FINNIUS

Cybersecurity in de financiële sector: waar staan we en wat komt eraan?

28 oktober 2021

8 MINUTEN

Inleiding: wat hebben kaas, paspoort-uitgiftes en olie gemeen?

Onlangs wijdde onderzoeksprogramma Zembla een uitzending aan de vraag hoe goed Nederland beschermd is tegen ransomware-aanvallen: pogingen van hackers om systemen van organisaties binnen te dringen, te versleutelen en pas weer vrij te geven nadat de getroffen organisatie het door de hackers geëiste losgeld heeft betaald. De meeste door Zembla benaderde getroffen organisaties willen hierover niet in de openbaarheid treden. Dat gold bijvoorbeeld voor een kaasproducent die na een ransomware-aanval eerder dit jaar tijdelijk geen kaas meer kon leveren, met lege kaasschappen bij de Albert Heijn tot gevolg. De burgemeester van Hof van Twente vertelt in de uitzending wel openlijk over wat haar gemeente vorig jaar overkwam: na een succesvolle aanval – vermoedelijk vanuit Rusland – op het account van de systeembeheerder kon de gemeente niet meer bij haar systemen. De hackers eisten EUR 750.000, volledig te voldoen in bitcoins. De gemeente weigerde te betalen en besloot IT-specialisten in te schakelen om het netwerk opnieuw op te bouwen. Totale kosten: meerdere miljoenen euro's.

In de uitzending wordt ook ingegaan op de ontwikkelingen wereldwijd. Zo vallen hackers inmiddels ook vitale organisaties aan, zoals energie- en drinkwaterbedrijven. Sprekend voorbeeld is de aanval van een hackerscollectief – wederom vermoedelijk vanuit Rusland – op de belangrijkste oliepijplijn van de VS dit voorjaar, met benzine hamsterende Amerikanen tot gevolg.

Net zoals een samenleving niet zonder goed opererende energie- en drinkwaterbedrijven kan, kan ze ook niet zonder een adequaat functionerende financiële sector. Gelukkig hebben zich in Nederland tot op heden geen ernstig ontwrichtende cyberincidenten in, bijvoorbeeld, het betalingsverkeer voorgedaan, maar de (Europese) wetgever en toezichthouders zijn er niet gerust op.[1] Voor mij aanleiding om in deze blog stil te staan bij het huidige regelgevend kader voor cybersecurity in de financiële sector en een blik te werpen op de wijzigingen die de Europese Commissie (**EC**) in dit verband heeft voorgesteld.

Huidige situatie: wettelijk kader is versnipperd en bestaat vooral uit (enkele) open normen

In Europa is de regelgeving voor de financiële sector grotendeels sectoraal ingericht en daarmee versnipperd. Dat geldt (dus) ook voor de in sectorale richtlijnen en verordeningen opgenomen voorschriften inzake cybersecurity.

In Nederland komen die Europese voorschriften in veel gevallen weer samen in de Wet op het financieel toezicht (**Wft**), het Besluit Gedragstoezicht financiële ondernemingen Wft (**BGfo**) en het Besluit prudentieel toezicht (**Bpr**). Zo bevatten artikelen 3:17 Wft en 20 Bpr normen inzake cybersecurity voor onder andere banken, verzekeraars en betaalinstellingen. De toepasselijke –

algemene – kernbepaling luidt op grond van artikel 20 Bpr als volgt:

"*De financiële onderneming (…) beschikt over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevensverwerking te waarborgen.*"

Voor instellingen die primair onder AFM-toezicht staan – zoals beheerders van beleggingsfondsen, bewaarders, beleggingsondernemingen en financiëledienstverleners – zijn er de algemene bepalingen van artikelen 4:14 en 4:15 Wft inzake de integere en beheerste bedrijfsvoering. Vervolgens moet in het BGfo met een lantaarn worden gezocht naar voorschriften inzake cybersecurity. Dan tref je bijvoorbeeld artikel 30 BGfo voor (beheerders van) icbe's en bewaarders aan, dat qua formulering net zo algemeen is als artikel 20 Bpr. Voor beleggingsondernemingen en beheerders is wel in rechtstreeks werkende Europese verordeningen de algemene opdracht opgenomen om in procedures en maatregelen te voorzien op het gebied van informatiebeveiliging en bedrijfscontinuïteit; daar valt cybersecurity uiteraard ook onder, maar erg specifiek is het allemaal nog niet.

Voor sommige type financiële instellingen gelden aanvullende IT-normen op grond van Europese (gedelegeerde) verordeningen, zoals voor centrale tegenpartijen (**CCP's**) en exploitanten van handelsplatformen. Ook gelden er specifieke beveiligingsvoorschriften voor het verlenen van betaaldiensten (artikel 26c e.v. Bpr). Echter, van een echt eenduidig en geconcretiseerd wettelijk kader voor cybersecurity binnen de financiële sector kan, gelet op de hiervoor aangehaalde algemene bepalingen, lastig worden gesproken.

Daar waar de wet niet een eenduidig en geconcretiseerd kader inzake cybersecurity voor de financiële sector voorschrijft, hebben toezichthouders in Nederland en Europa wel getracht financiële instellingen van concrete(re) handvatten met betrekking tot dit onderwerp te voorzien. In Nederland publiceert DNB bijvoorbeeld al sinds 2010 een Q&A Informatiebeveiliging, die zij in 2019 heeft geactualiseerd in de Good Practice Informatiebeveiliging 2019-2020. En ook de AFM heeft in 2019 haar 'Principes voor Informatiebeveiliging' gepubliceerd, waarmee zij haar verwachtingen uitspreekt over het gewenste gedrag van onder toezicht staande instellingen op het gebied van informatiebeveiliging. Op Europees niveau heeft de European Banking Authority (**EBA**) onder andere richtsnoeren inzake ICT-risicomanagement gepubliceerd. Deze richtsnoeren zijn van toepassing op (i) betaalinstellingen en (ii) banken en beleggingsondernemingen zoals bedoeld in artikel 4 lid 1 onder 3 CRR. Verder gelden sinds 31 juli 2021 de richtsnoeren van de European Securities and Markets Authority (**ESMA**) inzake uitbesteding aan aanbieders van clouddiensten. Voorts hebben toezichthouders ICT-testraamwerken ontwikkeld, zoals TIBER-NL (een initiatief van DNB en inmiddels ook toegepast door de AFM) en TIBER-EU (ontwikkeld door de Europese Centrale Bank).

Tot slot wijs ik hier nog op de sinds 9 november 2018 in Nederland van kracht zijnde Wet beveiliging netwerk- en informatiesystemen (Wbni, ook wel Cybersecuritywet genoemd). De Wbni

vormt de implementatie van de Europese NIS-richtlijn en verplicht aanbieders van essentiële diensten (AED's) om bepaalde IT-beveiligingseisen in acht te nemen. In de Wbni worden ook het bankwezen en infrastructuur voor de financiële markten als essentiële diensten aangemerkt. DNB is bevoegd om banken, exploitanten van handelsplatformen en CCP's als AED aan te merken. De materiële beveiligingseisen uit de Wbni gelden echter weer niet voor deze door DNB aangewezen entiteiten[2] (reden: er rusten op deze entiteiten volgens de wetgever al vergelijkbare eisen ingevolge financiële regelgeving, zie ook hiervoor). Wel moeten de door DNB aangewezen AED's op grond van de Wbni ernstige cyberincidenten melden bij DNB en het Nationaal Cyber Security Centrum.[3]

Toekomstige situatie: één Europese cybersecurity-verordening voor grootste deel financiële sector

De EC wil een einde maken aan de bestaande versnippering van cybersecurity-regels en ongecoördineerde initiatieven in de verschillende lidstaten. Om die reden heeft de EC op 24 september 2020 een nieuwe verordening voorgesteld die volledig is gewijd aan cybersecurity: de verordening betreffende digitale operationele veerkracht voor de financiële sector (**DORA**).

De bedoeling van de EC is dat DORA rechtstreeks van toepassing wordt op het overgrote deel van de financiële sector, waaronder banken, verzekeraars, beleggingsondernemingen, fondsbeheerders, elektronischgeldinstellingen, cryptodienstverleners, CCP's, handelsplatformen, effectenbewaarinstellingen en bepaalde bemiddelaars. Daarnaast komen op grond van het voorstel ook wettelijke auditors en auditkantoren onder het toepassingsbereik van DORA te vallen, evenals bepaalde aanbieders van ICT-diensten.

DORA bestaat grofweg uit vijf pijlers:

1. **ICT-risicomanagement:** voorschriften voor een juiste inrichting van het ICT-risicomanagement-raamwerk, inclusief regels over (i) governance en organisatie, (ii) beleid, procedures en protocollen ter bescherming tegen ICT-risico's (iii) voorwaarden die aan ICT-systemen moeten worden gesteld, (iv) beleid inzake detectie, respons en herstel bij ICT-gerelateerde incidenten, (v) backup-beleid en (vi) en het periodiek testen van (onder andere) de beveiliging van de eigen systemen.
2. **Behandeling van ICT-incidenten**: normen voor de identificatie, classificatie en behandeling van ICT-gerelateerde incidenten, alsmede een meldingsplicht bij ernstige ICT-gerelateerde incidenten aan de bevoegde autoriteiten.
3. **Beheer ICT-risico's bij uitbesteding:** regels voor het beheer van risico's als gevolg van uitbesteding van ICT-diensten aan derden, inclusief verplichtingen met betrekking tot de

inhoud van uitbestedingsovereenkomsten tussen financiële instellingen en ICT-aanbieders.

4. **Toezicht op cruciale ICT-dienstaanbieders**: introductie van een toezichtkader voor cruciale aanbieders van ICT-diensten aan de financiële sector.
5. **Samenwerking en handhaving**: regels inzake de onderlinge samenwerking tussen bevoegde autoriteiten en regels met betrekking tot het toezicht op en handhaving van DORA door bevoegde autoriteiten.

Al met al is DORA een omvangrijk wetgevingsinitiatief van de EC, waarbij van financiële instellingen veel gevraagd zal worden op het gebied van (het adequaat managen van) cybersecurity. Met een steeds verder digitaliserende financiële sector (en wereld) kan ik me dat ook voorstellen, zolang wetgever en toezichthouders voldoende oog blijven houden voor het belangrijke beginsel van proportionaliteit. ICT-risico's en vooral ook de potentiële impact daarvan zullen immers van instelling tot instelling verschillen. Positief vind ik dat het huidige gefragmenteerde landschap met DORA zal worden vervangen door één set aan cybersecurity-regels die op het grootste deel van de Europese financiële sector rechtstreeks van toepassing zal zijn.

Vanaf wanneer DORA precies van toepassing zal zijn, en in welke vorm, is op dit moment nog niet duidelijk. Onderhandelingen over de tekst zijn op dit moment in Europa gaande. De EC heeft in ieder geval voorgesteld om DORA van toepassing te laten zijn 12 maanden na de inwerkingtredingsdatum. Dat betekent dat financiële instellingen nog even de tijd hebben om zich op DORA voor te bereiden, maar het tegelijkertijd raadzaam is om – voor zover een instelling dat nog niet heeft gedaan – met die voorbereidingen alvast een begin mee te maken.

[1] Zie bijvoorbeeld de recente nieuwsbrief van het Basel comité van 20 september 2021 (link) en het recente ESA rapport inzake risico's en kwetsbaarheden in het Europese financiële systeem van 8 september 2021 (link).

[2] Op grond van artikel 4 Besluit beveiliging netwerk- en informatiesystemen (Bbni).

[3] Zie www.ncsc.nl. De meldplicht rust op grond van artikel 10 Wbni en artikel 3 Bbni ook op door DNB aangewezen afwikkelondernemingen en centrale effectenbewaarinstellingen.

Specialisten

Laurens Hillen

T +31 (0)20 767 01 80
T +31 (0)20 767 01 84 (direct)
M +31 (0)6 21 66 37 76
laurens.hillen@finnius.com