NIS2, wat moet ik ermee?

NIS2, wat moet ik ermee?

Een gids voor het MKB om te voldoen aan de NIS2-richtlijn

Inleiding

In deze whitepaper bespreken we de NIS2-richtlijn en wat deze betekent voor middelgrote ondernemingen. We leggen uit waarom naleving van deze richtlijn cruciaal is, wat de belangrijkste vereisten zijn en hoe u als ondernemer stappen kunt ondernemen om aan deze richtlijn te voldoen. Dit document dient als praktische gids en biedt u alle relevante informatie om direct aan de slag te gaan.

Wat is NIS2?

De NIS2-richtlijn is de opvolger van de oorspronkelijke NIS-richtlijn en is bedoeld om de cyberbeveiliging binnen de Europese Unie te versterken. Waar de eerste NIS-richtlijn zich richtte op de beveiliging van netwerk- en informatiesystemen, gaat NIS2 een stap verder door strengere eisen te stellen en een breder scala aan sectoren te dekken.

De doelstellingen van NIS2 zijn:

- Verhogen van het algemene beveiligingsniveau binnen de EU.
- Verbeteren van de samenwerking tussen EU-lidstaten.
- Versterken van de weerbaarheid tegen cyberdreigingen.

Belang van NIS2

Voor ondernemingen is de NIS2-richtlijn bijzonder relevant. Niet alleen vanwege de wettelijke verplichtingen, maar ook vanwege de toenemende dreiging van cyberaanvallen. Niet-naleving kan leiden tot zware boetes en reputatieschade.

Voordelen van naleving zijn onder andere:

- Verbeterde bescherming van bedrijfsgegevens.
- Verhoogd vertrouwen van klanten en partners.
- Lagere kans op financiële verliezen door cyberincidenten.

Voor wie is NIS2 relevant?

De NIS2-richtlijn richt zich op organisaties in vitale sectoren zoals energie, transport, bankwezen, financiële marktinfrastructuren, gezondheidszorg, drinkwatervoorziening en -distributie, digitale infrastructuur, openbare administratie en ruimtevaart. Naast deze vitale sectoren zijn ook organisaties in de voedselproductie, de chemische sector en de fabricage van medische apparatuur toegevoegd.

Organisaties kunnen controleren of zij onder NIS2 vallen door te kijken naar hun sector en de diensten die zij leveren. Dit kan door de richtlijn en bijbehorende nationale wetgeving te raadplegen en te bepalen of hun diensten als 'essentieel' of 'belangrijk' worden geclassificeerd. Ook is het raadzaam om contact op te nemen met nationale toezichthoudende autoriteiten voor specifieke richtlijnen.

De Rijksoverheid heeft een handige online NIS2 Zelfevaluatie ontwikkeld, waarmee je kan bepalen of de NIS2 van toepassing is voor jouw organisatie.

NIS2, wat moet ik ermee?

Belangrijkste vereisten van NIS2

NIS2 stelt verschillende verplichtingen aan organisaties, waaronder:

- Implementatie van risicobeheermaatregelen.
- Rapportage van incidenten binnen 24 uur.
- Bescherming van essentiële diensten en kritieke infrastructuren.

Voor middelgrote ondernemingen betekent dit dat zij hun huidige beveiligingsmaatregelen moeten evalueren en waar nodig moeten verbeteren om aan deze eisen te voldoen.

Stappen naar naleving

Om te voldoen aan NIS2, kunt u de volgende stappen volgen:

1. **Identificeer essentiële diensten en leveranciers**: Breng in kaart welke diensten en leveranciers essentieel zijn voor uw bedrijfsvoering.
2. **Beoordeel huidige beveiligingsmaatregelen**: Voer een grondige beoordeling uit van uw huidige beveiligingsbeleid en -maatregelen.
3. **Implementeer verbeteringen**: Voer noodzakelijke verbeteringen door, zoals het updaten van software, het trainen van personeel en het verbeteren van incidentresponsprocedures.
4. **Train en verhoog bewustwording**: Zorg ervoor dat alle medewerkers zich bewust zijn van de NIS2-verplichtingen en getraind zijn in cyberveiligheid.

Rol van management en IT-afdeling

Het naleven van NIS2 is een gezamenlijke verantwoordelijkheid. Het management moet de leiding nemen door een duidelijke strategie en beleid vast te stellen. De IT-afdeling is verantwoordelijk voor de technische implementatie en het onderhoud van beveiligingsmaatregelen. Effectieve communicatie en samenwerking tussen beide groepen is cruciaal.

Risicomanagement

Een solide risicomanagementstrategie omvat:

- **Identificatie en beoordeling van risico's**: Analyseer potentiële bedreigingen en kwetsbaarheden.
- **Implementatie van beheersmaatregelen**: Neem passende maatregelen om geïdentificeerde risico's te verminderen.
- **Monitoring en evaluatie**: Houd continu toezicht op de effectiviteit van uw risicomanagement-strategie en pas deze aan waar nodig.

Incidentbeheer

Een effectief incidentbeheerproces bevat:

- **Detectie**: Zorg voor systemen die cyberincidenten snel kunnen detecteren.
- **Respons**: Stel duidelijke procedures op voor een snelle en effectieve reactie op incidenten.
- **Rapportage**: Volg de NIS2-richtlijnen door incidenten binnen 24 uur te rapporteren aan de relevante autoriteiten.
- **Leren van incidenten**: Analyseer incidenten achteraf om zwakke punten in uw beveiliging te identificeren en te verbeteren.

Conclusie

Het naleven van de NIS2-richtlijn is essentieel voor ondernemingen om hun cyberbeveiliging te versterken en te voldoen aan wettelijke verplichtingen. Door de stappen in deze whitepaper te volgen, kunt u uw organisatie beter beschermen tegen cyberdreigingen en bijdragen aan een veiligere digitale omgeving.

NIS2, wat moet ik ermee?

Volgende stappen

- Beoordeel of uw organisatie onder NIS2 valt.
- Voer een risicobeoordeling uit.
- Ontwikkel een incident response plan.
- Zorg voor continue monitoring en onderhoud van systemen.
- Train medewerkers op het gebied van cyberveiligheid.
- Documenteer en rapporteer alle veiligheidsincidenten.

Door deze whitepaper zorgvuldig door te nemen en de stappen te volgen, ben je goed voorbereid om aan de NIS2-richtlijn te voldoen en uw organisatie te beschermen tegen cyberdreigingen. Voor verdere ondersteuning kun je altijd contact opnemen met ons via novins.nl, telefonisch via +316 50 62 72 67 of per mail: info@novins.nl.