Samen Digitaal Veilig

DOSSIER NIS2

CEO/BESTUUR
VERPLICHT AAN HET STUUR

Supply chain cybersecurity raakt vier functies tegelijk

Supply chain cybersecurity onder NIS2 is geen IT-project. Het raakt vier functies tegelijk: de directie, inkoop, IT en HR. Elk met een eigen rol. In dit document bespreken we wat NIS2 van elke functie vraagt en waar het misgaat in de praktijk.

Tot op heden blijkt dat organisaties hiermee worstelen. ENISA, KPMG en IVBB bevestigen dit. ***"A tough nut to crack"*** zegt KPMG. De reden: de NIS2 is nog niet erg bekend, het leveranciersgedeelte vereist samenwerking van meerdere afdelingen én iemand die de regie neemt. Cybersecurity ligt vrijwel altijd op het bord van IT – en die nemen zelden de regie op dit deel.

1. DE CEO / DIRECTIE / BESTUUR

U bent eindverantwoordelijk, ook voor de keten

NIS2 introduceert iets wat veel bestuurders nog niet volledig tot zich hebben laten doordringen: **persoonlijke aansprakelijkheid**. Niet voor het bedrijf in abstracte zin, maar voor u als individu. Als blijkt dat uw organisatie aantoonbaar nalatig is geweest op het gebied van cybersecurity, ook voor de keten, kan dat leiden tot persoonlijke sancties en bestuurdersaansprakelijkheid.

Maar de meeste directies delegeren het onderwerp meteen naar IT, die het oppakken als een technisch project. Het gevolg is een governance-gat: niemand heeft het totaalplaatje in handen en de directie kan niet aantonen dat er bewust is nagedacht over risico's in de keten.

Wat NIS2 van u als CEO vraagt:

- Wijs een verantwoordelijke aan op managementniveau voor het supply chain dossier.
- Stel kaders vast: welke norm verwacht u van leveranciers, en wanneer is een lichtere of zwaardere norm gerechtvaardigd?
- Zorg dat IT, inkoop en HR samenwerken in plaats van ieder afzonderlijk te handelen.
- Leg dit vast: in beleid, in contracten, in het bestuursverslag.

> **Bestuurders zijn verplicht een NIS2-opleiding te volgen binnen 2 jaar na inwerkingtreding (1 juli 2026).**

NIS2 vraagt niet dat u alles zelf uitvoert. Het vraagt dat u aantoonbaar **in control** bent. Dat begint niet bij de IT-afdeling. Dat begint bij u.

2. INKOOP

U zit klem tussen IT en uw leveranciers

Inkoopmanagers bevinden zich in een oncomfortabele positie onder NIS2. Zij zijn eigenaar van de leveranciersrelaties en de contracten, maar hebben vaak geen cybersecurity-expertise en krijgen vanuit IT steeds zwaardere eisen opgelegd die ze niet zelf kunnen beoordelen.

Het resultaat is voorspelbaar: IT vraagt om ISO 27001 voor alle leveranciers, inkoop stuurt de eis door, leveranciers haken af of verhogen hun tarieven. De relatie komt onder druk en niemand heeft nagedacht of die zware eis eigenlijk nodig was.

Belangrijk: NIS2 schrijft geen specifieke norm voor. De wet vraagt ***passende maatregelen op basis van risico***. Een lichte minimumnorm zoals NIS2 Supply Chain SC-10 is voor veel leveranciers wettelijk volledig voldoende en zet de leveranciersrelatie het minst onder druk.

SDV biedt inkoop de volgende tools:

- ERI (Estimated Risk Index) – snelle risicoinschatting per leverancier.
- Werkbaar contractaddendum (NEVI/SDV-model) – kosteloos en juridisch getoetst.
- Systematische leveranciersclassificatie zodat proportionaliteit een onderbouwde keuze is.

Inkoop hoeft geen cyberexpert te worden. Maar inkoop heeft rugdekking nodig van de directie.

3. IT

Focus op techniek en ondersteun de inkoopafdeling

IT-afdelingen spelen een cruciale rol in NIS2-implementatie. Zij kennen de risico's, begrijpen de technische kwetsbaarheden en weten wat er nodig is om systemen veilig te houden. Zonder IT-expertise is supply chain cybersecurity lastig uitvoerbaar.

Maar er is een belangrijk governance-probleem: **IT mag volgens de NIS2 Cyberbeveiligingswet geen bestuurlijke beslissingen nemen.** Deze taak ligt nadrukkelijk bij de directie. IT bepaalt dus niet welke norm inkoop aan leveranciers oplegt, en ook niet of een leverancier voldoet, dat oordeel ligt bij een onafhankelijke auditpartij.

De rol van IT is duidelijk: **inkoop ondersteunen**. Het is inkoop zelf die leveranciers classificeert, normen oplegt, certificaten ontvangt en contractuele voorwaarden vastlegt.

Estimated Risk Index (ERI)

Inzicht in leveranciersrisico's voor NIS2

De ERI geeft organisaties direct inzicht in het digitale risicoprofiel van leveranciers. Op basis van data van circa 170.000 Nederlandse bedrijven helpt de ERI om leveranciers te beoordelen en invulling te geven aan de NIS2 ketenzorgplicht.

Wat u met de ERI kunt:

- Leveranciers indelen in laag, middel en hoog risico
- Prioriteiten stellen in leveranciersbeheer
- Aantoonbaar risicogestuurd werken
- Invulling geven aan de NIS2 leverancierspliicht
- Focus leggen op leveranciers die echt risico vormen

Zonder prioritering is leveranciersmanagement onder NIS2 heel moeilijk uitvoerbaar. Sommige organisaties hebben honderden tot duizenden leveranciers. De ERI lost dit op door snel en onderbouwd te helpen bepalen waar de echte risico's zitten.

4. HR

Bewustwording is geen bijzaak, het is een wettelijke eis

HR is van alle vier de functies de meest onderschatte speler in het NIS2-dossier. NIS2 verplicht organisaties expliciet om bestuurders én medewerkers structureel te trainen op het gebied van cybersecurity, niet eenmalig en niet vrijblijvend.

Het is vaak een menselijke fout die aan de basis ligt van een succesvolle ransomware-aanval. Phishing, social engineering, het doorzetten van een verdacht verzoek: veel supply chain-aanvallen beginnen niet bij technische kwetsbaarheden maar bij mensen.

Zonder aantoonbaar opleidingsprogramma voldoet een organisatie niet aan NIS2. Training verlaagt de kans op menselijke fouten drastisch en is opgenomen als verplichte maatregel in de NIS2 Supply Chain certificeringsnormen.

Concreet vraagt NIS2 van HR om drie dingen:

- Training en bewustwording voor alle medewerkers, afgestemd op rol en risicoprofiel, niet één generieke sessie.
- Aandacht voor de digitale component in onboarding en offboarding: welke toegangen worden gegeven en ingetrokken?
- Aansluiting bij de bredere governance: op basis van kaders die de directie heeft vastgesteld.

Het SDV-platform biedt 28 trainingsvideo's die organisaties direct kunnen inzetten.

Bewustwording is een van de meest kosteneffectieve maatregelen, en onder NIS2 ook een verplichte.

Meer weten? Bezoek **samendigitaalveilig.nl** of mail naar info@samendigitaalveilig.nl