ManageEngine
AD360

Een uitgebreide handleiding voor

NALEVING*VAN DE NIS2 RICHTLEN

www.manageengine.com/nl/active-directory-360/

Introductie

In een wereld die wordt gedomineerd door digitale transformatie is het in acht nemen van nalevingsnormen niet alleen een wettlijke vereiste, maar een cruciaal aspect voor het behouden van vertrouwen, geloofwaardigheid en succes op de lange termijn.

Organisaties moeten navigeren door een steeds veranderend regelgevingslandschap en ervoor zorgen dat ze voldoen aan strenge normen voor gegevensbescherming en privacy. Deze naleving beschermt niet alleen gevoelige informatie, maar verbetert ook het vertrouwen van de klant en de bedrijfsreputatie. Naleving op het gebied van cyberbeveiliging is een voortdurende inspanning om an de wettelijke vereisten t voldoen en tegelijkertijd uw organisatie te beveiligen tegen de meedogenloze aanval van cyberdreigingen.

Wat is de NIS2-richtlijn?

De tweede Richtijn Netwerk- en Informatiebeveiliging (NIS2) is een Europese wetgeving voor cyberbeveliligin die strengere esisen telt op hest gebied van risicobeheer en het melden van incidenten. Het doel is de veerkracht van cyberbeveliliging in netwerken en informatiesystemen t vergroten door de goedkeuring van geschikte beveiligingsprotocollen af te dwingen en exploitanten te verplichten direct incidenten te melden aan de relevante autoriteiten.

De NIS-richtlijn versus de NIS2-richtlijn

De NIS-richtijn was gericht op het waarborgen van de veilgheid van essentiële diensten en digitale dienstverleners. Dit vereiste uitvoeringsmaatregelen om risico's an te pakken en de gevolgen van beveiligingsincidenten te vyoorkomen en te beperken.

In vergell king met zijn voorganger breidt NIS2 de reilkwijdte van gedekte organisaties en sectoren uit met online marktplaatsen en zoekmachines. Het introduceert verdere beveiligingsvoorwaarden voor het warborgen an d beveiligin van communicatienetwerken, amen mnet specifieke verantwoordeljkhede oor cloud-computin diensten. Het vereenvoudigt ok de meldingsverplichtingen en handhaaft strengere maatregelen.

Niet-monetaire sancties

NIS2 geeft nationale autoriteiten het recht om niet-monetaire sancties op te leggen, zoals:

- Nalevingsbevelen.
- Instructies voor binding
- Bevelen voor de implementatie van beveiligingscontrole
- Bevelen tot kennisgeving van dreigingen aan klanten van entiteiten.

Administratieve boetes

Als het gaat om administratieve boetes, maakt NIS2 een onderscheid tussen essentiéle en belangrijke entiteiten:

- Essentiële entiteiten krijgen een boete van minimaal **€ 10.000.000 of 2%** van de wereldwijde jaaromzet, afhankelijk van wat hoger is.
- Belangrijke entiteiten krigen een boete van minimaal **€ 7,000.000 of 1.4%** van de wereldwijde jaaromzet, afhankelijk van wat hoger is.

Strafrechtelijke sancties

NIS2 bevat nieuwe maatregelen om de leiding ter verantwoording te roepen in geval van niet- naleving. Hierdoor kunnen de autoriteiten van de lidstaten:

- Vereisen dat organisaties nalevingsschendingen openbaar maken.
- Een openbare verklaring afleggen waarin de verantwoordeljke personen, zowel natuurljke bersonen als rechtspersonen, worden bekendgemaakt voor de overtreding en de aard ervan.
- Personen tijdelijk verbieden om beheerrolen op zich te nemen binnen essentiële entiteiten in geval van herhaalde schendingen.

Bron: *nis2directive.eu/nis2-boeles/*

De tijdlijn

2016 — **Oorspronkelijke NIS-richtijn treedt in werking**

2020 — **NIS2-richtlijn is ingevoerd**

2023 — **NIS 2-richtijn treedt in werking**

2024 — **Deadline om aan de regelgeving te voldoen**

De 15 sectoren die onder NIS2 vallen

De sectoren die aan NIS2 moeten voldoen, zijin onderverdeeld in essentiële en belangrike entitleiten. Essentiële entiteiten bestaan uit rot bedrjven die actief zijn in sectoren die als cruciaa Worden beschouwd, met meer dan 250 werknemers of een omzet van meer dan 50 mijoen euro. Belangrjke entiteiten zijin onder meer grote bedrijen in andere vitale sectoren of middelgrote bedrijven met 50 tot 249 werknemers, of een omzet variërend van € 10 miljoen tot 50 miljoen euro en die actief zjn in de , andere sectoren binnen het bereik

Essentiële sectoren	Belangrijke sectoren
Transport	Levensmiddelen
Financie	Digitale aanbieders
Energie	Chemische stoffen
Drinkwater	Post-en koeriersdiensten
Gezondheidszorg	Afvalstofenbeheer
Ruintevaart	Vervaardiging
Digitale infrastructuur	Onderzoek
Openbaar bestuur	

Nieuwe organisatorische vereisten van NIS2

NIS2 heeft nieuwe vereisten geimplementeerd voor organisaties o vier over koepelende gebieden die gericht jin op et versterken van de weerbaarhelid tegen é cyberdreigingen. Deze gebieden zjn risicobeheer, verantwoordelijkheid van bedrijven, rapportageverplichtingen en bedrijfscontinuiteit.

Risicobeheer

Organisates wordt geadviseerd maatregelen te nemen on ybersico's te beperken, z0als het verbeteren van incidentbeheer, sterke beveiliging van de toeleveringsketen, verbeterde toegangscontrole en versleutelingstechnieken.

Yerantwoordelijicheid van bedrijven

Het bedrijfsbeheer moet toezicht houden op cyberbeveilingsprotocollen., deze goedkeuren en een training volgen. Het niet aanpakken van beveiligingsincidenten kan leiden tot boetes voor het beheerteam.

Rapportageverplichtingen

Zowel essentiële als belangrijke entitlien zjin verplichtom procedures op te stellen die de tijdige rapportage van beveilgingsincidenten, vergemakkelijken. NIS2 schrijft specifieke meldingstermijnen voor, zoals de vereiste "vroegtijdige waarschuwing"binnen 24 uur.

Bedrijfscontinuiteit

Organisaties moeten strategieën voorbereiden om de bedrijfscontinuiteit te behouden in het geval van cyberincidenten. Deze strategie moet protocollen yoor systeemherstel, noodprocedures en het opzetten yan een crisisresponsteam omvatten.

De 10 minimumvereisten van NIS2

NIS2 vereist dat de bovengenoemde essentiële en belangrijke sectoren de volgende fundamentele beveliligingsmaatregelen nemen, gericht op het beperken van waarschijinlijke cyberdreigingen.

01

Uitgebreide risicobeoordeling

Zorg voor risicobeoordelingen en en beveiligingsbeleid dat is afgestemd op de informatiesystemen binnen uw organisatie. Dezeé risicobeoordelingen moeten grondige evaluaties omvatten van potentiële bedreigingen en kwetsbaarheden, waarbij fekening wordt gehouden met factoren zoal gegevensgevoeligheid, systeemarchitectuur en potentiële aanvalsvectoren.

02

Geavanceerde authenticatie

Implementeer maatregelen zoals MFA, continue authenticatieoplossingen er tekstversleuteling in uw organisatie, indien nodig.

03

Plan voor incidentreactie

Bereid en onmiddellijk reactieplan voor om mogelijke beveliligingsinbreuker Onmiaa.u... aan te pakken zodra deze zich Dit lan moet snelle en doortastende maatregelen bevatten om risico's te beperken en gevoelige activa te beschermen tegen ongeoorloofde toegang of compromittering.

04

Effectiviteit van beveiliging

Stel bpeleid e rocedures op" en handhaaf deze om d fficienti van de beveliligingsmaatregelen i ine w rganisati zji geinplementeerd te evalueren. Dit ornvat het uitvoeren van regelmatige evaluaties en controles om de soliditeit an beveilingsprotocollen e meten, potentiële kwetsbaarheden te identificeren en de algehele effectiviteit van de bestaande beveliligingsinfrastructuur te bepalen.

05

Beheer van toegangscontrole

Implementee beveligingsprocedures voor werknemers i toegang hebben o gevoelige of belangrijke gegevens en stel beleid op voor toegang tot gegevens. Zorg ook voor een overzicht yan alle relevante assets in uw organisatie en zorg eryoor dat deze op de juiste manier worden benut en behandeld.

06

Versleutelingsbeleid

Implementeer beleid en procedures met betrekking tot het gebruik van cryptograie en versleuteling voor het beheren van gevoelige gegevens binnen uw organisatie. Dit beleid moet richtlijinen bevatten voor de juiste toepassing van cryptografische methoden om data-at-rest, tijdens overdracht en tijdens verwerking te beschermen.

07

Herstel na noodgeval

Bereid een back-up en herstelplan voor om uw bedrifsactiviteiten te beheren na een mogeljke beveiligingsaanval. Zorg voor regelmatige back-ups en zorg voor een plan om de juiste toegan ot informalietechnologiesystemen te garanderen tjdens en na een beveiligingsincident.

08

Beveiligingsmaatregelen

Bevelig de aanschaf, ontwikkeling en werking van systemen en stel beleid op yoor het omgaan met en rapporteren van kwetsbaarheden die zich kunnen voordoen.

09

Risicobeheer in de toeleveringsketen

Zorg oor en Strikte beveiliging van toeleveringsketens. Stel beveilingsmaatregelen op die passen bij de kwetsbaarheden van elke directe leverancier en beoordeel de algehele beveilingsniveaus van alle leveranciers

10

Training op het gebied van cyberbeveiliging

Geef niet alleen training aan het beheer, maar ook aan werknemers om hun begrip yan cyberbeveiliging te vergroten.

IAM en NIS2

De NIS2 bestaat uit negen hoofdstuken die verder zijin onderverdeeld in 46 artikelen. Onder deze hoodstuken bevindt zich hoofdstuk IV: Matregelen woor het beheer van cyberbevelingsrisico's en rapportageverplichtingen definiëren de cyberbeveiligingsstappen die de essentiële en belangrijke enititliten rmoeten nemen om aan de NIS2 te voldoen: Dit hoofdstuk omvat zes artikelen (artikelen 20 tot en met 25).

In dit hoofdstuk worden de AM-vereisten uitgewerkt die door de NIS2 zijin opgelegd.

Artikel	NIS2 vereiste
Artikel 19 Beoordelingen door colega's zullen	• Beoordelingen door collega's zullen worden uitgevoerd door experts op het gebied ran cyberbeveiliging. • Deze zullen betrekking hebben op verschillende aspecten, waaronder het uitvoeringsniveau van maatregelen op het gebied van cyberbeveliliging en rapportage en regelingen voor de uitwisseling van informatie op het gebied van cyberbeveiliging.
Artikel 20, Governance	• Dit heeft tot doel te garanderen dat de bestuursorganen van essentiële en belangrijke entiteiten de door deze entiteiten geïmplementeerde maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren om te voldoen aan artikel 21, toezicht te houden op de uitvoering ervan en de erantwoordelikheid op zich te nemen voor eventuele inbreuken die door de entiteiten worden gepleegd. • De bestuursorganen moeten er ook voor zorgen dat de bestuursorganen een training op het gebied van Cyberbeveiling volgen en de bedrijven aanmoedigen om al hun werknemers een soortgelijke training aan te bieden.
Artkel 21, Maatregelen voor het beheer van cyberbeveliging-srisico's	• Zorg Jervoor dat er passende maatregelen worden genomen om beveiligingsrisico's te beheersen die van invloed kunnen zijn op netwerken en informatiesystemen en om beveiligingsincidenten te voorkomen of de impact van beveiligingsincidenten te verminderen. • Deze maatregelen moeten het volgende omvatten: ◦ 21.2.b- Afhandeling van incidenten. ◦ 21.2.c-Bedrijfscontinuïteit, zoals back-upbeheer, calamiteiten herstel en crisisbeheersing. ◦ 21.2.i-oegangscontrolebeleid en activabeheer. ◦ 21.2.j- Het gebruik van MFA of continue authenticatieoplossingen waar nodig.
Artikel 22, GecoÖrdineerde veligheidsrisicob eoordelingen op Unieniveau van kritieke toeleverings-ketens	• De samenwerkingsgroep kan, in samenwerking met de Commissieen het Agents chap van de Europese Unie voor cyberbeveliging (ENISA), velligheidsrisicobeoordelingen uitvoeren van bepaalde, kritieke informatie en diensten op het gebied van informatie en communicatietechnologie (ICT), ICT systemen, of toeleveringsketens van ICT-producten. • Bij deze beoordelingen wordt rekening gehouden met 2owel technische als, indien van toepassing, niet-technische risicofactoren.

ManageEngine AD360 biedt de oplossing

ManageEngine AD360 is een AM-oplossing voor ndenemingen die is ontworpen om u te helpen bi het gpheren van dlentitliten et beveligen van tloegang. Met i uigebreid unlils vereenvoudigt AD360 het proces voor naleving van de normen,

Velige toegang tot de informattetechnologlesystemen van de organisatile

(helpt bij artikel 21.2.i)

- Voer eenvoudig op rollen gebaseerde toegangscontrole (RBAC) uit in uw hele organisatie
- Identificeer en controleer periodiek de toegang die gebruikers hebben tot bronnen in uw organisatie met behulp van de 1toegangscertificeringscampagne van AD360.

Implementeer uitgebreid risicobeheer

(helpt bij artikel 21.2.b, artikel 7.1.d, artikel 18.1.a, artikel 22)

- Identificeer, analyseer en evalueer de risicofactoren in uw organisatie met het Identiteit risicobeoordeling rapport.
- Voer herstelmaatregelen uit en bewaak de infrastructur yan uw informatietechnologie nauwlettend om risico-indicatoren te beperken en identificeren.

Ontvang incidentrapporten om de veiligheid van het systeem te beheren

(helpt bij artikel 11.3.b)

- Ontvang realtime e-mailwvaarschuwingen over verdachte activiteiten in uw systemen.
- Bekijk alle potentièle kwetsbaartheden in uw AD-ogeving en beperk ze met brulikbare aanbevelingen.

Behoud het overzicht over al uw digitale activa

(helpt bij artikel 11.3.a)

- Met de intuitieve rapportage en bewakingsmogelikheden van AD360 kunt u inzichten verkriigen en gedetailleerde controlerapporten kriigen over uw AD, Exchange en Microsoft 365 omgevingen.
- Houd al uw bronnen in de gaten vanaf één console.

Implementeer MFA

(helpt bij artikel 21.2.j)

- De adaptieve MFA-functie van AD360, samen met SSO en beleid voor voorwaardeljke toegang, kan u helpen een Zero Trust omgeving in uw organisatie te creëren.
- Beveilig meerdere bronnen en beheer de toegang tot het netwerk zonder concessies te doen aan de gebruikerservaring.

Bijgewerkte back-ups uitvoeren

(helpt bij artikel 9.3, artikel 21.2.c)

- Maak eenvoudig een back-up van uw AD, Azure AD, Microsoft 365, Google Workspace en Exchange omgevingen en herstel deze
- Plan back-ups om er zeker van te zijn dat u een back-up heeft gemaakt van de bijgewerkte versies van uw gegevens.

Zorg vandaag nog voor NIS2-naleving met AD360! Begin uw reis met een gratis proefperiode van 60 dagen van AD360 of een gratis demosessie met één van onze productexperts.

Onze producten

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine
AD360

ManageEngine AD360 is een uniforme oplossing voor identiteits- en toegangsbeheer (IAM) die helpt bij het beheren van identiteiten, het beveiligen van toegang en het waarborgen van naleving. Het wordt geleverd met krachtige mogelijkheden zoals geautomatiseerd beheer van de levenscyclus van identiteiten, toegangscertificering, risicobeoordeling, veilige eenmalige aanmelding, adaptieve MFA, op goedkeuring gebaseerde workflows, UBA gestuurde bescherming tegen identiteitsbedreigingen en historische controlerapporten van AD, Exchange Server en Microsoft 365. De intuïtieve interface en krachtige mogelijkheden van AD360 maken het de ideale oplossing voor uw IAM-behoeften, inclusief het bevorderen van een Zero Trust-omgeving.

Ga voor meer informatie naar www.manageengine.com/nl/active-directory-360/.

$ Offerte aanvragen Downloaden