Cyberbeveiligingswet (NIS2)

Van verplichting naar aantoonbare grip

Praktische gids

De Cyberbeveiligingswet komt eraan. Voor veel organisaties voelt dat als een compliancevraagstuk. In de praktijk raakt deze wet echter de kern van je onderneming. Het gaat over continuïteit, risico's en bestuurlijke verantwoordelijkheid. De essentie is eenvoudig. Je moet als organisatie kunnen uitleggen welke risico's je loopt, welke maatregelen je hebt genomen en waarom die passend zijn. En als het nodig is, moet je dat ook kunnen bewijzen.

Deze gids helpt je om dat scherp te krijgen en om gestructureerd in beweging te komen.

De Cyberbeveiligingswet vraagt daarbij niet om perfectie, maar wel om structuur, onderbouwing en bestuurlijke betrokkenheid. In de volgende hoofdstukken werken de dit uit langs tien thema's. Niet als losse onderdelen, maar als samenhangend geheel dat bepaalt of je organisatie daadwerkelijk in control is. Per thema maken we duidelijk wat de wet van je vraagt, waar het in de praktijk misgaat en wat je vandaag al kunt doen om stappen te zetten.

Niels van den Bogaard,
NIS2 advocaat

1. Val je onder de Cyberbeveiligings-wet?

Val je onder de Cyberbeveiligingswet?

Voor veel bestuurders is dit de eerste en meest bepalende vraag. De wet is van toepassing op organisaties die actief zijn in specifieke sectoren zoals energie, vervoer, levensmiddelen, productie, chemische stoffen, bankwezen, gezondheidszorg en digitale diensten. Denk daarbij ook aan cloudproviders, datacenters en online platforms.

De kwalificatie bestaat uit twee stappen:
Eerst bepaal je of je kernactiviteiten onder een (sub)sector uit bijlage 1 of 2 van de CBW vallen. Daarna kijk je of je de drempel voor middelgrote ondernemingen overschrijdt.

Voldoe je aan beide, dan geldt:
- Bijlage 1: essentiële entiteit
- Bijlage 2: belangrijke entiteit

In de praktijk ontstaat hier vaak onduidelijkheid. Zeker bij organisaties met meerdere activiteiten of een groepsstructuur is het niet altijd direct helder hoe de indeling uitpakt. De wet vraagt daarom niet alleen om een conclusie, maar vooral om een onderbouwing.

Wat je moet kunnen laten zien:
- Breng per groepsmaatschappij de sector, kernactiviteiten, omzet/balans en FTE’s in kaart.
- Zoek uit waarom een entiteit wél of niet als essentiële of belangrijke entiteit kwalificeert inclusies aannames.

Dit leg je vast in een kort en scherp scope-document. Dat document vormt de basis voor gesprekken met toezichthouders, verzekeraars en klanten.

De kernvraag is simpel: kun je dit helder vastleggen, ook als je er kritisch op wordt bevraagd?

2. Zorgplicht en risicoanalyse

Zorgplicht en risicoanalyse

De zorgplicht is het fundament van de Cyberbeveiligingswet. Organisaties moeten passende en evenredige maatregelen nemen om risico's voor hun netwerk- en informatiesystemen te beheersen, incidenten te voorkomen en de impact te beperken.

Dat betekent dat standaardoplossingen niet volstaan. Wat passend is, verschilt per organisatie. Juist daarom moet je kunnen onderbouwen waarom jouw maatregelen logisch en evenredig zijn.

De wet gaat uit van een risicogebaseerde aanpak. Een losse lijst met risico's of een eenmalige audit is niet voldoende. Het gaat om een structureel proces waarin risico's worden geïdentificeerd, beoordeeld en opgevolgd.

Minimaal moet je kunnen aantonen:
- Een vastgelegde **risicomethodiek**, inclusief criteria voor impact en de kwalificatie 'kritiek'
- Een **risk management policy** die beschrijft hoe je risico's identificeert en opvolgt
- Een actueel **risicoregister** met eigenaars, maatregelen en rest-risico's

In de praktijk helpt het om IT en business samen te brengen:
- Stel gezamenlijk een top-10 cyberrisico's op
- Koppel per risico concrete maatregelen en eigenaarschap
- Laat het bestuur expliciet rest-risico's accepteren en leg dit vast

Het draait uiteindelijk om overzicht en keuzes. Kun je die keuzes compact en helder toelichten, dan zit je goed.

3. Mens, toegang en assets

Mens, toegang en assets

Veel incidenten beginnen niet met geavanceerde kwetsbaarheden, maar bij de basis. Mensen, toegangsrechten en het ontbreken van overzicht vormen in de praktijk de grootste kwetsbaarheden.

De Cyberbeveiligingswet verplicht daarom expliciet aandacht voor **personeelsprocessen**, **toegangsbeheer** en **asset management**. Dit betekent dat je moet weten wie toegang heet tot welke systemen, op basis waarvan die toegang is verleend en welke systemen en apparaten onderdeel zijn van je dienstverlening.

Minimaal vereist zijn:
- Securityprocedures voor in-, door- en uitstroom van personeel. Wat gebeurt er met accounts en autorisaties als iemand in dienst komt, van rol verandert of uit dienst gaat?
- Een formeel access control beleid, waarin rollen, rechten en besluitvorming zijn vastgelegd.
- Een actueel asset register van systemen, applicaties en devices.

Om dit werkbaar te maken:
- Laat HR en IT samen een checklist maken voor in- en uitdiensttreding (accounts, rechten, apparatuur, NDA'S.
- Voer periodieke controles uit op accounts, inclusief admin- en gedeelde accounts.
- Maak managers verantwoordelijk voor het actueel houden van rechten.

Juist hier zit de sleutel tot verbetering. Door processen te koppelen en verantwoordelijkheid expliciet te maken, ontstaat controle.

4. Business continuity & Business Impact Analysis

Business continuity & Business Impact Analysis

De Cyberbeveiligingswet richt zich niet alleen op het voorkomen van incidenten, maar ook op het beperken van de impact ervan. Organisaties moeten maatregelen nemen om ervoor te zorgen dat hun dienstverlening niet langdurig stilvalt.

Daarom zijn een **Business Impact Analysis (BIA)** en een **Business Continuity Plan (BCP)** essentieel. In de impactanalyse bepaal je welke processen kritiek zijn, hoeveel uitval acceptabel is en van welke systemen, leveranciers en locaties je afhankelijk ben. Deze afspraken moeten bovendien terugkomen in contracten met IT-leveranciers. Het continuity plan beschrijft vervolgens hoe je omgaat met verstoringen zoals cyberincidenten, uitval van een datacenter of een langdurige stroomstoring.

Het verschil wordt gemaakt in de voorbereiding. Door scenario's, zoals ransomware of uitval van kernapplicaties, te oefenen met directie en leveranciers wordt zichtbaar waar de zwakke plekken zitten.

Belangrijk is dat deze plannen niet alleen op papier bestaan. Ze moeten aansluiten op de werkelijkheid van je organisatie. Dat betekent dat je jaarlijks rekening houdt met veranderingen zoals nieuwe systemen, fusies of internationale afhankelijkheden.

5. Incident response en meldplicht

Incident response en meldplicht

Wanneer zich een incident voordoet, is snelheid bepalend. De Cyberbeveiligingswet verplicht organisaties om significante incidenten te melden. Dat zijn incidenten die leiden tot ernstige verstoringen of aanzienlijke schade, of dat kunnen veroorzaken.

De termijnen zijn scherp. Binnen 24 uur moet een eerste melding worden gedaan. Binnen 72 uur volgt een nadere beoordeling en binnen één maand een eindverslag.

Dit betekent dat je organisatie voorbereid moet zijn. Niet alleen technisch, maar vooral organisatorisch. Er moet een duidelijk Incident Response Plan (IRP) zijn, met duidelijke stappen voor detectie, respons en herstel.

Zorg dat je beschikt over:
- Draaiboeken voor specifieke scenario's zoals ransomware, incidenten bij leveranciers en identity compromise.
- Een gestructureerd incidentdossier, waarin onder andere een tijdlijn, impactanalyse en te nemen maatregelen worden vastgelegd.

In de praktijk zit de grootste uitdaging vaak in besluitvorming onder druk. Wie mag beslissen over het stilleggen van systemen? Wie bepaalt of er wordt betaald bij ransomware? Wie verzorgt de communicatie?

Dit kun je nu al voorbereiden:
- Leg vast wie waarover beslist
- Organiseer een tableton-oefening met MT, CISO, CFO en Communicatie
- Borg in contracten dat leveranciers snel informatie aanleveren, zodat jij je meldtermijnen haalt

6. Basishygiëne cyberweerbaarheid en training

Basishygiëne cyberweerbaarheid en training

De Cyberbeveiligingswet vraagt om maatregelen die aansluiten bij de stand van de techniek en de risico's van de organisatie. Dat begint bij de basishygiëne, maar stopt daar niet.

Technische maatregelen zoals multi-factor authenticatie, actuele beveiligingssoftware, back-ups en logging vormen de basis. Zonder deze maatregelen is het vrijwel onmogelijk om risico's effectief te beheersen.

Minstens zo belangrijk is het gedrag van mensen. Medewerkers moeten zich bewust zijn van risico's en weten hoe ze moeten handelen. Daarom is een structureel **awarenessprogramma** noodzakelijk, met aandacht voor onboarding, periodieke training en bijvoorbeeld phising-simulaties.

De wet gaat nog een stap verder door te eisen dat ook **bestuurders** beschikken over voldoende kennis en vaardigheden om cyberrisico's te begrijpen en te beoordelen. Dit moet aantoonbaar zijn, bijvoorbeeld door middel van **training en certificering**.

In de praktijk werkt dit alleen als het onderdeel wordt van de organisatiecultuur. Door training structureel te maken en te koppelen aan doelstellingen en prestaties ontstaat blijvende aandacht.

7. Veilige ontwikkeling, beheer en inkoop

Veilige ontwikkeling, beheer en inkoop

De Cyberbeveiligingswet verlangt dat beveiliging wordt geïntegreerd in de volledige lifecycle van systemen. Dat betekent dat security geen sluitpost is, maar een uitgangspunt bij ontwikkeling, beheer en inkoop.

Dit vraagt om beleid en processen op verschillende vlakken. Denk aan configuratiebeheer, wijzigingsbeheer, patchmanagement en kwetsbaarhedenmanagement. Daarnaast moet er aandacht zijn voor veilige ontwikkelprocessen, zoals code reviews en testomgevingen.

Een belangrijk onderdeel is de rol van leveranciers. Inkoopbeslissingen bepalen in grote mate het risicoprofiel van de organisatie. Daarom moeten security-eisen expliciet worden opgenomen in contracten met IT-dienstverleners, inclusief afspraken over updates, ondersteuning en verantwoordelijkheden.

Concreet betekent dit:

- Nieuwe systemen en wijzigingen moeten vooraf beoordeeld worden op security
- Borg in RFP's en contracten dat leveranciers verplicht zijn tijdig security-updates te leveren en kwetsbaarheden te melden
- Evalueer regelmatig of bestaande systemen nog passen binnen een acceptabel risicoprofiel

Zorg dus dat security een vast onderdeel is van besluitvorming. En dat het niet pas wordt meegenomen als er al een probleem is.

8. Supply chain security

Supply chain security

De Cyberbeveiligingswet benadrukt dat organisaties verantwoordelijk blijven voor hun keten. Een incident bij een leverancier kan direct leiden tot problemen binnen de eigen organisatie.

Daarom is het noodzakelijk om leveranciersrisico's structureel te beheersen via een supply chain policy plan. Dat begint bij selectie. Security moet een expliciet criterium zijn bij het kiezen van leveranciers. Daarnaast moet je inzicht hebben in afhankelijkheden. Welke leveranciers zijn kritisch voor je dienstverlening? Waar zitten de zwakke schakels? Vervolgens leg je contractueel vast hoe wordt omgegaan met incidenten, meldingen en ondersteuning.

Dit komt neer op het volgende:
Identificeer kritieke leveranciers en controleer of je contracten dit daadwerkelijk borgen:

- Incidenten worden direct gemeld, in uren en niet pas na dagen
- Leveranciers leveren snel de juiste informatie aan, zodat jij aan je meldplicht kunt voldoen (zoals onder NIS2 en AVG)
- Logging en forensisch onderzoek zijn geregeld en direct inzetbaar
- Duidelijke afspraken over updates en patches, inclusief hoe wordt omgegaan met uitzonderingen
- Transparantie over subleveranciers en heldere afspraken over vervanging of beëindiging van de samenwerking

Ga na of je voldoende grip hebt op de risico's in je keten en of je daar ook op kunt sturen.

9. Cryptografie, MFA en veilige communicatie

Cryptografie, MFA en veilige communicatie

Om te voldoen aan de Cyberbeveiligingswet moeten systemen en data worden beschermd op een niveau dat past bij de risico's. Dat vertaalt zich in concrete maatregelen rondom toegang en communicatie.

Encryptie speelt daarbij een belangrijke rol. Organisaties moeten vastleggen wanneer data wordt versleuteld en hoe cryptografische sleutels worden beheerd.

Daarnaast is het verplicht om multi-factor authenticatie (MFA) toe te passen voor kritieke toegang, zoals beheerdersaccounts en externe toegang.

Ook communicatie moet veilig worden ingericht. Dit geldt niet voor reguliere communicatie, maar juist ook voor situaties waarin systemen uitvallen. Alternatieven voor beveiligde communicatiekanalen zijn dan essentieel.

Hier kun je in de praktijk op letten:

- Stel als bestuur één heldere norm: geen beheer- of externe toegang zonder MFA
- Laat security en IT samen bepalen welke data en systemen verplicht versleuteld moeten worden (bijv. back-ups, laptops, gevoelige klant- en productiegegevens)
- Test periodiek of alternatieve communicatiekanalen werken bij een grote verstoring

De vraag die centraal staat is of je kunt uitsluiten dat er nog onbeveiligde toegang bestaat tot kritieke systemen.

10. Boetes en bestuurlijke aansprakelijkheid

Boetes en bestuurlijke aansprakelijkheid

Het is niet voldoende om alleen maatregelen op papier te hebben staan. Je moet ook kunnen laten zien dat ze werken.

Toezichthouders krijgen vergaande bevoegdheden, waaronder het uitvoeren van audits en beveiligingsscans. Bij ernstige tekortkomingen kunnen ze boetes opleggen die kunnen oplopen tot 10 miljoen euro of 2% van de wereldwijde jaaromzet voor essentiële entiteiten, en 7 miljoen of 1,4% voor belangrijke entiteiten. Tevens ben je als bestuurder persoonlijk aansprakelijk voor verwijtbare tekortkomingen.

Daarom moet je beschikken over een actueel en samenhangend CBW-dossier waarin je vastlegt wat je hebt gedaan, waarom en met welk resultaat. Dit dossier bevat onder andere de scope van je verplichtingen, risicoanalyses, maatregelen, incidenten en besluiten.

Daarnaast zijn periodieke audits en tests noodzakelijk om de effectiviteit van maatregelen te beoordelen. Denk aan controles op toegang, patching, back-ups en incidentrespons.

Praktisch helpt het om structuur aan te brengen:

- Verzamel per periode bewijs, zoals rapportages, testresultaten, auditbevindingen en actielijsten.
- Koppel bevindingen aan acties en eigenaars
- Hergebruik dit dossier voor klantassessments, verzekeraars en M&A-due diligence.

Vraag jezelf dus af of je in staat bent om op korte termijn overtuigend te laten zien dat je organisatie in control is.

Aan de slag in 30 dagen

Om van inzicht naar actie te komen, helpt een gestructureerde aanpak. In de eerste week ligt de focus op het bepalen van de scope en het in kaart brengen van de belangrijkste risico’s. Vervolgens richt je de organisatie in, met duidelijk eigenaarschap en een eerste structuur voor risicomanagement en incident response. Daarna verschuift de aandacht naar de basismaatregelen, zoals toegangsbeheer en leveranciersrisico’s, en wordt gewerkt aan inzicht in continuïteit. In de laatste fase ligt de nadruk op documentatie, bewijs en het prioriteren van verbeteracties.

Deze aanpak zorgt ervoor dat je niet blijft hangen in analyse, maar daadwerkelijk stappen zet richting aantoonbare grip.

Conclusie

De Cyberbeveiligingswet vraagt niet om perfectie, maar om controle en onderbouwing. Organisaties die dit goed inrichten, voldoen niet alleen aan de wet, maar versterken hun weerbaarheid, besluitvorming en concurrentiepositie.

De kern is dat je kunt uitleggen wat je doet, waarom je dat doet en dat je kunt laten zien dat het werkt. Dat is waar het verschil wordt gemaakt.