijn de verwachtingen dan ook hoger dan voor kleine entiteiten. Desalniettemin moeten ook kleine entiteiten de digitale weerbaarheid organisatiebreed versterken.

Derden blijven een aandachtspunt

Een bijzonder aspect van Dora is de focus op derde partijen. Financiële entiteiten die afhankelijk zijn van externe IT-leveranciers - bijvoorbeeld *cloudproviders* en *cybersecurity*-specialisten - moeten in hun contracten strikte weerbaarheidsvereisten opnemen.

Daarnaast moeten zij rapporteren met welke IT-leveranciers zij samenwerken, zodat toezichthouders op Europees niveau een overzicht krijgen van de leveranciers die bij falen mogelijk de stabiliteit van de financiële sector in gevaar kunnen brengen. Deze 'kritieke' IT-leveranciers komen onder direct toezicht van een Europese toezichthouder te staan. Welke toezichthouder dat is – EBA, Esma of Eiopa – hangt af van welk type financiële entiteiten het grootste klantbestand van de kritieke IT-leverancier vormen. Zijn dat bijvoorbeeld banken, dan zal de EBA als primaire opzichter optreden.

Toch ontslaat dit de financiële entiteiten niet van hun eigen verantwoordelijkheid. De weerbaarheid van de hele keten – inclusief uitbesteed werk – blijft uiteindelijk hun verantwoordelijkheid. Dit vereist naast robuuste contracten ook een cultuur van voortdurende controle en verbetering.

Toezicht: serieuze aandacht

Intussen krijgt Dora serieuze aandacht van zowel Europese als Nederlandse toezichthouders. In 2025 zullen zij onder andere thematische en individuele onderzoeken uitvoeren, het register van IT-leveranciers opvragen en de meest significante entiteiten uitnodigen voor verplichte deelname aan 'dreigingsgestuurde' penetratietesten op live productiesystemen.

Toezichthouder DNB heeft daarnaast aangekondigd dat aanstaande bestuurders en andere beleidsbepalers bij hun geschiktheidsbeoordeling getoetst worden op kennis van IT-risicomanagement. Het bestuur is eindverantwoordelijk voor de beheersing van IT-risico's en de digitale operationele weerbaarheid-strategie.

Kosten versus kansen

Hoewel de *compliance-deadline* van 17 januari 2025 inmiddels verstreken is, worstelen veel entiteiten nog met de volledige implementatie van Dora. De kosten en inspanningen zijn aanzienlijk, maar moeten in breder perspectief worden gezien. De financiële- en reputatieschade van een grote *ransomware*-aanval, IT-storing of datalek kan immers vele

malen hoger uitvallen. De gemiddelde kosten van een datalek zijn volgens onderzoek ongeveer 4,8 miljoen dollar, die van een cyberaanval tot wel 5 miljoen dollar, terwijl de schadeposten van incidenten zelfs kunnen oplopen tot 10 miljoen dollar. De belangen zijn dus groot.

Dora biedt een unieke kans om een structurele verbetering van de digitale weerbaarheid te realiseren. Een soort verzekering: je hoopt het nooit nodig te hebben, maar als de storm komt, ben je blij dat je voorbereid bent.

Klaar voor de toekomst

De digitale wereld wordt steeds complexer en bedreigingen worden steeds geavanceerder. Met Dora geeft Europa een krachtig signaal: de financiële sector moet niet alleen bestand zijn tegen huidige dreigingen, maar ook klaar zijn voor wat de toekomst brengt. Het is een stap naar een veerkrachtiger, veiliger en duurzamer digitaal landschap.

Zijn we klaar voor de storm? Met Dora wordt die kans aanzienlijk groter.

Can Yilmaz is Regulatory Consultant, lid van de Advocacy Committee van CFA Society Netherlands en werkte onder meer op het Global Dora Programma van ING Bank.

Dit artikel is afkomstig van Investment Officer, een journalistiek platform voor professionals werkzaam in de beleggingsindustrie.

www.investmentofficer.com