

Cyberbeveiligingswet: bent u voorbereid op de nieuwe verplichtingen?

Nieuwe wet, nieuwe verantwoordelijkheden

Vanaf 15 augustus 2026 treedt de Cyberbeveiligingswet (Cbw), de Nederlandse uitwerking van de Europese NIS2-richtlijn in werking. Organisaties die onder de wet vallen, moeten aantoonbaar werken aan hun cyberweerbaarheid. De wet vraagt niet dat alle maatregelen op deze datum volledig zijn afgerond. Wel moeten organisaties inzicht hebben in hun belangrijkste cyberrisico's, verantwoordelijkheden hebben belegd en kunnen aantonen dat zij stappen zetten om hun digitale weerbaarheid te versterken. De kern van de Cyberbeveiligingswet is aantoonbaarheid.

Wat verwacht de Cyberbeveiligingswet van uw organisatie?

De wet stelt eisen op vier onderdelen.

1. Registratie

De eerste stap is vaststellen dat de organisatie onder de Cyberbeveiligingswet valt en dit vervolgens registreren. Het is het moment waarop de organisatie expliciet erkent dat zij binnen de reikwijdte van de wet valt en daarmee verantwoordelijkheden heeft op het gebied van cyberweerbaarheid.

2. Meldproces

Organisaties moeten beschikken over een duidelijk proces voor het melden van significante cyberincidenten. Belangrijk is dat duidelijk is wanneer een incident meldingsplichtig is, wie verantwoordelijk is voor de beoordeling en welke stappen moeten worden genomen.

3. Bestuurlijke verantwoordelijkheid

De Cyberbeveiligingswet maakt bestuurders expliciet verantwoordelijk voor de cyberweerbaarheid van hun organisatie. Bestuurders moeten aantoonbaar op de hoogte zijn van de belangrijkste cyberrisico's, keuzes maken over maatregelen en toezicht houden op de voortgang. Deze verantwoordelijkheid moet ook aantoonbaar zijn vastgelegd.

4. Risicobeheersing

Organisaties dienen aantoonbaar bezig te zijn met passende maatregelen om cyber-risico's te beheersen. Op 15 augustus hoeft niet alles volledig ingericht te zijn, maar organisaties moeten wel kunnen aantonen dat zij risico's in kaart hebben gebracht en werken aan verdere verbetering.





Kunt u dit vandaag aantonen?

Veel organisaties beschikken al over onderdelen die bijdragen aan naleving van de Cyberbeveiligingswet, zoals beveiligingsmaatregelen, risicoanalyses of incidentprocedures. De uitdaging zit vaak in het aantoonbaar maken dat deze onderdelen samenkomen en bestuurlijk zijn geborgd.

Een goede basis bestaat uit:

- ▶ Een actueel beeld van cyberrisico's
- ▶ Duidelijke verantwoordelijkheden
- ▶ Een ingericht incidentproces
- ▶ Vastlegging van bestuurlijke betrokkenheid
- ▶ Een plan voor verdere verbetering

Van wetgeving naar weerbaarheid

De Cyberbeveiligingswet vraagt niet dat alle maatregelen op 15 augustus 2026 volledig zijn geïmplementeerd. Wel moeten organisaties kunnen aantonen dat zij hun risico's kennen, verantwoordelijkheden hebben belegd en actief werken aan het versterken van hun cyberweerbaarheid. Zo werkt u niet alleen toe naar naleving van de Cyberbeveiligingswet, maar ook aan een structureel weerbare organisatie.

HOE HELPT BDO?

BDO helpt organisaties bij het vertalen van de Cyberbeveiligingswet naar concrete acties. Van het bepalen van de impact en het uitvoeren van een nulmeting tot het versterken van governance, risicobeheersing en processen rondom cyberweerbaarheid.



Robert van Vianen

Partner BDO Digital
E robert.van.vianen@bdo.nl
T +31 (0)6 30 07 99 09



Marijke Stokkel

Senior Manager, BDO Risk Advisory
E marijke.stokkel@bdo.nl
T +31 (0)6 22 95 70 80

Vond u dit interessant? Ontvang - net als 14.000 andere abonnees - het laatste nieuws over bijvoorbeeld actuele publicaties en onderzoeken, fiscale regelgeving en wetwijzigingen tweewekelijks in uw mailbox! Meld u aan via: bdo.nl/nieuwsbrief

Deze publicatie is zorgvuldig voorbereid en tot stand gekomen, maar is in algemene bewoordingen gesteld en bevat alleen informatie van algemene aard. Deze publicatie bevat geen advies voor concrete situaties, zodat uitdrukkelijk wordt afgeraden om zonder advies van een deskundige op basis van de informatie in deze publicatie te handelen, na te laten of besluiten te nemen. Voor het verkrijgen van een advies dat is toegesneden op uw concrete situatie, kunt u zich wenden tot BDO Advisory B.V. of een van haar adviseurs. BDO Advisory B.V., de met haar gelieerde partijen en haar adviseurs aanvaarden geen aansprakelijkheid voor schade die het gevolg is van handelen, nalaten of het nemen van besluiten op basis van de informatie in deze publicatie.

BDO is een op naam van Stichting BDO te Amsterdam geregistreerd merk.

In deze publicatie wordt 'BDO' gebruikt ter aanduiding van de organisatie die onder de merknaam 'BDO' actief is op het gebied van de professionele dienstverlening (accountancy, belastingadvies en advisory).

BDO Advisory B.V. handelt tevens onder de namen: BDO Advisory, BDO Risk Advisory Services, BDO Familiebeprijven, BDO Business Restructuring Services, BDO Adviesgroep Familiebeprijven, BDO Digital, BDO IT Risk Services, BDO Executive Search & Interim.

BDO Advisory B.V. is lid van BDO International Ltd, een rechtspersoon naar Engels recht met beperkte aansprakelijkheid, en maakt deel uit van het wereldwijde netwerk van juridisch zelfstandige organisaties die onder de naam 'BDO' optreden.

BDO is de merknaam die wordt gebruikt ter aanduiding van het BDO-netwerk en van elk van de BDO Member Firms.