Factsheet over de Wet beveiliging netwerk- en informatiesystemen

Implementatie EU-richtlijn

- De Wet beveiliging netwerk- en informatiesystemen (Wbni) is in 2018 in werking getreden en betreft in hoofdzaak de implementatie van de Europese Netwerk- en informatiebeveiligingsrichtlijn (NIB-richtlijn). Die richtlijn beoogt de digitale weerbaarheid van de Europese Unie te vergroten en de gevolgen van cyberincidenten te verkleinen.
- Daarnaast bevat de Wbni bepalingen die tot dan toe waren opgenomen in de voorganger van de Wbni (de Wet gegevensverwerking en meldplicht cybersecurity, in werking getreden in 2016).
- Momenteel wordt onderhandeld over de herziening van de NIB-richtlijn. De verwachting is dat er grote veranderingen in de Wbni nodig zijn om de herziene richtlijn te implementeren.

De Wbni regelt in hoofdlijnen de volgende onderwerpen:

A. Meldplicht en zorgplicht voor bepaalde aanbieders

- De Wbni bevat een zorgplicht en meldplicht voor aanbieders van essentiële diensten (AED's) en digitale dienstverleners (*digital service provider*, DSP's).
- AED's zijn vitale aanbieders die diensten leveren in sectoren die zijn genoemd in de NIB-richtlijn (zoals de sector energie en de sector luchtvervoer). Dit zijn diensten waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Denk bijvoorbeeld aan drinkwaterbedrijven of de netbeheerder van het landelijk hoogspanningsnet. Als hun diensten uitvallen, kan dat leiden tot een ernstige maatschappelijke ontwrichting.
- DSP's zijn aanbieders van onlinemarktplaatsen en -zoekmachines en cloudcomputerdiensten.

Voorbeelden (niet uitputtend)

AED's:
- de netbeheerder van het landelijk hoogspanningsnet
- Luchtverkeersleiding Nederland
- drinkwaterbedrijven
- de Nederlandse Aardolie Maatschappij B.V.

DSP's:
- Google Cloud (clouddienst)
- Google, Bing, Yahoo! (onlinezoekmachine)
- eBay, AliExpress, Amazon (onlinemarktplaats)

- De Wbni verplicht AED's en DSP's om passende technische en organisatorische maatregelen te nemen ter beveiliging van hun netwerk- en informatiesystemen (zorgplicht).

Voorbeelden (niet uitputtend)

Passende technische en organisatorische maatregelen (zorgplicht):
- het opstellen van een risicoanalyse, die ingaat op beveiligingsrisico's en de wijze waarop de aanbieder die risico's naar een passend niveau verkleint
- het hebben van een gelaagde beveiligingsstrategie, gebaseerd op de risico's uit de risicoanalyse
- het zodanig inrichten van de beveiliging van de netwerk- en informatiesystemen dat de aanbieder incidenten kan detecteren, analyseren en vastleggen en de gevolgen daarvan zoveel mogelijk kan beperken
- het opstellen van een bedrijfscontinuïteitsbeleid en een crisismanagementbeleid voor de netwerk- en informatiesystemen

- Ook verplicht de Wbni deze groepen om ernstige ICT-incidenten te melden bij de voor hen aangewezen instantie voor de verlening van bijstand bij digitale dreigingen en incidenten (Computer security incident response teams, CSIRT) en bij de bevoegde autoriteit die belast is met toezicht en handhaving (meldplicht). Voor AED's is het Nationaal Cyber Security Centrum (NCSC) het CSIRT, voor DSP's is een onderdeel van het ministerie van EZK het CSIRT.
- Daarnaast regelt de Wbni het toezicht op en de handhaving van de naleving van deze verplichtingen. Het toezicht is belegd bij sectorale toezichthouders, zoals Agentschap Telecom.

Sector	Bevoegde autoriteit	Toezichthoudende dienst
Energie	Minister van Economische Zaken en Klimaat	Agentschap Telecom
Digitale infrastructuur	Minister van Economische Zaken en Klimaat	Agentschap Telecom
Bankwezen	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Infrastructuur voor de financiële markt	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Vervoer	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Levering en distributie van drinkwater	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport

- AED's worden aangewezen in het Besluit beveiliging netwerk- en informatiesystemen. Dit is een algemene maatregel van bestuur (amvb).

B. De taken en bevoegdheden van het NCSC

- De Wbni regelt de taken en bevoegdheden van de minister van JenV op het terrein van cybersecurity. Deze taken en bevoegdheden worden in de praktijk uitgevoerd door het Nationaal Cyber Security Centrum (NCSC).
- Het NCSC heeft op grond van de Wbni primair de taak om vitale aanbieders[1] en aanbieders die deel uitmaken van de rijksoverheid te informeren en te adviseren over digitale dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen en hen in dat kader bijstand te leveren bij het treffen van maatregelen. Ook heeft het NCSC de taak om ten behoeve daarvan analyses en technisch onderzoek te verrichten.

Voorbeelden (niet uitputtend)

Vitale aanbieders:
- de netbeheerder van het landelijk hoogspanningsnet
- Luchtverkeersleiding Nederland
- drinkwaterbedrijven
- de Nederlandse Aardolie Maatschappij B.V.
- de Kamer van Koophandel
- de bij besluit van de minister van IenW aangewezen waterkeringen of onderdelen daarvan

Organisaties die deel uitmaken van de rijksoverheid:
- ministeries

- Voor vitale aanbieders en aanbieders die deel uitmaken van de rijksoverheid geldt hiermee dus dat al wettelijk is voorzien in bijstand van overheidswege bij digitale dreigingen en incidenten. De reden voor dit onderscheid met andere aanbieders is met name gelegen in het grotere maatschappelijke belang dat wordt toegekend aan vitale processen en binnen die processen aan vitale aanbieders. De uitval of verstoring van een vitaal proces leidt tot ernstige maatschappelijke ontwrichting en vitale aanbieders zijn belangrijk voor de continuïteit van een vitaal proces. Hierbij valt bijvoorbeeld te denken aan het uitvallen van de dienstverlening van een drinkwaterbedrijf of van de netbeheerder van het landelijk hoogspanningsnet als gevolg van een ICT-incident, met alle maatschappelijke gevolgen van dien.
- Het NCSC kan bij de uitoefening van zijn primaire taken de beschikking krijgen over dreigings- en incidentinformatie over de netwerk- en informatiesystemen van aanbieders die niet behoren tot de doelgroep (vitaal en rijksoverheid) van het NCSC. Deze aanbieders worden ook wel "andere aanbieders" genoemd. De Wbni regelt dat het NCSC die data kan delen met in de Wbni genoemde schakelorganisaties. Schakelorganisaties hebben de taak om aanbieders in hun achterban te informeren en te adviseren over de hen aangaande digitale dreigingen en incidenten. Zij zijn het meest bekend met de in hun achterban aanwezige netwerk- en informatiesystemen, bijbehorende belangen en risico's en informatiebehoeften. Onder de in de Wbni genoemde schakelorganisaties vallen onder meer computercrisisteams en zogeheten organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten (OKTT).

Voorbeelden (niet uitputtend)

[1] Hieronder vallen zowel de AED's als andere vitale aanbieders (bijv. nucleaire inrichtingen).

Computercrisisteams (op grond van de Wbni bij ministeriële regeling aangewezen):
- de Stichting Z-CERT, een expertisecentrum voor cybersecurity in de zorg
- CERT Watermanagement, onderdeel van het openbaar lichaam Het Waterschapshuis, ondersteunt bij cyberincidenten in watermanagement

OKTT (een organisatie die objectief kenbaar tot taak heeft om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten):
- Cyberweerbaarheidscentrum Brainport, een stichting opgericht t.b.v. ondernemingen die deel uitmaken van de Nederlandse kennisintensieve industrie, geïnitieerd door grote bedrijven in de Eindhovense hightech regio
- het Digital Trust Center (DTC)
- Cyberveilig Nederland, een belangenvereniging ten behoeve van de cybersecurity sector.
- FERM, opgericht ten behoeve van de bedrijven die onderdeel zijn van de Rotterdamse haven

- Die schakelorganisaties kunnen op hun beurt de informatie delen met de aanbieders in hun achterban. Dankzij die informatie kunnen deze aanbieders maatregelen treffen om digitale incidenten te voorkomen of de gevolgen daarvan te beperken.
- Voor zover het bij de hiervoor bedoelde data gaat om vertrouwelijke tot specifieke aanbieders herleidbare gegevens (bijvoorbeeld de namen van aanbieders of getroffen IP-adressen) is verstrekking hiervan door het NCSC, ten behoeve van het waarborgen van de vertrouwelijkheid hiervan, slechts in beperkte kring mogelijk. Tot die kring horen bijvoorbeeld computercrisisteams, maar op dit moment (nog) niet OKTT's.

Wat regelt het wetsvoorstel tot wijziging van de Wbni?
- Op dit moment kan het NCSC de hiervoor bedoelde data lang niet altijd delen met de hiervoor bedoelde andere aanbieders (die dus niet behoren tot de doelgroep van het NCSC) of met de schakelorganisaties die deze aanbieders in hun achterban hebben. Het delen is nog niet mogelijk, omdat de Wbni nog niet voorziet in de bevoegdheid om die data telkens aan die schakelorganisaties of direct aan de andere aanbieders te verstrekken. Zonder een wettelijke grondslag mag niet worden overgegaan tot het delen van informatie.
- Zonder deze informatie weten andere aanbieders bij dreigingen of incidenten niet dat hun netwerk- en informatiesystemen kwetsbaar zijn en kunnen zij hier geen maatregelen tegen nemen. Als die systemen kwetsbaar blijven, kunnen aanvallers die kwetsbaarheden misbruiken en kan de continuïteit van de dienstverlening van andere aanbieders in gevaar komen.
- Dit voorstel regelt daarom dat het NCSC in ruimere mate dreigings- en incidentinformatie over de netwerk- en informatiesystemen van andere aanbieders aan de schakelorganisaties van deze andere aanbieders kan verstrekken, of direct aan deze andere aanbieders als zo'n schakelorganisatie niet aanwezig is. Dit laatste wordt in het wetsvoorstel expliciet geregeld, want lang niet elke andere aanbieder wordt bediend door een schakelorganisatie. Dit geldt bijvoorbeeld voor politieke partijen en provincies.
- Het doel van die verstrekkingen is dat deze andere aanbieders dankzij die informatie maatregelen kunnen nemen om digitale incidenten te voorkomen of de gevolgen daarvan te beperken.
- Concreet regelt dit wetsvoorstel het volgende:
  - Het NCSC kan vertrouwelijke herleidbare gegevens over aanbieders zonder instemming ook verstrekken aan OKTT's. Hiermee kunnen OKTT's de aanbieders in hun doelgroepen informeren over voor die aanbieders relevante dreigingen en incidenten. Deze aanbieders kunnen vervolgens maatregelen nemen om incidenten te voorkomen of de gevolgen daarvan te beperken.
  - Wanneer de hiervoor bedoelde data ziet op een dreiging of incident met (potentiële) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de andere aanbieder én er geen schakelorganisatie is die de andere aanbieder van die informatie kan voorzien, dan kan het NCSC deze informatie delen aan deze aanbieders.
  - De aanwijzing van organisaties als OKTT geschiedt voortaan bij ministeriële regeling en niet meer bij ministeriële aanwijzing.
- De Algemene verordening gegevensbescherming (AVG) vereist een wettelijke grondslag voor de verstrekking van persoonsgegevens. De dreigings- en incidentinformatie kan ook persoonsgegevens bevatten. Dit wetsvoorstel regelt met de ruimere bevoegdheid tot verstrekking ook die vereiste grondslag.

Aanbieders die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid (in het wetsvoorstel aangeduid als "andere aanbieders"):
- veiligheidsregio's
- politieke partijen
- provincies

Digitale dreigingen of aanvallen op andere aanbieders die hebben plaatsgevonden:
- de besmetting van een containeroverslagbedrijf met Petya-ransomware waardoor de dienstverlening van dit bedrijf in 2017 dagenlang stil kwam te liggen
- de in de e-mailsoftware van Microsoft Exchange aanwezige kwetsbaarheid, die gebruikt is om gijzelsoftware te installeren bij een logistiek bedrijf voor voedselwaren in 2021, deze aanval leidde ertoe dat de distributie van kaas aan diverse supermarkten circa een week stil kwam te liggen
- de digitale aanval in 2021 op een ICT-leverancier van bijna honderd notarissen, de aanval leidde er onder andere toe dat geen aktes gepasseerd konden worden

De door het NCSC te verstrekken gegevens:
- IP-adressen van gebruikers van kwetsbare systemen of van aanvallers
- domeinnamen van gebruikers van kwetsbare systemen of van aanvallers
- e-mailadressen van gebruikers van kwetsbare systemen of van aanvallers
- let op: het gaat niet om bijzondere persoonsgegevens; dat zijn persoonsgegevens die door hun aard bijzonder gevoelig zijn, bijvoorbeeld omdat daaruit ras, etniciteit, religie of seksuele geaardheid uit blijken
- de namen van de bedrijven waarop een dreiging of incident betrekking heeft

Voorbeeldcasus (fictief)
Een onderzoeker van een universiteit heeft een publicatie gedaan over een kwetsbaarheid in veelgebruikte kantoorautomatiseringssoftware. Zij heeft een scan gedraaid naar kwetsbare systemen in Nederland en een lijst met de IP-adressen van die kwetsbare systemen gedeeld met het NCSC.
Het NCSC heeft op grond van de Wbni de taak om vitale aanbieders en andere aanbieders die deel uitmaken van de Rijksoverheid te informeren en adviseren over dit soort digitale kwetsbaarheden. Ten behoeve van die taak verricht het NCSC analyses en technisch onderzoek. Bij het analyseren van de lijst stuit het NCSC op IP-adressen van andere dan voornoemde aanbieders die ook kwetsbaar zijn. Deze aanbieders vallen niet onder de primaire doelgroep (vitaal en Rijk) van het NCSC, denk bijvoorbeeld aan een provincie of een distributeur van voedselwaren. Het NCSC kan op grond van de Wbni die data delen met een aantal schakelorganisaties (artikel 3, tweede lid, Wbni). Zo'n schakelorganisatie kan vervolgens zijn achterban informeren over de dreiging. Krachtens de huidige wet kunnen echter verschillende schakelorganisaties (OKTT's) lang niet altijd van al deze informatie worden voorzien. Daarnaast zijn er ook verschillende aanbieders die niet worden bediend door een schakelorganisatie, bijvoorbeeld politieke partijen en provincies. Hierdoor kan de informatie niet belanden bij de kwetsbare aanbieder. De aanbieder weet dan niet dat hij kwetsbaar is en kan geen maatregelen nemen om deze kwetsbaarheid te verhelpen.
Het wetsvoorstel zorgt ervoor dat de informatie in bovenstaande gevallen wel kan belanden bij die aanbieder.

Grondslagenkwestie NCTV

De grondslagenkwestie NCTV betreft een andere kwestie dan die kwestie waarop het hiervoor besproken wetsvoorstel tot wijziging van de Wbni betrekking heeft:
- De Wbni regelt de taken van de minister van JenV met betrekking tot de beveiliging van netwerk- en informatiesystemen, die in de praktijk door het NCSC worden uitgevoerd. De in de Wbni geregelde taken zien – kort samengevat – op het informeren en adviseren van aanbieders uit zijn doelgroep over digitale dreigingen en incidenten.
- Het wetsvoorstel over de grondslagenkwestie ziet op de analyse- en coördinatietaken van de minister van JenV op het terrein van de bestrijding van terrorisme en bescherming van de nationale veiligheid en de daarmee gepaard gaande verwerking van (bijzondere) persoonsgegevens.

Alle afkortingen op een rij

Wbni	Wet beveiliging netwerk- en informatiesystemen
NIB-richtlijn	Netwerk- en informatiebeveiligingsrichtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016
AED	aanbieder van een essentiële dienst
DSP	digital service provider (digitaledienstverlener)
CSIRT	Computer security incident response team (computercrisisteam)
NCSC	Nationaal Cyber Security Centrum
OKTT	organisatie die objectief kenbaar tot taak heeft om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten