

VALT MIJN BEDRIJF ONDER DE NIS2 ?

Rob Hulsebos / rh@enodenetworks.com

Note for foreign readers: this document is meant for Dutch readers only. Although the NIS2 is of course applicable to other countries, the local situation is always different and the information herein may not be applicable.

De Europese Unie scherpt de eisen op het gebied van cybersecurity van organisaties aan. De onlangs gepubliceerde “NIS2” richtlijn gaat een impact hebben voor veel sectoren in de Nederlandse economie, en zeker ook de maakindustrie. Er is nauwkeurig opgesomd welke bedrijven eronder gaan vallen.

Als uw bedrijf daaronder valt, dan is de consequentie is dat er fors werk moet worden gestoken op het cyberveilig houden van het bedrijf, de processen en activiteiten daaromheen, de toeleveranciers, het reageren op incidenten, en rapportages aan de autoriteiten. Een stok achter de deur zijn forse boetes en aansprakelijkheid van de directie. De eerste vraag is dus: “Valt *mijn* bedrijf onder de NIS2 of niet?”

Wat is de NIS2 ?

Eind 2022 is vanuit Brussel de “NIS2 Richtlijn” (Network & Information Systems) uitgekomen, en 3 weken na publicatie geactiveerd. Als opvolger van de oudere “NIS” (in het Nederlands: Wbni – Wet Beveiliging Netwerken en Infrastructuur) gaat het de eisen op het gebied van cybersecurity van bedrijven aanscherpen.



Figuur: Titelblad NIS (bron: EU)

Nederland heeft 21 maanden de tijd om de NIS2 in nationale wetgeving om te zetten. De deadline hiervoor staat (vanuit Brussel) op 17 oktober 2024, maar het is al bekend dat Nederland deze datum niet gaat halen. Inmiddels begint Nederland een beetje wakker te worden, want de datum komt nu toch wel heel snel dichtbij. Bovendien gaat het eigenlijk niet om de wetgeving zelf, maar: *organisaties moeten per die datum ook aan de wet voldoen*. En dat is soms best nog veel werk.

Over alle consequenties van de NIS2 ga ik het nu niet hebben, daarover is op internet al genoeg te vinden. Bovendien zijn de specifieke Nederlandse details nog niet bekend, er komt (2024 Q2) ook nog een internetconsultatie.

Valt mijn bedrijf eronder of niet?

Interessant is wel te weten “Gaaf de NIS2 ook voor *mij* gelden?”. Wat ik hierover kon vinden op internet als allemaal vrij algemeen. Bijna iedereen soms gewoon het rijtje bedrijfssectoren op dat de NIS2 noemt, maar dat is niet erg specifiek genoeg. Bijvoorbeeld, het “Digital Trust Center” van de Rijksoverheid publiceerde¹ het volgende overzicht:

| Sectoren bijlage 1 | Sectoren bijlage 2 |
|--|---|
| <ul style="list-style-type: none">▪ Energie▪ Transport▪ Bankwezen▪ Infrastructuur▪ Gezondheidszorg▪ Drinkwater▪ Digitale infrastructuur▪ Afvalwater▪ Overheidsdiensten▪ Ruimtevaart | <ul style="list-style-type: none">▪ Digitale aanbieders▪ Post- en koeriersdiensten▪ Afvalstoffenbeheer▪ Levensmiddelen▪ Chemische stoffen▪ Onderzoek▪ Vervaardiging / manufacturing |

Figuur: In de NIS2 genoemde sectoren (bron: digitaltrustcenter.nl)

Er is een verschil tussen bijlage 1 en bijlage 2, voor wat betreft grootte van bedrijven (dit komt verderop nog aan de orde).

De tabel is exact de opsomming zoals die ook in de NIS2-tekst staat. In de Engelse variant van de NIS2 spreekt men over “Manufacturing”, in de Nederlandse vertaling over “Vervaardiging”². Maar wat wordt *precies* bedoeld met “Vervaardiging” ? Wat verder onderzoeken op internet leverde weinig details op; in een publicatie van een grote IT-dienstverlener werd enkel “Fabrikanten van medische hulpmiddelen” genoemd. Verder kon ik er op internet ook niet veel details over vinden, iedereen copy/paste altijd hetzelfde rijtje.

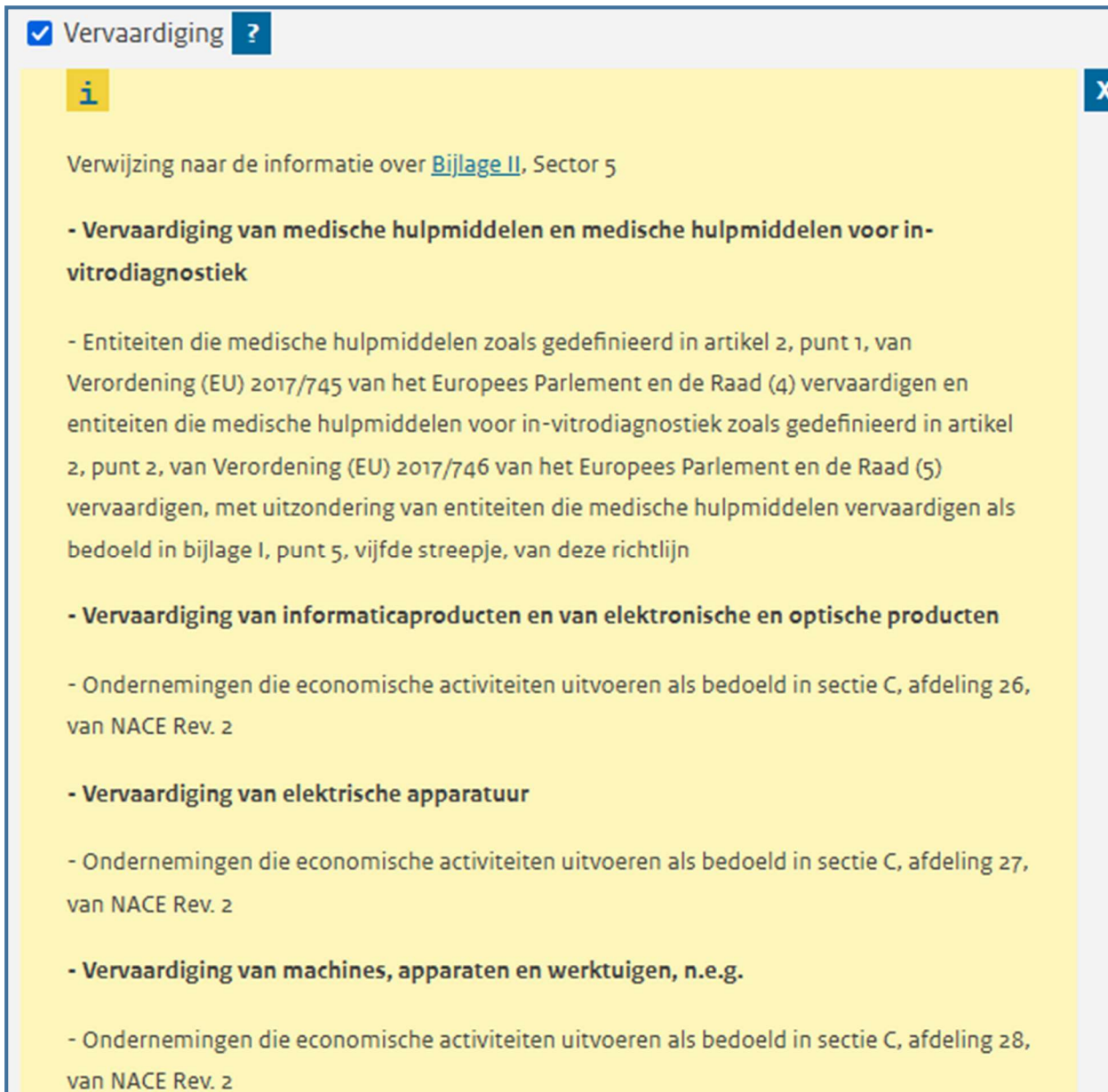
¹ Zie DTC: <https://www.digitaltrustcenter.nl/wat-gaat-de-nis2-richtlijn-betekenen-voor-jouw-organisatie>

² M.i. niet zo’n duidelijke vertaling, had dit niet beter “Maakindustrie” kunnen zijn

Regelhulp

Eind 2023 lanceerde de Rijksoverheid een “regelhulp”³ website voor de NIS2. Door het invullen van een aantal vragen krijgt u een indicatieve uitslag (mét voorbehoud) of uw bedrijf wel of niet onder de NIS2 valt. Nuttig, maar de regelhulp is niet gedetailleerd genoeg, en voor verdere details verwijst het gewoon naar de NIS2-wettekst.

Een voorbeeld: u selecteert dat uw organisatie actief is in de sector “Vervaardiging”. Dan geeft de website een aantal categorieën, en verwijst voor sommige door naar een document genaamd “NACE”. Geen uitleg, geen doorklik, niets. Dus het blijft nog even een raadsel of uw bedrijf nu wel, of misschien toch juist niet, onder de NIS2 gaat vallen.



The screenshot shows a web interface with a header bar containing a checkmark and the text 'Vervaardiging' followed by a question mark icon. Below this is a yellow information box with an 'i' icon in the top left and an 'x' icon in the top right. The text inside the box reads: 'Verwijzing naar de informatie over [Bijlage II](#), Sector 5'. Below this are several bullet points, each starting with a hyphen and a bolded title, followed by a description of the entities covered. The categories are: 1. 'Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek', 2. 'Vervaardiging van informaticaproducten en van elektronische en optische producten', 3. 'Vervaardiging van elektrische apparatuur', and 4. 'Vervaardiging van machines, apparaten en werktuigen, n.e.g.'. Each category is followed by a reference to 'NACE Rev. 2' and a specific section and division.

Verwijzing naar de informatie over [Bijlage II](#), Sector 5

- **Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek**
- Entiteiten die medische hulpmiddelen zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2017/745 van het Europees Parlement en de Raad (4) vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek zoals gedefinieerd in artikel 2, punt 2, van Verordening (EU) 2017/746 van het Europees Parlement en de Raad (5) vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen vervaardigen als bedoeld in bijlage I, punt 5, vijfde streepje, van deze richtlijn
- **Vervaardiging van informaticaproducten en van elektronische en optische producten**
- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 26, van NACE Rev. 2
- **Vervaardiging van elektrische apparatuur**
- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 27, van NACE Rev. 2
- **Vervaardiging van machines, apparaten en werktuigen, n.e.g.**
- Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 28, van NACE Rev. 2

Figuur: Verwijzing naar “NACE Rev. 2”

³ Zie: <https://regelhulpenvoorbedrijven.nl/NIS-2-NL/>

Juridisch klopt het wel wat de regelhulp-website aangeeft, maar praktisch is anders. Niet iedereen zal bekend zijn met deze methode van classificatie van bedrijven.

Grootte van het bedrijf

Artikel 3 van de NIS2 specificeert precies welke categorieën bedrijven onder NIS2 vallen: de sectoren uit bijlage 1 en bijlage 2 (hierboven al weergegeven).

Maar puur het actief zijn in een van de genoemde categorieën is niet genoeg. Een bedrijf moet ook een bepaalde omvang hebben. Dat is zo gedaan om kleine bedrijven en ZZP'ers niet te belasten met de NIS2.

Voor het bepalen van de grootte van een organisatie verwijst de NIS2 naar andere (reeds lang bestaande) Europese criteria. Voor de NIS2 is het minimum criterium: of een bedrijf 50 werknemers (of meer) heeft, óf een jaaromzet én balanstotaal van \geq € 10 miljoen. Wie daaronder zit, valt dus niet onder de NIS2.

De exacte definitie van wat "één werknemer" is, is ook vastgelegd. Bijvoorbeeld, hoe hard tellen parttimers⁴ en uitzendkrachten en stagiaires mee, hoe diegenen die pas halverwege het jaar instromen, hoe om te gaan met zwangerschapsverlof, meewerkende eigenaren, etc.? En hoe tellen dochterondernemingen mee, investeerders, en andere juridische constructies? Het valt buiten de doelstelling van dit artikel om dit allemaal precies uit te leggen. Maar dat hoeft ook niet, de EU heeft hierover een goed leesbaar document⁵ opgesteld: "Gebruikersgids bij de definitie van kmo's". Ook is er de website van de RVO⁶ die kan helpen.



Afbeelding: titelpagina van de EU gebruikersgids

⁴ Wij noemen dat FTE's, maar in EU-jargon zijn dat "Annual Work Units", in het Nederlands "Arbeidsjareneenheden".

⁵ Zie: <https://ec.europa.eu/docsroom/documents/42921/attachments/1/translations/nl/renditions/native>

⁶ Zie Rijksdienst voor Ondernemend Nederland: <https://www.rvo.nl/onderwerpen/subsidiespelregels/ezk/mkb-toets>

Essentieel of belangrijk?

De NIS2 richt zich op organisaties die “essentieel” of “belangrijk” zijn voor de Nederlandse samenleving. Dat gaat een stuk verder dan alleen water, stroom, gas en internet.

De criteria om een “essentiële entiteit” te zijn, zijn:

- Actief in een sector uit bijlage 1
- Minimaal 250 werknemers, **of** een jaaromzet van \geq € 50 miljoen én een balanstotaal van \geq € 43 miljoen

De criteria om een “belangrijke entiteit” te zijn:

- Actief in een sector uit bijlage 1 of bijlage 2
- Minimaal 50 werknemers, **of** een jaaromzet én balanstotaal van \geq € 10 miljoen.

Waarom is het onderscheid tussen “essentieel” en “belangrijk” relevant? In de basis worden aan beide dezelfde eisen gesteld. Maar op een aantal punten is het toch anders, en de bijbehorende boetes verschillen ook. Bijvoorbeeld, een audit kan onaangekondigd bij een essentiële entiteit plaatsvinden. Bij een belangrijke entiteit kan ook ge-audit worden, maar alleen na een incident.

Uitzonderingen

Er zijn nog uitzonderingen mogelijk zijn voor het geval dat een bepaalde activiteit in uw bedrijf van ondergeschikt belang is. Anderzijds kan een organisatie ook door de minister nog worden aangewezen⁷ als “essentieel” of “belangrijk”. Het blijft dus van belang om de ontwikkelingen rondom de NIS2 te blijven volgen, eventueel met juridische hulp.

Bedrijven die niet “essentieel”, niet “belangrijk”, en niet door de minister aangewezen, zijn voor de Nederlandse samenleving niet belangrijk genoeg, vallen dan niet onder de NIS2. Dat kan een opluchting zijn, maar moet geen reden zijn om niets aan cybersecurity te doen (maar dat is een ander verhaal).

Terug naar de bron

Zoals hierboven aangegeven, is de overheids-regelhulp geen oplossing voor organisaties die actief zijn in de sector “vervaardiging”. De website verwijst gewoon naar de NIS2-wettekst, en die verwijst weer naar andere documenten.

Dan blijft maar één oplossing over: terug naar de bron.

De tekst van de NIS2 is (uiteraard) op internet⁸ te vinden, zelfs nog vertaald in het Nederlands. Het document is 73 pagina's groot, en ik vond het (als niet-jurist) nog wel redelijk te lezen.

Lastig is wel dat héél vaak verwezen wordt naar andere Europese documenten, die dan ook weer doorverwijzen naar weer andere documenten, etc. Maar in een middag had ik toch wel de uiteindelijke

⁷ Een voorbeeld hiervan is dat ook alle gemeentes in Nederland zijn aangewezen als NIS2-plichtig.

⁸ Nederlandse vertaling: <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555>

precieze definitie van “Vervaardiging” gevonden, en een gedetailleerde opsomming van welke types bedrijven onder deze NIS2 sector vallen (en de uitzonderingen daar op).

Hieronder zal ik bespreken hoe ik in een drietal stappen bij de exacte lijst van bedrijven ben uitgekomen die de NIS2 noemt voor de “Vervaardiging/Manufacturing” sector 5b-5f. Voor andere soorten activiteiten wordt verwezen naar andere Europese wetgeving.

Wat vervaardig ik precies ?

Niet alles wat “vervaardigd” wordt, is NIS2-plichtig. Het maken van bezemstelen of gummen bijvoorbeeld niet. Maar wat wel? Dat staat in de NIS2-tekst, bijlage II, over de sector “Vervaardiging”:

| | | |
|------------------|--|---|
| 5. Vervaardiging | a) Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek | Entiteiten die medische hulpmiddelen zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2017/745 van het Europees Parlement en de Raad (*) vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek zoals gedefinieerd in artikel 2, punt 2, van Verordening (EU) 2017/746 van het Europees Parlement en de Raad (†) vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen vervaardigen als bedoeld in bijlage I, punt 5, vijfde streepje, van deze richtlijn |
| | b) Vervaardiging van informaticaproducten en van elektronische en optische producten | Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 26, van NACE Rev. 2 |
| | c) Vervaardiging van elektrische apparatuur | Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 27, van NACE Rev. 2 |
| | d) Vervaardiging van machines, apparaten en werktuigen, n.e.g. | Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 28, van NACE Rev. 2 |
| | e) Vervaardiging van motorvoertuigen, aanhangers en opleggers | Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 29, van NACE Rev. 2 |
| | f) Vervaardiging van andere transportmiddelen | Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 30, van NACE Rev. 2 |

Figuur: de in de NIS2 genoemde “Vervaardiging” (bron: EU)

Hier dus ook weer verwijzingen naar een andere regeling. Voor sectoren 5b-5f is het de “NACE”⁹, de statistische classificatie van economische activiteiten in de Europese Unie. Dit document bevat een zeer gedetailleerde opsomming van alle mogelijke soorten activiteiten die bedrijven kunnen uitvoeren, van kernreactoren tot puntenslijpers.

Het Nederlandstalige equivalent van de NACE-classificatie is de “SBI”- Standaard Bedrijfsindeling. Deze wordt vastgesteld door de Kamer van Koophandel¹⁰. Het lijkt verder dezelfde nummering. De KVK bepaalt de definitieve SBI-code op basis van de activiteiten van een bedrijf. Via de website van de KVK kan de SBI-code opgezocht worden. Let op dat een bedrijf meerdere SBI-codes kan hebben. Of de SBI-code ook straks gekoppeld wordt aan de Nederlandse wetgeving, is nog niet bekend. De website van het Centraal Bureau voor de Statistiek biedt ook een interactieve SBI browser¹¹

Laten we inzoomen op wat in de vorige figuur onder (d) genoemd is: “Section C division 28”, getiteld “Manufacture of machinery and equipment”. De NACE plaatst hieronder de volgende soorten bedrijven:

⁹ Zie Eurostat: NACE V2: <https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF>

¹⁰ Zie KVK: https://www.kvk.nl/download/Standaard_Bedrijfsindeling_2008_NL_tcm109-510162.pdf

¹¹ Zie CBS: <https://sbi.cbs.nl/>

| | | | | |
|----|-------|--|---|-------|
| 28 | | Manufacture of machinery and equipment n.e.c. | | |
| | 28.1 | Manufacture of general — purpose machinery | | |
| | | 28.11 | Manufacture of engines and turbines, except aircraft, vehicle and cycle engines | 2811 |
| | | 28.12 | Manufacture of fluid power equipment | 2812 |
| | | 28.13 | Manufacture of other pumps and compressors | 2813* |
| | | 28.14 | Manufacture of other taps and valves | 2813* |
| | | 28.15 | Manufacture of bearings, gears, gearing and driving elements | 2814 |
| | | 28.2 | Manufacture of other general-purpose machinery | |
| | | 28.21 | Manufacture of ovens, furnaces and furnace burners | 2815 |
| | | 28.22 | Manufacture of lifting and handling equipment | 2816 |
| | | 28.23 | Manufacture of office machinery and equipment (except computers and peripheral equipment) | 2817 |
| | | 28.24 | Manufacture of power-driven hand tools | 2818 |
| | | 28.25 | Manufacture of non-domestic cooling and ventilation equipment | 2819* |
| | | 28.29 | Manufacture of other general-purpose machinery n.e.c. | 2819* |
| | | 28.3 | Manufacture of agricultural and forestry machinery | |
| | | 28.30 | Manufacture of agricultural and forestry machinery | 2821 |
| | | 28.4 | Manufacture of metal forming machinery and machine tools | |
| | | 28.41 | Manufacture of metal forming machinery | 2822* |
| | | 28.49 | Manufacture of other machine tools | 2822* |
| | | 28.9 | Manufacture of other special-purpose machinery | |
| | 28.91 | Manufacture of machinery for metallurgy | 2823 | |
| | 28.92 | Manufacture of machinery for mining, quarrying and construction | 2824 | |
| | 28.93 | Manufacture of machinery for food, beverage and tobacco processing | 2825 | |
| | 28.94 | Manufacture of machinery for textile, apparel and leather production | 2826 | |
| | 28.95 | Manufacture of machinery for paper and paperboard production | 2829* | |
| | 28.96 | Manufacture of plastic and rubber machinery | 2829* | |
| | 28.99 | Manufacture of other special-purpose machinery n.e.c. | 2829* | |

Figuur: Inhoudsopgave van de NACE Rev. 2 'Afdeling 28' (bron: Eurostat)

De gedetailleerde uitwerking van deze inhoudsopgave omvat 10 velletjes A4, te groot om hier te herhalen. Een voorbeeld van paragraaf 28.41 "Manufacture of metal forming machinery and machine tools":

| |
|---|
| <p>28.4 Manufacture of metal forming machinery and machine tools</p> <p>This group includes the manufacture of metal forming machinery and machine tools, e.g. manufacture of machine tools for working metals and other materials (wood, bone, stone, hard rubber, hard plastics, cold glass etc.), including those using a laser beam, ultrasonic waves, plasma arc, magnetic pulse etc.</p> <p>28.41 Manufacture of metal forming machinery</p> <p>This class includes:</p> <ul style="list-style-type: none"> - manufacture of machine tools for working metals, including those using a laser beam, ultrasonic waves, plasma arc, magnetic pulse etc. - manufacture of machine tools for turning, drilling, milling, shaping, planing, boring, grinding etc. - manufacture of stamping or pressing machine tools - manufacture of punch presses, hydraulic presses, hydraulic brakes, drop hammers, forging machines etc. - manufacture of draw-benches, thread rollers or machines for working wires |
|---|

Figuur: Detailbeschrijving van de NACE 28.41 (bron: Eurostat)

Kortom, al deze machinebouwers vallen dus onder de NIS2. En dit is alleen nog maar paragraaf 41 van sectie 28. Verder in detail gaan de NIS2 en NACE niet.

Conclusie

Met enig zoekwerk op internet zijn alle Europese regelingen makkelijk terug te vinden, en dan zelfs ook nog vaak in het Nederlands. Of uw bedrijf dus wel of niet onder NIS2 gaat vallen, is dus al veel nauwkeuriger te bepalen dan veel eenvoudige samenvattingen van de NIS2 op internet suggereren, of wat de eerdergenoemde “regelhulp” aangeeft. Voor een definitieve vaststelling wordt aanbevolen juridische expertise te raadplegen.

O ja, dan nog dit: de NIS2 betref de cybersecurity van uw bedrijf. Het zegt niets over de cybersecurity van uw *producten* (voor zover toepasselijk, natuurlijk). Dat is een ander verhaal... dat wordt de CRA (Cyber Resilience Act), maar dat duurt nog tot 2026.

De auteur is werkzaam in de industriële cybersecurity. Dit artikel is op persoonlijke titel geschreven.

Updates:

- 25 April 2023 “SBI-code” (Standaard Bedrijfs Indeling) toegevoegd.
- 18 Oktober 2023 Verwijzing naar de “regelhulp” van DTC toegevoegd.
- 28 April 2024 Aanpassing naar huidige situatie, extra uitleg over definitie van kmo's, classificatie