OT en Cybersecurity wetgeving

www.ipcs.nl

IPCS
INDUSTRIEEL
PLATFORM
CYBER SECURITY

1. Inleiding

1.1. Doel van deze publicatie

Met deze publicatie beoogt het Industrieel Platform Cyber Security inzicht te geven in de regelgeving die door de Europese Unie is en wordt opgesteld met als doel de weerbaarheid van Europa te vergroten. We plaatsen deze regelgeving in de context van de wereld van de Operationele Technologie (OT) en proberen antwoorden te geven op de vraag in hoeverre je als bedrijf last of gemak hebt van deze regels.

Deze publicatie is bedoeld voor het midden- en kleinbedrijf om inzichtelijk te maken waar men mee te maken gaat krijgen en hoe daarmee om te gaan.

1.2. Opbouw van dit document

Omdat in veel van de cybersecurity regelgeving sprake is van risicoanalyses gaat hoofdstuk 2daar wat verder op in. Vervolgens wordt in hoofdstuk 3 de Europese regelgeving die de laatste jaren verschenen is beschreven terwijl hoofdstuk 5 aandacht geeft aan de daaruit voorvloeiende Nederlandse wet- en regelgeving. Omdat ook de regels rond het aanbrengen van een CE-markering op producten zijn gewijzigd ten gevolge van het verbeteren van de weerbaarheid tegen cybersecurity risico's gaat hoofdstuk 4 daar kort op in.

In hoofdstuk 6 geven we een idee wat al deze regels en richtlijnen gaan betekenen voor de dagelijkse bedrijfsvoering van een bedrijf in de sector MKB en in hoofdstuk 7 trekken we nog een conclusie.

2. Risicoanalyses

2.1. Belang van risicoanalyses

Voor elke organisatie (entiteit genoemd in de regelgeving) is het van belang te weten welke risico's het bestaan van de organisatie kunnen bedreigen. Het kennen van die risico's betekent dat je als organisatie bewuste keuzes kunt maken over hoe je met die risico's omgaat. Zodra je hebt bepaald welk risiconiveau je als organisatie wilt en kunt accepteren kun je voor elke risico bepalen hoe je het wilt beheersen. De traditionele opties zijn "wegnemen", "overdragen", "beheersen" en "accepteren". Elk van die opties heeft zo zijn gevolgen:

1. **Wegnemen**
   Deze optie betekent dat de organisatie stopt met uitvoeren van de activiteit die het risico veroorzaakt, of ze past de activiteit zodanig aan dat het risico verdwijnt. Dat kan tamelijk ingrijpend zijn.

2. **Overdragen**
   Deze optie houdt in dat een andere partij (gedeeltelijk) de verantwoordelijkheid voor het risico en de financiële gevolgen bij het optreden overneemt. In de praktijk gaat het vaak om

het afsluiten van een verzekering. Verzekeraars beoordelen daarbij het risico en kunnen voorwaarden stellen aan beheersmaatregelen om het risico beheersbaar te houden. Op basis daarvan wordt bepaald onder welke condities en tegen welke premie het risico kan worden overgenomen.

3. **Beheersen**
   Deze veel gebruikte optie houdt in dat één of meer beheersmaatregelen worden geformuleerd en geïmplementeerd met als doel het risiconiveau te verlagen. Dit kan bereikt worden door de kans dat het optreedt te verkleinen, of door de gevolgen te beperken of een combinatie daarvan. Soms zal blijken dat een beheersmaatregel effect heeft op meerdere eisen en/of dat meerdere maatregelen nodig zijn om een acceptabel risiconiveau te bereiken.

4. **Accepteren**
   De laatste optie in dit kader is het risico accepteren. Veelal wordt gedacht dat dit gelijk staat aan “verder niets doen”. Dat is niet altijd waar. Als een risico wordt geaccepteerd dan houdt dat in dat de risico-eigenaar bereid is de gevolgen te dragen als de negatieve gebeurtenis uit het risico zich voordoet. Als de kosten van het implementeren van een beheersmaatregel hoger zijn dan de kosten van het reageren op een incident, ook al is dat incident groot zal een “Incident Response Plan” (IRP) moeten worden opgesteld om de organisatie hierop voor te bereiden (een IRP geeft antwoorden op vragen als “wat moet er gebeuren als het incident optreedt”, “wie moet daarbij betrokken worden in welke rol” en “hoe kom je weer terug bij “business as usual”?).Het IRP moet vervolgens met regelmaat worden geoefend en bijgewerkt (na elke oefening wordt deze geëvalueerd met als doel het plan te verbeteren, wijzigingen in de organisatie en/of personeelsbestand moeten worden verwerkt, etc.

Bovenstaande opsomming laat zien dat elk risico dat in de risico-inventarisatie is opgenomen na afloop van de analyse verdere acties met zich meebrengt. Het niet uitvoeren van een dergelijke analyse betekent in feite dat de risico’s stilzwijgend en onbewust geaccepteerd worden en dat de organisatie niet is voorbereid op het optreden van een ongewenste gebeurtenis. Het periodiek uitvoeren van risicoanalyses is ook van belang om te voorkomen dat nieuwe risico’s onontdekt blijven.

2.2. Belang van industriële cybersecurity

Het voldoen aan regelgeving op het gebied van cybersecurity moet niet worden gezien als een vervelende verplichting die geld kost. Het moet ook geen doel op zichzelf zijn. Het doel moet zijn het zeker stellen van de continuïteit van de organisatie en om dat te bereiken moet zicht bestaan op de risico’s die een organisatie loopt en daar moet bewust mee omgegaan worden. Cybersecurity is, als onderdeel van het business risicomanagement, niet méér dan één van de onderwerpen die risico’s met zich meebrengt en waar je als onderneming moet omgaan.

Gemiddeld worden elke week 3 Nederlandse bedrijven geraakt en dat aantal stijgt. De regelgeving die in het volgende hoofdstuk wordt behandeld is daar ook op gericht, de Europese samenleving wil beschermd worden tegen de gevaren die haar bedreigen en daarvoor moeten we gezamenlijk en individueel maatregelen treffen. Het voldoen aan de regelgeving is dan een bijproduct van een goede bedrijfsvoering. Er zijn genoeg voorbeelden te vinden van organisaties die zich “keurig” aan de regelgeving hadden gehouden en toch slachtoffer zijn geworden omdat ze niet verder hadden gekeken dan wat de regels voorschrijven en dus een hulpmiddel tot doel hadden verheven.

3. Europese regelgeving

De Europese Unie heeft de noodzaak onderkend dat de Unie weerbaarder moet worden tegen cyberaanvallen. De noodzaak daartoe wordt versterkt door de hybride oorlogsvoering die de afgelopen jaren steeds heviger is geworden. Om dat doel te bereiken heeft de EU diverse wetten en richtlijnen in het leven geroepen. In december 2020 is de Europese cybersecuritystrategie voor het digitale decennium gepubliceerd. Kernaspect van de daaruit voortvloeiende regelgeving is dat onderscheid gemaakt wordt tussen “kritieke entiteiten”, “belangrijke entiteiten” en “gewone entiteiten”.

3.1. Critical Entities Resilience (CER, 2022/2557)

Deze richtlijn stelt regels en rechten vast voor de lidstaten en de door hen aan te wijzen kritieke entiteiten en heeft vooral als doel de fysieke weerbaarheid van die entiteiten te vergroten, maar stelt ook dat deze entiteiten *ook* moeten voldoen aan NIS2.

3.2. Network and Information Systems Security Directive (NIS2, 2022/2555)

De NIS2 is een Europese richtlijn die in landelijke wetgeving “vertaald” moet worden.

Deze richtlijn volgt de welbekende NIS op, die in Nederland is omgezet in de Wbni (Wet Beveiliging Netwerk- en Informatiesystemen), en sinds 2018 van kracht is. De NIS2 is op 24 oktober 2024 van kracht geworden en moest op dat moment in nationale wetgeving van de lidstaten zijn “getransponeerd”. In Nederland wordt de nationale wetgeving pas op 15 augustus 2026 van kracht.

NIS2 gaat een stuk verder dan de NIS/Wbni. Er zijn veel marktsectoren toegevoegd, waardoor de richtlijn voor veel meer bedrijven geldt. In deze nieuwe richtlijn zijn de kritieke en belangrijke sectoren centraal vastgesteld. De lidstaten mogen daar alleen van afwijken door extra sectoren toe te voegen.

Een groot gedeelte van de richtlijn handelt over wat de landen moeten regelen en inrichten (toezicht). Slechts een beperkt aantal artikelen geeft regels en rechten voor de entiteiten (zorgplicht en meldplicht).

- Artikel 20 stelt dat bestuurders van een entiteit aantoonbaar in staat moeten zijn een risicoanalyse te beoordelen. Daartoe moeten ze elke twee jaar een opleiding met certificaat volgen.
- Artikel 21 stelt dat elke entiteit een risicoanalyse moet uitvoeren als onderdeel van de “Due Care” of “Zorgplicht”. Deze risicoanalyse moet alle risico’s omvatten die voor de entiteit relevant zijn, niet alléén cybersecurity gerelateerde onderwerpen. Vervolgens moeten de niet acceptabele risico’s op redelijke wijze worden beheerst. Als onderdeel van de risico-analyse moeten ook de risico’s die verband houden met de (dienst)leveranciers in kaart worden gebracht.
  Verder vereist NIS2 geïmplementeerd beleid met betrekking tot bedrijfscontinuïteit (o.a. backup & recovery); cyberhygiëne (basisregels); asset management; multi-factor authenticatie; encryptie; training; en security tijdens de hele levenscyclus van systemen: van aanschaf/ ontwerp tot en met verwijdering.

- Artikel 23 stelt dat incidenten moeten worden gemeld bij de juiste autoriteiten. Dit wordt vaak met de term “Due Diligence” of “Meldplicht” aangeduid. Kort samengevat:
    - Als levering aan klanten in gevaar komt, deze onmiddellijk informeren;
    - Incidenten binnen 24 uur na ontdekking melden aan autoriteiten;
    - Binnen 72 uur na ontdekking ernst, omvang en “indicators of compromise” melden;
    - Binnen een maand een gedetailleerd rapport opleveren.
- Artikel 30 regelt de mogelijkheid om vrijwillige meldingen te doen.

Daarnaast wordt nu (anders dan onder de NIS) centraal geregeld welke mogelijke sancties kunnen worden toegepast:

- Artikel 32 regelt welke handhavingsmaatregelen kunnen worden toegepast voor essentiële entiteiten, waaronder het (tijdelijk) ontheffen uit de functie van de bestuurder(s)
- Artikel 33 regelt welke handhavingsmaatregelen kunnen worden toegepast voor belangrijke entiteiten
- Artikel 34 regelt de mogelijke hoogte van eventueel op te leggen boetes, voor essentiële entiteiten is dat 2 % van de wereldwijde jaaromzet met een minimum van M€ 10; voor belangrijke entiteiten is dat 1,4% van de wereldwijde jaaromzet met een minimum van M€7.
- Artikel 37 regelt dat bedrijven die worden aangevallen een beroep op bijstand kunnen doen bij de overheid. Bedrijven kunnen zich vanaf 24 oktober 2024 beroepen op dit artikel, óók in Nederland.

3.3. Uitvoeringsverordening (2024/2690)

Dit is een Europese wet die voor alle lidstaten van de EU geldt en niet meer in landelijke wetgeving behoeft te worden omgezet. Deze wet geldt (kort samengevat) voor digitale serviceproviders en legt vast dat een incident als significant moet worden beschouwd als het aan één van onderstaande voorwaarden voldoet:

- Het veroorzaakt (mogelijk) een schade van €500.000 of meer;
- Het veroorzaakt (mogelijk) het verlies van bedrijfsgeheimen;
- Het veroorzaakt (mogelijk) het overlijden van een natuurlijk persoon;
- Het veroorzaakt (mogelijk) aanzienlijke schade aan de gezondheid van een persoon;
- Het veroorzaakt (mogelijk) operationele verstoringen.

Daarnaast geldt een incident als significant wanneer onderstaande voorwaarden alle drie van toepassing zijn:

- Binnen 6 maanden hebben zich twee of meer kleinere incidenten voorgedaan; en
- De incidenten hebben dezelfde basisoorzaak; en
- De incidenten veroorzaken gezamenlijk (mogelijk) een schade van €500.000 of meer.

Ten slotte zijn per type digitale serviceprovider nog specifieke extra definities gegeven die een incident significant maken. Denk aan onbereikbaarheid van datacenters, slechte respons van DNS, etc.

3.4. Wanneer val je onder deze regelgeving?

In de NIS2 wordt gesteld dat deze richtlijn geldt voor middelgrote en grotere ondernemingen, maar, wat betekent dat eigenlijk? Daarbij wordt verwezen naar een aanbeveling van de EG uit 2003:

Volgens de aanbeveling 2003/361/EG van 6 mei 2003 geldt dat als een **zelfstandig** bedrijf aan één van de volgende voorwaarden voldoet dan is het middelgroot of groter:

- 50 medewerkers of meer
- Omzet €10.000.000 of meer per jaar
- Balanstotaal van €10.000.000 of meer.

Een bedrijf wordt als **zelfstandig** aangemerkt als er niet een ander bedrijf is dat 25% of meer van het kapitaal of de stemrechten bezit (partneronderneming, er worden 4 uitzonderingen op deze regel vermeld).

Dus, als je actief bent in één van de sectoren die in NIS2 worden genoemd én je organisatie is middelgroot of groter dan ben je verplicht je aan te melden als vallende onder de NIS2.

4. CE-markering

Om een product te mogen voorzien van een CE-markering moet het aantoonbaar voldoen aan:

1. Verordening Machineproducten
2. Cyber Resilience Act
3. Radio Equipment Directive

4.1. Verordening Machineproducten (2023/1230)

Deze verordening vervangt de machinerichtlijn. De verschillen met de eerdere richtlijn lijken inhoudelijk niet groot te zijn. Wel is het zo dat het nu een verordening is en daarmee een hogere ”wettelijke” status heeft dan een richtlijn. Eén verschil springt er wel uit en dat is het feit dat de verordening stelt dat rekening moet worden gehouden in het ontwerp met voorzienbare “acts of malicious third parties”. Ofwel, in het ontwerp van de machineproducten moeten beheers-maatregelen worden geïmplementeerd die de kans dat kwaadwillenden kwalijke handelingen kunnen uitvoeren acceptabel moeten houden.

4.2. Cybersecurity Resilience Act (CRA, 2024/2847)

Dit is een Europese wet die regelt dat “alles met een stekker” veilig moet zijn en blijven. Niet alleen het product moet veilig zijn, ook het ontwikkelproces moet veilig zijn, zorgend dat security is ingebakken in het product.

De CRA stelt dat producten “Secure by default” moeten zijn (Artikel 6) en geeft conformiteitseisen (artikel 7) voor belangrijke en kritieke producten. De artikelen 13 tot en met 15 geven de eisen aan fabrikanten van producten met een minimum ondersteuningsperiode van 5 jaar, security updates moeten gratis beschikbaar worden gesteld. Artikel 19 geeft de eisen aan importeurs en artikel 20 doet dat voor de distributeurs. Voor beide categorieën komen die erop neer dat zij moeten zorgen

dat de fabrikant aan de eisen voor fabrikanten voldoet. In de artikelen 27 tot en met 35 komen de conformiteitseisen en de documentatie eisen aan de orde. Daarin wordt onder andere een “Software Bill of Materials” (SBOM) verplicht gesteld. Een SBOM is een lijst met alle softwareproducten die zijn opgenomen in het eindproduct; daaronder vallen een eventueel besturingssysteem, applicaties die daarop draaien, maar ook de softwarebibliotheken die gebruikt zijn bij het samenstellen van de software. De SBOM moet naast de naam van de onderdelen ook het versienummer en de publicatie-datum vermelden. Die gegevens kunnen dan gebruikt worden om bij het bekend worden van kwetsbaarheden te onderzoeken of die in het product voorkomen en of die een risico veroorzaken.

Voor de CRA zijn “geharmoniseerde” Europese standaarden in ontwikkeling. Daarbij wordt uitgegaan van de IEC62443-4-1 voor het ontwikkelproces en de IEC62443-4-2 voor de producten.

4.3. Radio Equipment Directive (RED, 2014/53)

De Radio Equipment Directive is een oudere richtlijn die van alles regelt rond apparatuur die draadloos communiceert. Daaraan zijn in 2022 drie bepalingen toegevoegd die eisen stellen aan de beveiliging tegen cyberrisico’s. De wijziging betreft artikel 3.3, daaraan zijn de punten d, e en f toegevoegd. Voor het voldoen aan deze richtlijn kan gebruik gemaakt worden van de geharmoniseerde normen EN18031-1, EN18031-2 en EN18031-3.

5. Nederlandse regelgeving

De in het vorige hoofdstuk behandelde Europese regelgeving (CER en NIS2 richtlijnen) moet in wetgeving van de lidstaten worden omgezet. In Nederland is dat deels in wetten en deels in Besluiten en algemene maatregelen van bestuur.

5.1. Wet weerbaarheid kritieke entiteiten

Het wetsvoorstel “Wet weerbaarheid kritieke entiteiten” (officiële afkorting: ”Wwke”) is de Nederlandse implementatie van de CER-directive. Onder deze wet zullen organisaties worden aangewezen als kritieke of belangrijke entiteit. Het gevolg is dat deze organisaties te maken krijgen (als ze dat al niet hebben) met een toezichthouder die controleert of men zich aan de regels houdt die in de wet zijn voorgeschreven. Organisaties die hiermee te maken krijgen vallen automatisch ook onder de regelgeving van de Cyberbeveiligingswet.

Dit voorstel van wet is in de zomer van 2025 aan de Tweede Kamer voor behandeling aangeboden, is op 15 april 2026 door de Tweede Kamer aangenomen en is op 7 juli 2026 in de Eerste Kamer behandeld en aangenomen. De wet gaat in op 15 augustus 2026.

5.2. Besluit weerbaarheid kritieke entiteiten

Dit besluit (officiële afkorting: ”Bwke”, een Algemene Maatregel van Bestuur) geeft aanvullende regels over hoe entiteiten kunnen voldoen aan de Wwke. Ook biedt het mogelijkheden voor het opstellen van ministeriële regelingen die, ten aanzien van de zorgplicht, onderscheid kunnen maken tussen de verschillende sectoren.

5.3. Cyberbeveiligingswet

De Cyberbeveiligingswet (officiële afkorting: “Cbw”) is de Nederlandse implementatie (transpositie) van de NIS2-richtlijn. Deze wet onderscheidt essentiële en belangrijke entiteiten en legt de regels vast waar deze entiteiten aan moeten voldoen, wat de mogelijke sancties zijn en welke rechten ze hebben. Merk op dat deze wet regels vastlegt over entiteiten en niet, zoals zijn voorganger, de “Wet beveiliging netwerk- en informatiesystemen” aan kritieke en belangrijke diensten en producten.

In de memorie van toelichting op de Cyberbeveiligingswet is een tabel opgenomen waarin wordt aangegeven op welke wijze de artikelen uit de NIS-2 richtlijn in de Nederlandse wetgeving zijn verwerkt. Daarin valt op dat de NIS2-richtlijn niet alleen de nieuwe Cyberbeveiligingswet tot gevolg heeft, maar ook enkele wijzigingen in de Algemene Wet Bestuursrecht (Abw). Daarin zijn namelijk al bepalingen opgenomen die de implantatie van de meldplicht (deels) ondersteunen.

De zorgplicht in de wet wordt omschreven als “... de verplichting om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen [...] te beheersen.”

Dit voorstel van wet is in de zomer van 2025 aan de Tweede Kamer voor behandeling aangeboden, is in april 2026 door de Tweede Kamer aangenomen en is op 7 juli 2026 in de Eerste Kamer behandeld en aangenomen. De wet gaat in op 15 augustus 2026.

5.4. Cyberbeveiligingsbesluit

Dit besluit (officiële afkorting: “Cbb”, een Algemene Maatregel van Bestuur) geeft aanvullende regels over hoe entiteiten kunnen voldoen aan de Cbw. Hierbij wordt verwezen naar de Europese Uitvoeringsverordening (2024/2690) voor een bepaalde sector. Dit besluit geldt voor de overige sectoren waarbij de beschreven maatregelen gericht zijn op het inrichten van een ISMS. Daarbij wordt overigens niet geëist dat dit conform ISO 27001 zou moeten zijn (of dat de Security Programma Elementen van IEC 62443-2-1 gebruikt moeten worden). Ook dit besluit biedt de mogelijkheid voor het opstellen van ministeriële regelingen (zie de volgende paragraaf) die, ten aanzien van de zorgplicht, onderscheid kunnen maken tussen de verschillende sectoren.

5.5. Ministeriële regelingen

In de ministeriële regelingen is vastgelegd wat de criteria zijn waarbij verplicht melding gemaakt moet worden van een incident, Daarbij zal, net als in de uitvoeringsverordening 2024/2690, gelden dat wanneer een incident dat in eerste instantie niet gemeld hoefde te worden, dat wel moet gebeuren als binnen een bepaalde periode een incident optreedt met dezelfde oorzaak.

De Ministeriële regelingen geven ook nadere invulling geven aan de Zorgplicht door het toepassen van ISO 27001 verplicht te stellen voor overheidsdiensten. Voor de sector Overheid is de basis hiervoor de BIO2.

De volgende ministeries hebben regelingen gepubliceerd:

- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (concept regeling)
- Ministerie van Economische zaken (definitieve regeling)
- Ministerie van Infrastructuur en Waterstaat (definitieve regeling)
- Ministerie van Klimaat en Groene Groei (definitieve regeling)

- Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur (concept regeling)
- Ministerie van Volksgezondheid, Welzijn en Sport (concept regeling).

In de volgende paragrafen wordt kort beschreven wat de regelingen inhouden.

5.5.1. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De regeling van dit ministerie heeft betrekking op essentiële entiteiten van de sector overheid (behalve de waterschappen).

Voor deze entiteiten wordt het toepassen van NEN-EN-ISO/IEC 27002:2022 en BIO2 verplicht gesteld in het kader van de zorgplicht. Opzet, bestaan en werking moeten aantoonbaar zijn.

De entiteiten moeten een overzicht bijhouden van hun cruciale netwerk- en informatiesystemen. Voor de meldplicht van incidenten worden drempelwaarden vastgesteld, wanneer een incident als significant wordt aangemerkt. Incidenten zijn significant als de dienstverlening voor vier uur of langer wordt onderbroken, als de schade voor staat of samenleving meer is dan 500 miljoen, als iemand ernstig verwondt raakt of sterft, als misbruik van informatie een financiële schade van 5 miljoen of meer veroorzaakt of als hoog geclassificeerde informatie (zoals Staatsgeheim CONFIDENTIEEL) gelekt wordt.

5.5.2. Ministerie van Economische zaken

De regeling van dit ministerie heeft betrekking op essentiële en belangrijke entiteiten in de sectoren Digitale infrastructuur, Onderzoek, Ruimtevaart, Post- en koeriersdiensten, en vervaardiging van producten voor deze sectoren.

De regeling stelt dat de entiteiten zélf moeten bepalen op welke wijze invulling wordt gegeven aan de zorgplicht en de daarbij horende verantwoordelijkheden. De regeling stelt wel eisen aan beleid en procedures op het gebeid van beveiliging van netwerk- en informatiesystemen, bedrijfscontinuïteit, aan het verwerven ontwikkelen en onderhouden van netwerk- en informatiesystemen en beleid ten aanzien van logische toegang.

Voor de meldplicht geldt voor alle sectoren dat een incident met potentieel dodelijke gevolgen of ernstige schade aan de gezondheid van een of meer personen als significant wordt aangemerkt. Ook succesvolle ongeoorloofde toegang tot de netwerk- en informatiesystemen geldt als significant incident. Verder zijn per sector en of subsector meer specifieke grenzen gesteld, zoals 50.000 gebruikers of meer zijn getroffen bij een onderbreking van minimaal 4 uur van de levering van een openbare elektronische communicatiedienst of 30% van de gebruikers of meer van een postdienst ontvangen hun stukken minimaal 2 dagen later dan zou moeten.

5.5.3. Ministerie van Infrastructuur en Waterstaat

De regeling van dit ministerie heeft betrekking op essentiële en belangrijke entiteiten in de sectoren Vervoer, Drinkwater, Afvalwater, Avalstoffenbeheer, Overheid (Waterschappen), Meteorologie, vervaardiging, productie en distributie van chemische stoffen en onderzoek in deze sectoren.

Voor de entiteiten in deze sectoren die overheidsinstanties zijn wordt het toepassen van NEN-EN-ISO/IEC 27002:2022 en BIO2 verplicht gesteld in het kader van de zorgplicht. Opzet, bestaan en werking moeten aantoonbaar zijn.
Voor de niet-overheidsinstanties worden in het kader van de zorgplicht eisen gesteld aan het beleid en procedures op het gebeid van beveiliging van netwerk- en informatiesystemen, bedrijfs-continuïteit, aan het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen en beleid ten aanzien van logische toegang.

Voor de meldplicht worden per sector grenswaarden voor significante incidenten gesteld; bijvoorbeeld voor de sector drinkwater als gedurende 6 uur of langer geen drinkwater geleverd kan worden aan 10,000 aansluitingen of meer.

5.5.4. Ministerie van Klimaat en Groene Groei

De regeling van dit ministerie bevat zowel bepalingen voor de Wwke (hoofdstuk 1) als voor de Cbw (Hoofdstuk 2). Voor de Cbw heeft de regeling betrekking op essentiële en belangrijke entiteiten in de sector energie, subsectoren elektriciteit, stadsverwarming- en -koeling, aardollie, aardgas en waterstof.

In het kader van de zorgplicht worden eisen gesteld aan het beleid en procedures op het gebeid van beveiliging van netwerk- en informatiesystemen, bedrijfscontinuïteit, aan het verwerven ontwikkelen en onderhouden van netwerk- en informatiesystemen en beleid ten aanzien van logische toegang.

Voor de meldplicht worden per sector grenswaarden voor significante incidenten gesteld; bijvoorbeeld voor de subsector elektriciteit een ongeplande, operationele verstoring met gevolgen voor de transmissie en distributie van 100 MW aan vermogen of meer, de beschikbaarheid van 100 MW vermogen bij (onder andere) een producent, de levering van elektriciteit aan 20.000 afnemers of meer.

5.5.5. Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur

De regeling van dit ministerie heeft betrekking op essentiële en belangrijke entiteiten in de sector productie, verwerking en distributie van levensmiddelen en (toegepast) onderzoek naar levensmiddelen voor commerciële tepassingen.

In het kader van de zorgplicht worden eisen gesteld aan het beleid en procedures op het gebeid van beveiliging van netwerk- en informatiesystemen, bedrijfscontinuïteit, aan het verwerven ontwikkelen en onderhouden van netwerk- en informatiesystemen en beleid ten aanzien van logische toegang.

Voor de meldplicht worden per sector grenswaarden voor significante incidenten gesteld. Bijvoorbeeld de productie, verwerking of distributie van levensmiddelen is gedurende 24 uur of langer geheel of gedeeltelijk onderbroken, of gedurende 6 uur geheel onderbroken.

5.5.6. Ministerie van Volksgezondheid, Welzijn en Sport

De regeling van dit ministerie heeft betrekking op essentiële en belangrijke entiteiten in de sector Gezondheidszorg en de subsector Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitro diagnostiek.

In het kader van de zorgplicht wordt verplicht gesteld om te voldoen aan ófwel NEN 7510:2024, ófwel NEN-ISO-IEC 27001:2022 met toepassing van NEN-ISO-IEC 27002:2022, óf gelijkwaardig beschermingsniveau.

Voor de meldplicht worden aanvullende eisen gesteld aan de inhoud van de melding en aan de inhoud van het voortgangs- en eindverslag.
Een incident wordt als significant aangemerkt als het tot mogelijk gevolg heeft dat een kritisch bedrijfsproces 4 uur of langer gedeeltelijk of geheel wordt onderbroken, cruciale netwerk- en informatiesystemen zijn gecompromitteerd of vernietigd, als de integriteit, vertrouwelijkheid of beschikbaarheid van bedrijfsgevoelige informatie ernstig is aangetast, als de vertrouwelijkheid van bijzondere persoonsgegevens of BSN-nummers is aangetast, of als sprake is van blijvend letsel, ziekenhuisopname of overlijden van een persoon.

6. Wat betekent dit?

In dit hoofdstuk wordt toegelicht hoe al het bovenstaande praktisch kan worden ingevuld door het MKB.

6.1. Wanneer van toepassing?

Na goedkeuring door de Tweede Kamer in april 2026, en door de Eerste Kamer in juli 2026, zullen de Wwke en Cbw op 15 augustus 2026 in werking treden. Dat betekent niet dat alle organisaties op dat moment moeten wachten, Het is verstandig om, op basis van de beschikbare concepten, zo snel mogelijk van start te gaan met de voorbereidingen. Het inrichten van een security management-systeem vergt veel (doorloop)tijd, daarbij is het verstandig om de controls uit ISO 27002 aan te vullen met controls uit de IEC62443-2-4 en IEC62443-3-3 als die van toepassing zijn voor de organisatie vanwege de aanwezigheid van industriële automatisering.

6.2. Hoe te voldoen aan de eisen?

6.2.1. Organisatorische maatregelen

De Cyberbeveiligingswet is uitgewerkt in het Cyberbeveiligingsbesluit en heeft voor verschillende sectoren verdieping in de ministeriële regelingen voor de Meldplicht en Zorgplicht, uiteindelijk bestaat de wet zoals eerder gezegd uit 4 gedeeltes;

1. Opleidingsplicht voor topmanagement
2. Registratieplicht
3. Meldingsplicht
4. Zorgplicht.

Om invulling te geven aan deze verplichtingen zijn maatregelen nodig in de inrichting van een organisatie.

De **opleidingsplicht** voor topmanagers is direct van kracht wanneer de wet in werking wordt gesteld en behelst dat het topmanagement van een organisatie aantoonbaar in staat is om een risicoanalyse te beoordelen en er gevolg aan te geven. Het topmanagement moet hiervoor elke twee jaar een certificaat kunnen overleggen dat bewijst dat zij aan de opleidingseisen die de Cbw en het Cbb stellen voldoen.

De **registratieplicht** is direct van kracht wanneer de wet in werking wordt gesteld en behelst dat essentiële en belangrijke entiteiten een wettelijke verplichting hebben om zich te registreren. Dit kan men nu al doen op mijn.ncsc.nl, vanuit deze portaal kan je je zelf zowel bij een CSIRT als bij de toezichthouder van de betreffende sector aanmelden.

De **meldplicht** gebeurt op hetzelfde portaal waar men zich registreert, en dit gaat dan om de zogenoemde significante incidenten die per sector en toezichthouder verschillen. Dit kan je uiteindelijk vinden in de ministeriële regelingen. Algemeen geldt dat significante incidenten binnen 24 uur (vroegtijdige waarschuwing) tot 72 uur (volledige melding) moeten worden gemeld.
Om invulling te kunnen geven aan de **meldplicht** moet je als organisatie in staat zijn om het optreden van een incident op te merken. Dat betekent dat zaken als logging en monitoring moeten worden ingericht, dat de op die manier verzamelde data regelmatig moet worden beoordeeld op

verdachte meldingen. Die verdachte meldingen moeten dan nader worden onderzocht om vast te stellen of het ene significant incident betreft. Er zijn serviceproviders in de markt die hierbij kunnen helpen.

De **zorgplicht** vormt het inhoudelijke kernonderdeel van de Cyberbeveiligingswet en verplicht essentiële en belangrijke entiteiten om **passende en evenredige maatregelen** te nemen om risico's voor netwerk en informatiesystemen te beheersen en de continuïteit van hun dienstverlening te waarborgen.

De wet hanteert hierbij bewust een **open norm**. Organisaties moeten op basis van hun risicoprofiel, omvang en maatschappelijke of economische impact kunnen onderbouwen welke maatregelen zij treffen. Deze invulling is nader uitgewerkt in het **Cyberbeveiligingsbesluit**, waarin onder meer eisen zijn opgenomen voor risicoanalyse, incidentafhandeling, bedrijfscontinuïteit, leveranciers-ketens, toegangsbeheer en het gebruik van multi-factor authenticatie.

De zorgplicht kan per sector verder worden geconcretiseerd via **ministeriële regelingen**. Het bestuur van de entiteit is expliciet eindverantwoordelijk voor de goedkeuring, uitvoering en borging van deze maatregelen, waarmee cyberbeveiliging een structureel onderdeel wordt van governance en risicomanagement.

Samenvattend kan je stellen dat voldoen aan de cyberbeveiligingswet betekent dat je in controle moet zijn en bewust bent wat belangrijk is en wat niet en vandaaruit keuze maken, Het beste kan je daarom ook beginnen met het uitwerken van het primaire bedrijfsdoel naar installaties, processen, locaties, mensen en leveranciers als je de afhankelijkheden van deze goed in kaart hebt gebracht dan weet je wat je kroonjuwelen zijn en wat prioriteit is.

De cyberbeveiligingswet is dus allesbehalve een afvinklijstje voor industriële omgevingen; het is ook vaak een utopie om het zo te behandelen.

6.2.2. Technische maatregelen

Bovenstaande maatregelen in de inrichting van een organisatie kunnen vaak ondersteund worden met technische maatregelen om beleid praktisch vorm te geven en organisatorische processen te ondersteunen. Ten aanzien van de zorgplicht kunnen technische maatregelen helpen beleid af te dwingen. Ten aanzien van de meldplicht zijn technische maatregelen nodig om afwijkingen tijdig te signaleren, te analyseren en daarop adequaat te reageren.

6.3. Compliance en regelgeving

Invoering van wetgeving leidt bij organisaties vaak tot de vraag: "wat moet ik (minimaal) doen om aan de wet te voldoen?". Het beantwoorden van die vraag geeft vaak aanleiding tot het opstellen van een "vinklijstje" waarin alles staat dat moet gebeuren En als alle vinkjes geplaatst zijn dan voldoe ik aan de wet. Dat lijkt mooi, maar dan handel je naar de letter van de wet en niet naar de bedoeling van de wet.

De bedoeling van de wetgeving is namelijk dat organisaties "in control" komen én blijven over hun risico's waardoor de weerbaarheid van die organisaties wordt versterkt. En daarmee wordt bedoeld de weerbaarheid tegen bedreigingen, en niet de weerbaarheid tegen auditors. Er zijn voldoende voorbeelden in de literatuur en in de pers (zie bijvoorbeeld de casus van Clinical Diagnostics. De organisatie had een ISO 27001 certificaat, dus ze hadden een systeem mo met

informatiebeveiligingsrisico's om te gaan. Maar dat certificaat zegt niet zoveel over de effectiviteit van de getroffen maatregelen.

Veel beter is om als organisatie de bedreigingen in kaart te brengen waar je mee te maken zou kunnen krijgen. En dan bedreigingen van allerlei aard, van brand in de productiehal of het kantoor, of ene overstroming, of een inbreuk op het netwerk. Als je een beeld hebt van wat je organisatie zou kunnen bedreigen en wat de mogelijke gevolgen zouden kunnen zijn wanneer een dreiging werkelijkheid wordt ben je in staat bewuste keuzes te maken op welke wijze je de risico's wilt beheersen. Tegen een brand kun je verzekeren (risico overdragen) maar voor het tijdig herstel van de productie is dat niet voldoende, je zult ook een plan moeten hebben (Incident Response Plan) hoe te handelen als die brand zich onverhoopt echt voordoet. Het in kaart brengen en beoordelen van de bedrijfsrisico's is een terugkeren proces dat in een regelmatig terugkerende cyclus aan de orde moet komen. Dat kan jaarlijks zijn, dat kan ook één keer per kwartaal als een organisatie zich daar beter bij voelt. Ook deze frequentie is onderdeel van bewuste besluitvorming die resulteert in bedrijfsbeleid.

Daarmee wordt Bedrijfscontinuïteit de werkelijk drijfveer van besluiten en het handelen van de organisatie omdat daarmee een aantal reële bedrijfsrisico's kunnen worden beheerst. Door het op die manier aan te pakken wordt het voldoen aan de wetgeving een gevolg in plaats van de oorzaak van het nemen van maatregelen.

6.4. Praktische hulpmiddelen

Voor organisaties die invulling willen geven aan de Cyberbeveiligingswet en de NIS2-richtlijn zijn verschillende praktische hulpmiddelen beschikbaar. Deze ondersteunen bij oriëntatie, eerste beoordeling en het starten van de implementatie.

Het **NCSC** biedt algemene informatie over de NIS2 en de Cyberbeveiligingswet. Dit geeft inzicht in de reikwijdte en verplichtingen en is geschikt als startpunt voor organisaties die de impact willen bepalen.
https://www.ncsc.nl/cyberbeveiligingswet-nis2

Daarnaast stelt het NCSC een **stappenplan** beschikbaar waarmee organisaties gestructureerd aan de slag kunnen, van inventarisatie tot implementatie van maatregelen.
https://www.ncsc.nl/cyberbeveiligingswet-nis2/aan-de-slag

De **RDI** biedt via Regelhulpen voor Bedrijven een **NIS2-zelfevaluatie** en een **quickscan**. Hiermee kan een organisatie snel inzicht krijgen in haar huidige situatie en in hoeverre de regelgeving van toepassing is.
https://regelhulpenvoorbedrijven.nl/NIS-2-NL/
https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/

Voor kennisdeling en het uitwisselen van ervaringen is de **Digital Trust Community** beschikbaar. Dit platform ondersteunt met praktische informatie, waarschuwingen en inzichten uit de praktijk.
https://digitaltrustcommunity.nl/

De genoemde hulpmiddelen helpen bij het verkrijgen van inzicht en structuur, maar vervangen niet de eigen risicoanalyse en invulling van de zorgplicht.

7. Conclusie

7.1. Samenvatting van belangrijkste punten

De NIS2 en CER vergroten de reikwijdte van cybersecuritywetgeving met meer sectoren en middelgrote organisaties die vallen onder de verplichtingen. Er wordt onderscheid gemaakt tussen essentiële en belangrijke entiteiten. De centrale gedachte is dat cybersecurity een onderdeel is van goed bestuur en risicomanagement, gericht op het waarborgen van continuïteit en weerbaarheid.

Kernverplichtingen zijn:

- zorgplicht,
- meldplicht,
- toezicht en handhaving,
- expliciete bestuurlijke betrokkenheid.

Organisaties moeten zelf onderbouwen wat passend en evenredig is.

Het bestuur en de directie zijn eindverantwoordelijk.

7.2. Aanbevelingen voor de industrie

De ISO/IEC 27001 en 27002 kunnen als basiskader dienen, maar voor industriële omgevingen is aanvulling met IEC 62443 aan te bevelen. Deze normen ondersteunen aantoonbaarheid en samenhang over de levenscyclus.

Cybersecuritywetgeving is geen afvinklijst, maar een risico gedreven kader.

Organisaties moeten aantoonbaar:

- begrijpen welke risico’s zij lopen,
- prioriteiten stellen,
- bewuste keuzes maken voor het beheersen van de risico’s.

8. Bijlagen

8.1. Bronnen

De in dit document aangehaalde wetten en regelingen zijn via internet ontsloten, hieronder een lijst met url's.

Wetten en regelingen	url
EU Cybersecurity strategie	https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
CER, 2022/2557	https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2557
NIS2, 2022/2555	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32022L2555:NL:NOT
Uitvoerings-verordening, 2024/2690	https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202402690
CRA, 2024/2847	https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202402847
RED, 2014/53	https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:02014L0053-20241228
Verordening Machineproducten, 2023/1230	https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32023R1230
Wwke	Wettekst: https://zoek.officielebekendmakingen.nl/stb-2026-188.pdf
Bwke	https://zoek.officielebekendmakingen.nl/stb-2026-190.pdf
Cbw	Wettekst: https://zoek.officielebekendmakingen.nl/stb-2026-187.pdf
Cbb	https://zoek.officielebekendmakingen.nl/stb-2026-189.pdf
BZK	Wwke: https://zoek.officielebekendmakingen.nl/stcrt-2026-27700.pdf Cbw: https://zoek.officielebekendmakingen.nl/stcrt-2026-27679.pdf
EZ	https://zoek.officielebekendmakingen.nl/stcrt-2026-25627.pdf
I&W	Wwke: https://zoek.officielebekendmakingen.nl/stcrt-2026-24092.pdf Cbw: https://zoek.officielebekendmakingen.nl/stcrt-2026-24093.pdf
KGG	https://zoek.officielebekendmakingen.nl/stcrt-2026-22078.pdf
LVVN	https://zoek.officielebekendmakingen.nl/stcrt-2026-25478.pdf2
VWS	Wwke: https://zoek.officielebekendmakingen.nl/stcrt-2026-28023.pdf Cbw: https://zoek.officielebekendmakingen.nl/stcrt-2026-28763.pdf
BIO2 v1.3	https://zoek.officielebekendmakingen.nl/stcrt-2026-7416-n1.pdf

8.2. Afkortingen en begrippen

AAVA:	Andere Aangewezen Vitale Aanbieder
AED:	Aanbieder Essentiële Dienstverlener
Bbni:	Besluit beveiliging netwerk- & informatiesystemen
Bwke:	Besluit weerbaarheid kritieke entiteiten
Cbw:	Cyberbeveiligingswet (Nederlandse implementatie van de NIS2)
Cbb:	Cyberbeveiligingsbesluit
CRA:	Cybersecurity Resilience Act
IACS:	Industrial Automation & Control Systems
IEC:	International Electrotechnical Commission.
ISO:	International Organization for Standardization
NIS2:	Network and Information Systems (NIS2 Directive)
OT:	Operationele Technologie
Wbni:	Wet Beveiliging Netwerk- & Informatiesystemen
Wwke:	Wet weerbaarheid kritieke entiteiten

8.3. Publicaties van het Industrieel Platform Cybersecurity

Kijk voor meer informatie over het IPCS op https://securitydelta.nl/nl/diensten/kennis/ipcs.

Andere publicaties van het IPCS zijn:

- Beveiliging van OT voor het (top) management
- High Level risicoanalyse in vogelvlucht
- Korte beschrijving delen van de IEC 62443
- Korte handleiding start IEC 62443
- Incident respons/Incident recovery
- Cybergevoeligheid van tijd
- CMDB en tooling in de PA/OT/IACS

Deze publicaties kunt u opvragen via https://securitydelta.nl/services/knowledge/ipcs

8.4. Auteurs

Dit document is opgesteld door de volgende leden van het Industrieel Platform Cyber Security:

- Johannes Braams
- Philip Roodzant
- Gert Ippel
- Menjur Ossel

Met dank aan Rob Hulsebos, Michael Theuerzeit en Thomas Vasen voor het redigeren van de teksten, en de overige leden van de 'IPCS-werkgroep NIS2 voor het reviewen van dit document.

8.5. Risico Acceptatie

Citaat m.b.t. risk acceptation, uit: Fernando Maymi, Shon Harris "CISSP All-in-One Exam Guide, Ninth Edition"

The last approach is to accept the risk, which means the organization understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. Many organizations will accept risk when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the potential loss value. A crucial issue with risk acceptance is understanding why this is the best approach for a specific situation. Unfortunately, today many people in organizations are accepting risk and not understanding fully what they are accepting. This usually has to do with the relative newness of risk management in the security field and the lack of education and experience in those personnel who make risk decisions. When business managers are charged with the responsibility of dealing with risk in their department, most of the time they will accept whatever risk is put in front of them because their real goals pertain to getting a project finished and out the door. They don't want to be bogged down by this silly and irritating security stuff. Risk acceptance should be based on several factors. For example, is the potential loss lower than the countermeasure? Can the organization deal with the '"pain" that will come with accepting this risk? This second consideration is not purely a cost decision, but may entail noncost issues surrounding the decision. For example, ifwe accept this risk, we must add three more steps in our production process. Does that make sense for us? Or ifwe accept this risk, more security incidents may arise from it, and are we prepared to handle those?

The individual or group accepting risk must also understand the potential visibility of this decision. Let's say a company has determined that it is not legally required to protect customers' first names, but that it does have to protect other items like Social Security numbers, account numbers, and so on. So, the company ensures that its current activities are in compliance with the regulations and laws, but what if its customers find out that it is not protecting their full names and they associate this with identity fraud because of their lack of education on the matter? The company may not be able to handle this potential reputation hit, even if it is doing all it is supposed to be doing. Perceptions of a company's customer base are not always rooted in fact, but the possibility that customers will move their business to another company is a potential fact your company must comprehend.

Security Delta (HSD)
Wilhelmina van Pruisenweg 104
2595 AN The Hague
070 204 41 80

info@securitydelta.nl
www.securitydelta.nl