Cybercriminaliteit: regelgeving

Alom wordt cyber gezien als één de grootste risico's van de huidige tijd. Cybersecurity en voorkomen van (schade veroorzaakt door) verstoring, uitval of misbruik van ICT staan bovenaan de prioriteitenlijstjes van ondernemingen en overheden. Ook in het recht krijgt dit meer een plaats door middel van bijvoorbeeld zorgplichten. Door onder meer de complexiteit van de (Europese) regelgeving, het open karakter van veel (Europese) normen en de snelheid van de digitalisering is het lastig om die in kaart te brengen en daaraan uitvoering te geven.[1] In dit tweede deel zullen Robert Pessers en Annevi Etienne trachten enig inzicht te verschaffen en aandacht besteden aan de (op handen zijnde) wet- en regelgeving op het gebied van cybersecurity.

1. Inleiding

Cybercriminaliteit blijft zich ontwikkelen zoals de tragische ontwikkelingen in Oekraïne aantonen. Onderdeel van de oorlogsstrategie van Rusland vormen cyberaanvallen die op hun beurt weer hebben geleid tot cyberaanvallen door hackers die Oekraïne steunen. Ook buiten dit publieke domein ontwikkelt de cybercriminaliteit zich snel doordat de uitvoering steeds eenvoudiger wordt. *Cybercrime-as-a-service* is een zeer lucratief business model.

Overheden, ondernemingen en consumenten moeten zich hiertegen wapenen. De gevolgen van cyberaanvallen kunnen immers groot zijn: de maatschappij kan ontwricht raken, ondernemingen kunnen (volledig) stilvallen en vertrouwelijke bedrijfs- en persoonsgegevens kunnen verloren gaan of een pressiemiddel worden bij een losgeldeis na het succesvol plaatsen van *ransomware*.[2]

Deze ontwikkelingen en de toenemende wereldwijde digitalisering hebben geleid tot en zullen leiden tot nog meer (Europese) en nationale regelgeving op het gebied van cybersecurity.[3] De regulering van de digitalisering geschiedt voor een groot deel via Europese richtlijnen, verordeningen, standaarden en aanbevelingen.[4] Zij leggen allerlei verplichtingen op het gebied van digitale veiligheid op.

Ter verduidelijking van deze verplichtingen wordt in deze bijdrage ingegaan op de huidige cybersecurity wet- en regelgeving. Allereerst wordt stilgestaan bij de Europese regelgeving. Vervolgens wordt ingegaan op de Nederlandse wet- en regelgeving, waaronder de wijze waarop de Europese richtlijnen in Nederland zijn geïmplementeerd. Ten slotte wordt aandacht besteed aan de (Europese) ontwikkelingen.

> *"Dit is een vorm van digitale oorlogsvoering die we nog niet eerder hebben gezien"*[5]

2. Europese regelgeving

De Europese Commissie lanceerde in 2020 de EU-strategie over cyberbeveiliging voor het digitale tijdperk.[6] Deze strategie omvat onder meer de inzet van alle nodige regelgevingsinstrumenten om de cyberveerkracht te verhogen voor alle private en publieke sectoren die een belangrijke rol vervullen in de economie en de samenleving.[7]

Deze regelgeving betreft onder meer de hierna te bespreken Algemene verordening gegevensbescherming (AVG) voor zover van belang voor cybersecurity, de Netwerk- en informatiebeveiligingsrichtlijn (NIB-richtlijn) en de Cyberbeveiligingsverordening (Cybersecurity Act).

[1] C. Bulten & C. Jansen, 'De taak van de commissaris in een digitale wereld: de noodzaak van awareness van cyber security', *Ondernemingsrecht* 2016/74, afl. 9, p. 355.
[2] N.M. Brouwer, 'De cyberverzekering: over incident response, boetes en ransomware', *MvV* 2022, nummer 2, p. 63; N. van der Voort & W. Warnaars, 'Crimineel of slachtoffer', *NJB* 2020/1385.
[3] Zie onze eerdere bijdrage voor meer uitleg over het feitelijk kader van cybercrime, waarin onder meer is ingegaan op de bekende cyberrisico's en wat er bekend is over de hackers achter de cyberaanvallen.
[4] C. Bulten & C. Jansen, 'De taak van de commissaris in een digitale wereld: de noodzaak van awareness van cyber security', *Ondernemingsrecht* 2016/74, afl. 9, p. 355.
[5] 'Cyberaanvallen op Oekraïne in volle gang: malware verspreid die computers sloopt', rtlnieuws.nl.
[6] Gezamenlijke mededeling aan het Europees parlement en de Raad, *De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk*, Europese Commissie, JOIN(2020)18 final, Brussel, 16 december 2020, p. 3.
[7] *De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk*, Europese Commissie, p. 6.

2.1 Netwerk- en informatiebeveiligingsrichtlijn (NIB-richtlijn)

De toegenomen digitalisering vraagt om een hoog niveau van cybersecurity in de Europese Unie.[8] In dit verband is de NIB-richtlijn in 2016 in werking getreden.[9] Deze richtlijn beoogt het tot stand brengen van een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen, de digitale weerbaarheid te vergroten en de gevolgen van cyberincidenten te verkleinen.[10] Deze NIB-richtlijn is in Nederland geïmplementeerd door middel van de Wet beveiliging netwerk- en informatiesystemen ('Wbni') waarop hierna nog separaat terug zal worden gekomen.

De noodzaak om deze beveiliging op orde te hebben, werd recent weer duidelijk. Ten tijde van de inval in Oekraïne werd een nieuw computervirus ingezet, waarmee door middel van een zogeheten 'HermeticWiper' geprobeerd werd om het land verder te ontwrichten. Deze destructieve 'wiper' malware brengt zware schade toe aan complete pc's of computernetwerken en richt zich op Oekraïense overheidsorganisaties en financiële instellingen.[11]

Maar er zijn ook minder dramatische maar wel impactvolle andere voorbeelden zoals de 'opzettelijke en kwaadaardige' cyberaanval op Vodafone Portugal, waardoor het landelijk netwerk werd geraakt.[12] Ruim zeven miljoen mensen ondervonden problemen aan de 4G/5G, televisie-, telefonie- en SMS-diensten.[13]

> *"A newly discovered strain of data-wiping malware has surfaced in Ukraine, coinciding with the physical invasion of the country by Russian forces."*[14]

De NIB-richtlijn is van toepassing op 'netwerk- en informatiesystemen' en gericht op de volgende twee groepen: Aanbieders van Essentiële diensten (AED's) en 'digitaledienstverleners' (Digitale Dienstverlener(s)). AED's zijn publieke en private entiteiten die diensten verlenen die essentieel zijn voor de economie en maatschappij van de EU, en waarvoor geldt dat een cyberincident aanzienlijke verstorende effecten zal hebben voor de verlening van die diensten.[15] Digitale Dienstverleners (digitale service providers) worden onderverdeeld in aanbieders van onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten.[16]

Nu deze groep niet nader gespecificeerd wordt en lidstaten niet gehouden zijn om Digitale Dienstverleners aan te wijzen, is het in beginsel aan iedere Digitale Dienstverlener zelf om te bezien of zij onder het bereik van de NIB-richtlijn (en de op basis daarvan opgestelde nationale regelgeving) valt.[17]

De NIB-richtlijn bepaalt kort gezegd dat AED's en Digitale Dienstverleners passende en

[8] J.P. Kalis, 'De Netwerk en informatiebeveiligingsrichtlijn, *Computerrecht* 2017/48, paragraaf 1.
[9] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (*PbEU* 2016, L 194). Te raadplegen op https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016L1148.
[10] A.W. Hagdorn, 'De Wet beveiliging netwerk- en informatiesystemen', *Tijdschrift Vervoer & Recht* 2021-5, p. 311.
[11] 'Data wiper deployed in cyber-attacks targeting Ukrainian systems', portswigger.net; 'Cyberaanvallen op Oekraïne in volle gang: malware verspreid die computers sloopt', rtlnieuws.nl.
[12] 'Cyber-attack at Vodafone portugal knocks mobile network services offline', portswigger.net.
[13] 'Landelijk netwerk Portagal geraakt door 'terroristische cyberaanval', techzine.nl.
[14] 'Data wiper deployed in cyber-attacks targeting Ukrainian systems', portswigger.net.
[15] Zie artikelen 4 lid 4 jo. 5 lid 2 NIB-richtlijn. Het betreft (publiek- en privaatrechtelijke) entiteiten in de sectoren energie, vervoer, bankwezen, infrastructuur van financiële markten, gezondheidszorg, drinkwatervoorzieningen en digitale infrastructuur. Het is aan de lidstaten om te bepalen welke organisaties hier concreet onder vallen
[16] Blijkens art. 16 lid 11 NIB-richtlijn moet het wel gaan om digitale dienstverleners van enige omvang, omdat de kleine en micro-ondernemingen zijn uitgezonderd van de NIB-richtlijn. Meer concreet gelden de volgende omzet- en personeelseisen: de Wbni is alleen van toepassing op digitale dienstverleners met meer dan 50 werknemers in dienst en een omzet van meer dan € 10 miljoen per jaar. Zie hiervoor onder meer de definitie van Digitale Dienstverleners in artikel 1 Wbni jo. artikel 16 NIB-richtlijn.
[17] Het Ministerie van Economische Zaken en Klimaat heeft een document gepubliceerd die als leidraad kan dienen om te bepalen of men kan worden beschouwd als een Digitale Dienstverlener (en dientengevolge de Wbni moet naleven. Zie Ministerie van Economische Zaken en Klimaat, 'Wet Beveiliging Netwerk en Informatiesystemen (Wbni) voor Digitale dienstverleners', september 2018, 388. Te raadplegen op https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners.

evenredige technische en organisatorische maatregelen moeten nemen om hun ICT adequaat te beveiligen.[18] Het niveau van beveiliging moet zijn afgestemd op de risico's die (kunnen) optreden. Nu sprake is van een open norm, heeft de Cyber Security Raad een Handreiking uitgegeven waarin zij meer concrete handvaten geeft.[19] De CSR adviseert om onder meer gebruik te maken van een 'tweefactorauthenticatie', het nemen van maatregelen om ICT te beschermen tegen virussen en malware en aansluiting te zoeken bij gedragscodes en/of certificeringsmechanismen.[20]

Mochten zich incidenten voordoen met 'aanzienlijke gevolgen voor de continuïteit van de door hen verleende diensten', dan dienen AED's en Digitale Dienstverleners onverwijld aan de bevoegde autoriteit of het 'Computer Security Incident Response Team' (CSIRT) een melding te doen. Hierbij van belang is dat beveiligingseisen en meldplichten uit de NIB-richtlijn niet enkel gelden voor moedigwillige aanvallen (zoals hacking), maar ook voor ICT-incidenten als gevolg van menselijke fouten of incidenten die de beschikbaarheid van gegevens of diensten in gevaar brengen.[21]

2.2 De Europese Cyberbeveiligingsverordening (Cybersecurity Act)

Op 17 april 2019 is de Europese verordening 2019/881 inzake ENISA (het Agentschap van de Europese Unie voor cyberbeveiliging) en de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (de 'Cyberbeveiligingsverordening') tot stand gekomen.[22] Deze is op 27 juni 2019[23] in werking getreden en wordt ook wel de 'Cybersecurity Act' genoemd. Omdat sprake is van een verordening geldt deze rechtstreeks in alle lidstaten. Anders dan de NIB-richtlijn, hoeft de Cyberbeveiligingsverordening dus niet te worden omgezet in nationale regelgeving.

Het doel van deze Cyberbeveiligingsverordening is onder meer het verhogen van de cyberveiligheid in de Europese Unie door bijvoorbeeld het verbeteren van de coördinatie tussen lidstaten en instellingen en het ontwikkelen van systemen die ertoe leiden dat burgers en organisaties inzicht krijgen in de mate van veiligheid van de systemen. Dat laatste wordt beoogd met de introductie van eenvormige certificeringssystemen.

Deze Cyberbeveiligingsverordening sluit aan bij het potentieel grensoverschrijdende karakter van cyberincidenten. Een ernstige verstoring van ICT-systemen in één lidstaat kan ook andere lidstaten treffen.[24] Illustratief is in dit verband een cyberaanval op de IT-diensten van het opslagbedrijf Evos, die heeft geresulteerd in laad- en losproblemen van olie in de havens van Terneuzen, Gent en Malta.[25]

Tot de inwerkingtreding van deze Cyberbeveiligingsverordening waren de bevoegdheden en beleidsmaatregelen van cyberbeveiligingsautoriteiten en rechtshandhavingsinstanties voornamelijk nationaal geregeld.[26] Lidstaten hanteerden op het gebied van certificering voor cyberbeveiliging verschillende standaarden en werkwijzen hetgeen leidde tot versnippering.

[18] Hagdorn, *TVR* 2021, p. 313.
[19] CSR, *Ieder bedrijf heeft digitale zorgplichten. Een handreiking voor bedrijven op het gebied van cybersecurity*, Nijmegen: 2017.
[20] CSR, 2017, p. 14-15.
[21] J.P. Kalis & G.P. van Duijvenvoorde, 'Een nieuw kader voor netwerk- en informatiebeveiliging; een cultuuromslag?', *NtER* 2018, r. 3/4, p. 116.
[22] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (*PbEU* 2019, L 151/15). Te raadplegen op https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:32019R0881.
[23] Niet de gehele Cyberbeveiligingsverordening is toen in werking getreden. Enkele bepalingen zijn op 28 juni 2021 in werking getreden.
[24] S. van der Hof, A.R. Lodder & G.J. Zwenne, *Recht en computer(Recht en Praktijk, nr. ICT4)*, Deventer: Kluwer 2014, par. 13.5.3.
[25] 'Olieopslagplaatsen in Terneuzen en Gent hebben vertragingen na cyberaanval', tweakers.net; 'IT-systemen olieterminals in Terneuzen 'verstoord' na cyberaanval Terneuzen', rtlnieuws.nl.
[26] Zie overweging 5 bij de Verordening (EU) 2019/881.

Het Europese cyberbeveiligingscertificaat dient om die 'lappendeken' aan beveiligingseisen te ondervangen en te komen tot een uniform systeem. Momenteel is certificering niet verplicht voor digitale dienstverleners. In 2023 wordt dit heroverwogen en bezien of in bepaalde gevallen certificering verplicht dient te worden.

Teneinde dit hoge gemeenschappelijke cyberbeveiligingsniveau in de hele Unie te bewerkstelligen, is ENISA belast met het actief steun verlenen aan lidstaten, instellingen, organen en instanties van de Unie met het oog op een betere cyberbeveiliging.[27] Het is aan ENISA om expertise op het gebied van beveiligingscertificering te ontwikkelen en in stand te houden en het gebruik van beveiligingscertificering binnen de EU te bevorderen.

2.3 Algemene Verordening Gegevensbescherming (AVG)

Bij een cyberincident komen veelal bedoeld of onbedoeld persoonsgegevens van natuurlijke personen vrij. De AVG dient tot het beschermen van die persoonsgegevens.[28] Dit houdt verband met het feit dat privacy in Europa wordt beschouwd als een mensenrecht. Het recht op privacy is bijvoorbeeld neergelegd in artikel 8 van het Europees Verdrag voor de rechten van de mens (EVRM) en artikel 94 van de Grondwet. Geheel vanzelfsprekend is dat niet. De Verenigde Staten erkennen privacy bijvoorbeeld niet als mensenrecht en daar wordt om die reden dan ook anders omgegaan met datalekken.[29]

Het feit dat privacy in Europa een mensenrecht is, maakt de staat verantwoordelijk voor het waarborgen van dit recht. Een dergelijk fundamenteel recht leent zich naar zijn aard bovendien minder voor 'verhandelbaarheid' dan een commodity, zoals privacy in de VS wordt gezien.[30]

De AVG geldt in beginsel voor alle organisaties die persoonsgegevens verwerken en bevat een verplichting om passende technische of organisatorische maatregelen te nemen om die data te beveiligen.[31] Artikel 32 lid 1 AVG stelt dat deze 'passende' maatregelen een op het risico afgestemd beveiligingsniveau moeten waarborgen, mede gelet op de stand van de techniek, kosten van de tenuitvoerlegging, de aard, omvang en context van de verwerking, de verwerkingsdoeleinden en de mogelijke risico's voor betrokkenen.

In de Handleiding AVG en UAVG van het Ministerie van Justitie en Veiligheid worden enkele voorbeelden van dergelijke technische en organisatorische maatregelen gegeven, zoals pseudonimisering en versleuteling van persoonsgegevens, toepassen van encryptie, opzetten van een firewall, het opslaan van gegevens in een beveiligde omgeving en het hanteren van een autorisatiebeleid waarbij de toegang tot gegevens wordt beperkt tot bepaalde medewerkers.[32]

In het geval dat zich een beveiligingsincident voordoet waarbij persoonsgegevens zijn betrokken, kan sprake zijn van een datalek dat in Nederland aan de Autoriteit Persoonsgegevens (AP) moet worden gemeld (en mogelijk aan de betrokkenen zelf). De AP is de onafhankelijke toezichthoudende autoriteit in Nederland zoals beschreven in Hoofdstuk VI AVG.

[27] J.C. Hulsebosch, 'De Europese 'Cybersecurity Act'', *Computerrecht* 2019/215, afl. 6, p. 398-399.
[28] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming) (*PbEU* 2016, L 119/1). De AVG vervangt de Wet bescherming persoonsgegevens (Wbp). Te raadplegen op https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679.
[29] N.M. Brouwer, *De cyberverzekering vanuit civielrechtelijk perspectief*, Deventer: Wolters Kluwer 2021, p. 59-60.
[30] N.M. Brouwer, *De cyberverzekering vanuit civielrechtelijk perspectief*, Deventer: Wolters Kluwer 2021, p. 59.
[31] Artikel 5 lid 1 sub f AVG; J.C. Hulsebosch, 'De Europese 'Cybersecurity Act'', *Computerrecht* 2019/215, afl. 6, p. 395-396.
[32] Schermer e.a., *Handleiding AVG en UAVG, Ministerie van Justitie en Veiligheid*, januari 2018, p. 62. Te raadplegen op https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming.

Blijkens artikel 4 onder 12 AVG kan van een inbreuk in verband met persoonsgegevens worden gesproken indien sprake is van een 'inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijzing of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens'. Er moet zich daadwerkelijk een beveiligingsincident hebben voorgedaan, en niet uitsluitend een dreiging of tekortkoming in de beveiliging die zou kunnen leiden tot een beveiligingsincident om te kunnen spreken van een datalek.[33]

De melding van een datalek is alleen verplicht indien sprake is van 'een inbreuk in verband met persoonsgegevens' die waarschijnlijk een 'risico inhoudt voor de rechten en vrijheden van natuurlijke personen'.[34] Als de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen zelf, moeten zij ook direct door de verwerkingsverantwoordelijke worden geïnformeerd.[35]

In geval van overtreding van de AVG is de AP bevoegd om een bestuurlijke boete op te leggen die maximaal € 20 miljoen of 4% van de wereldwijde jaaromzet bedraagt.[36] Binnen Europa loopt Nederland wat betreft de melding van datalekken voorop. Nederland had begin 2021 het op een na hoogste aantal gemelde datalekken (66.527) in Europa sinds in de invoering van de AVG.[37] Alleen Duitsland had op dat moment meer officiële meldingen van datalekken (77.747). De hoogte van de boetes is echter relatief laag. In Nederland bedroegen de in de eerste drie jaar opgelegde boetes in totaal € 2.5 miljoen. De Italiaanse toezichthouder heeft daarentegen al een boete van bijna € 70 miljoen opgelegd. DLA Piper heeft becijferd dat in Europa in het afgelopen jaar circa € 1,1 miljard aan boetes zijn opgelegd voor overtredingen van de AVG. Dit is een toename van 594 procent in vergelijking met het jaar ervoor.[38]

[33] J.C. Hulsebosch, 'Cybersecurity & Privacy: overlap van beveiligingseisen en samenloop van meldplichten?', *Computerrecht* 2018/250, p. 311.
[34] Artikel 33 lid 1 AVG.
[35] Artikel 34 AVG; Hagdorn, *TVR* 2021, p. 120.
[36] Schermer e.a., *Handleiding AVG en UAVG*, Ministerie van Justitie en Veiligheid, januari 2018, p. 91.
[37] 'Nederland tweede van Europa qua aantal meldingen datalekken sinds de invoering AVG', advocatie.nl.
[38] 'Onderzoek DLA Piper: 1,1 miljard euro aan AVG boetes', advocatie.nl.

Overigens vormen boetes niet de enige mogelijke sanctie. Artikel 82 AVG bepaalt dat "elke verwerkingsverantwoordelijke die bij verwerking is betrokken, (…) aansprakelijk [is] voor de schade die wordt veroorzaakt door verwerking die inbreuk maakt op deze verordening". Blijkens het vierde lid is sprake van een hoofdelijke aansprakelijkheid wanneer meerdere verwerkers betrokken zijn.

3. Nederlandse regelgeving

De NIB-richtlijn moest uiterlijk op 9 mei 2018 geïmplementeerd zijn in de nationale regelgeving van de lidstaten.[39] Nederland heeft dat niet gehaald. Per 9 november 2018 traden echter de Wet beveiliging netwerk- en informatiesystemen (Wbni) en het Besluit beveiliging netwerk- en informatiesystemen (Bbni) grotendeels in werking.

3.1 Wet beveiliging netwerk- en informatiesystemen (Wbni)

De Wbni strekt tot uitvoering van de NIB-richtlijn, voorheen ook wel de 'Cybersecuritywet' genoemd.[40] De Wbni beoogt de digitale weerbaarheid van Nederland, in het bijzonder van 'vitale aanbieders' en Digitale Dienstverleners, te bevorderen. Het begrip 'vitale aanbieders' volgt niet uit de NIB-richtlijn, maar is een Nederlandse invulling.[41] De groep 'vitale aanbieders' is onder te verdelen in twee categorieën: aanbieders van een essentiële dienst (AED) en andere aangewezen vitale aanbieders (AAVA), zoals telefoonnetbeheerders.[42] De AAVA zijn aanbieders van een dienst die niet zijn aangeduid als AED maar waarvan de continuïteit desondanks van vitaal belang wordt geacht voor de Nederlandse samenleving.[43]

Onder AED's vallen bijvoorbeeld Royal Schiphol Group N.V., waterleidingbedrijven zoals Evides en Waternet en de Divisie Havenmeester als

[39] Artikel 25 NIB-richtlijn.
[40] Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen), *Stb.* 2018, 387. Te raadplegen op https://wetten.overheid.nl/BWBR0041515/2021-08-01.
[41] Hagdorn, *TVR* 2021, p. 115.
[42] In het Bbni staat vermeld welke bestuursorganen een AED of een AAVA zijn; N. van der Voort & W. Warnaars, 'Crimineel of slachtoffer', *NJB* 2020/1385, afl. 22.
[43] Artikel 1 Wbni.

onderdeel van het Havenbedrijf Rotterdam. Het afwikkelen van scheepvaartverkeer in de Rotterdamse haven is van vitaal belang voor de Nederlandse samenleving. Nu het proces in hoge mate afhankelijk is van ICT-systemen, staat of valt de toegankelijkheid van de haven bij een veilig scheepvaartverkeer en een adequate afhandeling van lading.[44]

Voor AED's en Digitale Dienstverleners (hierna tezamen: aanbieders) geldt op grond van de Wbni een zorgplicht en een meldplicht.[45] De AAVA heeft enkel een meldplicht daar de zorgplicht voor deze categorie niet geldt. De zorgplicht van artikel 7 Wbni houdt in dat de aanbieders 'passende en evenredige technische en organisatorische maatregelen' moeten nemen om hun ICT-systemen te beheersen en de gevolgen van incidenten te verkleinen.[46] Die beveiligingsmaatregelen moeten onder meer rekening houden met de volgende aspecten: beveiliging van systemen en voorzieningen, behandeling van incidenten, beheer van bedrijfscontinuïteit, toezicht (monitoring), controle (auditing) en testen alsmede inachtneming van de internationale normen.[47]

De Wbni vult niet in hoe de aanbieders aan deze 'zorgplicht' moeten voldoen. Het is aan de organisaties zelf om te bepalen welke concrete maatregelen voor hen passend en evenredig zijn en dat periodiek te heroverwegen. Immers, wat nu passend en evenredig is, hoeft dat over zes maanden niet meer te zijn.

Incidenten die zich voordoen, moeten op grond van artikel 10 Wbni onverwijld worden gemeld. Ingeval van een Digitale Dienstverlener dient melding plaats vinden bij zowel het 'CSIRT voor digitale diensten' alsook bij de bevoegde autoriteit.[48] Een 'vitale aanbieder' is gehouden aan de Minister van Justitie en Veiligheid (NCSC) en aan de bevoegde autoriteit te melden.[49] De bevoegde autoriteit is in dit verband de Minister van Economische Zaken en Klimaat voor de energie sector en de digitale infrastructuur sector, De Nederlandsche Bank voor het bankwezen en de financiële sector, de Minister voor Medische Zorg voor de gezondheidszorg en de Minister van Infrastructuur en Waterstaat voor de vervoers- en drinkwatersector.

Nederland had begin 2021 het op een na hoogste aantal gemelde datalekken (66.527) in Europa sinds in de invoering van de AVG.[50]

Er is dus sprake van een dubbele meldplicht.[51] Dit geldt enkel voor incidenten ('elke gebeurtenis met een schadelijk effect op de beveiliging van netwerk- en informatiesystemen') of inbreuken op de beveiliging van netwerk- en informatiesystemen die *aanzienlijke* gevolgen voor de continuïteit van de verleende dienst kan hebben. Het gaat hierbij ondermeer om het aantal gebruikers dat door de verstoring van de dienst wordt getroffen of de gevolgen van een incident voor economische en maatschappelijke activiteiten.[52]

De bevoegde autoriteit heeft ingevolge hoofdstuk 6 Wbni specifieke bevoegdheden jegens essentiële diensten en digitale dienstverleners, waaronder het geven van een bindende aanwijzing (zoals de verplichting tot het nemen van een concrete beveiligingsmaatregel) en het nemen van corrigerende maatregelen zoals het opleggen van een last onder dwangsom en/of bestuurlijke (administratieve) boete.[53] De boetes kunnen oplopen tot maximaal € 5 miljoen.[54] Illustratief is in dit verband de beslissing in april 2021 om Waternet, die het waterbeheer in Amsterdam en omstreken verzorgt, onder

[44] Besluit beveiliging- en informatiesystemen. Zie artikelsgewijze toelichting, p. 10; 'Cybersecurity', reporting.portofrotterdam.com.
[45] N. van der Voort & W. Warnaars, 'Crimineel of slachtoffer', *NJB* 2020/1385, afl. 22, p. 1588.
[46] Artikel 14 NIB-richtlijn en artikel 7 Wbni.
[47] Artikel 7 lid 2 Wbni.
[48] Zie voor de bevoegde autoriteit artikel 4 lid 1 Wbni.
[49] Zie voor de bevoegde autoriteit artikel 4 lid 1 Wbni.
[50] 'Nederland tweede van Europa qua aantal meldingen datalekken sinds de invoering AVG', advocatie.nl.
[51] J.C. Hulsebosch, 'Cybersecurity & Privacy: overlap van beveiligingseisen en samenloop van meldplichten?', *Computerrecht* 2018/250, afl. 6, p. 316.
[52] Ministerie van Economische Zaken en Klimaat, *Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor digitale dienstverleners*, 2018. Te raadplegen op https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners.
[53] Zie voor de bevoegde autoriteit voor AED's: https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/wie-doet-wat/bevoegde-autoriteiten. De bevoegde autoriteit voor de digitale dienstverleners is Agentschap Telecom (AT).
[54] Artikel 29 Wbni.

verscherpt toezicht te plaatsen omdat "de drinkwaterorganisatie zowel op bestuurlijk als organisatorisch niveau onvoldoende grip heeft op de eigen cybersecurity" waardoor "een verhoogd risico aanwezig [is] op een cyberincident met mogelijke gevolgen voor de kwaliteit en/of de continuïteit van drinkwater".[55]

3.2 Besluit beveiliging netwerk- en informatiesystemen (Bbni)

Naast de Wbni is het Bbni eveneens op 9 november 2018 in werking getreden.[56] In het Bbni worden onder meer AED's en andere vitale aanbieders aangewezen die onder de reikwijdte vallen van de verplichtingen van de Wbni.[57]

4. Sector specifieke regelgeving

Naast deze algemene regelgeving is er ook sector specifieke regelgeving, bijvoorbeeld voor de zee- en luchtvaart. Wij zullen daar in een latere bijdrage separaat op ingaan en dan focussen op de verschillende vervoersmodaliteiten.

5. (Europese) ontwikkelingen

5.1 De NIB-richtlijn II

Op 16 december 2020, vijf jaar na de NIB-richtlijn, presenteerde de Commissie een (ingrijpend) voorstel tot herziening van de NIB-richtlijn.[58] Dit Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/118 (NIB 2-richtlijn) is gericht op het moderniseren van het bestaande rechtskader, rekening houdend met de toegenomen digitalisering van de afgelopen jaren.[59] Het streven is om in het eerste kwartaal van 2022 een akkoord te bereiken, waarna het aan de Europese landen is om de richtlijn binnen 18 maanden uit te voeren.[60]

Een voor de praktijk belangrijke aanpassing die uit het concept van de NIB 2-richtlijn volgt is onder meer dat het toepassingsgebied wordt uitgebreid. Het toepassingsgebied van de huidige richtlijn is zoals hiervoor toegelicht beperkt, met dien verstande dat de Nederlandse wetgever deze al heeft verbreed. Onder de NIB 2-richtlijn wordt het toepassingsgebied veel ruimer. Daarbij wordt onderscheid gemaakt tussen essentiële sectoren[61] (die niet identiek zijn maar wel in enige mate vergelijkbaar zijn met het toepassingsgebied van de huidige richtlijn) en belangrijke sectoren.[62] Die laatste categorie is nieuw en omvat bijvoorbeeld post- en koeriersdiensten en producenten van medische apparatuur. Bij deze indeling in sectoren moet rekening worden gehouden met de mate van kriticiteit van de sector of het soort dienst, alsmede met de mate van afhankelijkheid van andere sectoren of soorten diensten. De toezichts- en sanctieregelingen tussen deze twee sectoren moeten worden gedifferentieerd om onder meer het toezicht op de naleving van de richtlijn werkbaar te houden.[63]

---

[55] 'ILT stelt Waternet onder verscherpt toezicht', ilent.nl. Te raadplegen op https://www.ilent.nl/actueel/nieuws/2021/04/02/ilt-stelt-waternet-onder-verscherpt-toezicht.

[56] Besluit van 30 oktober 2018, houdende regels ter uitvoering van Wet beveiliging netwerk- en informatiesystemen (Besluit beveiliging netwerk- en informatiesystemen), *Stb*. 2018, 388. Te raadplegen op https://wetten.overheid.nl/BWBR0041520/2021-06-01.

[57] J.C. Hulsebosch, 'Cybersecurity & Privacy: overlap van beveiligingseisen en samenloop van meldplichten?', *Computerrecht* 2018/250.

[58] 'Proposal for directive on measures for high common level of cybersecurity across the Union', https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

[59] Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/118, COM(2020) 823 final. Te raadplegen op https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:52020PC0823.

[60] 'Europese cyberwetten: dit gaan ze voor je bedrijf betekenen', kvk.nl.

[61] *Essentiële sectoren* zijn energie (elektriciteit, stadsverwarming en –koeling, olie, gas en waterstof), vervoer (door de lucht, per spoor, over water en over de weg) bankwezen, infrastructuur van de financiële markten, gezondheid, farmaceutische producten (waaronder vaccins) en kritieke medische apparatuur, drinkwater, afvalwater, digitale infrastructuur (internetknooppunten), Domain Name System (DNS) Providers, Top Level Domein (TLD) registraties, cloudcomputerdiensten, datacentrumdiensten, inhoudaanbieders, vertrouwensdiensten, openbare elektronische-communicatienetwerken en –diensten, overheidsdiensten en ruimtevaar.

[62] *Belangrijke sectoren* zijn post- en koeriersdiensten, afvalbeheer, chemische stoffen, voedselvoorziening, productie van andere medische apparatuur, computers en elektronica, machines en motorvoertuigen, en online-aanbieders (marktplaatsen, zoekmachines en sociale netwerken).

[63] Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/118, COM(2020) 823 final, p. 16.

Een andere aanpassing betreft de voorgestelde persoonlijke aansprakelijkheid van de natuurlijke persoon die verantwoordelijk is voor een bedrijf dat onder een van de essentiële sectoren valt, die op basis van de NIB 2-richtlijn geïmplementeerde nationale bepalingen niet nakomt.[64] In art. 29 lid 6 NIB 2-richtlijn is opgenomen dat de lidstaten ervoor dienen te zorgen dat "*natuurlijke personen aansprakelijk kunnen worden gesteld voor het niet nakomen van hun verplichtingen om de in deze richtlijn vastgestelde verplichtingen na te komen.*" Op 25 februari 2022 kondigde Europarlementariër Bart Groothuis, rapporteur voor de NIB-richtlijn, al aan dat de overheid harder gaat optreden tegen bestuurders die hun internetbeveiliging niet op orde hebben. Zo vertelde Groothuis: "*We willen liever geen boetes uitdelen. Maar als een bestuurder aantoonbaar nalatig is, en keer op keer gewaarschuwd is, dan willen we tanden hebben om te bijten. Dat is nieuw. We maken cybersecurity voor het eerst 'chefsache', ofwel cybersecurity is niet meer een zaak die je overlaat aan je IT-beheerder, maar waar je zelf als bestuurder verantwoordelijk voor bent.*"[65]

5.2 Toezichthouders 2021-2021

Een kritische en professionele blik van toezichthouders op cybersecurity wordt van meerwaarde geacht om potentiële risico's of digitale dreigingen bij vitale sectoren te signaleren en hen te wijzen op het nemen van passende maatregelen. Dit volgt uit een door het Inspectie Justitie en Veiligheid (IJenV) gepubliceerde rapport, getiteld 'Rapport Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021'.[66]

Kortweg komt uit de toezichtresultaten van de toezichthouders[67] naar voren dat bewustzijn op cybersecurity bij een aanzienlijk deel van de vitale organisaties aanwezig is.[68] Desondanks hebben de vier toezichthouders op basis van de inspecties en analyses op basis van hun toezicht verbeterpunten en/of knelpunten bij vitale organisaties gevonden.[69] Op basis van die bevindingen hebben de onderzochte organisaties verbetermaatregelen getroffen. Om alert te blijven op die verbeteringen is een kritische blik van toezichthouders noodzakelijk, aldus deze toezichthouders.

6. Meer informatie en contact

Wanneer de nieuwe richtlijn wordt vastgesteld, zullen wij daar vanzelfsprekend aandacht aan besteden. In onze volgende bijdrage zullen de aansprakelijkheidsrisico's als gevolg van cybercrime centraal staan.

Wilt u meer weten over cyber, dan kunt u contact opnemen met Robert Pessers of Annevi Etienne.

Robert Pessers

pessers@vantraa.nl
+31 6 50 51 26 62
+31 10 22 45 502

Annevi Etienne

etienne@vantraa.nl
+31 6 82 06 69 96
+31 10 22 45 520

[64] Hagdorn, *TVR* 2021, p. 120.
[65] 'Europese cyberwetten: dit gaan ze voor je bedrijf betekenen', kvk.nl.
[66] Inspectie Justitie en Veiligheid, *Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021*, Den Haag: 2021. Te raadplegen op https://www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-2020-2021.
[67] Zie Rapport Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021, IJenV 2021, p. 42.
[68] Autoriteit Nucleaire Veiligheid en Stralingsbescherming, Agentschap Telecom, De Nederlandsche Bank, Inspectie Gezondheidszorg en Jeugd, Inspectie Justitie en Veiligheid en Inspectie Leefomgeving en Veiligheid.
[69] Zie Rapport Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021, IJenV 2021, p. 40.