DIGITAL

FACTSHEET

NIS2 Cybersecurity-ondersteuning

Geen organisatie kan nog opereren zonder focus op cybersecurity en databeveiliging. Veranderende regelgeving, groeiende cyberdreigingen en het toenemende belang van digitale veiligheid dwingt organisaties om proactieve strategieën te ontwikkelen en te implementeren om hun digitale ecosystemen te beschermen en te versterken.

Regelgeving legt organisaties verantwoordelijkheden op

De opkomst van strengere regelgeving, zoals de Network and Information Security Directive 2 (NIS2), legt organisaties verhoogde verantwoordelijkheden op om de digitale veiligheid te waarborgen. Organisaties moeten cybersecuritymaatregelen implementeren, hun digitale systemen beschermen tegen geavanceerde cyberdreigingen en kunnen aantonen dat zij voldoen aan de nieuwe regelgeving. De regelgeving richt zich op essentiële en belangrijke sectoren, waaronder energie, transport, financiën en gezondheidszorg.

Evolutie van cyberdreiging

Vrijwel al deze sectoren worden daarbij geconfronteerd met een voortdurende evolutie van cyberdreigingen. Hackers, malware en andere kwaadwillende activiteiten worden steeds geavanceerder en bedreigen de integriteit en veiligheid van digitale systemen. Dit legt druk op organisaties om niet alleen te voldoen aan regelgeving, maar ook om proactief in te spelen op de voortdurende evolutie van cyberaanvallen.

Actie gevraagd

Niet in actie komen verhoogt de kans op reputatieschade, financiële verliezen en verstoring van bedrijfsactiviteiten als gevolg van cyberaanvallen of datalekken. Het is van cruciaal belang dat organisaties proactief actie ondernemen, veerkrachtige digitale systemen te ontwikkelen en te onderhouden. De complexiteit van digitale infrastructuren, de noodzaak van samenwerking met toeleveringsketenpartners en de groeiende afhankelijkheid van digitale processen vergroten de uitdagingen. BDO begrijpt de complexiteit van deze ontwikkelingen en de impact ervan op organisaties. We voorzien de behoefte aan praktische, op maat gemaakte oplossingen die organisaties helpen bij het ontwikkelen en implementeren van effectieve cybersecuritymaatregelen. Ons framework, gebaseerd op internationale standaarden zoals ISO 27001, biedt organisaties een gedegen aanpak om hun digitale veiligheid te versterken, te voldoen aan de NIS2-regelgeving en hun algehele digitale veerkracht te verbeteren. We geloven dat proactieve investeringen in digitale beveiliging niet alleen wettelijk verplicht zijn, maar ook de veerkracht en reputatie van organisaties op de lange termijn versterken.

Onze dienstverlening

Onze aangeboden dienstverlening om organisaties te helpen bij het aanpakken van de uitdagingen van NIS2, omvat een uitgebreid cybersecurityadvies en implementatieprogramma.

Cybersecurity-assessment

We beginnen met een diepgaande beoordeling van de huidige digitale infrastructuur, risico's en kwetsbaarheden van een organisatie. Dit omvat technische evaluaties, maar ook een analyse van beleid, procedures en menselijke aspecten.

Op maat gemaakte oplossing

Op basis van de beoordeling ontwikkelen we een op maat gemaakte cybersecuritystrategie die voldoet aan de NIS2-eisen en past bij de specifieke behoeften van een organisatie. Hierin nemen we technische maatregelen op, evenals beleidsrichtlijnen, processen en trainingsprogramma's.

Implementatie en training

We ondersteunen organisaties bij het daadwerkelijk implementeren van de voorgestelde maatregelen. Dit omvat technische configuraties, beleidsimplementatie en training van medewerkers om bewustzijn en betrokkenheid bij cybersecurity te vergroten.

Monitoring en incidentrespons

We helpen organisaties bij het opzetten van monitoring- en incidentresponsmechanismen, zodat ze snel kunnen reageren op mogelijke bedreigingen en incidenten kunnen aanpakken voordat ze zich verspreiden.

Certificering en compliance

We begeleiden organisaties bij het verkrijgen van relevante certificeringen, zoals ISO 27001, om aan te tonen dat ze voldoen aan internationale cybersecuritystandaarden en NIS2-vereisten.

Onze aanpak is gebaseerd op jarenlange ervaring en expertise op het gebied van cybersecurity. We begrijpen dat elk bedrijf uniek is, dus onze dienstverlening is flexibel en afgestemd op de specifieke behoeften van de klant. Altijd met het doel om organisaties te helpen bij het versterken van hun digitale beveiliging, het voldoen aan de NIS2-regelgeving en het opbouwen van een veerkrachtige digitale infrastructuur die hen beschermt tegen toenemende cyberdreigingen.

Uw voordelen en resultaten

Door onze dienstverlening kunnen organisaties de volgende voordelen en resultaten verwachten.

Verhoogde cybersecurity

Organisaties profiteren van een versterkte digitale beveiliging die hen beschermt tegen geavanceerde en steeds evoluerende cyberdreigingen.

Naleving van NIS2

We zorgen ervoor dat organisaties volledig voldoen aan de vereisten van NIS2, waardoor ze juridische en regelgevende risico's vermijden.

Bescherming van bedrijfscontinuïteit

Onze maatregelen en strategieën waarborgen de bedrijfscontinuïteit, waardoor organisaties in staat zijn om onverwachte incidenten effectief aan te pakken en minimale verstoringen te garanderen.

Verbeterd vertrouwen

Organisaties kunnen hun klanten en stakeholders geruststellen door te laten zien dat ze de beveiliging serieus nemen en in staat zijn om gevoelige informatie te beschermen.

Minimale reputatieschade

Door proactief te handelen en incidenten snel te identificeren en aan te pakken, kunnen organisaties de impact van mogelijke datalekken en cyberaanvallen minimaliseren, wat resulteert in minder reputatieschade.

Efficiënte samenwerking

Onze diensten omvatten ook het in kaart brengen van de toeleveringsketen en samenwerkingsverbanden, wat resulteert in betere beveiliging van deze relaties en effectievere samenwerking.

Inzicht en bewustzijn

Organisaties zullen een dieper inzicht krijgen in hun eigen digitale omgeving en de mogelijke risico's. Bovendien worden medewerkers getraind om zich bewust te zijn van cyberdreigingen en best practices.

Bescherming tegen boetes en sancties

Door te voldoen aan de NIS2-regelgeving voorkomen organisaties mogelijke boetes en sancties, wat hun financiële positie beschermt.

Voorsprong op concurrenten

Organisaties die vroegtijdig investeren in cybersecurity en voldoen aan NIS2, kunnen zich onderscheiden van concurrenten en klanten aantrekken die prioriteit geven aan veiligheid.

Langetermijnveiligheid

Onze holistische aanpak en maatregelen helpen organisaties om een duurzame en adaptieve digitale beveiligingsinfrastructuur op te bouwen die hen ook in de toekomst beschermt tegen opkomende bedreigingen.

Deze voordelen bieden organisaties niet alleen bescherming tegen toenemende cyberdreigingen, maar helpen ook bij het opbouwen van veerkrachtige en betrouwbare digitale ecosystemen die essentieel zijn voor hun voortdurende succes.

Onderscheidend vermogen

Het onderscheidend vermogen van BDO in het leveren van deze dienst ligt in de feitelijke expertise, ervaring en bewijslast die we bieden.

Diepgaande Expertise

Ons team van cybersecurity-experts beschikt over diepgaande kennis van zowel cybersecurity, informatiebeveiliging en privacy, inclusief wet- en regelgeving, waaronder NIS2. Hierdoor kunnen we klanten nauwkeurig adviseren over het identificeren, evalueren en aanpakken van digitale risico's.

Bewezen Trackrecord

BDO heeft een bewezen staat van dienst in het succesvol ondersteunen van organisaties bij complexe uitdagingen. We hebben al talloze klanten geholpen bij het implementeren van effectieve cybersecuritymaatregelen, het voldoen aan regelgeving en het (technisch) toetsen van deze maatregelen, bijvoorbeeld met security testen.

Op maat gemaakte oplossingen

In plaats van one-size-fits-all-benaderingen biedt BDO op maat gemaakte oplossingen die aansluiten bij de specifieke behoeften van elke klant. We begrijpen dat elke organisatie uniek is en een gepersonaliseerde aanpak vereist.

Actuele kennis

Onze experts blijven voortdurend op de hoogte van de nieuwste ontwikkelingen in de cyberwereld en regelgeving. We passen onze aanpak aan op basis van de meest actuele dreigingslandschappen en vereisten.

Uitgebreide middelen

BDO beschikt over uitgebreide middelen en tools om organisaties te ondersteunen bij het identificeren, evalueren en mitigeren van cyberdreigingen. Onze investering in de nieuwste technologieën stelt ons in staat om efficiënt en effectief te opereren.

Concrete resultaten

Onze aanpak heeft geleid tot meetbare resultaten voor organisaties, met aantoonbare verbeteringen in cybersecuritymaatregelen, naleving van regelgeving en bedrijfscontinuïteit.

Diepgaande analyse

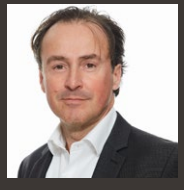
We bieden diepgaande analyses, ondersteund door cijfers en statistieken, om organisaties te helpen de daadwerkelijke impact van onze diensten op hun organisatie te begrijpen. Hierbij gebruiken we percentages en kwantitatieve gegevens om de effectiviteit aan te tonen.

Focus op educatie

Naast het bieden van oplossingen hechten we veel belang aan het educatieve aspect. We zorgen ervoor dat organisaties en hun medewerkers begrijpen waarom bepaalde maatregelen nodig zijn en hoe ze bij kunnen dragen aan een veiligere digitale omgeving.

Meer informatie?

We nodigen u uit om actie te ondernemen en uw organisatie voor te bereiden op de uitdagingen van NIS2 en de evoluerende cyberdreigingen. Samen met BDO kunt u de weg inslaan naar een veiligere digitale toekomst. Neem daartoe contact op met één van onze specialisten.



Kees Plas
Partner Advisory – Cyber Security
E kees.plas@bdo.nl
T 030 – 633 62 30

Ronald Westerveen
Senior Manager – Cyber Security
E ronald.westerveen@bdo.nl
T 030 – 284 97 28

Rick van Dijk
Senior Manager – Cyber Security
E rick.van.dijk@bdo.nl
T 020 – 363 42 21

09/2023 – AD2331