Den Haag, 20 juli 2026

Kenmerk	L-26-011
Onderwerp	Wat betekent de nieuwe Cyberbeveiligingswet voor de chemische industrie?
Samenvatting	Deze VNCI ledeninformatie geeft toelichting op de belangrijkste wettelijke verplichtingen van de nieuwe Cyberbeveiligingswet, die op 15 augustus in werking treedt. Ook vind je relevante links met meer informatie en hulpmiddelen, om te voldoen aan de wettelijke eisen. De Cyberbeveiligingswet moet leiden tot een structurele aanpak van cyberweerbaarheid van kritische processen door een risico gebaseerde managementaanpak, bestuurlijke betrokkenheid en een goed georganiseerde cyberincident respons.

Beste ,

Op 15 augustus treedt de Cyberbeveiligingswet (Cbw), het Besluit Cyberbeveiliging (Cbb) en de Cyberbeveiligingsregeling IenW in werking. De Cbw is de Nederlandse implementatie van de Europese NIS2-richtlijn[1].
De wet heeft als doel de digitale weerbaarheid van essentiële diensten en belangrijke organisaties te versterken. De digitale weerbaarheid richt zich op de beveiliging van de IT- en OT systemen[2] van de kritische processen van een organisatie. De chemiesector is binnen de Cbw aangewezen als belangrijke sector. Voor bedrijven in de chemische industrie betekent dit dat zij nieuwe wettelijke verplichtingen krijgen op het gebied van cyberbeveiliging. Daarbij is van belang dat cyberbeveiliging een verantwoordelijkheid van de bestuurders van de organisatie.

Deze VNCI ledeninformatie geeft toelichting over de belangrijkste wettelijke verplichtingen, namelijk de registratie-, zorg- en incidentmeldplicht. Deze verplichtingen, inclusief de opleidingseisen voor bestuurders, zijn nader uitgewerkt in het Cyberbeveiligingsbesluit (Cbb) en de Cyberbeveiligingsregeling IenW.
Verder gaan we kort in op het overheidstoezicht op deze verplichtingen.

Registratieplicht
Chemiebedrijven die onder de Cyberbeveiligingswet vallen, moeten zich registreren in het landelijke entiteitenregister. Hiermee krijgen de toezichthouder en het Nationaal Cyber Security Centrum (NCSC) inzicht in de organisaties die onder de wet vallen (flowchart, registratieplicht).

[1] Richtlijn (EU) 2022/2555 Network and Information Security directive (NIS2).
[2] Onder een netwerk- en informatiesysteem valt ook Operationele Technologie (OT), ook wel bekend als Industrial Automation & Control Systems (IACS).

Zorgplicht

Bedrijven zijn verplicht een risicoanalyse uit te voeren en op basis daarvan passende technische, organisatorische en operationele beveiligingsmaatregelen te treffen. Deze maatregelen moeten passend en evenredig zijn in verhouding tot de risico's voor de bedrijfsvoering en de mogelijke gevolgen van cyberincidenten.

De zorgplicht omvat 10 zorgplichtmaatregelen[3] (infosheet zorgplicht):

1. Maak een risicoanalyse van de netwerk- en informatiesystemen (IT/OT)
2. Richt cyberincident respons in
3. Bereid je voor op IT/OT uitval
4. Maak je toeleveringsketen veilig
5. Breng cyberhygiëne op orde (incl. opleiding)
6. Beveilig je netwerk- en informatiesystemen
7. Versterk beveiliging rond personeel, toegang en assetbeheer
8. Beheer toegang tot data en diensten
9. Stel cryptografiebeleid op
10. Beoordeel effectiviteit maatregelen

Meldplicht

Significante cyberincidenten moeten binnen 24 uur na ontdekking worden gemeld (een vroegtijdige waarschuwing) aan het bevoegde Computer security incident response team CSIRT (i.c. NCSC) en de toezichthouder (i.c. ILT). Organisaties moeten daarom beschikken over procedures voor detectie, beoordeling, escalatie en melding van incidenten (NCSC meldplicht). In artikel 25 van de Cyberbeveiligingsregeling IenW is nader uitgelegd wanneer sprake is van een significant cyberincident binnen de chemische industrie.

Bestuursverantwoordelijkheid

De Cyberbeveiligingswet legt nadrukkelijk verantwoordelijkheid voor Cyberbeveiliging bij bestuurders. Het bestuur moet cyberrisico's actief beoordelen, beveiligingsmaatregelen goedkeuren en toezicht houden op de naleving. Ook moeten de bestuurders van het chemiebedrijf een training volgen (zie hoofdstuk 5 Cbb). Cybersecurity wordt daarmee een integraal onderdeel van governance en risicomanagement.

Toezicht en handhaving

Binnen de chemische sector zal het toezicht worden uitgevoerd door de Inspectie Leefomgeving en Transport (ILT). Omdat de chemische industrie is aangewezen als belangrijke sector, is er sprake van zogenaamd reactief toezicht. Toezicht kan dan plaatsvinden naar aanleiding van een cyberincident.

[3] Zie artikel 21 Cbw, hoofdstuk 4 Cbb en paragraaf 4.2 (zorgplicht niet-overheidsorganisaties) Cyberbeveiligingsregeling IenW.

Toezichthouders kunnen informatie opvragen, audits uitvoeren en onderzoeken instellen naar de naleving van de wet. Bij overtredingen kunnen bestuursrechtelijke maatregelen en sancties worden opgelegd. Ook bestuurders kunnen in bepaalde gevallen worden aangesproken op hun verantwoordelijkheden.

Ondersteuning
Het Nationaal Cyber Security Centrum (NCSC) is onder meer het kennis- en adviescentrum voor cybersecurity. Ook biedt het NCSC gerichte ondersteuning voor bedrijven die vallen onder de Cbw. Dit doet ze via het sectoraal Computer Security Incident Response Team (CSIRT) door het verstrekken van dreigingsinformatie, waarschuwingen, adviezen en ondersteuning bij cyber-incidenten. Zie ook:
Cyberbeveiligingswet
Aan de slag met de Cyberbeveiligingswet
FAQ Cyberbeveiligingswet

Wet weerbaarheid kritieke entiteiten (Wwke)
Naast de Cbw treden op 15 augustus ook de Wet weerbaarheid kritieke entiteiten (Wwke), het Besluit weerbaarheid kritieke entiteiten en de Regeling weerbaarheid kritieke entiteiten IenW in werking. Bedrijven die onder de Wwke vallen, hoeven zich niet zelf te melden of te registreren. Zij worden door de overheid aangewezen. Die aanwijzing moet binnen één maand na de inwerkingtreding van de wet plaatsvinden. Binnen negen maanden na aanwijzing moeten de bedrijven een risicobeoordeling hebben uitgevoerd en binnen tien maanden na aanwijzing moeten zij voldoen aan de zorgplicht en meldplicht.

Voor de chemiebedrijven die worden aangewezen als kritieke entiteit zal de VNCI nog een aparte VNCI ledeninformatie opstellen.

Tenslotte attendeer ik je nog op de website over versterking weerbaarheid van het ministerie van Infrastructuur en Waterstaat, waar ook specifieke informatie is te vinden is over de Cbw en de Wwke: I&W versterking weerbaarheid.

Heb je nog vragen en/of uitvoeringsknelpunten, neem dan gerust contact met mij op.

Met vriendelijke groet,

Peter Bareman
Senior Beleidsadviseur
bareman@vnci.nl
T: 06 - 349 248 72