eshgro

NIS2 Made Simple:

Een Praktisch stappenplan voor de Cyberbeveiligingswet

Inhoudsopgave

In de snel evoluerende digitale wereld is de bescherming van vitale informatiesystemen en digitale diensten van essentieel belang. In dit kader heeft de Europese Unie de NIS2-richtlijn (Network and Information Systems 2) geïntroduceerd als een cruciaal instrument om de veerkracht en beveiliging van de Europese digitale infrastructuur te waarborgen. De NIS2-richtlijn, wordt in Nederland vertaald in de Cyberbeveiligingswet. De Cyberbeveiligingswet vervangt de WBNI (Wet Beveiliging Netwerk en Informatiesystemen) en zal in 2025 in werking treden. Dit markeert een belangrijke mijlpaal in het streven naar een uniform en hoog niveau van cybersecurity binnen Nederland.

Wat is de Cyberbeveiligingswet?

De Cyberbeveiligingswet is de vertaling van de NIS2-richtlijn, formeel bekend als de **Network and Information Security Directive** naar Nederlandse wetgeving. Het is niet zomaar een opvolger van de WBNI, maar een uitgebreidere en strengere versie die bedoeld is om de **weerbaarheid van essentiële diensten in Nederland (en de EU) te versterken.** De wet wordt ontworpen om organisaties te dwingen hun **cybersecurity te verbeteren** en een **bepaald minimumniveau** te garanderen.

Voor wie geldt de nieuwe wetgeving?

De nieuwe Cyberbeveiligingwet is relevant voor een breed scala aan sectoren in Nederland. **Bijna elk midden- en kleinbedrijf (MKB) of grootbedrijf valt eronder**, of ervaart de effecten er van. Alleen die bedrijven die bij een cyberincident geen significante impact hebben op onze maatschappij of economie zijn uitgesloten. Deze richtlijn maakt **onderscheid tussen 'essentiële' en 'belangrijke' organisaties**, gericht op bedrijven en instellingen met een sleutelrol in de samenleving.

Ontdek via onze tool of jouw organisatie onder de Cyberbeveiligingswet valt en of je als belangrijk of essentieel wordt gekenmerkt.

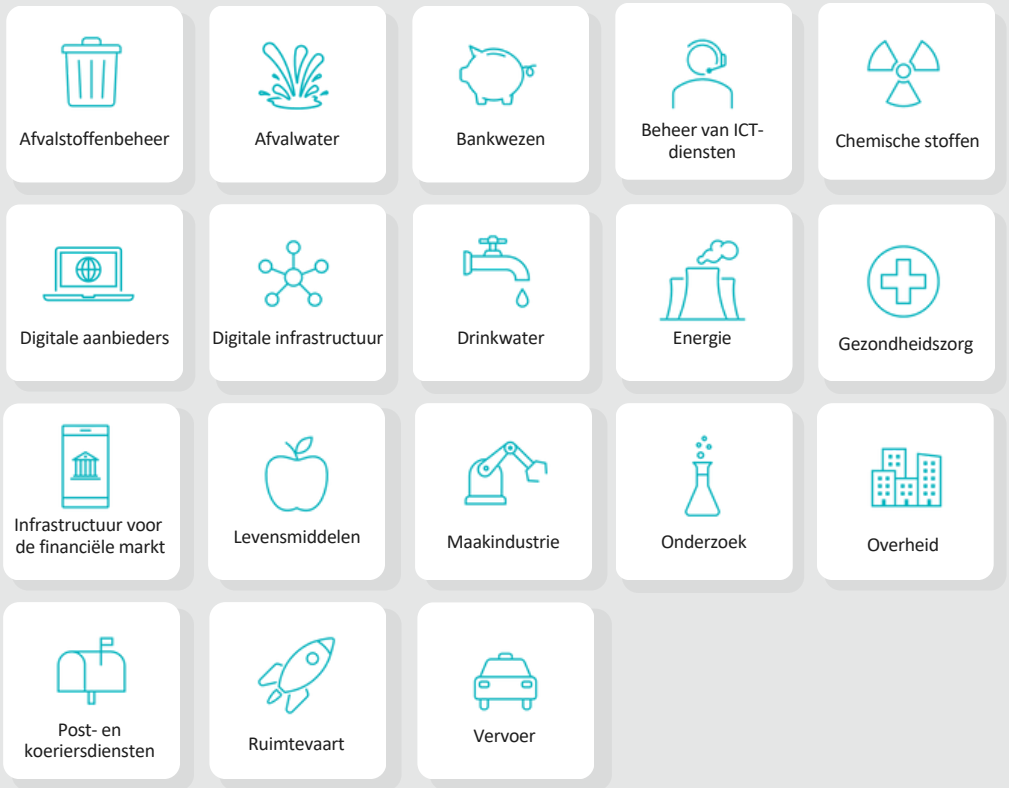
Check nu: Valt jouw organisatie onder Cyberbeveiligingswet?

Organisaties met meer dan **50 FTE** en/of **€10 miljoen** omzet

en

Organisaties die **essentiële diensten** aanbieden

Wat zijn essentiële diensten?



Wat gaat er precies veranderen?

- **Strengere eisen** rondom cybersecurity
- **Toezicht** op naleving van de Cyberbeveiligingswet
- Er komt een **meldplicht** op verstoringen in de digitale dienstverlening, zoals een DDoS-aanval die toegang tot klantaccounts blokkeert
- Er komt een **zorgplicht**: organisaties moeten de nodige beveiligingsmaatregelen treffen voor digitale veiligheid en de continuïteit van de dienstverlening. Dit omvat het beveiligen van netwerk- en informatiesystemen, proactieve monitoring en het verhogen van de bewustwording rondom cybersecurity

Tijdlijn rondom de Cyberbeveiligingswet

Dec 2022
Definitieve versie van de NIS2-richtlijn gepresenteerd

Dec 2022-medio mei 2024
NIS2 Wordt vertaald in Nederlandse wetgeving, de naam van deze wetgeving is bepaald “de Cyberbeveiligingswet”

Mei -juli 2024
Van 21 mei tot en met 1 juli was de internetconsultatie. In deze periode konden burgers, bedrijven en overheidsinstellingen mogelijke verbeteringen aangeven in de wet in voorbereiding

2025
Naar verwachting zal de Cyberbeveiligingswet in 2025 in werking treden, nadat deze door het parlement is behandeld. Organisaties die onder de Cyberbeveiligings-wet vallen moeten vanaf dat moment aan de plichten voldoen.

De vereisten om te voldoen aan de Cyberbeveiligingswet

De inwerkingtreding van de Cyberbeveiligingswet betekent een grote verandering voor je organisatie, vanwege de **omvangrijke hoeveelheid eisen** waaraan voldaan moet worden. Hieronder volgt een overzicht van de belangrijkste eisen:

Regelgeving	Oplossingen
• Respons en ondersteuning bij kwetsbaarheden • Back-up van bedrijfsinformatie en persoonsgegevens • Gebruik van multifactor authenticatie, authenticatie-oplossingen, beveiligde communicatie en encryptie	**Systemen** **SOC/SIEM** **Back-up** **Microsoft E3 + E5 security** **DMARC/DKIM**
Beveiliging bij netwerk- en informatiesystemen • Bekendmaking van kwetsbaarheden • Cyberbeveiligingsrisico's herkennen en • aanpakken	**Hardware** **Netwerk audit** **Vulnerability scanning** **Pentest**
• Toets de weerbaarheid en bewustwording van je organisatie • Beoordeling effectiviteit van (cyber)maatregelen • Opleiding op het gebied van cyberbeveiliging	**Gebruiker** **Attack simulator** **Mystery visit** **Managed awareness training**
• Incidentenregistratie en opvolging • Bedrijfscontinuïteit zoals crisisbeheer • Leveranciersbeoordelingen en beveiliging van de toeleveringsketen	**Compliance** **ISO gap analyse** **ISO security consulting** **Incident respons plan** **Business impact analyse** **Disaster recovery plan**
TIP: Haal onzekerheid weg, check of jouw organisatie volledig voorbereid is op de Cyberbeveiligingswet met onze 'NIS2 readiness check'	**NIS2** **NIS2 readiness check**

eshgro

Jouw routekaart naar compliance aan de cyberbeveiligingswet

In een tijdperk waarin cybersecurity belangrijker is dan ooit, heeft Eshgro zijn beveiligingsbasis aanzienlijk verhoogd. Dit is gedaan niet alleen om onze dienstverlening te optimaliseren, maar ook om te voldoen aan de eisen van de Cyberbeveiligingswet. Uit gesprekken met onze klanten hebben we een routekaart voor compliance aan de Cyberbeveiligingswet opgesteld: van risicoanalyse tot de implementatie van beveiligingsmaatregelen.

Stap 1:

Risicoanalyse

ISO gap analyse
Met een ISO Gap-analyse bepalen we de huidige status van jouw bedrijf en maken we de NIS2-eisen duidelijk door te voldoen aan de normen van ISO27001, 27002 en aanverwant

Business impact analyse
Verduidelijkt de impact van risico's met een lage waarschijnlijkheid maar aanzienlijke gevolgen voor de bedrijfsprocessen, wat belangrijk is voor een effectieve risicoanalyse

Stap 2:

Implementatie van beveiliging

ISO security consulting
Persoonlijke ondersteuning in het nemen van maatregelen om aan de NIS2 te voldoen en het behalen van een eventueel gewenste certificering (ISO27001)

Microsoft E3 + E5 security
Het inrichten van je IT-omgeving conform de hoge beveiligingsstandaard van Microsoft

Back-up
Veiligstellen van bedrijfskritieke informatie om data-integriteit te waarborgen

DMARC/DKIM
Encryptie-oplossingen voor e-mailbeveiliging

Stap 3:

Incident response plan opstellen

Disaster recovery plan
Gedetailleerd plan dat expliciet beschrijft hoe adequaat te reageren op een calamiteit, belangrijk voor een goed incident response plan

Attack simulator en Mystery visit
Deze diensten identificeren phishingrisico's en testen de fysieke IT-beveiligingsbewustzijn van medewerkers, een belangrijk onderdeel van je incident response strategie

Managed awareness training
Driejarig programma met fysieke en digitale trainingen voor bewustwording van medewerkers

Stap 4:

Bewaking, monitoring en evaluatie

SOC/SIEM
Proactieve monitoring van je IT-omgeving om cyberdreigingen vroegtijdig te herkennen

Netwerkaudit & Pentest
Regelmatige controles en gesimuleerde aanvallen om je digitale beveiliging te testen en te verbeteren

Wacht niet, maar start nu al met de voorbereiding op de wet (zie NIS2: Bereid je voor op de Cyberbeveiligingswet | Over het NCSC | Nationaal Cyber Security Centrum)

Benieuwd hoe we jouw organisatie klaarstomen voor de Cyberbeveiligingswet?

Bij Eshgro begrijpen we de essentie van compliance en cybersecurity. Met onze bewezen staat van dienst in het implementeren van beveiligingsoplossingen staat ons team van experts klaar om jouw organisatie te begeleiden bij de overgang naar de Cyberbeveiligingswet.

Neem vandaag nog contact op met onze dichtstbijzijnde IT-specialist voor een vrijblijvend gesprek. Ontdek samen hoe Eshgro jouw organisatie kan ondersteunen bij het voldoen aan de Nederlandse NIS2 wetgeving en het versterken van jouw cybersecurity.

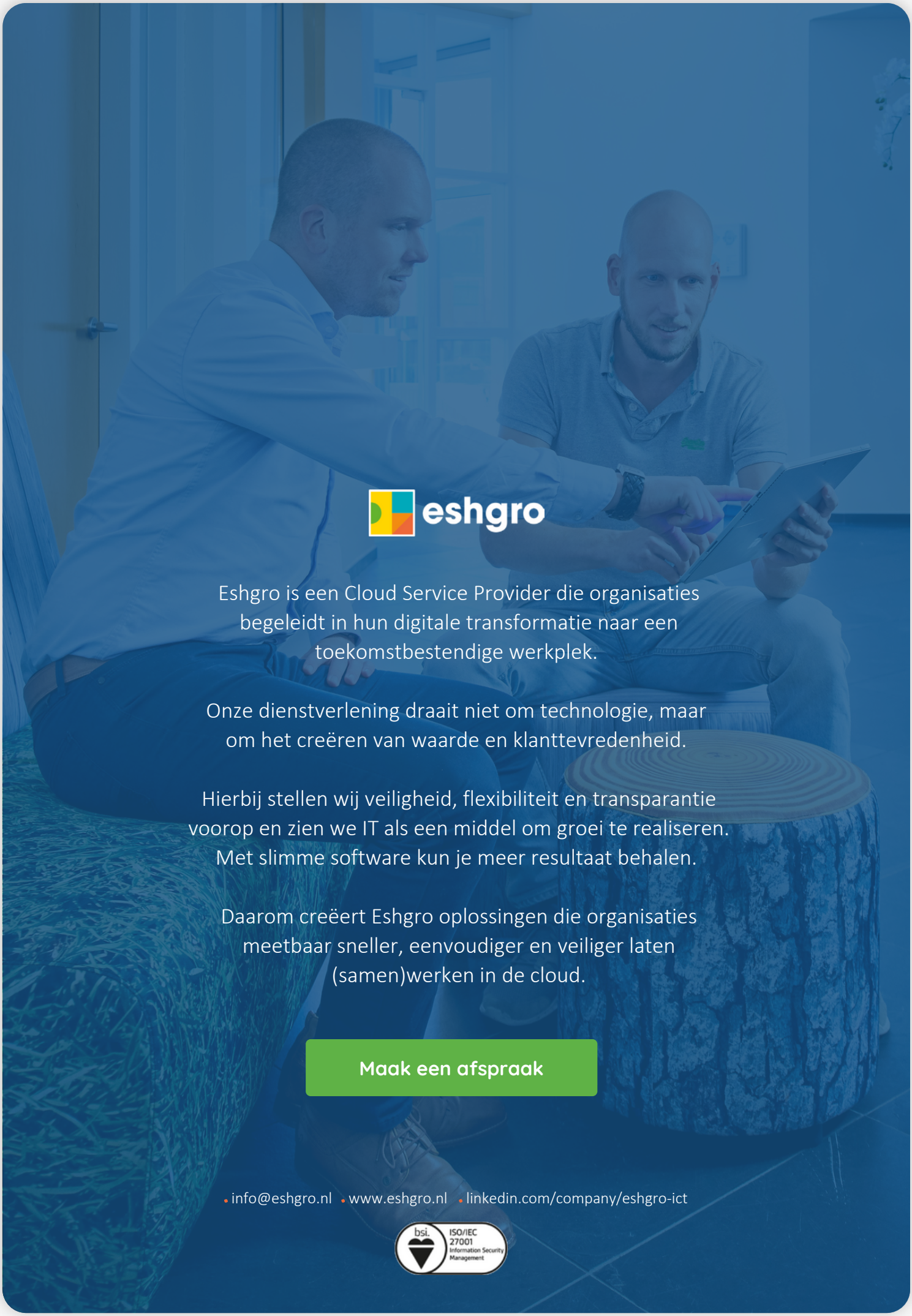
Manfred Pallencaöe
IT-specialist Almere
m.pallencaoe@eshgro.nl
06 29 54 72 47

Menker Johannes
IT-specialist Apeldoorn
m.johannes@eshgro.nl
06 53 20 52 12

Bram van Eck
IT-specialist Arnhem
b.vaneck@eshgro.nl
06 81 38 29 63

Luc Meijs
IT-specialist Boxmeer
l.meijs@eshgro.nl
06 83 44 38 24

Monique Bisschops
IT-specialist Weert
m.bisschops@eshgro.nl
06 12 15 34 85



eshgro

Eshgro is een Cloud Service Provider die organisaties begeleidt in hun digitale transformatie naar een toekomstbestendige werkplek.

Onze dienstverlening draait niet om technologie, maar om het creëren van waarde en klanttevredenheid.

Hierbij stellen wij veiligheid, flexibiliteit en transparantie voorop en zien we IT als een middel om groei te realiseren. Met slimme software kun je meer resultaat behalen.

Daarom creëert Eshgro oplossingen die organisaties meetbaar sneller, eenvoudiger en veiliger laten (samen)werken in de cloud.

Maak een afspraak

• info@eshgro.nl • www.eshgro.nl • linkedin.com/company/eshgro-ict

bsi. ISO/IEC 27001 Information Security Management