De wet dwingt NIS2 bedrijven en organisaties om de hele keten, dus alle leveranciers, te controleren.

De overheid heeft hierover gepubliceerd. Hier enkele voorbeelden:

Op de website DTC staat veel informatie over de keten in de NIS2. Voorbeelden van risico's:

1. *Een toeleverancier levert niet meer als gevolg van een digitale aanval;*
2. *Je (IT-)dienstverlener is gehackt en hierdoor heeft de aanvaller mogelijk ook toegang tot jouw (digitale) systemen;*
3. *Er is een kritieke kwetsbaarheid ontdekt in één van de (digitale) producten of diensten die je gebruikt in je bedrijfsproces.*

Het eerste punt is kristalhelder: als *Een toeleverancier levert niet meer als gevolg van een digitale aanval,* heeft dat directe impact.

Conclusie: Alleen IT-en OT-risico's bekijken zijn dus NIET meer voldoende.

Oplossing: We hebben een lijst met alle mogelijk type risico leveranciers gemaakt. Zie document **50.000mkb**.

Op de website NCSC staan alle te beschermen belangen en leveranciers

NCSC spreekt in het kader van NIS2 en cybersecurity in het algemeen over de Te Beschermen Belangen en hebben een inspiratielijst opgesteld. Wij hebben die aangevuld met type risicobedrijven. Een voorbeelden van te beschermen belangen:

Financiële belangen:

- Integriteit van financiële gegevens
- Beschikbaarheid van budgetten en prognoses
- Vertrouwelijkheid van salarisadministratie
- Vertrouwelijkheid van bankgegevens en transacties

Deze gegevens liggen vaak buiten bij de accountant, bij de boekhouder en payroll provider. Allemaal leveranciers en zijn dus Te Beschermen Belangen.

Er zijn 12 rubrieken te beschermen belangen met ongeveer 600 leveranciers mogelijk een risico kunnen zijn. **Zie document TBB + 50000mkb**

Op de website van het ministerie van Infrastructuur en Waterstaat

Berenschot rapport in opdracht van ministerie I&W

Berenschot heeft, in opdracht van het ministerie van I&W, onderzoek gedaan naar de NIS2-ketenimpact in de chemische sector. De conclusie: NIS2 heeft een bredere scope dan alleen IT en OT. Er wordt specifiek ingezoomd op fysieke risico's, die ook voortkomen uit de term *alle leveranciers* (Artikel 21.2d).

Het rapport benadrukt dat de toeleveringsketen, inclusief subleveranciers, binnen de reikwijdte van NIS2 valt. Interessante punten:

- **Pagina 8:** Relevante praktijkvoorbeelden.
- **Pagina 11:** Beslisboom, inclusief de *toeleverancier zonder ICT-component*.
- **Pagina 12, punt 3:** Verduidelijking over subleveranciers.

Dit rapport wordt vaak besproken door cyberexperts, omdat het een van de eerste publicaties was die dit onderwerp uitdiepte. Inmiddels, ruim twee jaar later, is de realiteit verder ontwikkeld. Het cascade-effect in de keten bestaat al jaren. Ook zonder NIS2 wordt dit al geregeld, omdat het logisch is: bedrijven vragen leveranciers om een bewijs van cybersecurity in de vorm van certificering.

NIS2-SC10 is de meest geschikte en haalbare certificering voor het gros van de leveranciers. Bij grotere risico's, zoals IT en OT, wordt **NIS2-SC20** of **NIS2-SC30** gebruikt.

https://open.overheid.nl/documenten/2f8a0ad3-8b50-42f0-8b39-62ac59615600/file