Samen Digitaal Veilig

De makkelijkste oplossing voor een NIS2 veilige toeleveringsketen

Samen Digitaal Veilig is de oplossing voor NIS2 bedrijven die hun supply chain moeten controleren om te voldoen aan de NIS2 toeleveringsketeneisen.

De makkelijkste oplossing voor NIS2 Supply Chain Compliance

Met het Corporate Supply Chain pakket bent u verzekerd van:

- De oplossing voor NIS2-bedrijven om te voldoen aan de verplichting om de beveiliging van hun leveranciers te beoordelen.
- Gestandaardiseerd proces dat tijd en kosten bespaart.

De NIS2-richtlijn vereist een proactieve aanpak van cybersecurity, zowel binnen jouw organisatie als in de gehele supply chain. Naast het beschermen van interne IT-processen, moet je ook de beveiligingsstandaarden en risico's van leveranciers continu monitoren. Dit is de kern van de zorgplicht die NIS2 oplegt. Begin met een grondige risicoanalyse en versterk de ketenbeveiliging van jouw organisatie met een duidelijk stappenplan. Zo beschermt je cruciale processen en voldoe je aan de NIS2-eisen, terwijl je de weerbaarheid tegen cyberrisico's vergroot.

Conformiteit met artikel 21.2d

- Zorgt voor naleving van de wettelijke eisen zoals gesteld in artikel 21.2d van de NIS2-richtlijn.
- Helpt bedrijven te voldoen aan hun verplichting om passende beveiligingsmaatregelen in de toeleveringsketen te garanderen.

Als NIS2-plichtig bedrijf draag je de verantwoordelijkheid voor de veiligheid van je eigen netwerk- en informatiesystemen én voor jouw supply chain. Artikel 21.2d vereist dat je passende technische, operationele en organisatorische maatregelen neemt om risico's te beheersen binnen de gehele keten. Door te voldoen aan de NIS2 wetgeving en jouw zorgplicht actief uit te dragen, minimaliseer je aansprakelijkheid en voorkom je boetes.

Gelaagde veiligheid die past bij het risiconiveau

- Risico gebaseerde benadering: leveranciers worden beoordeeld en waar nodig gecertificeerd op een niveau dat past bij hun specifieke risico.
- Vermijdt overbelasting van leveranciers door onnodig zware eisen. Het voorkomt dat je leveranciers te veel tijd kwijt zijn of te hoge kosten maken.

Wanneer risico's worden geïdentificeerd, moeten duidelijke afspraken met leveranciers worden gemaakt. Het gebruik van een gestandaardiseerde norm is hierbij cruciaal. Binnen Samen Digitaal Veilig werken we met het NIS2 Supply Chain – de meest haalbare en breed toegepaste oplossing voor ketenbeveiliging.

Behoud van de supply chain

- Flexibele certificering voorkomt dat leveranciers afhaken door te hoge eisen.
- Helpt bedrijven hun bestaande supply chain te behouden en te versterken zonder verstoringen.

Een volledig inzicht in de beveiliging van jouw supply chain is essentieel voor effectieve samenwerking met leveranciers. Door samen te werken en inzicht te krijgen in hun beveiligingsstandaarden, verklein je niet alleen de risico's voor je eigen organisatie, maar versterkt je ook de veiligheid van de gehele keten.

Uitvraag bij alle leveranciers

- Een efficiënte uitvraag naar het beveiligingsniveau van alle leveranciers.
- Voorkomt handmatig werk en minimaliseert administratieve lasten.

Een eenmalige controle biedt slechts een momentopname. De NIS2 richtlijn verplicht een doorlopende evaluatie en monitoring van de beveiligings-standaarden van jouw leveranciers. Met het Corporate Supply Chain pakket pas je de PDCA-cyclus effectief toe en houdt je jouw keten continu veilig en compliant.

Transparantie in beveiligingsniveaus

- Directe inzage in het beveiligingsniveau van je leveranciers.
- Zorgt voor een duidelijke en betrouwbare beoordeling van risico's in de keten.

Door met één standaard te werken, verminder je de complexiteit, verlaag je kosten en biedt je jouw leveranciers heldere richtlijnen. Dit zorgt voor een veerkrachtige en stabiele keten, zelfs in crisissituaties.

NIS2 wetgeving: de beveiliging van de toeleveringsketen is verplicht.

Verplicht aan de slag met je leveranciers.

Productiesystemen en machines
Van lopende banden tot verpakkingsmachines: als deze systemen worden gehackt, kunnen productieprocessen stilvallen.

Facilitaire leveranciers
Schoonmaakdiensten of beveiligings-bedrijven met fysieke toegang spelen rol in de veiligheid van je bedrijf.

ICT-dienstverleners en software
Leveranciers die je netwerk, firewalls en back-ups beheren, zijn een stevig risico voor je cyberveiligheid. En ook je software is natuurlijk een risico.

Logistieke partners
Transporteurs en opslagbedrijven zorgen dat je producten op tijd bij klanten komen. Een cyberaanval op hen kan dit proces verstoren.

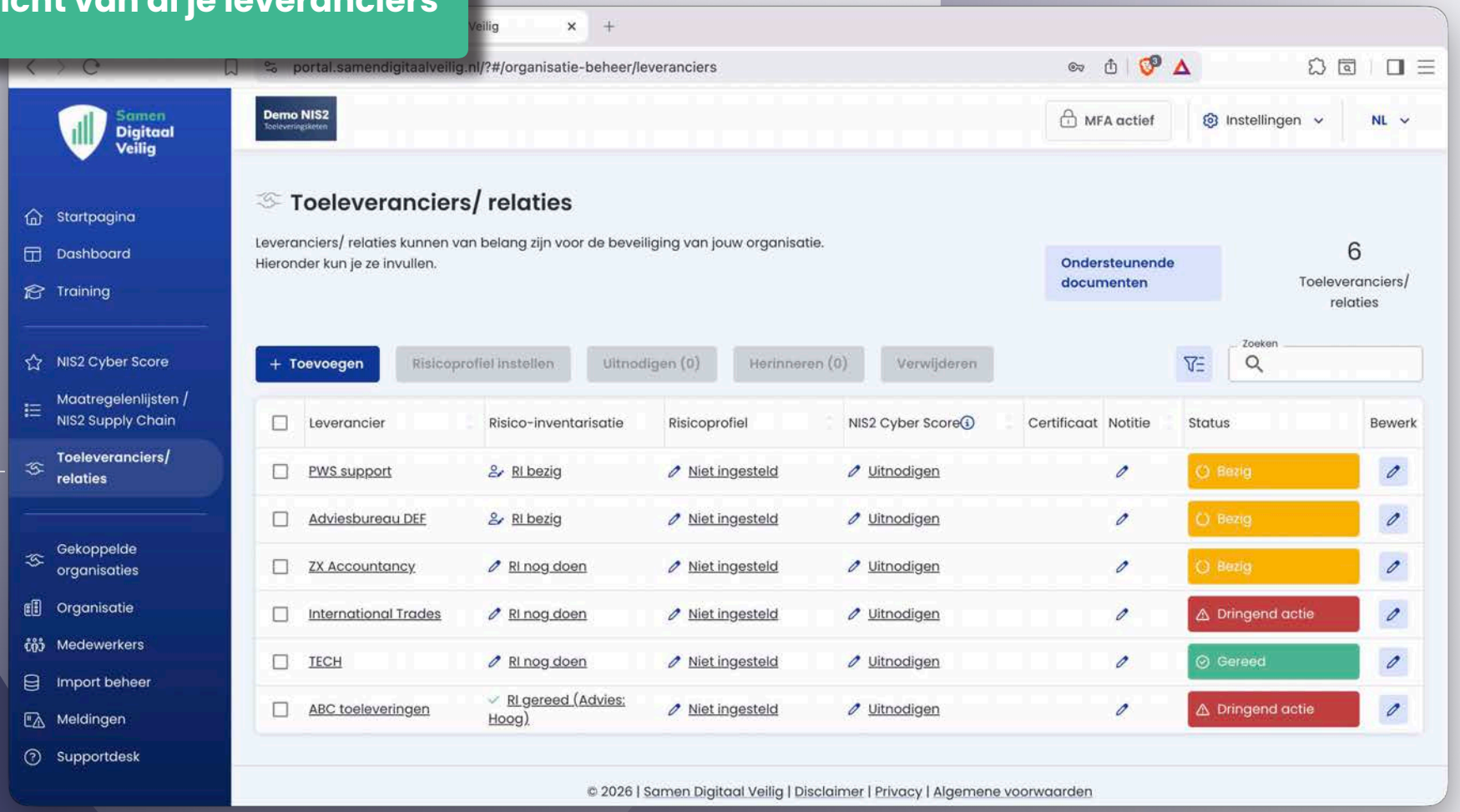
Leveranciers zoals ontwerpers of marketing- en communicatiebureaus
Beschermen van je ontwerpen en patenten voorkomt dat concurrenten technologie en nieuws stelen of gebruiken. Toegang tot vertrouwelijke informatie moet goed beveiligd worden om reputatieschade en verlies van concurrentievoordeel te voorkomen.

Financiële dienstverleners
Je accountant, boekhouder of payroll-provider beheert gevoelige financiële gegevens. Een hack bij hen kan eventueel leiden tot financieel misbruik.

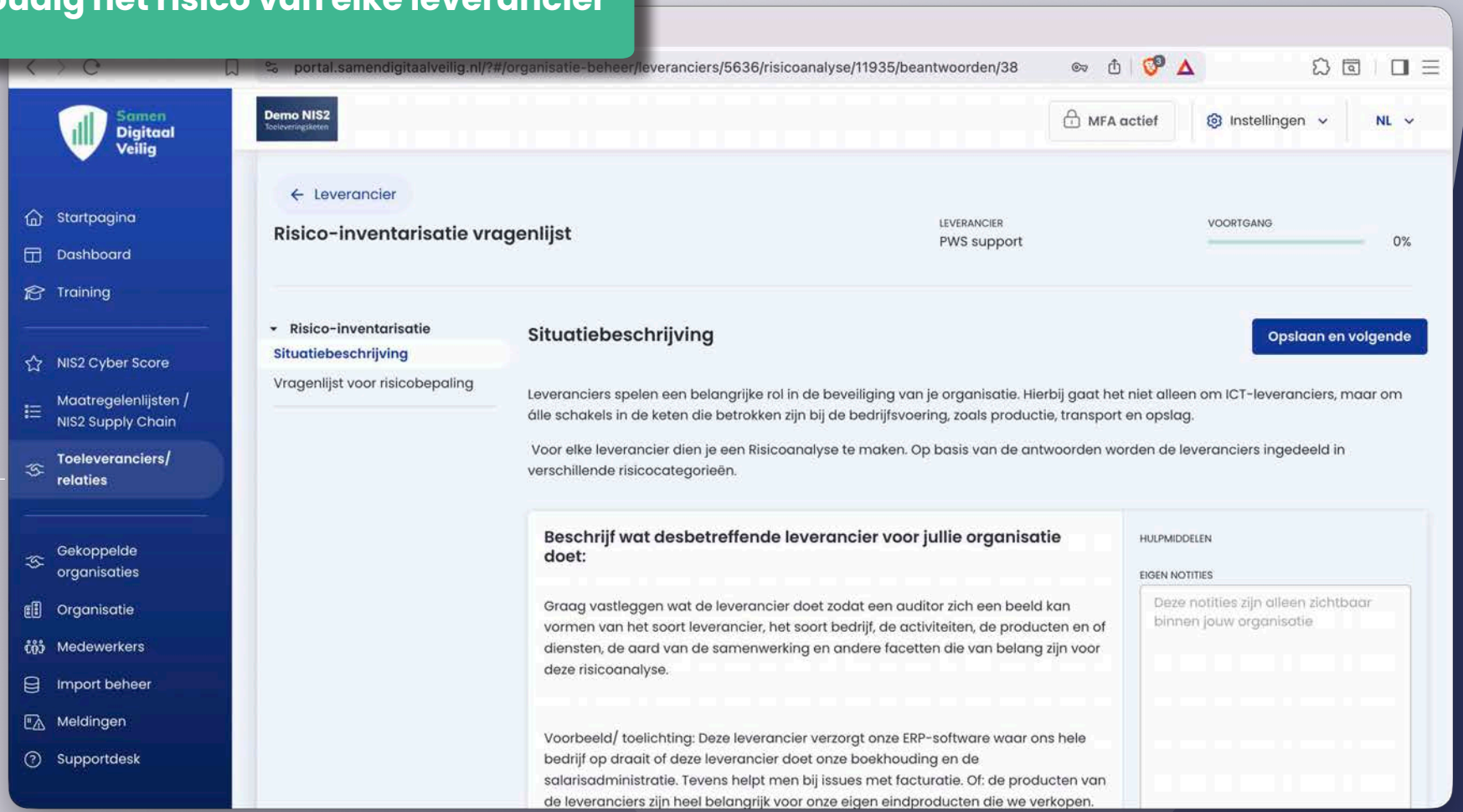
Alle leveranciers zijn een potentieel risico

Voor je bedrijfsprocessen, je plannen, je financiële gegevens, de contracten met grote klanten. Jij bent daar zelf voor verantwoordelijk. Vraag certificering aan je leveranciers. Kijk op **www.samendigitaalveilig.nl/inkoop**

Handig overzicht van al je leveranciers



Bepaal eenvoudig het risico van elke leverancier



Hoe bepaal je welke leveranciers een risico vormen?

Met zoveel leveranciers is het een uitdaging om te bepalen welke een risico kunnen vormen. De NIS2-richtlijn hanteert een *All Hazards*-aanpak, wat betekent dat álle risico's van belang kunnen zijn: IT, OT, fysieke, financiële en andere risico's. Maar waar begin je, en hoe maak je de juiste keuzes?

Wij helpen je op weg! Met ons voorbeeldmateriaal en praktische checklists krijg je snel inzicht. We starten samen bij de kroonjuwelen van je bedrijf: wat moet absoluut beschermd worden? Vervolgens brengen we stap voor stap in kaart welke risico's en bijbehorende leveranciers extra aandacht verdienen.

Zo maak je een slimme en goed onderbouwde start.

Wij ondersteunen je en hebben hiervoor een checklist

Samen Digitaal Veilig

ALL HAZARD

Voorbeelden van risico's in

Voorbeelden van toeleveringsketenrisico's:

- Machineleverancier: hack vertraagt vervangi
- Installatiebedrijf: planning en communicatie
- Freight broker: ransomware-gijzeling leidt to
- Personeelsleverancier voor banken: lekt pe
- Serviceprovider: pinterminals geblokkeerd
- Distributie in transport: ransomware-aanval
- Chemische bedrijven: software werkt niet
- SaaS software leverancier: uitgeverij kan
- Schoonmaakbedrijf: medewerker creëert
- Transportbedrijf: risicovolle situatie bij hac
- Architect: bouwplannen gehackt, vertraag
- Distributiecentrum: opslag en overslag ve
- Ziekenhuis wasserij gehackt: geen hygië
- Trustkantoor: klantdata wordt als chanta
- Clearing house: ligt enkele uren stil door
- Installateurs HVAC-systemen: zorginste
- Opslag chemicaliën: levensgevaarlijke
- Directe leverancier: hack verstoort proc
- Analisten: kunnen hun werk niet doen
- Leverancier van ziekenhuisdeuren: de
- AI-bedrijf met planningssoftware geha
- Productiebedrijf verpakkingsmateriaal
- Verhuurder bedrijfspanden: getroffen

aangetast.
voor infecties.
een hack.
gebruiken, corrupte code geïnfiltreerd
meer.

Samen Digitaal Veilig

HOE CONTROLEER JE GRO

Het is begrijpelijk dat mkb-bedrijven willen vertrouwen o
grote leveranciers zoals Google en Microsoft. Deze grot
doorgaans hun beveiliging goed geregeld. Toch blijft he
nemen om ervoor te zorgen dat jouw bedrijf voldoet aa
uitvoerige controles te hoeven uitvoeren. Hier zijn enke

1. Vertrouwen op certificeringen en rapporten

Je kunt vertrouwen op de certificeringen en auditrappo
bijvoorbeeld naar:

- ISO 27001: een veelgebruikte standaard voor
- SOC 2 Type II: een rapport dat de controles va
  beschikbaarheid, verwerkingsintegriteit, vertro

2. Service Level Agreements (SLA's)

Check de SLA's die je afsluit met deze leveranciers.
beveiligingsmaatregelen beschreven of men verwijs
uitgelegd.

3. Advies inwinnen

Overweeg om advies in te winnen van beveiligings
beoordelen of jouw gebruik van cloud- en software
NIS2.

Hoewel het dus niet altijd haalbaar is voor mkb-be
voeren bij grote leveranciers, kunnen ze vertrouw
duidelijke SLA's.

Disclaimer:

*Samendigitaalveilig.nl neemt de grootst mogelijke zor
onderhoud van de op deze website en/of webapplica
samendigitaalveilig.nl niet garanderen dat deze infor
De informatie verstrekt op en via deze website en/of
algemene informatie en hier kunnen verder geen rec
website en/of webapplicatie kan worden gebruikt om
informatiebeveiliging en internet bedreigingen, maar
(juridisch of technisch) advies, noch als enige garan
internet bedreigingen. Het gebruik van deze website
rekening.*

Samen Digitaal Veilig

NIS2 RISICO'S IN DE KETEN AANPAKKEN

Waarom zijn bedrijven verplicht om aan leveranciers vo
Anders krijgen ze zelf geen positieve audit en geen certifica
van de NIS2.

Levels in de keten

N.B. Er zijn meer levels dan de hierboven genoemde.
van de leverancier (en ook de levels daaronder) kunne
het eerste level van hun eigen leveranciers. Je hoeft d
controleren. Jouw leverancier moet zijn eigen leveranc

Het doel van de NIS2 wetgeving is het voorkomen

Het veilig maken van de keten wordt gerealiseerd doo

1. Inventarisatie van risico's
2. Aankondiging van gewenste compliance naar
3. Opleggen en afspreken van een te halen norm
4. Project opvolgen en vragen naar norm
5. Inkoopvoorwaarden afstemming
6. Ontvangen van norm
7. Jaarlijks opvolgen van je leveranciers

Samen Digitaal Veilig

Digitale veiligheid voor zakelijk Nederland

WAAROM BASIS CYBERHYGIËNE OPLEGGEN AAN ALLE LEVERANCIERS?

In de moderne zakelijke wereld is cybersecurity een cruciale pijler geworden. Met de toename van cyberaanvallen en datalekken is het van groot belang dat bedrijven niet alleen hun eigen systemen beveiligen, maar ook de systemen van hun leveranciers. In dit kader wordt steeds vaker een minimum aan basis cyberhygiënemaatregelen geëist van alle leveranciers. Het NIS2 QM-10 certificaat is hierbij een vaak gehanteerde standaard. Uiteraard zijn er ook andere, zwaardere cybersecuritynormen die men kan opleggen.

Het belang van cyberhygiëne

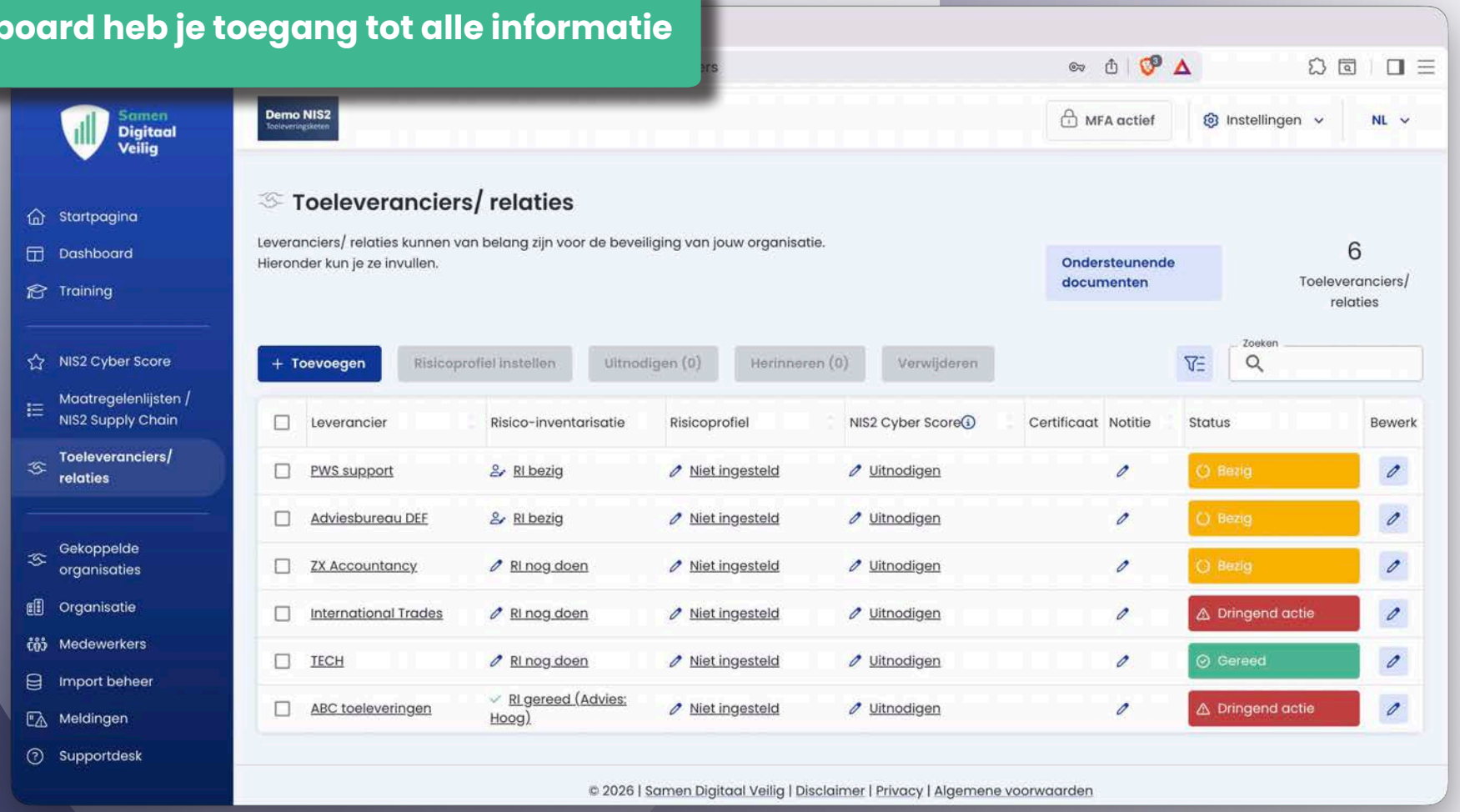
1. Naleving van regelgeving: in veel sectoren en regio's wordt cybersecurity steeds vaker gereguleerd. Het naleven van basis cyberhygiënemaatregelen helpt bedrijven om te voldoen aan wettelijke vereisten en voorkomt boetes en sancties.
2. Bescherming tegen cyberaanvallen: leveranciers vormen vaak een zwakke schakel in de keten. Een succesvolle aanval op een leverancier kan desastreuze gevolgen hebben voor het gehele netwerk. Basis cyberhygiëne helpt bij het verminderen van deze risico's door fundamentele beveiligingsmaatregelen te implementeren.
3. Kostenbesparing op de lange termijn: de financiële impact van een cyberaanval kan enorm zijn. Dit omvat niet alleen de directe kosten van herstel, maar ook de kosten van reputatieschade en juridische consequenties. Door een minimum aan basis cyberhygiëne te eisen, kunnen bedrijven deze risico's aanzienlijk verkleinen en op de lange termijn kosten besparen.
4. Vertrouwen en reputatie: bedrijven di
   opleggen
   reputa
5. Integra
   grote p
   cyberhy
   van ten

Het opleggen van basis cyberhygiëne

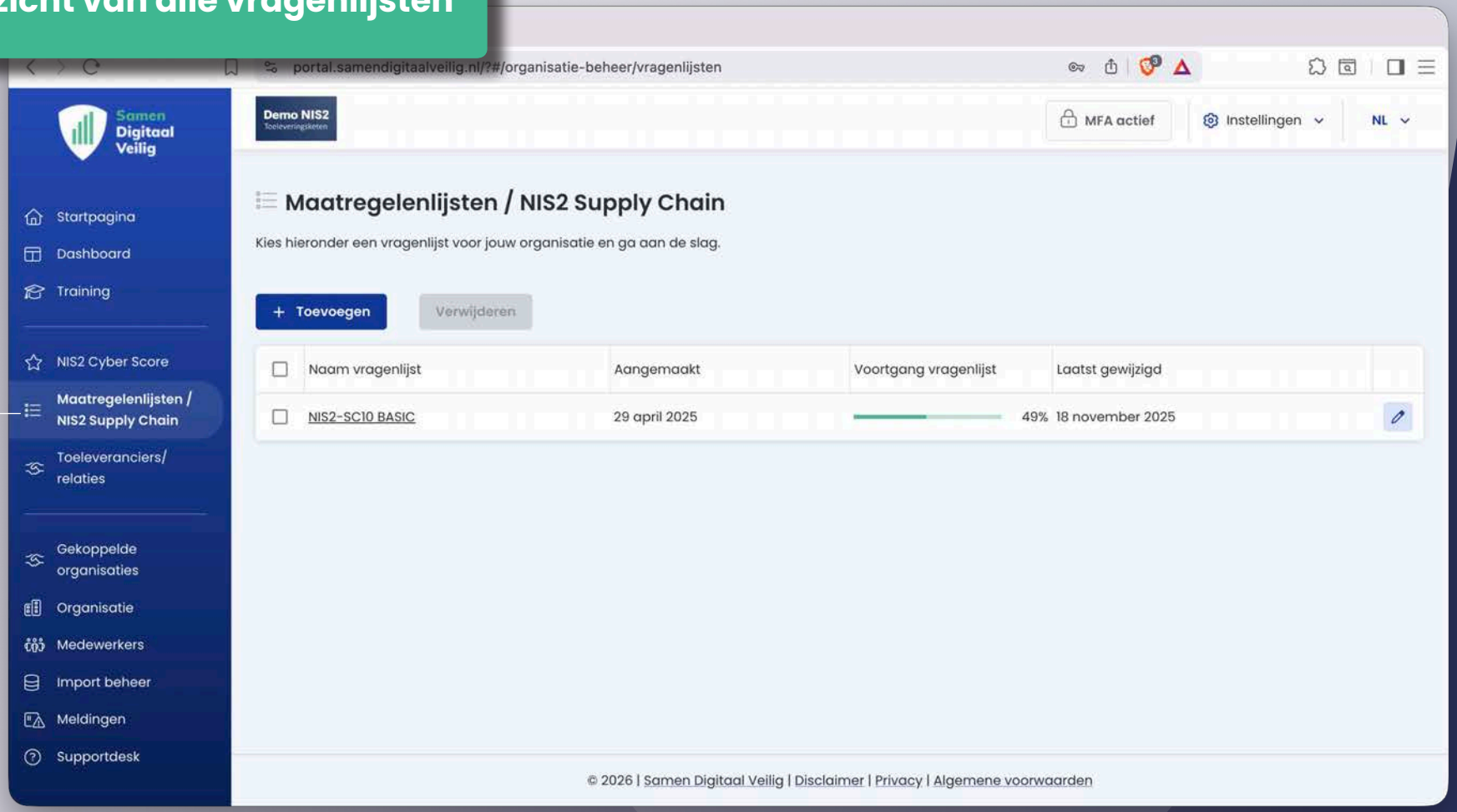
1. Standaardisering in inkoopvoorwaarden: grote bedrijven zijn al enige jaren geleden begonnen met het standaard opnemen van basis cyberhygiënemaatregelen in hun

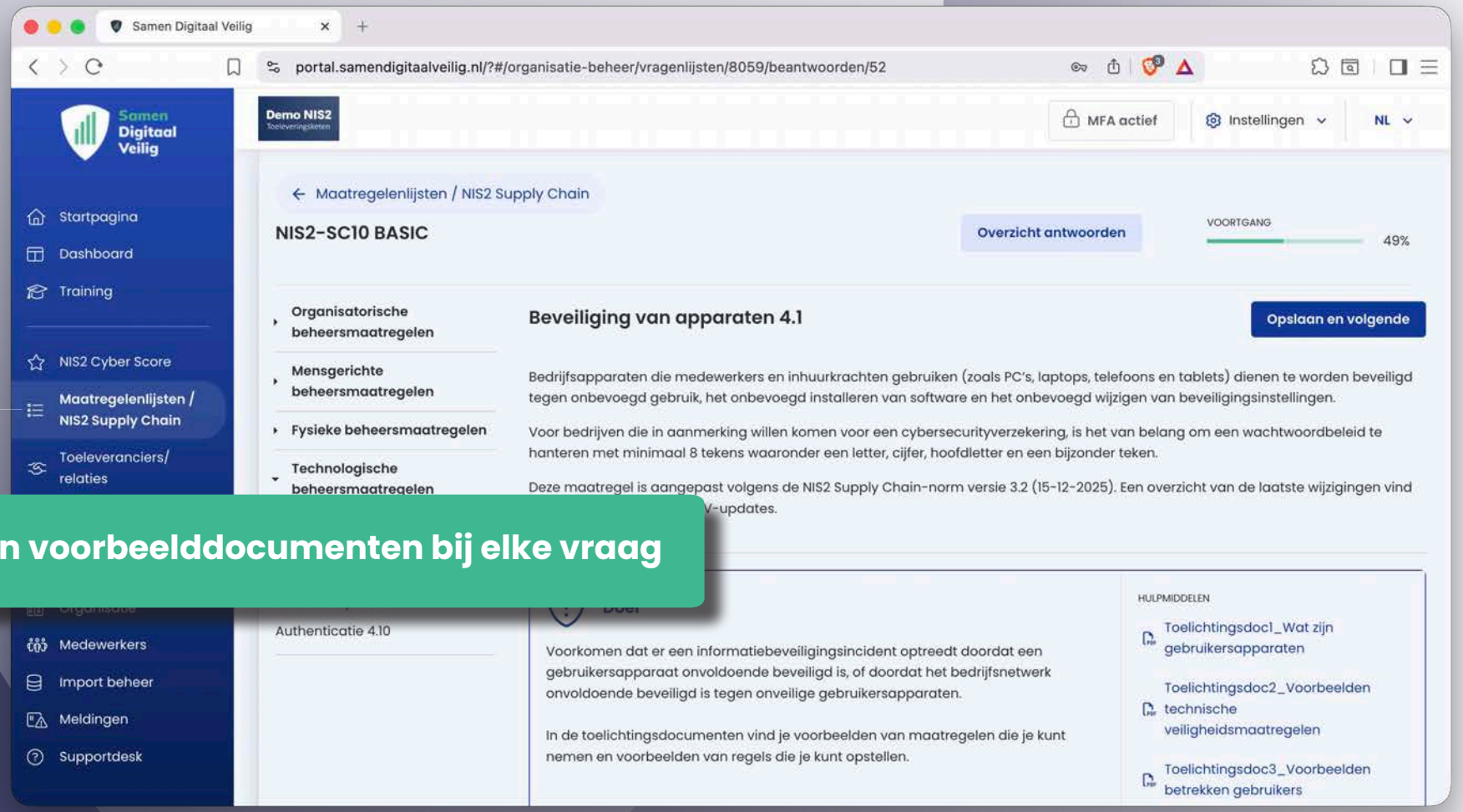
Extra uitleg zodat je alles goed regelt

Via het dashboard heb je toegang tot alle informatie



Handig overzicht van alle vragenlijsten





Toelichting en voorbeelddocumenten bij elke vraag

GAP NIS2 met ISO27001

- Registratieplicht
- Meldplicht
- Opleiding directie
- Strategisch plan inclusief handtekening directie
- Onder toezicht van een toezichthouder (vanuit de overheid dus)
- De leveringsketen is veel zwaarder qua controle en compliance voor jullie (zorgplicht)

Er zijn ook 15 (ook technische) verschillen met ISO 27001

Met Samen Digitaal Veilig voldoet u efficiënt en betrouwbaar aan de zorgplicht eis, zonder onnodige complexiteit.

Vraag onze demo aan

Samen Digitaal Veilig