easy secure

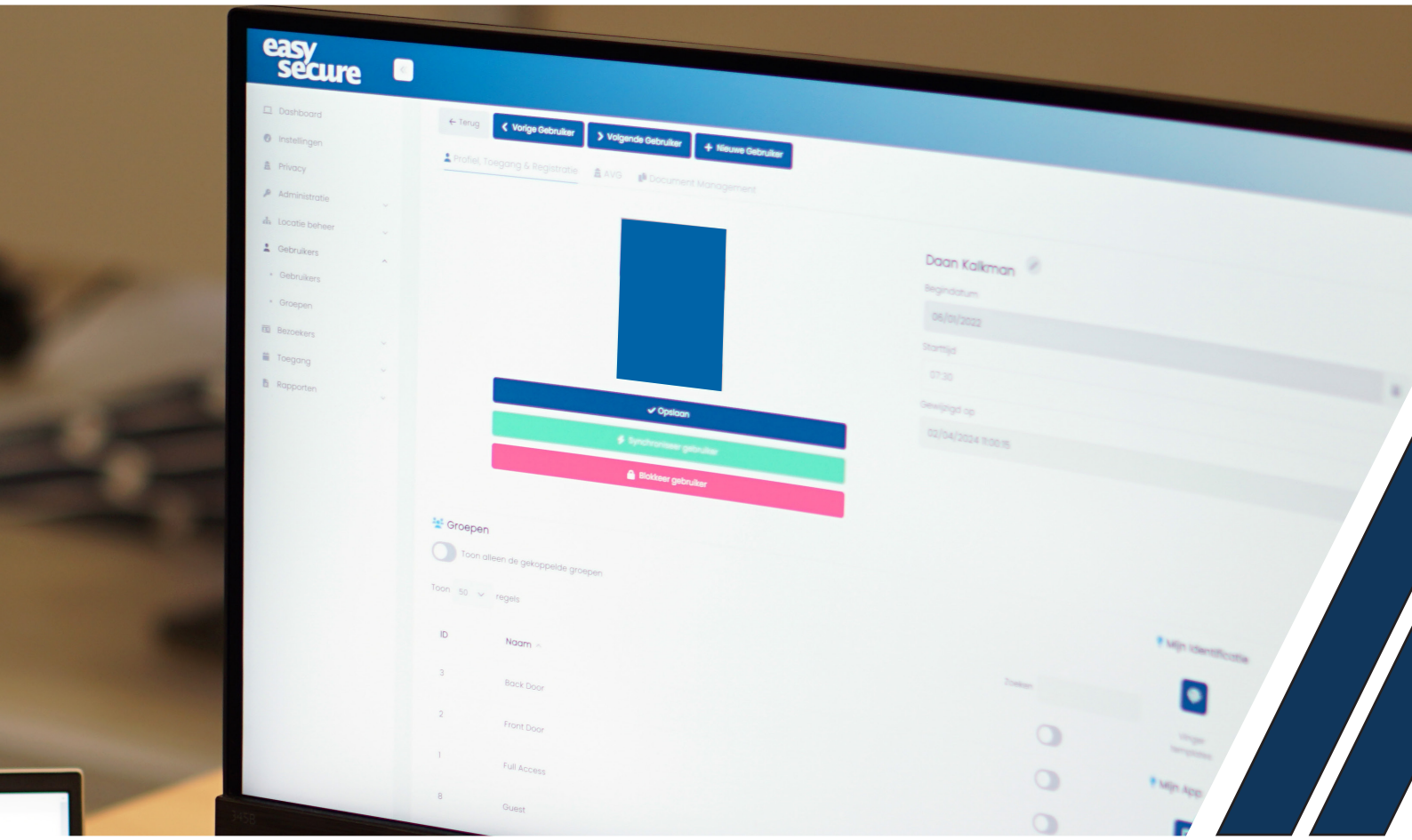
ACCESS CONTROL
TIME REGISTRATION
ATTENDANCE
PROJECT REGISTRATION
VISITOR MANAGEMENT

LESS COST ◐ MORE CONTROL

Nieuwe Europese wet- en regelgeving: NIS2 / NIB2

Dit is wat u kunt verwachten.

Met EasySecure bent u optimaal voorbereid!



De nieuwe wet NIS2 komt eraan. Weet u wat u te wachten staat?

In 2025 gaat er een nieuwe Europese wet van kracht. De NIS2 (Network and Information Security Directive)-wet wordt in Nederland bekend als NIB2 en is gebaseerd op de Europese NIS2-richtlijn. Wat houdt deze wet in? En voor wie is deze wet toepasbaar? We vertellen je het in dit document!

De NIS2 (Network and Information Security Directive) is een Europese wet die de beveiliging van digitale netwerken en informatiesystemen reguleert.

De nieuwe wet is bedoeld om de beveiliging van digitale netwerken en informatiesystemen op orde te hebben om cybercrime tegen te gaan. Dit geldt voor bepaalde organisaties, maar ook voor hun toeleveranciers. In 2018 werd de voorloper, - *de NIS1-richtlijn* - geïntroduceerd in Europa. Deze wet was vooral van toepassing op digitale dienstverleners en op vitale aanbieders in belangrijke sectoren. De nieuwe NIS2-richtlijn voegt hier een aantal sectoren aan toe.

De NIS2 wetgeving verplicht alle essentiële en belangrijke organisaties en toeleveranciers in de volgende sectoren om de richtlijnen te volgen:

Sectoren die onder NIS2 vallen:

Essentiële sectoren:

- Energie
- Transport
- Bankwezen
- Infrastructuur financiële markt
- Gezondheidszorg
- Drinkwater
- Digitale infrastructuur
- Beheerders van ICT-diensten
- Afvalwater
- Overheidsdiensten
- Lokale overheden
- Ruimtevaart

Belangrijke sectoren:

- Digitale aanbieders
- Post- en koeriersdiensten
- Afvalstoffenbeheer
- Levensmiddelen
- Chemische stoffen
- Onderzoek
- Vervaardiging / Manufacturing

Grote organisaties die actief zijn in de essentiële sectoren van de **Cyberbeveiligingswet** worden als **essentiële organisaties** gezien. Een organisatie wordt als **groot** beschouwd als deze minimaal 250 werknemers heeft of een jaaromzet van meer dan €50 miljoen en een balanstotaal van meer dan €43 miljoen.

Middelgrote organisaties hebben minimaal 50 werknemers of een jaaromzet en balanstotaal van meer dan €10 miljoen. Middelgrote organisaties in de essentiële sectoren worden gezien als **belangrijke organisaties**.

Verplichtingen van de NIS2

Zorgplicht: U bent zelf verantwoordelijk voor het inschatten van de risico's in de diensten die u levert en dient passende maatregelen te nemen om deze te correct te beveiligen. Een voorbeeld hiervan is loggen van toegang of het monitoren van netwerkactiviteiten binnen uw netwerk of systemen.

Meldplicht na een incident

U bent verplicht om dit te melden volgens onderstaand protocol:

U bent verplicht om binnen 24 uur, 72 uur en 1 maand meldingen te maken bij de officiële instanties in het geval van een cyberincident.

Voldoen aan de wet- en regelgeving:

Alle organisaties uit de eerder genoemde essentiële en belangrijke sectoren moeten voldoen aan de NIS2 regelgeving. Wanneer een organisatie niet voldoet aan de eisen kan de organisatie te maken krijgen met hoge boetes. (2% van de wereldwijde jaaromzet of maximaal 10 miljoen euro).

- **Beveilingsbeleid:** Iedere organisatie dient een beveiligingsbeleid te implementeren om informatie veilig te houden en informatie te beschermen voor ongeautoriseerden.
- **Periodieke uitvoer van risicoanalyses & de controle:** Organisaties dienen periodiek te inventariseren welke risico's en bedreigingen er zijn en actief maatregelen nemen om deze risico's te verkleinen.
- **Incident Response Planning:** Komt er een indicent voor? Dan dienen er plannen klaar te liggen die gedetailleerd beschrijven welke stappen er genomen moeten worden.
- **Business Continuity & Crisisbeheer:** Organisaties dienen plannen te hebben welke stappen zij mogelijk dienen te ondernemen om ervoor te zorgen dat de continuïteit van het bedrijf wordt gewaarborgd en hoe ze mogelijke schade dienen te herstellen.
- **Leveranciers-ketenbeheer:** Organisaties in de betrokken sectoren dienen ervoor te zorgen dat leveranciers aan dezelfde eisen voldoen om beveiligd te zijn.
- **Versleuteling:** Data dient versleuteld te worden verzonden of versleuteld opgeslagen te zijn, zodat er in het geval van een cyberaanval geen vertrouwelijke data wordt ontvreemd.
- **Delen van kwetsbaarheden:** De Europese Unie zet in op een generieke samenwerking in de IT-wereld en het delen van informatie over cyberaanvallen om toekomstige aanvallen te voorkomen.

Waarom EasySecure?

Binnen EasySecure hebben wij veiligheid en privacy zeer hoog in het vaandel staan. Wij kiezen dan ook voor de beste beveiliging en werken samen met de beste hosting partijen, met een eigen Europees datacenter. Onze cloud software wordt maandelijks gecontroleerd, getest en geüpdatet om onze hoge kwaliteitsnorm te waarborgen.

EasySecure is **ISO-27001 gecertificeerd** en onze bedrijfsvoering is gebaseerd op de richtlijn NIS2. Wij richting ons op constante verbetering van onze veiligheidsmaatregelen en leggen dit ook vast in overeenkomsten met onze leveranciers, samenwerking- en ketenpartners. Hierdoor zorgen wij dat de EasySecure Software en bijbehorende dienstverlening compliant is met de NIS2-richtlijn.

In de komende periode wordt deze wet- en regelgeving verder uitgewerkt en Europees geïmplementeerd. De komende jaren zal de richtlijn zich verder door ontwikkelen en voeren wij direct door in onze bedrijfsvoering.

Vragen?

Heeft u vragen over de NIS2-richtlijn? Wij helpen u graag op weg en staan voor u klaar om u van informatie te voorzien. Neem contact met ons op voor een vrijblijvend kennismakingsgesprek, zodat we u zo goed mogelijk kunnen adviseren.

EasySecure International
+31(0)85 01500 00

info@easysecure.com
www.easysecure.com