BEREID U VOOR OP DE NIS2-RICHTLIJN

APPROACH CYBER HELPT U UW WEG TE VINDEN IN DE NIEUWE WETGEVING TER VERSTERKING VAN DE CYBERBEVEILIGING IN EUROPA EN DE JUISTE STAPPEN TE NEMEN OM SNEL AAN DE RICHTLIJN TE VOLDOEN.

Begin op tijd

Met de goedkeuring van de NIS2-richtlijn (richtlijn inzake netwerk- en informatiesystemen) versterkt de Europese Unie (EU) haar eisen op het gebied van cyberveiligheid voor een groot aantal bedrijven en organisaties. De richtlijn werd omgezet in Belgisch recht door de wet die op 19 april 2024 werd aangenomen door het federale parlement. Er zijn veel sectoren bij betrokken en NIS2 vereist dat ze verbeterde cyberbeveiligingsmaatregelen nemen, incidenten melden en onder toezicht staan van de nationale cyberbeveiligingsautoriteit.

De betrokken entiteiten hebben tot 18 oktober 2024 de tijd om aan de Belgische NIS2-wet te voldoen.
Dit betekent dat ze alle vereiste maatregelen al moeten hebben genomen.

Is NIS2 op uw organisatie van toepassing?

Het toepassingsgebied van de NIS2-richtlijn is aanzienlijk breder dan dat van zijn voorganger, NIS1, en omvat een groter aantal bedrijven en organisaties in verschillende sectoren. De NIS2-richtlijn is gericht op organisaties van een bepaalde omvang die diensten verlenen in kritieke sectoren. Entiteiten in deze sectoren worden beschouwd als vitaal voor het behoud van kritieke maatschappelijke of economische functies in België. Omvang en de geleverde dienst zijn daarom de twee belangrijkste criteria om te bepalen of de NIS2-richtlijn van toepassing is op een organisatie.
Het gaat om de volgende sectoren:

- **Zeer kritieke sectoren:** energie, vervoer, bankwezen, infrastructuur financiële markten (ook onderworpen aan DORA), gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, beheer van ICT-diensten, overheid (centraal en regionaal) en ruimtevaart.

- **Andere kritieke sectoren:** post- en koerierdiensten, afvalstoffenbeheer, vervaardiging, productie en distributie van chemische stoffen, productie, verwerking en distributie van levensmiddelen, industrie, leveranciers van digitale diensten en onderzoek.

Op bepaalde uitzonderingen na moet een organisatie ten minste als een middelgrote onderneming worden beschouwd om onder de NIS2-richtlijn te vallen. Een middelgrote onderneming heeft ten minste 50 werknemers en/of een jaaromzet (of jaarlijks balanstotaal) van meer dan 10 miljoen euro.

De NIS-richtlijn maakt ook onderscheid tussen "essentiële" en "belangrijke" entiteiten. Dit onderscheid wordt gemaakt op basis van de omvang van de entiteit en de verleende dienst.
Het verschil tussen essentiële en belangrijke entiteiten ligt vooral in de controle- en sanctiemechanismen. Essentiële entiteiten zullen regelmatiger en strenger worden gecontroleerd dan belangrijke entiteiten.

Hoe zit het met bedrijven die niet tot de doelgroep behoren?

NIS2 specificeert niet expliciet de verplichtingen voor bedrijven die niet binnen het toepassingsgebied vallen. Maar zelfs als een bedrijf niet binnen de reikwijdte van NIS2 valt, kan het toch indirect worden geraakt als leverancier, of ervoor kiezen bepaalde aanbevolen praktijken te volgen om zijn cyberbeveiliging te verbeteren.

De NIS2-richtlijn is gericht op organisaties van een bepaalde omvang die diensten verlenen in kritieke sectoren, de zogenaamde "essentiële" en "belangrijke" entiteiten.

Een toezichts- en controleorgaan, het CCB

Elke EU-lidstaat moet een of meer bevoegde autoriteiten aanwijzen om toezicht te houden op de toepassing van de richtlijn, te zorgen voor de implementatie van passende beveiligingsmaatregelen en incidenten en crises op het gebied van cyberbeveiliging te beheren. In België is de bevoegde autoriteit het Centrum voor Cybersecurity België (CCB). De betrokken entiteiten moeten zich registreren bij het CCB via het Safeonweb@work portaal. Uitzonderingen daargelaten, kan aan deze verplichting worden voldaan tot 18 maart 2025.

De betrokken Belgische organisaties moeten zich vóór 18 maart 2025 registreren bij het Centrum voor Cybersecurity België (CCB).

Wat zijn uw verplichtingen?

De betrokken entiteiten moeten gepaste en evenredige maatregelen nemen om de risico's te beheren die de veiligheid van hun netwerken en informatiesystemen bedreigen en om de gevolgen van incidenten voor de ontvangers van hun diensten en voor andere diensten weg te nemen of te beperken.

De betrokken entiteiten moeten ook zonder onnodige vertraging het nationale CSIRT op de hoogte brengen van belangrijke cyberincidenten (in België het CCB, cert.be). Tot slot moeten essentiële entiteiten regelmatige conformiteitsbeoordelingen uitvoeren, gecontroleerd door een instantie die toezicht houdt op de naleving.

Neem contact met ons op voor meer informatie over passende en evenredige maatregelen.

Het CCB heeft de bevoegdheid om maatregelen te nemen om entiteiten aan te moedigen passende actie te ondernemen. Daartoe kan ze bijvoorbeeld regelmatige externe audits opleggen, inspecties uitvoeren of inzage in bepaalde documentatie eisen.

Het CCB kan met name waarschuwingen of bindende instructies geven aan entiteiten om vastgestelde tekortkomingen te verhelpen of om hun klanten hierover te informeren.

NIS2 vereist dat u uw maatregelen voor risicobeheer op het gebied van cyberbeveiliging versterkt en incidenten binnen vastgestelde termijnen meldt bij het CCB.

Wat zijn de sancties voor niet-naleving?

De NIS2-richtlijn versterkt niet alleen de eisen en verplichtingen op het gebied van cyberbeveiliging, maar voorziet ook in strengere sancties om naleving te garanderen.

Inbreuken op risicobeheersmaatregelen of de melding van incidenten kunnen bijvoorbeeld worden bestraft met afschrikkende administratieve boetes.

Voor essentiële entiteiten kunnen deze boetes oplopen tot 10 miljoen of 2% van de wereldwijde jaaromzet. Voor belangrijke entiteiten is dit 7 miljoen of 1,4% van de wereldwijde jaaromzet. In geval van recidive voor dezelfde feiten binnen een periode van drie jaar, wordt het bedrag van de administratieve boete verdubbeld. Er moet worden opgemerkt dat deze boetes niet van toepassing zijn op overheidsinstanties, in tegenstelling tot de andere administratieve boetes, die wel van toepassing zijn.

De sancties zijn streng en afschrikkend om naleving te garanderen. In sommige gevallen zijn ze vergelijkbaar met die van de GDPR.

Topmanagement nu direct betrokken

NIS2 legt meer verantwoordelijkheid bij het management, zodat cyberbeveiliging een echt gespreksonderwerp wordt tot op directieniveau. Om het bewustzijn te vergroten, kunnen de personen die deze entiteiten vertegenwoordigen aansprakelijk worden gesteld voor het niet naleven van de verplichtingen van de richtlijn.

De straffen zijn zwaar, variërend van een persoonlijke boete voor de CEO en directeurs, tot een tijdelijk verbod op het bekleden van een bestuursfunctie.

Het is daarom noodzakelijk dat de Raad van Bestuur de uitdagingen van Informatiebeveiliging begrijpt en de relevantie van de genomen maatregelen kan beoordelen.

Het topmanagement wordt rechtstreeks verantwoordelijk gehouden voor de naleving van NIS2. Niet-naleving van deze verplichtingen kan leiden tot persoonlijke sancties en boetes.

Welke maatregelen moeten worden genomen?

Vooreerst, wat betreft governance, zal het topmanagement maatregelen voor risicobeheer op het gebied van cyberbeveiliging moeten goedkeuren, toezicht moeten houden op de implementatie ervan en verantwoordelijk kunnen worden gehouden voor eventuele tekortkomingen.

Om er zeker van te zijn dat ze de maatregelen die ze goedkeuren begrijpen, moeten leden van het hogere management cyberbeveiligingstraining volgen en regelmatig soortgelijke training aanbieden aan hun personeel.

Beveiligingsmaatregelen moeten passend en proportioneel zijn, gebaseerd op een risicoanalyse. Natuurlijk moeten alle basale cyberhygiënepraktijken worden toegepast, maar in de context van NIS2 zijn deze maatregelen zijn niet voldoende.

NIS2 vereist een totaalaanpak, een beheersysteem en continue verbetering, inclusief een reeks technische (zoals encryptie, cryptografie, multifactorauthenticatie etc) en niet-technische, organisatorische maatregelen (zoals governance, beleid en procedures, een continuïteitsplan, back-upbeheer, crisisbeheer, beveiligingsbeheer van leveranciers en dienstverleners, fysieke beveiliging en beveiliging van de omgeving, beveiliging van personeel, enz.) Er zijn ook extra maatregelen toegevoegd aan de Belgische NIS2-wet.

De te nemen maatregelen zijn zowel technisch als niet-technisch. Naast deze maatregelen is een echt systeem voor risicobeheer en voortdurende verbetering nodig.

Je staat er niet alleen voor! Approach Cyber staat aan je zijde

NIS2-compliance is een van de belangrijkste compliance-kwesties in 2024 en een effectieve respons vereist een grondige voorbereiding en expertise. Hier leest u hoe wij u kunnen helpen bij de voorbereiding op en naleving van NIS2:

1.Gap-analyse en risicobeoordeling

- We voeren een uitgebreide gap-analyse uit om uw huidige praktijken te vergelijken met de vereisten van NIS2, op basis van de frameworks die door het CCB worden genoemd (zoals CyberFundamentals of "CyFun", en ISO27001).
- We onderwerpen de kwetsbaarheden die uit de gap-analyse naar voor komen aan een risicobeoordeling, om de risico's en potentiële bedreigingen in uw omgevingen, informatiesystemen en bedrijfsvoering te identificeren.

2.Implementatie van veiligheidsmaatregelen

- We implementeren de juiste technische en organisatorische maatregelen om de geïdentificeerde risico's te beheren, in overeenstemming met de aanbevelingen van het CCB.
- We zorgen ervoor dat alle beveiligingsmaatregelen regelmatig worden bijgesteld en getest om te voldoen aan nieuwe bedreigingen en NIS2-vereisten.

3.Incident response protocollen opstellen

- We ontwikkelen gedetailleerde protocollen voor het detecteren, melden, rapporteren en reageren op cyberbeveiligingsincidenten, in lijn met CCB- en de toepasselijke GDPR-vereisten.
- We trainen uw personeel om beveiligingsincidenten, waaronder lekken van persoonsgegevens, te herkennen en hier efficiënt op te reageren.

4.Bewustmaking en training

- We trainen het management en uw medewerkers in goede cyberbeveiligingspraktijken en de te volgen procedures in het geval van een incident.
- We maken uw hele organisatie bewust van het belang van NIS2-compliance.

5.Documentatie en naleving van regelgeving

- We documenteren alle policies, inclusief het informatiebeveiligingsbeleid en het gecoördineerde kwetsbaarhedenbeleid, die essentiële NIS2-voorwaarden zijn, alsook de geïmplementeerde beveiligingsprocedures en -maatregelen.
- We houden documentatie up-to-date, zodat u uw compliance kunt aantonen aan de autoriteiten mocht dat nodig zijn.

6.Controle, onderhoud en certificering

- We zorgen voor regelmatige monitoring en continue updates van uw beveiligingsmaatregelen om duurzame naleving te garanderen, inclusief het opstellen van dashboards voor het management en de raad van bestuur.
- Voor essentiële entiteiten kunnen we u helpen bij de voorbereiding op en het slagen voor CyFun- of ISO27001-audits, inspecties en certificeringen binnen de wettelijk opgelegde termijn (18 april 2027).

Daadwerkelijke expertise en praktijkervaring zijn van cruciaal belang om conformiteit te waarborgen, effectief te reageren op incidenten en uw kritieke infrastructuren te beschermen.

Neem contact met ons op voor meer informatie over de belangrijkste stappen voor NIS2-compliance en ontdek hoe wij deze in de praktijk brengen. Op basis van de referentiekaders die door het CCB aanhaalt en met onze succesvolle ervaring bij tal van organisaties, staan we klaar om u te ondersteunen in elke fase van uw compliance traject.

Approach Cyber ondersteunt u in elke fase van uw compliance traject. Gebaseerd op de frameworks aangehaald door het CCB en onze succesvolle ervaring met vele organisaties.

Wat zijn de voordelen van de NIS2-richtlijn voor uw organisatie?

Naast naleving biedt NIS2 een kans om je te onderscheiden op de markt, of om het goede voorbeeld te geven als je een overheidsinstantie bent. Bedrijven die blijk geven van een proactieve inzet op het gebied van cyberbeveiliging kunnen niet alleen het risico op operationele verstoringen minimaliseren, maar ook het vertrouwen van hun klanten en partners vergroten.

Met NIS2 kunnen bedrijven zich onderscheiden in de markt en het vertrouwen van klanten en partners versterken door een proactieve inzet voor cyberbeveiliging te tonen.

Getuigenis van onze CEO

"*Dit is een van de hotste compliance-onderwerpen van het jaar, naast de AI-Act. In plaats van NIS2 te zien als een tweede GDPR, met zijn regeldruk en boetes, moeten we het zien als een kans om de cybersereniteit van uw bedrijf te versterken in een bedreigend digitaal landschap,*" **David Vanderoost, CEO van Approach Cyber.**

Waarom kiezen voor Approach Cyber als uw compliance partner?

Wij bieden u de middelen, tools en expertise om op doeltreffende wijze door dit complexe regelgevingslandschap te navigeren. Door met ons samen te werken, kunt u erop vertrouwen dat uw organisatie goed is voorbereid om de uitdagingen van NIS2 aan te gaan en uw digitale bedrijfsmiddelen te beschermen tegen potentiële bedreigingen.

Approach Cyber is uw partner bij uitstek in dit proces:

- **Een solide, erkende partner:** Approach Cyber bestaat al meer dan 20 jaar, heeft tal van referenties en is ISO 27001/27701 gecertificeerd.
- **Ondersteuning via regionale subsidies mogelijk:** als uw bedrijf een KMO is, kunt u profiteren van aanzienlijke financiële steun van uw regio. Approach Cyber is een dienstverlener die erkend/gelabeld is door de autoriteiten in de drie regio's van het land.
- **Sectorale samenwerking:** We nemen actief deel aan initiatieven om informatie en ervaring over NIS2 te delen en aan sectoriële werkgroepen om bedrijven te ondersteunen (zoals Agoria, Cyber Security Coalition, SecAppDev, ISACA, FSMA, enz.)
- **Een multidisciplinair team van meer dan 100 mensen:** Wij bieden zowel technische, strategische als juridische expertise om u door de complexe vereisten van NIS2 te loodsen.
- **Bedrijfsgerichte oplossingen op maat:** we ontwikkelen oplossingen die zijn afgestemd op uw specifieke behoeften en op de omvang van uw organisatie. We pakken uitdagingen en behoeften op het gebied van cyberbeveiliging op elk niveau aan, tot in de Raad van Bestuur.
- **Een complete en geïntegreerde "approach":** we bieden een complete reeks cyberbeveiligingsdiensten (360°) met een alles-in-één aanpak. Dankzij onze sterke technologische partnerschappen kunnen we geavanceerde, geïntegreerde oplossingen leveren die het beheer van uw beveiliging vereenvoudigen. Hierdoor kunt u zich concentreren op uw kernactiviteiten, zonder de complexiteit van het coördineren van meerdere serviceproviders.

Neem contact met ons op

Neem contact met ons op voor meer informatie over de NIS2-richtlijn en hoe wij u kunnen helpen om hieraan te voldoen.

info@approach-cyber.com
+32 3 366 21 76
+32 10 83 22 11