

e-book

# NIS2: Grip op digitale veiligheid en bestuurlijke verantwoordelijkheid





# Inhoud

- 1** Introductie
- 2** Wat is NIS2 en op wie is het van toepassing?
- 3** Niet NIS2-plichtig, wel verantwoordelijk?
- 4** Wat vraagt NIS2 van jouw organisatie?
- 5** Verantwoordelijkheden van bestuurders
- 6** Van risico naar actie: risicomanagement en maatregelen
- 7** Gedragsverandering en meldcultuur
- 8** Concreet aan de slag
- 9** Aanbevelingen voor bestuurders en beslissers
- 10** Bijlage





[Terug naar inhoud](#)

# Introductie

## Goed om te weten

Met de invoering van de NIS2-richtlijn scherpt de Europese Unie de regels voor cybersecurity flink aan. Bestuurders en senior management dragen daarin een sleutelrol en kunnen zelfs persoonlijk aansprakelijk worden gesteld bij non-compliance.

In dit e-book ontdek je:

- ⦿ Wat de NIS2-richtlijn inhoudt en welke organisaties hieronder vallen;
- ⦿ Welke verplichtingen en verantwoordelijkheden voortvloeien uit deze wetgeving;
- ⦿ Hoe je als organisatie risico's in kaart brengt en beheersmaatregelen neemt;
- ⦿ Waarom een meldcultuur, training en bewustwording onmisbaar zijn voor succes.

## Voor wie?

Dit e-book is bedoeld voor bestuurders, directieleden, CISO's, IT-managers en compliance-verantwoordelijken van organisaties die geraakt worden door NIS2 – nu of in de nabije toekomst. Ook partners en leveranciers in de keten vinden hierin waardevolle handvatten om hun rol te verduidelijken en risico's te verkleinen.

## Wat levert het je op?

Na het lezen weet je precies wat NIS2 van je organisatie verlangt en welke stappen je moet zetten om compliant te worden én te blijven. Het helpt je om digitale risico's te beheersen, bestuurders te beschermen tegen aansprakelijkheid en je organisatie weerbaarder te maken tegen de steeds veranderende dreigingen.



[Terug naar inhoud](#)

# Wat is NIS2 en op wie is het van toepassing?

## Belangrijk verschil met NIS1

NIS2 is de opvolger van de eerdere NIS1-wetgeving. Een belangrijk verschil is dat NIS2 voor veel meer organisaties geldt. Waar NIS1 vooral gericht was op vitale infrastructuur, zoals energie en water, breidt NIS2 dit uit naar andere belangrijke en essentiële sectoren.

Voorbeelden van essentiële sectoren zijn energie, vervoer, bankwezen, gezondheidszorg en digitale infrastructuur. Belangrijke sectoren omvatten onder andere postdiensten, voedselproductie, afvalverwerking en digitale dienstverleners. Die uitbreiding is nodig, omdat het dreigingsbeeld is veranderd en er meer sectoren kwetsbaar zijn geworden voor cyberaanvallen.

**Ontdek alle sectoren:** [NIS2 in één overzicht: wat je moet weten](#)

## Let op

NIS2 overlapt deels met de ISO/NEN, maar richt zich specifiek op operationele beveiliging en continuïteit. Beide wetgevingen versterken elkaar, maar kennen andere doelen, verplichtingen en sancties.

**Meer informatie:** [Ben je met ISO of NEN al klaar voor NIS2? Niet helemaal](#)



[Terug naar inhoud](#)

# Niet NIS2-plichtig, wel verantwoordelijk?

## Ook in de keten krijg je met NIS2 te maken

Misschien valt jouw organisatie niet direct onder de NIS2-richtlijn. Je hoort niet bij de aangewezen sectoren, of je organisatie is te klein om onder de formele drempelwaarden te vallen. Maar dat betekent niet dat je niets met NIS2 te maken hebt.

Steeds vaker worden organisaties indirect geraakt, omdat ze onderdeel zijn van de toeleveringsketen van een NIS2-plichtige organisatie. En dat heeft grote gevolgen – voor je verantwoordelijkheden, je commerciële kansen en zelfs je reputatie.

### Hoe werkt dat precies?

NIS2 verplicht organisaties in essentiële en belangrijke sectoren om niet alleen hun eigen beveiliging op orde te hebben, maar ook die van hun leveranciers. Dat betekent dat zij hun ketenpartners gaan controleren op:

- ⦿ Informatiebeveiliging (o.a. ISO 27001 of gelijkwaardige maatregelen);
- ⦿ Incident meldprocedures;
- ⦿ Business continuity plannen;
- ⦿ Contractuele afspraken over verantwoordelijkheid en aansprakelijkheid.

### Concreet voorbeeld

Een ziekenhuis (NIS2-plichtig) maakt gebruik van een softwareleverancier die dossiers digitaal verwerkt. Als deze leverancier slecht beveiligd is en slachtoffer wordt van een ransomware-aanval, heeft dat direct gevolgen voor de continuïteit van het ziekenhuis. Volgens NIS2 moet het ziekenhuis kunnen aantonen dat zij ook deze leverancier hebben meegenomen in hun risicobeoordeling en dat er duidelijke afspraken zijn gemaakt over beveiliging en incidentmelding.



[Terug naar inhoud](#)

# Niet NIS2-plichtig, wel verantwoordelijk?

Ook in de keten krijg je met NIS2 te maken

## Waarom jij dus wél iets moet doen:

### 1. Je komt onder de loop te liggen

NIS2-plichtige klanten zullen je vragen naar je securitybeleid, certificeringen, procedures en meldstructuren. Als je daarop geen antwoord hebt, loop je risico dat je contracten misloopt of verliest.

### 2. Je wordt medeverantwoordelijk

Een lek of incident bij jou kan juridische of financiële gevolgen hebben voor je klant. Die verantwoordelijkheid vertaalt zich steeds vaker in aansprakelijkheidsclausules, boetebepalingen of verplichte audits.

### 3. Je commerciële positie verandert

Organisaties die actief kunnen aantonen dat ze hun informatiebeveiliging op orde hebben, winnen het van concurrenten. Cybersecurity wordt een verkoopargument – geen IT-vraagstuk.

### 4. Je wordt alsnog betrokken bij toezicht

Toezichthouders mogen ketenpartners van NIS2-organisaties bevragen of betrekken bij onderzoek als daar aanleiding toe is. Dat betekent dat je ook zonder directe plicht tóch aan tafel komt bij incidentonderzoeken of audits.

## Wat kun je als leverancier doen?

Wacht niet op vragen van je klant, maar neem zelf het initiatief.

### 🕒 **Breng je risico's in kaart**

Wat kan er gebeuren als jouw systemen of dienstverlening uitvalt bij een NIS2-klant?

### 🕒 **Documenteer je beveiligingsmaatregelen**

Zorg voor een helder overzicht van technische en organisatorische maatregelen. Denk aan toegangsbeheer, backups, versleuteling, monitoring, etc.

### 🕒 **Stel een meldprocedure op**

Laat zien hoe je incidenten detecteert, afhandelt en communiceert. Maak afspraken met klanten over wie wat meldt en wanneer.

### 🕒 **Bespreek contractuele verantwoordelijkheden**

Zorg dat afspraken over informatiebeveiliging en aansprakelijkheid helder zijn vastgelegd.

### 🕒 **Laat je proactief toetsen of certificeren**

Denk aan ISO 27001, NEN 7510 (zorg), of specifieke auditrapportages zoals ISAE 3402. Dit verhoogt je betrouwbaarheid in de keten.



[Terug naar inhoud](#)

# Wat vraagt NIS2 van jouw organisatie?

Je krijgt met de onderstaande onderwerpen te maken

## Verplichtingen

Met de komst van NIS2 krijgen bestuurders en het senior management een grotere verantwoordelijkheid. Zij moeten ervoor zorgen dat hun organisatie de juiste maatregelen neemt om digitale risico's te beheersen en aan de regels te voldoen. Dit betekent onder andere dat zij beleid moeten opstellen én naleven op het gebied van risicomanagement, continuïteit van de bedrijfsvoering, het omgaan met incidenten en het samenwerken met leveranciers en andere partners.

## Risicomanagement

Onder NIS2 moeten organisaties aan een aantal belangrijke verplichtingen voldoen. Zo is het verplicht om een goed risicomanagementbeleid te hebben. Dat betekent dat je als organisatie moet weten welke risico's je loopt, hoe groot die risico's zijn, en wat je doet om ze te beperken.

## Business Continuity

Daarnaast is een business continuity plan verplicht. Dit plan zorgt ervoor dat je als organisatie kunt blijven draaien tijdens én na een incident, zoals een cyberaanval. Belangrijk hierbij is dat je dit plan niet eenmalig opstelt, maar het regelmatig test en bijwerkt.

Ook moet je als organisatie voorbereid zijn op incidenten met een goed incident management beleid. Denk aan duidelijke procedures voor het melden van incidenten, het achterhalen van de oorzaak en het nemen van maatregelen om herhaling te voorkomen.

## Leveranciersmanagement

Tot slot stelt NIS2 ook eisen aan leveranciersmanagement. Je moet ervoor zorgen dat jouw partners in de keten ook veilig werken en zich aan de NIS2-regels houden. Maak daarom heldere afspraken over verantwoordelijkheden en wat er moet gebeuren bij een incident.

## Meldplicht

Onder NIS2 zijn organisaties verplicht om ernstige beveiligingsincidenten snel te melden. Binnen 24 uur moet een eerste melding worden gedaan, zodat de toezichthouder op de hoogte is. Uiterlijk binnen 72 uur moet er een kosteninschatting en een voorstel voor een oplossing worden aangeleverd. Binnen 30 dagen moet het incident helemaal zijn afgehandeld. Lukt dat niet omdat het onderzoek nog loopt? Dan is een duidelijke statusupdate verplicht.

## Toezichthouders

Wie toezicht houdt, hangt af van de sector waarin je actief bent. Voor de meeste organisaties is de Rijksdienst voor Digitale Infrastructuur (RDI) de aangewezen toezichthouder. Werk je in de zorg? Dan valt jouw organisatie waarschijnlijk onder de Inspectie Gezondheidszorg en Jeugd (IGJ).

Er wordt momenteel gewerkt aan een centrale manier van melden, zodat je niet meerdere toezichthouders afzonderlijk hoeft te informeren. Dat moet het melden makkelijker maken en de administratieve druk verlagen.

# Verantwoordelijkheid van bestuurders

## Aansprakelijkheid & verplichte training



### Aansprakelijkheid

Bestuurders krijgen onder NIS2 niet alleen meer verantwoordelijkheid, maar ook meer risico. Ze kunnen namelijk persoonlijk aansprakelijk worden gesteld als hun organisatie de regels niet naleeft. Dit betekent dat zij zelf financieel en juridisch verantwoordelijk kunnen worden gehouden bij fouten of nalatigheid.

De financiële gevolgen kunnen groot zijn. De boetes kunnen oplopen tot 10 miljoen euro of 2% van de wereldwijde jaaromzet – afhankelijk van welk bedrag hoger is. Maar het blijft niet bij geld: bestuurders kunnen ook juridische sancties krijgen, zoals ontslag of persoonlijke rechtszaken.

Daarom is het belangrijk dat bestuurders precies weten wat er van hen wordt verwacht. Training en bewustwording spelen hierin een sleutelrol. Alleen met de juiste kennis kunnen zij hun rol goed vervullen en de risico's voor henzelf én hun organisatie beperken.

### Verplichte training

Onder NIS2 zijn bestuurders verplicht om een training te volgen. Deze training is bedoeld om hen inzicht te geven in de risico's en de maatregelen die nodig zijn om aan de regels te voldoen. Bestuurders leren onder andere over risicomanagement, incident management en hun eigen verantwoordelijkheden onder NIS2.

De training is belangrijk om de rol van bestuurder goed te kunnen vervullen. Het helpt om betere beslissingen te nemen en de organisatie op koers te houden richting compliance. Daarmee verklein je ook het risico op fouten en de financiële of juridische gevolgen van non-compliance.

Kortom: deze training is geen formaliteit, maar een belangrijk hulpmiddel om als bestuurder grip te houden op de digitale veiligheid van je organisatie.





[Terug naar inhoud](#)

# Van risico naar actie: risicomanagement en maatregelen

## Contextbepaling

Goed risicomanagement begint met het begrijpen van de context waarin je als organisatie werkt. Dat betekent dat je niet alleen kijkt naar interne factoren, zoals je processen en systemen, maar ook naar externe invloeden zoals wet- en regelgeving, marktontwikkelingen of toeleveranciers. Dit helpt om risico's beter te herkennen en passende maatregelen te nemen.

Binnen een organisatie kijken mensen op verschillende manieren naar risico's. Iemand op strategisch niveau ziet andere risico's dan iemand op de werkvloer. Het is daarom belangrijk om inzichten te verzamelen uit alle lagen van de organisatie.

Daarnaast is het betrekken van zowel interne als externe stakeholders essentieel. Door in gesprek te gaan met collega's, partners en leveranciers krijg je een completer beeld en voorkom je dat belangrijke risico's over het hoofd worden gezien.

## Risicoanalyse

Het herkennen van risico's is de eerste stap in goed risicomanagement. Daarbij breng je in kaart wat je als organisatie te beschermen hebt (zoals systemen, data of processen), welke dreigingen er zijn, waar je kwetsbaar bent, en wat de mogelijke gevolgen kunnen zijn als er iets misgaat.

## Beheersmaatregelen

Na het identificeren van risico's volgt de analyse. Hierbij kijk je naar hoe groot de kans is dat een risico zich voordoet, en wat de impact zou zijn. Zo kun je bepalen welke risico's de meeste aandacht verdienen en welke maatregelen nodig zijn.

Er zijn vier manieren om risico's te beheersen:

1. Je kunt ze verkleinen, bijvoorbeeld door betere beveiliging;
2. Vermijden, bijvoorbeeld door een risicovolle activiteit niet uit te voeren;
3. Overdragen, bijvoorbeeld door het risico te verzekeren of uit te besteden;
4. Of accepteren, als het risico klein genoeg is.

Het is belangrijk dat risico's duidelijk en specifiek worden beschreven. Vage omschrijvingen maken het lastig om effectieve maatregelen te nemen. Hoe concreter het risico, hoe gericht je het kunt aanpakken.



[Terug naar inhoud](#)

# Gedragsverandering en meldcultuur

## Bewustwording, meldcultuur en training met impact

### Bewustwording begint met gedrag

Informatiebeveiliging is niet alleen een kwestie van technologie en processen, maar draait in grote mate om bewust gedrag binnen de hele organisatie. Medewerkers moeten weten wat hun rol is én gemotiveerd zijn om veilig te werken.

Een cultuurverandering is daarbij essentieel. Iedereen – van directie tot werkvloer – moet informatiebeveiliging serieus nemen. De rol van het management is hierin cruciaal: leidinggevend en moeten het goede voorbeeld geven en actief bijdragen aan een open en veilige werkomgeving.

### Meldcultuur als sleutel tot snelle actie

Een sterke meldcultuur is onmisbaar in het digitale dreigingslandschap, dat steeds complexer wordt. Denk aan CEO-fraude of geavanceerde phishing campagnes – dreigingen die snel schade kunnen aanrichten. Hoe eerder een incident wordt gemeld, hoe kleiner de impact.

Daarom moeten medewerkers zich vrij voelen om incidenten of fouten te melden, zonder angst voor straf of repercussies. Alleen dan kun je als organisatie snel reageren én leren van wat er misgaat. Het draait om vertrouwen, open communicatie en het wegnemen van angst.

De uitdaging is om een balans te vinden: medewerkers motiveren om risico's te melden, zonder een sfeer van wantrouwen of controle te creëren. Een open, lerende houding maakt meldingen normaal en gewenst gedrag.

### Van training naar meetbare impact

Trainingen over cybersecurity en risicobewustzijn zijn een krachtig hulpmiddel om meldgedrag te verbeteren. Tijdens deze sessies leren medewerkers hoe ze bijvoorbeeld phishing, social engineering of verdachte patronen kunnen herkennen én melden.

Om de effectiviteit van die inspanningen aan te tonen, is het belangrijk om meetbare resultaten te koppelen aan bewustwording. Denk aan:

- 🕒 Het aantal gemelde incidenten (zoals phishing pogingen);
- 🕒 De snelheid waarmee meldingen worden gedaan;
- 🕒 Het aantal medewerkers dat deelneemt aan trainingen.

Door dit soort data te verzamelen en te analyseren, kun je gerichte verbeteringen aanbrengen en aantonen dat bewustwording daadwerkelijk bijdraagt aan de digitale weerbaarheid van je organisatie.



[Terug naar inhoud](#)

## Concreet aan de slag

### Inclusief takenlijst

NIS2 naleven vraagt om een combinatie van beleid, techniek én gedrag. De volgende taken en stappen helpen je om grip te krijgen op wat er concreet moet gebeuren – zowel op bestuurlijk als operationeel niveau.

De takenlijst bevat essentiële acties die je organisatie op orde moet hebben, terwijl het

stappenplan helpt bij het vergroten van bewustwording, het verbeteren van leveranciersrelaties en het versterken van je incidentaanpak. Zie het als een praktische leidraad om structureel te bouwen aan digitale weerbaarheid.

**[Bekijk op de volgende pagina de takenlijst.](#)**



[Terug naar inhoud](#)

# Concreet aan de slag

## Takenlijst

### ☺ **Training voor bestuurders**

Organiseer een verplichte training voor bestuurders, zodat zij goed op de hoogte zijn van de NIS2-regels, hun verantwoordelijkheden en de risico's die daarbij horen.

### ☺ **Vorbereiden op wetgeving**

Zorg dat de organisatie klaar is voor de Nederlandse vertaling van NIS2 zodra deze officieel van kracht wordt. Dit voorkomt verrassingen achteraf.

### ☺ **Risicoanalyse voor klanten**

Voer een risicoanalyse uit voor klanten die onder NIS2 vallen en onderzoek wat dit betekent voor je eigen dienstverlening en verantwoordelijkheden.

### ☺ **Registratie onder NIS2**

Registreer je organisatie tijdig, zodat je gebruik kunt maken van beschikbare ondersteuning en weet wat er van je verwacht wordt.

### ☺ **Beoordelen van beheersmaatregelen**

Bekijk of je huidige beveiligingsmaatregelen nog voldoen. Pas ze zo nodig aan om aan de NIS2-eisen te voldoen.

### ☺ **Proces voor incidentmeldingen**

Zorg voor een duidelijk proces waarmee ernstige beveiligingsincidenten binnen 24 uur voorlopig gemeld worden, en binnen 72 uur een kostenanalyse en oplossing worden aangeleverd.

### ☺ **Aantoonbaar toezicht en governance**

Leg vast hoe je risico's en maatregelen beheert, en voer regelmatig evaluaties uit. Zo kun je aantonen dat er actief toezicht is binnen de organisatie.

### ☺ **Afspraken met ketenpartners**

Maak duidelijke afspraken met leveranciers en partners over informatiebeveiliging en de meldplicht bij incidenten. Leg deze vast in contracten.



[Terug naar inhoud](#)

# Stappenplan

**NIS2 helpt om organisaties structureel veiliger te werken**

## 1. Bewustwording rond incidenten

Onderzoek hoe incidenten zoals phishing en datalekken momenteel binnen de organisatie worden gemeld. Is er voldoende acceptatie om dit open te bespreken? Een goed beeld van de huidige situatie is de basis voor verbetering.

## 2. Meldingsbereidheid vergroten

Evalueer in hoeverre medewerkers bereid zijn om incidenten te melden. Identificeer knelpunten en werk aan een cultuur waarin melden als normaal en veilig wordt ervaren.

## 3. Sterk leveranciersmanagement

Zorg voor duidelijke, gedetailleerde contracten met leveranciers, inclusief clausules over informatiebeveiliging en meldplicht. Evalueer deze contracten regelmatig en stel bij waar nodig.

## 4. Exitstrategieën voor leveranciers

Ontwikkel een exitstrategie voor kritieke leveranciers. Leg vast hoe de organisatie snel kan overstappen of doorgaan bij problemen, om continuïteit te waarborgen.

## 5. Actueel Business Continuity Plan (BCP)

Werk een BCP uit dat inspeelt op verschillende scenario's, zoals cyberaanvallen of uitval van systemen. Test dit plan regelmatig en actualiseer het op basis van nieuwe inzichten.

## 6. Communicatieplan bij incidenten

Stel een helder communicatieplan op voor incidenten. Leg daarin vast wie waarvoor verantwoordelijk is, hoe snel er gecommuniceerd moet worden, en via welke kanalen.

## 7. Training en bewustwording

Organiseer structureel trainingen en sessies om medewerkers bewust te maken van actuele dreigingen, zoals phishing en social engineering, én van hun rol in het veilig houden van de organisatie.

## Wetgeving biedt ook kansen

Wetgeving zoals NIS2 zorgt ervoor dat organisaties hun informatiebeveiliging serieus moeten verbeteren. Ze worden verplicht om hun systemen, processen en beleid aan te passen om aan strengere eisen te voldoen.

Dit is geen eenvoudige opgave. NIS2 brengt complexiteit met zich mee en vraagt om tijd, kennis en middelen. Voor veel organisaties is het een flinke uitdaging om alle onderdelen goed op elkaar af te stemmen en volledig compliant te worden.

Toch biedt deze wet ook kansen: het helpt organisaties om structureel veiliger te werken en beter voorbereid te zijn op digitale dreigingen.



[Terug naar inhoud](#)

# Aanbevelingen voor bestuurders en beslissers

## Veiligheid is een proces

De invoering van NIS2 is meer dan een compliance-vraagstuk: het is een kans om de digitale weerbaarheid van je organisatie structureel te versterken. Bestuurders en senior management spelen daarin een sleutelrol. Door nu de juiste stappen te zetten, voorkom je niet alleen boetes of reputatieschade, maar bouw je aan een organisatie die klaar is voor de toekomst.

### Onze aanbevelingen

#### 1. Begin vandaag met bewustwording

Start het gesprek in de directiekamer. Wat weet jouw bestuur al over NIS2? Wat nog niet? Creëer draagvlak en urgentie, voordat je in actie schiet.

#### 2. Organiseer een NIS2-scan of risicoanalyse

Laat vaststellen of je organisatie onder NIS2 valt, waar je staat en waar de risico's zitten. Dit vormt de basis voor je plan van aanpak.

#### 3. Zorg voor betrokken bestuurders

Wijs één of meerdere verantwoordelijken aan binnen het bestuur. Zorg dat zij een verplichte NIS2-training volgen en actief betrokken zijn bij risicobeheersing en compliance.

#### 4. Maak cybersecurity een vast agendapunt

Bespreek digitale veiligheid structureel tijdens directie- of MT-overleggen. Governance vraagt om continuïteit, niet om eenmalige actie.

#### 5. Investeer in gedrag, niet alleen in techniek

Technologie is belangrijk, maar zonder een bewuste organisatiecultuur blijft veiligheid kwetsbaar. Zorg voor blijvende aandacht voor meldcultuur, training en communicatie.

#### 6. Bereid je voor op toezicht en toetsing

Richt je processen zó in dat je kunt aantonen dat je aan de NIS2-verplichtingen voldoet. Documenteer risicoanalyses, incidentprocessen en leveranciersafspraken goed.

### Veiligheid is een proces

De organisaties die NIS2 serieus nemen, leggen een fundament voor vertrouwen, continuïteit en toekomstbestendig leiderschap.

# Bijlage

## Extra content & bronnen

### Blogs over NIS2

- 🕒 [De impact van de cyberbeveiligingswet \(NIS2\) op Nederlandse bedrijven](#)
- 🕒 [NIS2: Waarom jouw rol als bestuurder cruciaal is](#)
- 🕒 [Gebrek aan bestuurlijke betrokkenheid rondom NIS2](#)
- 🕒 [NIS2: Samenwerking in de keten is verplicht](#)
- 🕒 [Zorgplicht NIS2: Tien belangrijke stappen](#)
- 🕒 [NIS2 in één overzicht: wat je moet weten](#)
- 🕒 [NIS2: Begin vandaag met deze 5 praktische stappen](#)
- 🕒 [Ben je met ISO of NEN al klaar voor NIS2? Niet helemaal](#)
- 🕒 [Waarom je nú moet starten met NIS2-voorbereidingen](#)
- 🕒 [Groei in cyberweerbaarheid met het NIS2 Quality Mark](#)
- 🕒 [NIS2 aanpakken? Zet een multidisciplinair team klaar](#)

### Bronnen

- 🕒 [Cyberbeveiligingswet \(NIS2-richtlijn\) | Over het NCSC | Nationaal Cyber Security Centrum](#)
- 🕒 [Samen Digitaal Veilig - Samen Digitaal Veilig](#)
- 🕒 [Homepage - NIS2](#)



EKCO



**Vragen? Neem gerust  
contact met ons op**

✉ [info\\_nl@ek.co](mailto:info_nl@ek.co)

🌐 [www.ekco.nl](http://www.ekco.nl)

☎ 088 – 070 -0600

📍 Nederland