Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Wet beveiliging netwerk- en informatiesystemen

Algemene informatie

Meer weten?
www.agentschaptelecom.nl/wbni

Introductie

Het lijkt allemaal zo vanzelfsprekend: er is elektriciteit, medewerkers reizen veilig met de trein, er komt water uit de kraan en klanten kunnen van alles aan- en verkopen via het internet. Al deze vanzelfsprekendheden zijn afhankelijk van netwerken en informatietechnologie. Met goedwerkende netwerken en de juiste, beschikbare informatie kunnen deze diensten betrouwbaar worden geleverd. Maar netwerken en informatie zijn kwetsbaar. Organisaties die essentiële diensten aanbieden of digitaledienstenleveren moeten hun kwetsbaarheid verlagen door de weerbaarheid tegen bedreigingen op peil te houden.

"Organisaties die essentiële diensten aanbieden of digitaledienstenleveren moeten hun kwetsbaarheid verlagen door de weerbaarheid tegen bedreigingen op peil te houden."

Agentschap Telecom is aankomend toezichthouder op de naleving van de voorgenomen Wet beveiliging netwerk- en informatiesystemen (Wbni) voor de energiesector, de digitale infrastructuur en digitaledienstverleners. Beveiligingsincidenten in hun netwerk- en informatiesystemen melden deze organisaties bij Agentschap Telecom.

In deze brochure vindt u algemene informatie over de NIB-richtlijn, de Europese uitvoeringsverordening voor digitaledienstverleners en de Wbni.

De **NIB**-richtlijn

Op Europees niveau is de Netwerk en Informatiebeveiliging (NIB) richtlijn (2016/1148) vastgesteld. De NIB-richtlijn verplicht landen in de Europese Unie om de weerbaarheid van netwerk- en informatiesystemen te vergroten. Daarbij kunt u denken aan een gedegen risicomanagement, organisatorische en technische beveiligingsmaatregelen en het melden van incidenten.

De NIB-richtlijn is voor Nederland vertaald naar de Wbni.

De basis: risicomanagement

Beheersing van informatiebeveiligingsrisico's in netwerk- en informatiesystemen vormt de basis van de NIB-richtlijn. Alleen als er inzicht is in die risico's kan een organisatie passende technische en organisatorische maatregelen treffen. Risico's schat je in door te kijken naar de kans dat een gebeurtenis zich voordoet en door te kijken naar de impact die de gebeurtenis heeft.

Risico = Kans x Impact

Zowel de vertrouwelijkheid, integriteit als beschikbaarheid en authenticiteit van netwerk- en informatiesystemen kunnen negatief worden beïnvloed. Als daardoor de dienstverlening van een organisatie wordt geraakt, is er sprake van een incident.

Samenwerking en organisatie

De NIB-richtlijn stimuleert nationale en internationale samenwerking. Dat doen de EU-lidstaten door informatie te delen, te participeren in samenwerkgroepen en door de aanpak om de weerbaarheid te vergroten te delen. Ook moeten bevoegde autoriteiten en Computer Security Incident Response Teams (CSIRT's) binnen een enkele lidstaat samenwerken en relevante kennis en informatie delen. In Nederland is de minister van Economische Zaken en Klimaat de bevoegde autoriteit voor toezicht op de sectoren Energie en Digitale Infrastructuur en op digitaledienstverleners. Een CSIRT is een team dat waarschuwt voor cyberrisico's en in geval van een incident hulp en bijstand levert.

De NIB-richtlijn schrijft voor dat elke lidstaat:

- Een nationaal contactpunt aanwijst voor samenwerking bij internationale incidenten
- tenminste één bevoegde autoriteit aanwijst
- tenminste één CSIRT aanwijst.

Dit zorgt er voor dat het voor organisaties die aan de regelgeving moeten voldoen duidelijk is waar zij met vragen en incidentmeldingen terecht kunnen en welke overheidsorganisatie optreedt als toezichthouder en handhaver.

Aanbieders van essentiële diensten en digitaledienstverleners

De NIB-richtlijn maakt onderscheid tussen aanbieders van essentiële diensten en digitaledienstverleners.

Aanbieder van essentiële diensten
Biedt essentiële diensten aan zoals genoemd in bijlage II NIB-richtlijn
Wordt door de nationale overheid aangewezen
Proactief toezicht op naleving
Treft passende en evenredige technische en organisatorische maatregelen, op basis van een gedegen risicoafweging
Meldt incidenten bij het nationale CSIRT/de bevoegde autoriteit
Toont beleidsmaatregelen en beveiliging aan door middel van documentatie
Toont aan dat beveiligingsbeleid daadwerkelijk wordt uitgevoerd

Digitaledienstverlener
Biedt digitaleddiensten zoals genoemd in bijlage III NIB-richtlijn
Wordt gedefinieerd in de NIB-richtlijn
Reactief toezicht op naleving
Treft passende en evenredige technische en organisatorische maatregelen, op basis van een gedegen risicoafweging
Meldt incidenten bij het nationale CSIRT-DSP/de bevoegde autoriteit, mits toegang tot de informatie
Uitvoeringsverordening 2018/151 stelt: beschikt over passende documentatie om beveiliging aan te kunnen tonen

Een aanbieder van een essentiële dienst is een publieke of private organisatie die een dienst levert die van essentieel belang is voor de instandhouding van kritieke economische of maatschappelijke activiteiten. Een netwerk- en/of informatie incident kan aanzienlijke verstorende effecten hebben op de verlening van de dienst.

Digitaledienstverleners met een meldplicht onder de Wbni worden niet aangewezen. Aan de hand van onderstaand schema kan een digitaledienstverlener zelf inschatten of hij volgens de Wbni een meldplicht heeft.

Doe hier de check:

Is mijn bedrijf een:
- Online **marktplaats**
- Online **zoekmachine**
- **Cloud** dienstverlener

Nee → Uw bedrijf valt NIET onder de Wbni

Ja ↓

Heeft mijn bedrijf een Europese hoofdvestiging in Nederland of vertegenwoordiging in Nederland?

Nee → Uw bedrijf valt NIET onder de Wbni

Ja ↓

Zijn bij mijn bedrijf 50 of meer medewerkers werkzaam?

Ja → Uw bedrijf valt **WEL** onder de Wbni

Nee ↓

Is mijn balanstotaal of jaaromzet meer dan 10 miljoen Euro?

Ja → Uw bedrijf valt **WEL** onder de Wbni

Nee → Uw bedrijf valt NIET onder de Wbni

Beveiligingselementen en aanzienlijke gevolgen

Digitaledienstverleners moeten zich houden aan Europese uitvoeringsverordening 2018/151. Daarin zijn bepalingen opgenomen over beveiligingselementen en het beoordelen van aanzienlijke gevolgen van een incident. De beveiligingselementen moeten met passende documentatie aangetoond worden. De definitie van aanzienlijke gevolgen is leidend voor de vraag of u een incident moet melden.

U vindt de verordening op de website https://eur-lex.europa.eu als u zoekt op '2018/151' en 'Regulation' aanvinkt.

Hoe bepaalt een digitaledienstverlener of een incident aanzienlijke gevolgen heeft?

Er geldt een meldplicht als een van de volgende drempelwaarden wordt bereikt:

Wbni

De Wet beveiliging netwerk- en informatiesystemen is de nationale vertaling van de Europese NIB-richtlijn. De Wbni komt overeen met de bepalingen van de NIB-richtlijn ten aanzien van risicobeheersing, het treffen van passende maatregelen en het voorkomen en/of melden van incidenten. De verwachting is dat de Wet beveiliging netwerk- en informatiesystemen najaar 2018 in werking treedt.

Wbni

Bevoegde autoriteit en CSIRT

In de Wbni wordt geregeld dat voor de sectoren Energie, Digitale infrastructuur en digitaledienstverleners de minister van Economische Zaken en Klimaat de bevoegde autoriteit is. Agentschap Telecom is namens de minister beoogd toezichthouder en handhaver.

Het Nationaal Cyber Security Centrum (NCSC) voert voor de sectoren Energie en Digitale Infrastructuur de CSIRT-functie uit. Digitaledienstverleners maken gebruik van CSIRT-DSP.

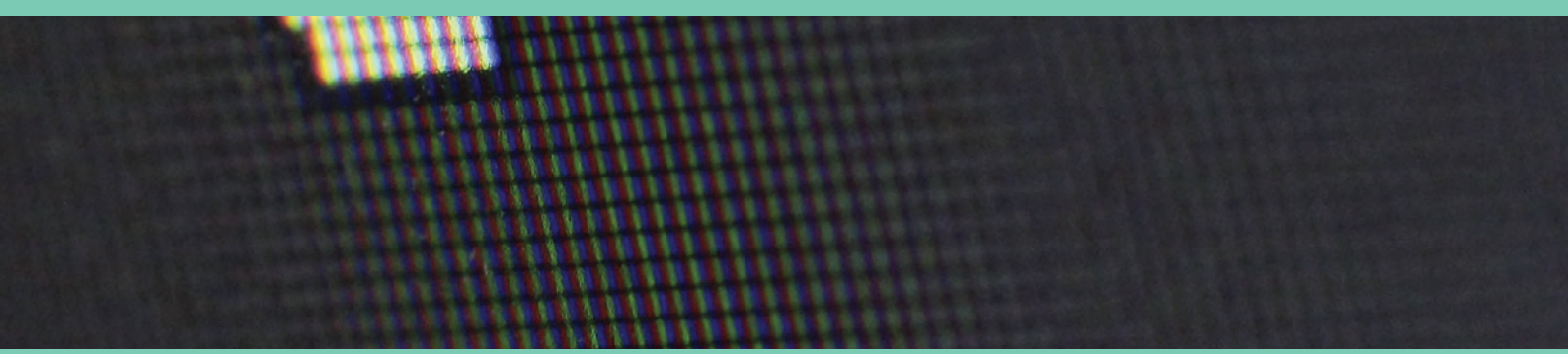
De Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) komt met de Wbni te vervallen. De bepalingen zijn opgegaan in de Wbni.

Samengevat

Sector	Bevoegde Autoriteit	CSIRT
Digitaledienstverleners	Agentschap Telecom	DSP-CSIRT
Sector Digitale Infrastructuur	Agentschap Telecom	Nationaal CSIRT (NCSC)
Sector Energie	Agentschap Telecom	Nationaal CSIRT (NCSC)

Gegevensverwerking

Er zijn voorwaarden gesteld aan het delen van informatie door bevoegde autoriteiten en CSIRT's. Zo wisselen bevoegde autoriteiten en CSIRT's niet zo maar onderling gegevens uit over organisaties, vallen vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder NIET onder de Wet openbaarheid van bestuur (Wob) en wordt de organisatie geraadpleegd voordat vanuit het CSIRT of de bevoegde autoriteit eventuele mededelingen aan het publiek worden gedaan over een incident.



Toezicht en handhaving

Aanbieders van essentiële diensten vallen onder een actief toezichtbeleid: er vinden geplande inspecties plaats gericht op opzet, bestaan en werking van het risicomanagementproces en het treffen van passende beheersingsmaatregelen. Voor digitaledienstverleners geldt reactief toezicht. Inspecties vinden alleen plaats op basis van signalen en incidenten.

Aanbieders van essentiële diensten binnen de sectoren Energie en Digitale infrastructuur melden incidenten bij het NCSC en Agentschap Telecom. Digitaledienstverleners melden een incident met aanzienlijke gevolgen bij het CSIRT-DSP en Agentschap Telecom. Incidenten mogen ook vrijwillig gemeld worden als ze nog niet onder de meldplicht vallen.

In het toezicht gaan we vroegtijdig en open het gesprek aan, zodat verwachtingen duidelijk zijn, ondertoezichtstaande organisaties weten waar ze zich aan moeten houden en dat uit volle overtuiging en uit zichzelf doen. Agentschap Telecom heeft net als andere toezichthouders bij de uitvoering van het toezicht diverse bevoegdheden. Zo kan het agentschap een beveiligingsaudit uitvoeren bij een aanbieder van essentiële diensten of deze organisatie verplichten om zo'n audit zelf te laten uitvoeren. Als Agentschap Telecom constateert dat een aanbieder van een essentiële dienst of een digitaledienstverlener zich niet aan wet- of regelgeving houdt dan biedt de wet verschillende mogelijkheden om handhavend op te treden, waaronder het opleggen van een bindende aanwijzing. Dat kan betekenen dat een organisatie een bepaalde maatregel moet treffen of juist een gedraging moet stoppen of nalaten. Ook heeft het agentschap de bevoegdheid om bijvoorbeeld boetes uit te delen.

Meer informatie of een vraag?

Kijk **op agentschaptelecom.nl/wbni**
of stuur een e-mail naar **info@agentschaptelecom.nl**

Digitale
Weerbaarheid