De NIS2-richtlijn verplicht betere cyberbeveiliging

RendementOnline

Door redactie FA Rendement

23 mei 2024 | 6 minuten

Eind 2024 wordt in Nederland de Network and Information Security Directive (NIS2) van kracht, de opvolger van de eerste Europese NIS-richtlijn. Het doel hiervan is het verbeteren van de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten. Hoewel de richtlijn niet direct betrekking heeft op het midden- en kleinbedrijf (mkb) kunnen toeleverende ondernemingen er wel aan worden onderworpen. De overheid biedt een helpende hand bij de implementatie van de richtlijn.

De NIS2, die op dit moment wordt vertaald naar Nederlandse wetgeving, geldt voor sectoren en organisaties die van vitaal belang zijn voor de maatschappij, zoals de energiesector, het bankwezen en de gezondheidszorg.

De NIS2 is de opvolger van de eerste richtlijn, die in Nederland in 2016 is opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). De nieuwe richtlijn geldt voor meer sectoren, waaronder de overheid. Daarnaast bevat de richtlijn strengere beveiligingsnormen en meldingseisen voor incidenten.

> **Vanuit de overheid kan worden bepaald dat ook een kleinere onderneming moet voldoen aan NIS2**

Verplicht voldoen aan NIS2

De NIS2-richtlijn richt zich op ondernemingen die als middelgroot of groot worden aangemerkt. Vanuit de overheid kan echter worden bepaald dat ook een kleinere onderneming moet voldoen aan NIS2 als blijkt uit een risicobeoordeling dat deze van essentieel belang is voor de Nederlandse economie of maatschappij.

Het gaat dan bijvoorbeeld om aanbieders van domeinnaamregistratie en elektronische communicatiediensten. Wordt een onderneming verplicht om te voldoen aan de NIS2, dan wordt deze daarvan op de hoogte gebracht.

Meldplicht voor cyberincidenten

Ondernemingen die binnen de reikwijdte van NIS2 vallen, hebben een zorg- en een meldplicht. De zorgplicht houdt in dat een onderneming op basis van een risicobeoordeling alle securitymaatregelen moet treffen die de digitale veiligheid en bedrijfscontinuïteit waarborgen.

De meldplicht houdt in dat een onderneming verplicht is om verstoringen op het gebied van cybersecurity binnen 24 uur te melden bij de toezichthouder die voor de sector van de desbetreffende onderneming geldt.

Bij een cyberincident moet deze ook worden gemeld bij het Computer Security Incident Response Team (CSIRT). Een computercrisisteam kan dan vervolgens ondersteuning bieden. Houdt een onderneming zich niet aan de NIS2-richtlijn, dan kan dit leiden tot hoge boetes. De toezichthouder bekijkt of de regelgeving wordt nageleefd.

Innovatie belemmerd?

Uit onderzoek van IT-specialist Telindus komt naar voren dat 41% van ondernemingen in essentiële sectoren vreest dat de implementatie van de NIS2-regelgeving een belemmering gaat vormen voor de ontwikkeling van nieuwe technologieën en innovaties. Toch ziet meer dan de helft van de ondernemingen (55%) deze richtlijn als een kans om onder andere de kwaliteit van de dienstverlening te verbeteren en de bedrijfscontinuïteit te waarborgen.

Begin nu met voorbereidingen

Hoewel de richtlijn pas eind 2024 van kracht wordt in Nederland, doen ondernemingen er goed aan om nu al te beginnen met de voorbereiding. Het Nationaal Cyber Security Centrum (NCSC), onderdeel van het ministerie van Justitie en Veiligheid dat als doel heeft een digitaal veilig Nederland, raadt aan om in ieder geval de volgende maatregelen te nemen:

- Maak een risicoanalyse.
- Neem passende maatregelen.
- Zorg voor procedures om goed te kunnen reageren op cyberincidenten.

Stel risicoanalyse op

Op basis van een risicoanalyse brengt een onderneming de te beschermen belangen in kaart. Dit zijn zaken die cruciaal zijn voor de onderneming en de dienstverlening. Daarnaast bekijkt de onderneming de dreigingen die er zijn ten opzichte van de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de te beschermen belangen en ten slotte moet de huidige weerbaarheid onder de loep worden genomen.

Op basis van de uitkomsten van de risicoanalyse bepaalt een onderneming de maatregelen die moeten worden getroffen om de risico's die aan het licht zijn gekomen het hoofd te bieden.

> **De eisen van de meldplicht van een incident moeten in de bedrijfsprocessen worden verankerd**

Ontwikkel procedures voor incidenten

Naast het nemen van passende maatregelen om incidenten te voorkomen, is het van belang voor ondernemingen om procedures te ontwikkelen voor het detecteren, monitoren, oplossen en melden van incidenten. Zo kan een onderneming snel en op een passende wijze reageren als deze wordt getroffen.

De eisen van de meldplicht van een incident moeten in de bedrijfsprocessen worden verankerd. Denk hierbij onder andere aan het aantal personen dat door de verstoring is geraakt, de tijdsduur van een verstoring en de mogelijke financiële gevolgen. Het opstellen van een incident response plan biedt hierbij uitkomst. Een dergelijk plan bevat instructies voor werknemers. Beschreven wordt hoe zij moeten handelen bij het optreden van een verstoring, datalek of cyberaanval.

Maatregelen onder NIS2

De website van het Digital Trust Center (DTC), in 2018 opgericht door het ministerie van Economische Zaken en Klimaat (EZK) met als doel Nederlandse organisaties weerbaarder maken tegen cyberdreigingen, gaat in op de maatregelen die onder de zorgplicht van de NIS2 vallen:

1. Een risicoanalyse en beveiliging van informatiesystemen.
2. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets.
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen.
4. Incidentenbehandeling.
5. Basis cyberhygiëne en trainingen op het gebied van cybersecurity.
6. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden.
7. Beveiliging van de toeleverancierskеten.
8. Beleid en procedures over het gebruik van cryptografie en encryptie.
9. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen.
10. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen.

Bestuurder aansprakelijk

De NIS2 stelt bestuurders verantwoordelijk voor het cyberbeleid. Zij moeten zorgen voor passend beleid en toezien op een goede uitvoering ervan. Is het beleid niet op orde, dan kunnen er sancties volgen. Als er na bijvoorbeeld een boete geen verbetering komt, zal de bestuurder persoonlijk worden aangesproken op zijn nalatigheid. Hij kan dan (tijdelijk) uit zijn functie worden gezet.

Basismaatregelen tegen cyberaanvallen

Hoewel de meeste mkb-ondernemingen niet in directe zin te maken krijgen met de eisen die gelden voor de NIS2, worden zij uiteraard wel geacht om hun digitale zaken op orde te hebben. Een aantal jaren publiceerde het NCSC de 'Handreiking Cybersecuritymaatregelen: Stap voor stap naar een digitaal veilige organisatie'. Daarin worden acht basismaatregelen uit de doeken gedaan die ondernemingen kunnen treffen om weerbaar te worden tegen cyberaanvallen. De volgende maatregelen worden voor elke mkb-onderneming aangeraden:

- Installeer zo snel mogelijk updates. Daarbij krijgen automatische updates een sterke voorkeur.
- Houd logbestanden bij. Deze zijn van belang bij het herkennen en afhandelen van cyberaanvallen.
- Voer multifactorauthenticatie uit voor accounts die vanaf het internet bereikbaar zijn, beheerrechten hebben of een essentieel systeem betreffen.
- Pas de 3-2-1-regel toe voor back-ups. Er moeten drie versies van data zijn op twee verschillende media. Daarnaast moet ook één kopie op een andere locatie worden bewaard voor noodherstel.
- Segmenteer het netwerk om zo de gevolgen van een cyberaanval te beperken.

- Beperk toegang tot data en diensten. Geef werknemers alleen toegang tot data en systemen die zij nodig hebben om hun werk te kunnen doen.
- Verleen minimale toegangsrechten. Persoonsgebonden toegang, waarbij elke werknemer een eigen gebruikersaccount heeft, hoort hier ook bij.
- Versleutel bedrijfsinformatie. Door encryptiesoftware te gebruiken, kunnen cybercriminelen data niet inzien.
- Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en zorg voor beschermende maatregelen.

Meldplicht bij datalek

Het niet op orde hebben van de cybersecurity kan een onderneming veel geld kosten. Niet alleen vanwege de directe schade die ontstaat bij een incident en doordat de bedrijfsvoering mogelijk stil is komen te liggen, maar ook door imagoschade en klantverlies.

Bij het optreden van een datalek heeft een onderneming ook een wettelijke meldplicht als onderdeel van de Algemene Verordening Gegevensbescherming (AVG). Treedt een datalek op als gevolg van bijvoorbeeld een hack, dan moeten betrokkenen hiervan op de hoogte worden gesteld als het datalek invloed heeft op hun rechten en vrijheden.

Het is dus voor alle ondernemingen van belang om cybersecurity serieus te nemen, of de NIS2 nu op hen van toepassing is of niet. De rijksoverheid biedt ondersteuning via het DTC en het NCSC.

Dit is een artikel van de redactie van FA Rendement

FA Rendement is dé informatiebron voor administrateurs, boekhouders, controllers en andere financiële professionals. Wat is er veranderd op het gebied van financieel-administratieve wet- en regelgeving, en hoe kun je als specialist deze informatie direct in je dagelijkse werk toepassen? Daarnaast moet je op de hoogte zijn van onder meer de fiscaliteit, automatisering, de loon- en salarisadministratie, sociale voorzieningen, debiteurenbeheer en inkoop.

De onafhankelijke en ervaren redactie van FA Rendement zit bovenop het nieuws en vertelt jou als eerste wat de ontwikkelingen zijn. Altijd in heldere taal en met een praktische insteek, zodat je de informatie direct kunt vertalen naar je eigen werksituatie. FA Rendement is daarnaast multimediaal. De voor jouw vakgebied relevante informatie verschijnt:

- ✓ dagelijks op het digitale platform Rendement Online, waar je onder meer het laatste nieuws, checklists, rekentools, maatwerkbrieven en verdiepingsartikelen tot je beschikking hebt;
- ✓ wekelijks gebundeld in een e-mailnieuwsbrief;
- ✓ maandelijks in het vakblad FA Rendement, boordevol nieuws en achtergrondartikelen, digitaal en op de mat;
- ✓ tweemaandelijks in een handzaam themadossier: een pocketboekje dat iedere editie een complex onderwerp uitdiept.