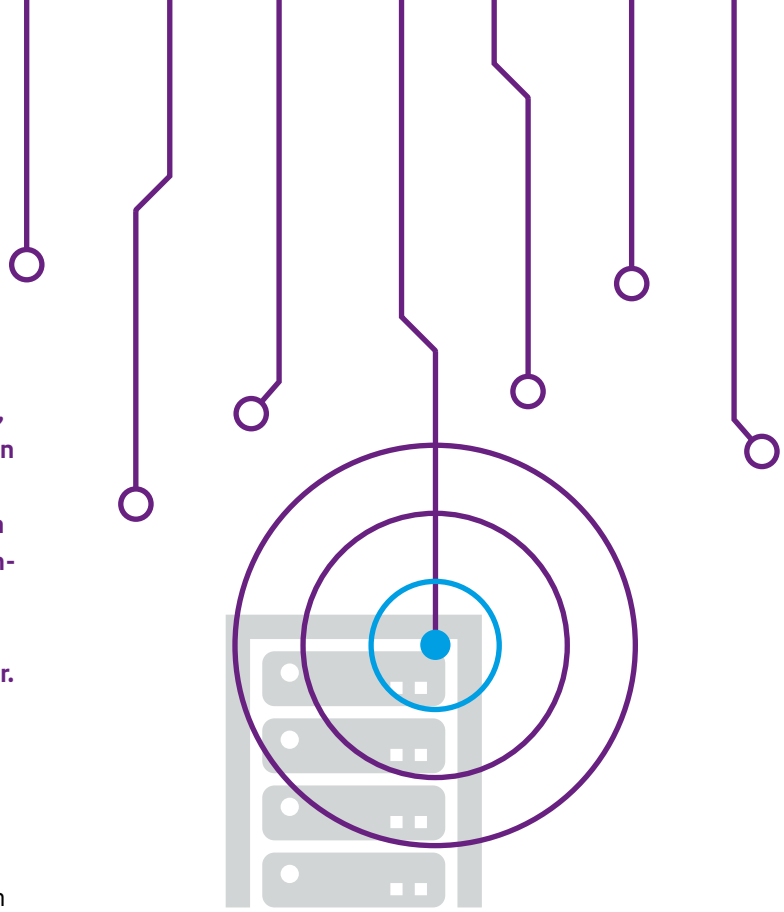
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Melden van incidenten

In deze brochure vindt u informatie over het proces voor het melden van incidenten door aanbieders van essentiële diensten (AED's) in het kader van de Wet beveiliging netwerk- en informatiesystemen (Wbni)



Aanbieders van essentiële diensten

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 informatiesystemen zijn kwetsbaar. Door de weerbaarheid tegen bedreigingen op peil te houden kunnen organisaties die essentiële diensten aanbieden hun risico's verlagen.

Rijksinspectie Digitale Infrastructuur (RDI) is door de Minister van Economische Zaken en Klimaat aangewezen als toezichthouder op de naleving van de Wet beveiliging netwerk- en informatiesystemen (Wbni) voor de Energiesector, de Digitale Infrastructuur en Digitale dienstverleners. Als u een aanbieder van essentiële diensten (AED) bent in de sector Energie of Digitale Infrastructuur waarop de Wbni van toepassing is dan krijgt u daarover een brief van het Ministerie van Economische Zaken en Klimaat. Deze organisaties melden beveiligingsincidenten in hun netwerk- en informatiesystemen bij de RDI.

Meldplicht voor aanbieders van essentiële diensten

AED's in de sectoren Energie en Digitale Infrastructuur zijn verplicht om alle incidenten die aanzienlijke gevolgen hebben voor de continuïteit van de dienstverlening en/of de drempelwaarde(n) overschrijden onverwijld te melden bij de RDI en het Nationaal Cyber Security Centrum (NCSC). De RDI heeft als belangrijkste taken om de digitale weerbaarheid van AED's te beoordelen en daar waar nodig de AED te bewegen om de weerbaarheid te verhogen. Bij incidenten doet de RDI nader onderzoek om de kwaliteit van de digitale weerbaarheid te verhogen en het lerend vermogen van de betreffende sectoren te stimuleren. Het NCSC fungeert als Cyber Security Incident Respons Team (CSIRT) en heeft als belangrijkste taken om incidenten op nationaal niveau te monitoren en om aanbieders vroegtijdig te waarschuwen en te informeren over kwetsbaarheden, risico's en incidenten.

Hoe meldt u een incident?

Bij de RDI:

Download het meldformulier op onze website en stuur het ons retour. Retourneren kan op de volgende manieren:

- Via ons beveiligde infoportal:
  https://infoportal.rdi.nl/
  Om gebruik te maken van het infoportal heeft u een account nodig. Neem hiervoor contact op met de RDI via wbni@rdi.nl. U krijgt dan de benodigde inloggegevens en informatie over de contactpersoon die u wordt toegewezen voor dit incident.
- Via e-mail naar wbni@rdi.nl
  Let op: de inhoudelijke incidentgegevens zijn mogelijk te gevoelig om via e-mail verzonden te worden!

Bij het Nationaal Cyber Security Centrum:

Voor de melding bij het NCSC verwijzen we u graag door naar de website van deze organisatie (https://www.ncsc.nl).

Welke incidenten meldt u?

Alle incidenten die de drempelwaarde(n) overschrijden en/of aanzienlijke gevolgen hebben voor de continuïteit van de diensten die u verleent, meldt u onverwijld altijd bij de RDI en het NCSC.

Het Ministerie van Economische Zaken en Klimaat maakt binnen de sectoren Energie en Digitale Infrastructuur de drempelwaarde(n) aan betreffende organisaties bekend. Een beveiligingsincident op het gebied van netwerk- en informatiesystemen waar u van verwacht dat het mogelijk aanzienlijke gevolgen kan hebben, hoeft u in eerste

instantie alleen bij het NCSC te melden. Zodra dat incident toch de drempelwaarde(n) overschrijdt en/of aanzienlijke gevolgen heeft, doet u alsnog een melding bij de RDI.

Ook bij digitale dienstverleners bij wie u diensten -zoals clouddiensten- afneemt, kunnen incidenten plaatsvinden. Als incidenten bij één van die leveranciers aanzienlijke gevolgen hebben voor de continuïteit van uw essentiële dienstverlening, moet u dit melden bij de RDI en het NCSC. Het maakt daarbij niet uit of deze digitale dienstverlener een vertegenwoordiging in Nederland heeft.

Vrijwillige melding van incidenten

Digitale weerbaarheid is gebaat bij kennisdeling. Ook van incidenten die onder de drempelwaarden blijven, kunnen we samen veel leren. Zoals de RDI eveneens in haar gesprekken met AED's duidelijk maakt, nodigen we u expliciet uit om ook incidenten met kleinere impact bij ons te melden. Wij behandelen deze vrijwillige meldingen met dezelfde vertrouwelijkheid als de verplichte incidentmeldingen. Met deze informatie weten we niet alleen beter wat er speelt, maar kunnen we ook samen met sector constructief werken aan het verhogen van de digitale weerbaarheid van essentiële diensten in Nederland. Op deze manier kunt u bovendien bijdragen aan het zo efficiënt en effectief mogelijk inrichten van het toezicht.

Welke gegevens heeft u nodig bij een melding?

Het is belangrijk dat u zo snel mogelijk een melding doet na ontdekking van een incident. Waarschijnlijk is op het moment van melden nog niet alle informatie over het incident bij u bekend, daarvoor hebben we begrip.

Meld wat u weet! Na een initiële melding bij de RDI is het mogelijk om op een later moment aanvullende informatie te verstrekken.

Bij een melding wordt u gevraagd om informatie te geven over:

- De aard en de omvang van het incident
- Het vermoedelijke tijdstip van aanvang van het incident
- De vermoedelijke gevolgen van het incident (in én buiten Nederland)
- Een prognose van de hersteltijd
- Zo mogelijk, de door uw organisatie genomen of te nemen maatregelen om de gevolgen van het incident te beperken of herhaling te voorkomen
- De contactgegevens van de medewerker die binnen uw organisatie verantwoordelijk is voor de melding

Wat doet de RDI na een melding?

Nadat u een melding heeft gedaan bij de RDI nemen we contact met u op. We vragen u dan om aanvullende informatie. Incidentmeldingen worden zo spoedig als mogelijk in behandeling genomen, ongeacht of het een verplichte of vrijwillige melding is. Indien het een meldplichtig incident betreft zal er op korte termijn nader onderzoek plaatsvinden. Ook in het geval van een vrijwillige melding is het mogelijk dat er onderzoek zal volgen. De RDI houdt u op de hoogte van het proces en past hoor en wederhoor toe.

Het melden van een incident leidt niet automatisch tot handhaven en ook niet tot verhoogde verwijtbaarheid. Als uw organisatie op een verwijtbare manier in overtreding met de Wbni heeft gehandeld, dan wordt er mogelijk wel handhavend opgetreden.

Als toezichthouder zullen wij er altijd naar streven om een afgewogen beeld te krijgen bij de achtergrond van een incident. De RDI zal incidenten en dreigingen op het gebied van beveiliging van netwerk- en informatiesystemen in bredere zin bestuderen en bespreken. In onze beschouwing zullen we ook incidenten die onder de drempelwaarden blijven en incidenten die in de media zijn gekomen in acht nemen.

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.

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 is niet van toepassing op deze vertrouwelijke gegevens.

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

Deze brochure is een uitgave van:

Rijksinspectie Digitale Infrastructuur
September 2021