Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NIS2 verplichtingen

Zorgplicht

De *Network and Information Security-richtlijn* (NIS2) is ontwikkeld door de Europese Unie. De richtlijn is gericht op de verbetering van de digitale weerbaarheid van belangrijke en essentiële diensten en organisaties. De richtlijn schrijft drie verplichtingen voor: de zorgplicht, registratieplicht en meldplicht. Deze infosheet gaat in op de zorgplicht.

Wat is de zorgplicht?

Essentiële en belangrijke entiteiten moeten maatregelen nemen om hun netwerk- en informatiesystemen tegen incidenten te beschermen. Hetzelfde geldt voor de fysieke omgeving waarin de systemen zich bevinden.

Moet mijn organisatie voldoen aan de zorgplicht?

Onder de NIS2-richtlijn vallen entiteiten die bij uitval van diensten zorgen voor een ontwrichtende impact op de economie en de samenleving. Hierbij wordt een onderscheid gemaakt tussen 'essentiële' en 'belangrijke' entiteiten. Voor alle entiteiten die aangewezen zijn als essentieel of belangrijk geldt de zorgplicht.

Via de NIS2 Zelfevaluatie komt u er snel achter of uw organisatie hieronder valt.

Welke maatregelen moet ik nemen om aan de zorgplicht te voldoen?

Onder de zorgplicht vallen ten minste:

1. Een risicoanalyse en beveiliging van informatiesystemen
2. (Beleid en procedures over) incidentenbehandeling
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen
4. Beveiliging van de toeleverancierssketen
5. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden
6. Beleid en procedures om de effectiviteit van beheers-maatregelen van cyberbeveiligingsrisico's te beoordelen
7. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging
8. Beleid en procedures over het gebruik van cryptografie en encryptie
9. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa
10. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde nood-communicatiesystemen binnen de entiteit

Zijn alle maatregelen van toepassing op mijn organisatie?

De NIS2-richtlijn schrijft voor dat de maatregelen passend en evenredig moeten zijn. Bij de beoordeling van de evenredigheid kunt u kijken naar de mate waarin uw organisatie is blootgesteld aan risico's, de omvang van de organisatie, de kans dat zich incidenten voordoen en de mogelijke impact op de maatschappij en economie.

Wie is verantwoordelijk voor het naleven van de zorgplicht?

Het bestuur van de NIS2-entiteit is eindverantwoordelijk voor het naleven van de zorgplicht. Zij kunnen voor het niet naleven aansprakelijk worden gesteld. Er ligt een actieve rol voor hen weggelegd in het goedkeuren van de voorgenomen maatregelen, het houden van toezicht op de implementatie, het volgen van training om kennis te vergroten en het aanbieden van trainingen aan medewerkers.

Houd voor meer informatie www.ncsc.nl in de gaten.

Versie: 6 december 2024

Stappenplan

Het is primair van belang dat een organisatie kan aantonen op passende wijze in control te zijn over haar (digitale) weerbaarheid. Start daarom met de volgende drie stappen.

Stap 1. Maak een risicoanalyse

Een passend niveau van (digitale) weerbaarheid kan slechts bereikt worden via een helder en cyclisch risico-managementbeleid. Dat begint met een risicoanalyse waarin uw te beschermen belangen, dreigingen en de huidige weerbaarheid van uw organisatie worden bekeken. Op basis hiervan kunt u weloverwogen keuzes maken hoe om te gaan met de gevonden risico's. Gebruik hiervoor bijvoorbeeld het 'Risicoanalyse stappenplan' van het Digital Trust Center (DTC).

U kunt uw risicoanalyse sturen door de volgende vragen te beantwoorden:

- Wat zijn de kroonjuwelen/te beschermen belangen van mijn organisatie?
- Welke dreigingen zijn er ten opzichte van mijn te beschermen belangen rondom de beschikbaarheid, integriteit en vertrouwelijkheid?
- Hoe verhoudt de huidige weerbaarheid van de te beschermen belangen zich tot de dreigingen?

Stap 2. Neem passende maatregelen

Via uw risicomanagementproces kunnen nu weloverwogen keuzes worden gemaakt ten aanzien van de maatregelen. Welke dat voor uw organisatie zijn, is afhankelijk van uw eigen analyse en vormt daarmee een maatwerkaanpak. Een goede start voor iedere organisatie is in ieder geval het toepassen van de basismaatregelen van het NCSC of de basisprincipes van het DTC. Andere voorbeelden van mogelijke maatregelen zijn:

- Het vaststellen van eigenaarschap van informatie
  - Meer informatie hierover kunt u vinden in de factsheet: 'Risico's beheersen: de waarde van informatie als uitgangspunt' van het NCSC.
- Het vergroten van cyberbewustwording onder personeel.
  - Meer informatie hierover kunt u vinden op de website van het DTC.
- Het verankeren van risicomanagement in uw organisatie.
  - Meer informatie hierover kunt u vinden op de website van het NCSC.

Stap 3. Ontwikkel procedures ten aanzien van incidenten

Naast het nemen van passende maatregelen om incidenten te voorkomen, is het van belang procedures te ontwikkelen voor het detecteren, monitoren, oplossen en melden van incidenten. Zo kunt u snel en adequaat reageren wanneer uw organisatie wordt getroffen.

NIS2-entiteiten zijn verplicht om incidenten te melden bij het centrale meldpunt en de toezichthouder. De eisen van de meldplicht moeten in de bedrijfsprocessen verankerd worden. Het opstellen van een incidentresponsplan kan hierbij helpen. Lees op de website van het DTC hoe u een responsplan opstelt. De handreiking 'Incidentresponsplan Ransomware' van het NCSC kan u helpen met het opstellen van een plan specifiek op de dreiging van ransomware.