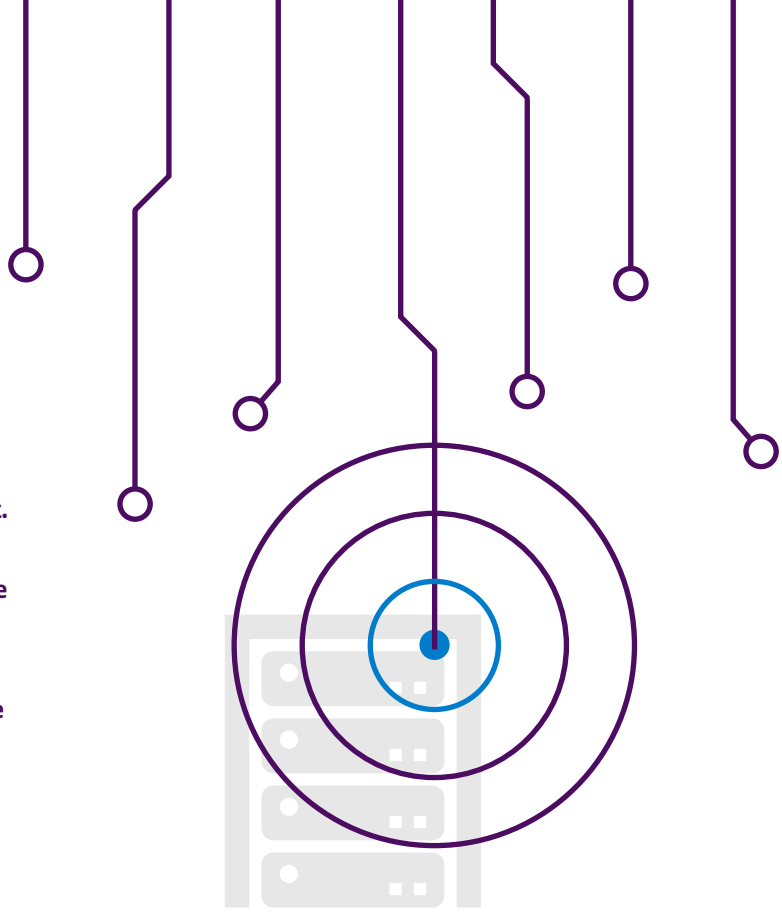
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Wet beveiliging netwerk- en informatiesystemen

In deze brochure vindt u algemene informatie over de NIB-richtlijn, de Wbni en aanvullende wet- en regelgeving.



Introductie

Het lijkt allemaal zo vanzelfsprekend: er is elektriciteit, we reizen veilig met de trein, er komt water uit de kraan en we 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 digitale diensten leveren moeten hun kwetsbaarheid verlagen door de weerbaarheid tegen bedreigingen op peil te houden.

Rijksinspectie Digitale Infrastructuur (RDI) is toezicht-houder op de naleving van de Wet beveiliging netwerk- en informatiesystemen (Wbni) voor de energiesector, de digitale infrastructuur en digitale dienstverleners. Deze organisaties melden beveiligingsincidenten in hun netwerk- en informatiesystemen bij de RDI.

De NIB-richtlijn

Op Europees niveau is de 'The Directive on security of Network and Information Systems (2016/1148)' (NIS Directive) vastgesteld. De Netwerk en Informatiebeveiliging (NIB) richtlijn is een Nederlandse vertaling van de NIS Directive. De NIB-richtlijn verplicht landen in de Europese Unie om de weerbaarheid van netwerk- en informatie-systemen te vergroten. Daarbij kunt u denken aan een gedegen risicomanagement, organisatorische en technische beveiligingsmaatregelen (zorgplicht) en het melden van incidenten (meldplicht).

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. Een CSIRT is een team dat waarschuwt voor informatiebeveiligingsrisico'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 ervoor 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.

De NIB-richtlijn zal in de nabije toekomst worden herzien. De nieuwe richtlijn zal een heldere reikwijdte formuleren, de aanwijzing van aanbieders van essentiële diensten door de lidstaten gelijktrekken, het handhavingsregime stroomlijnen, informatiedeling tussen de lidstaten verbeteren en het cybersecurity beleid in de gehele Europese Unie verstevigen.

Bevoegde autoriteit en CSIRT

In de Wbni is geregeld dat voor de sectoren Energie, Digitale infrastructuur en Digitale dienstverleners de minister van Economische Zaken en Klimaat de bevoegde autoriteit is. De RDI is namens de minister aangewezen als toezichthouder voor deze sectoren.

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

De Wbni

De Wet beveiliging netwerk- en informatiesystemen (Wbni) is de Nederlandse implementatie van de Europese NIB-richtlijn. De Wbni verplicht aanbieders van essentiële diensten en digitale dienstverleners om passende en evenredige technische en organisatorische maatregelen te nemen om hun ICT te beveiligen, en om passende maatregelen te treffen om incidenten te voorkomen en de gevolgen van incidenten zo veel mogelijk te beperken. De Wbni is op 9 november 2018 in werking getreden.

Tegelijkertijd met de Wbni is ook het Besluit Beveiliging Netwerk- en Informatiesystemen (Bbni) in werking getreden. Met het Bbni wordt er nadere invulling gegeven aan de bepalingen van de Wbni, zoals verdere specificering van de aanwijzing van aanbieders van essentiële diensten en nadere invulling van de zorgplicht. De meest actuele besluiten kunt u vinden in het Bbni; in juni 2021 is deze aangepast.

Voor digitale dienstverleners is ook de Europese uitvoeringsverordening 2018/151 van toepassing. Dit is een wettelijke aanvulling op de NIB-richtlijn en daarmee ook op de Wbni. In deze verordening worden de in aanmerking te nemen elementen voor het beheer van risico's en de parameters om te bepalen of een incident aanzienlijke gevolgen heeft nader gespecificeerd. U vindt de verordening op de website eur-lex.europa.eu als u zoekt op '2018/151' en 'Regulation' aanvinkt.

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.

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

Geen enkele organisatie is hetzelfde. Wat voor de ene organisatie een passende maatregel is, hoeft dat niet te zijn voor een andere organisatie. Daarom schrijft de RDI geen maatregelen voor, maar ligt de focus van toezicht op de risicobeheersing van processen.

"Als toezichthouder zullen wij er altijd naar streven om een afgewogen beeld te krijgen bij de achtergrond van een incident"

Aanbieders van essentiële diensten en digitale dienstverleners

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

Aanbieders van een essentiële diensten zijn publieke of private organisaties die een dienst leveren die van essentieel belang is voor de instandhouding van kritieke economische of maatschappelijke activiteiten. Een incident op gebied van netwerk- en informatiesystemen kan aanzienlijke gevolgen hebben voor de continuïteit van essentiële diensten en dienstverlening.

Digitale dienstverleners worden niet aangewezen. Aan de hand van onderstaande flowchart kan een digitale dienstverlener zelf inschatten of deze onder de Wbni valt.

Aanbieder van essentiële diensten
Biedt essentiële diensten aan zoals genoemd in bijlage II van de 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 en de toezichthouder
Toont beleidsmaatregelen en beveiliging aan door middel van documentatie
Toont aan dat beveiligingsbeleid daadwerkelijk wordt uitgevoerd

Digitale dienstverlener
Biedt digitale diensten aan zoals genoemd in bijlage III van de NIB-richtlijn
Wordt gedefinieerd in de NIB-richtlijn; zie onderstaande flowchart voor meer informatie
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 en de toezichthouder
Beschikt over de passende documentatie om beveiliging aan te kunnen tonen

Doe hier de check:

Meldplicht onder de Wbni

Aanbieders van essentiële diensten in de sectoren Energie en Digitale Infrastructuur zijn verplicht om alle incidenten die de drempelwaarde(n) overschrijden en/of aanzienlijke gevolgen hebben voor de continuïteit van de dienstverlening onverwijld te melden bij de RDI en het Nationaal Cyber Security Centrum (NCSC). Het Ministerie van Economische Zaken en Klimaat maakt binnen de sectoren Energie en Digitale Infrastructuur de drempelwaarde(n) aan betreffende organisaties bekend.

→ Raadpleeg de brochure 'Meldplicht voor aanbieders van essentiële diensten' voor meer informatie over de procedure rondom het melden van incidenten. Download deze via: www.rdi.nl

Digitale dienstverleners zijn verplicht om alle incidenten die de drempelwaarde(n) overschrijden en/of aanzienlijke gevolgen hebben voor de continuïteit van de dienstverlening onverwijld te melden bij de RDI en het CSIRT-DSP. De drempelwaarden die bepalen of een incident aanzienlijke gevolgen heeft zijn vastgesteld in de Europese uitvoeringsverordening voor digitale dienstverleners (2018/151).

→ Raadpleeg de brochure 'Meldplicht voor digitale dienstverleners' voor meer informatie over de drempelwaarden en over de procedure rondom het melden van incidenten. Download deze via: www.rdi.nl

Voor alle sectoren geldt dat incidenten ook vrijwillig gemeld mogen worden als ze (nog) niet onder de meldplicht vallen. Ook van incidenten met kleinere impact kunnen we samen veel leren. Daarom nodigen we u expliciet uit om ook deze incidenten bij ons te melden.

Als toezichthouder zullen wij er altijd naar streven om een afgewogen beeld te krijgen bij de achtergrond van een incident. Na melding van incidenten zal de RDI nader onderzoek doen om de kwaliteit van de netwerk- en informatiebeveiliging te verhogen en het lerend vermogen van de betreffende sectoren te stimuleren. De RDI zal incidenten en dreigingen op het gebied van beveiliging van netwerk- en informatiesystemen in bredere zin beschouwen, waarbij we ook incidenten die onder de drempelwaarden blijven en incidenten die in de media zijn gekomen in acht nemen. Met deze informatie kunnen we samen met de sectoren constructief werken aan het verhogen van de digitale weerbaarheid van essentiële diensten en digitale dienstverlening in Nederland.

Toezicht en handhaving

Aanbieders van essentiële diensten vallen onder een actief toezichtbeleid: er vinden reguliere inspecties plaats gericht op opzet, bestaan en werking van het risicomanagement-proces en het treffen van passende en evenredige beheersingsmaatregelen. Daarnaast zullen er ook thema inspecties plaatsvinden waarbij er dieper wordt ingegaan op een bepaald thema in het kader van de Wbni. In het toezicht gaan we vroegtijdig en open het gesprek aan, zodat verwachtingen over en weer duidelijk zijn en onder toezicht staande organisaties weten waar ze zich aan moeten houden.

Voor digitale dienstverleners geldt reactief toezicht: inspecties vinden alleen plaats op basis van signalen en incidenten.

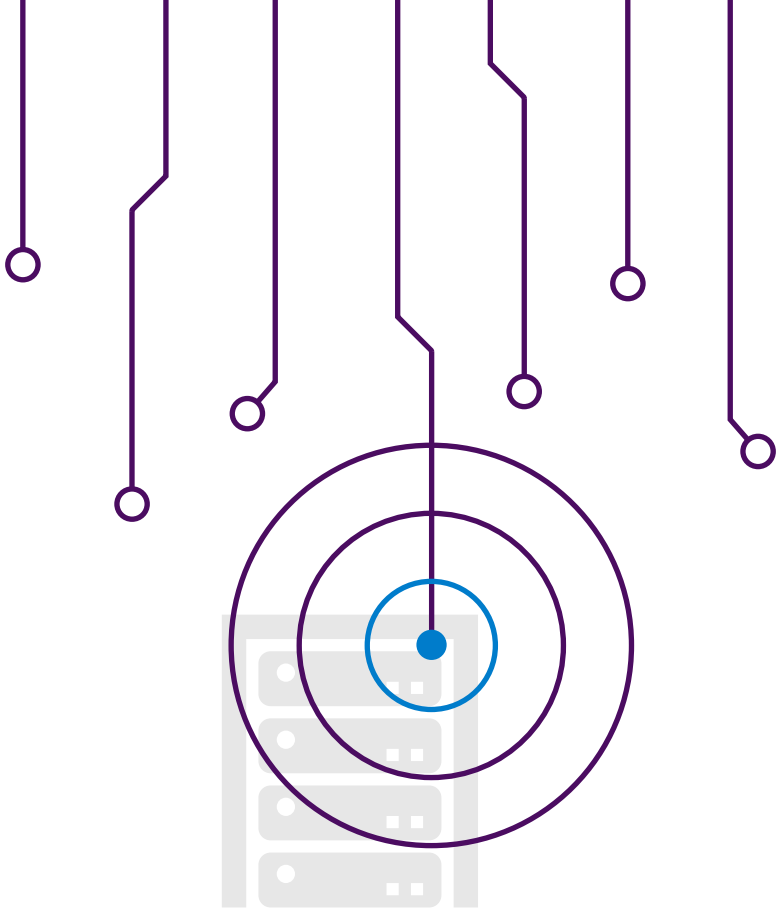
De RDI heeft bij de uitvoering van het toezicht diverse bevoegdheden. Als de RDI constateert dat een aanbieder van een essentiële dienst of een digitale dienstverlener zich niet aan wet- of regelgeving houdt dan biedt de wet verschillende mogelijkheden om handhavend op te treden, waaronder het opleggen 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 de RDI de bevoegdheid om bijvoorbeeld boetes uit te delen.

Gegevensverwerking

De RDI verstrekt vertrouwelijke gegevens met betrekking tot uw organisatie alleen aan derden voor zover wet- en regelgeving dit toestaat. Dat doen we op voorwaarde dat de geheimhouding voldoende is geborgd en als voldoende is gewaarborgd dat gegevens niet voor een ander doel worden gebruikt. De Wet openbaarheid van bestuur (Wob) is niet van toepassing op deze vertrouwelijke gegevens.

Als publieke bewustwording nodig is om een incident te beheersen of om escalatie te voorkomen, kan de RDI het publiek informeren over het door u gemelde incident. Hierover wordt u altijd vooraf geraadpleegd. Ook kan uw organisatie worden verzocht om zelf het publiek te informeren.

Heeft het incident gevolgen voor een essentiële dienst in een andere lidstaat van de Europese Unie? Dan kan de RDI het NCSC verzoeken om uw melding door te zetten naar het speciaal hiervoor ingerichte contactpunt in die lidstaat.



Meer informatie of een vraag?
Kijk op **www.rdi.nl/wbni**
of stuur een e-mail naar **wbni@rdi.nl**

September 2021