NIS2: wat het betekent en hoe je actie onderneemt

Huishoudelijke mededelingen

Sprekers

Jerry Hulzink| Ekco

Henk Bijsterbosch| SDV

Slides & Opname

Slidedeck, opname en vragen + antwoorden worden met iedereen na deze sessie gedeeld

Q&A

Heb je tijdens het webinar vragen? Gebruik daarvoor het Q&A (V&A) venster. We proberen alle vragen aan het einde door te nemen.

Over ons

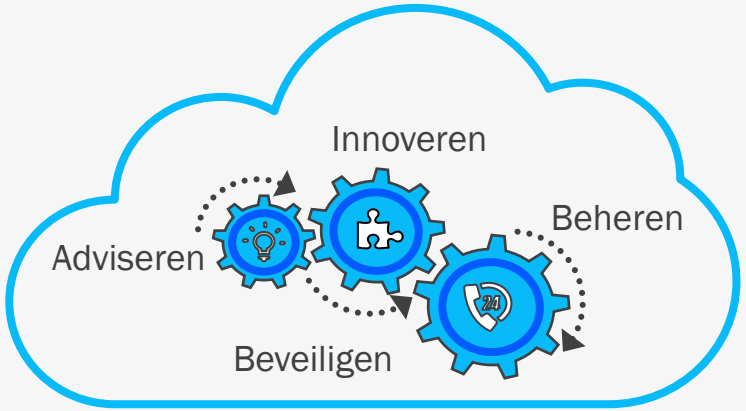
1000+ IT professionals, waarvan ruim 110 in NL

250 security specialisten

42 jaar IT & beheer & beveiliging

17 jaar cloud

Klantbeoordeling ★★★★½



Cloud Services

Workspace Services

Security Services

Managed Services

Business Continuity

Consultancy

Microsoft Gold Partner

Services Premier Support

Microsoft Azure Virtual Desktop Advanced Specialisation

Microsoft Fast Track Partner

DELL Technologies PLATINUM PARTNER

ISAE 3402 TYPE II CERTIFIED

Digitrust ISO 27001

EKCO

Aan de slag met de nieuwe Cyber Beveiligings Wet; NIS2

Agenda

- Introductie
- Over Samen Digitaal Veilig
- NIS2: wat is het ook alweer?
- Zorgplicht in de toeleveringsketen
- Cybersecurity Normering(en)
- Wat betekent dit voor jullie & demo
- Resumé

Even voorstellen

...

- Henk Bijsterbosch
- Partner Manager
- 06-10279705
- ✉ hb@samendigitaalveilig.nl
- Eigenaar: Fortune Consultancy

- Ervaring
  - Consultancy & Advies (oa. NIS2, Change mngt, Proces mngt)
  - Commercieel Directeur Cybersecurity, Infrastructure & Werkplek
  - Stagebegeleider & Assessor HAN

Over Samen Digitaal Veilig

Wij zijn ruim 78 samenwerkende brancheorganisaties die bedrijven helpen met informatie en tooling voor digitale veiligheid. En nu ook voor NIS2.

MKB Nederland

VNO NCW

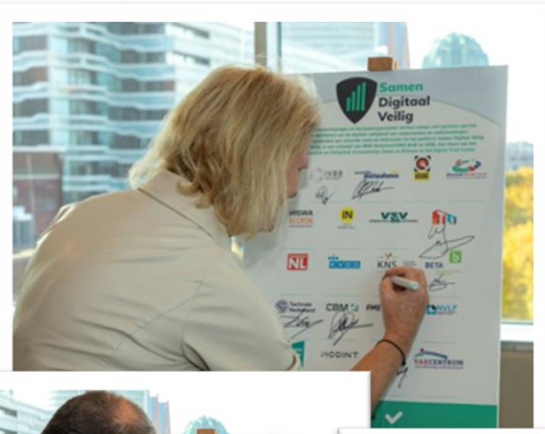
EKCO

Samen Digitaal Veilig

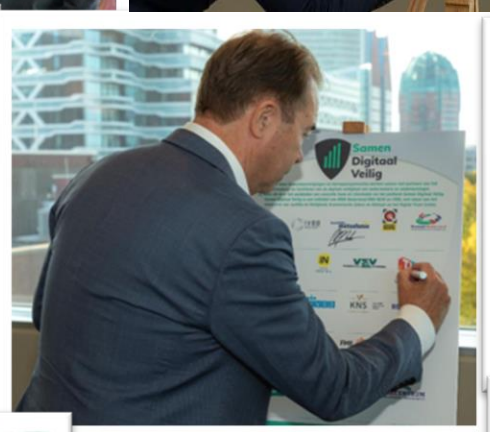
>78 branches. 125.000 bedrijven.

Samen Digitaal Veilig












Stelling 1

De implementatie van de NIS2 richtlijn naar lokale wetgeving is in NL uitgesteld, ik heb nu tijd genoeg om mij voor te bereiden

Antwoord:

Eens	44%
Oneens	55%

NIS2 in één overzicht

Organisaties in kritische sectoren

Grote organisaties

Minimaal 250 medewerkers of netto omzet van meer dan €50 mln én balanstotaal van meer dan €43 mln

Middelgrote organisaties

Minimaal 50 medewerkers of een jaaromzet of balanstotaal van meer dan €10 mln

Sectoren Essentieel

- Afvalwater
- Bankwezen
- Beheerders ICT-diensten
- Digitale infrastructuur
- Drinkwater
- Energie
- Gezondheidszorg
- Infrastructuur financiële markt
- Overheidsdiensten
- Ruimtevaart
- Transport

Sectoren Belangrijk

- Afvalstoffenbeheer
- Chemische stoffen
- Digitale aanbieders
- Levensmiddelen
- Onderzoek
- Post- en koeriersdiensten
- Vervaardiging en manufacturing

Proactief Toezicht | **Reactief Toezicht**

Cybersecurity naar een hoger niveau per 17 okt. 2024*

Toelichting

NIS2 is opvolger NIS-richtlijn EU en zal naar verwachting leiden tot een update van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Uitbreiding toepassingsgebied en maatregelen

Doelstelling

Hoger niveau van cybersecurity bij bedrijven en organisaties

Implementatie

*Oorspronkelijke deadline van 17 oktober 2024 wordt niet gehaald, verwachting is dat de NIS2 vanaf Q1/Q2 2025 in Nederland in zal gaan

Maatregelen, Meldplicht en Controle

Opleiding — Directie e/o bestuur moet een opleiding volgen waarmee voldoende kennis en kunde wordt verkregen om risico's te beheersen

Zorgplicht — Organisaties dienen een risico-inventarisatie uit te voeren en bijbehorende maatregelen te nemen om risico's te beperken

Meldplicht — Melding bij verstoring van de essentiële dienst dient aan desbetreffende toezichthouder en CSIRT aangegeven te worden

Toezicht — Controle op naleving opleiding, zorgplicht en meldplicht verplichtingen, inhoudelijk en waar nodig sancties

Samen Digitaal Veilig

Enkele hoofdpunten uit de NIS2

Technische zaken
- ✔ Backups
- ✔ MFA
- ✔ …..

Proceszaken
- ✔ Planmatig checken alle maatregelen
- ✔ Afspraken maken voor alerts

Organisatorische zaken
- ✔ Risico analyse
- ✔ Meldplicht en zorgplicht regelen
- ✔ Opleiden medewerkers, directie & bestuur

De toeleveringsketen op orde

Actie richting toeleveranciers
- ✔ Aankondiging sturen
- ✔ Risico-inventarisatie bij alle leveranciers
- ✔ Passende norm opleggen
- ✔ Juridisch vastleggen

Samen Digitaal Veilig

NIS2 Maatregelen voor het beheer van cyberbeveiligingsrisico’s voor essentiële en belangrijke entiteiten

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;

b) incidentenbehandeling;

c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;

d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico’s te beoordelen;

g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Samen Digitaal Veilig

Stelling 2

Mijn organisatie is niet NIS2 plichtig, dus ik hoef mij ook niet voor te bereiden

Antwoord:

Eens	6%
Oneens	93%

NIS2 in de keten

NIS2 - Artikel 21.2d

"Beveiliging van de toeleveringsketen, inclusief beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar directe leveranciers of dienstverleners."

- ✔ Uitbreiding maatregelen cyberveiligheid dus ook in de hele keten. Veel problemen ontstaan doordat bedrijven (leveranciers) worden gehackt. Dus die moeten zichzelf ook beter beveiligen omdat het risico daarvan nu ligt bij het NIS2 bedrijf.

Samen Digitaal Veilig

Eerst even een diepe zucht.

Veel werk ……

Samen Digitaal Veilig

Samenwerking in de keten is verplicht

Voor NIS2-bedrijven in genoemde sectoren:

- ✓ Jullie spelen een belangrijke rol in de toeleveringsketen.
- ✓ Jullie cybersecurity moet naar een hoger niveau.
- ✓ Ook jullie eigen leveranciers zijn belangrijk.

Samen Digitaal Veilig

NIS2: zorgplicht in de toeleveringsketen

"Cybersecurity is moeilijk af te spreken zonder norm."

"Kost veel tijd en geld."

"Leveranciers kunnen afhaken of prijsverhogingen doen."

Samen Digitaal Veilig

Welke leveranciers? (Voorbeelden)

Grondstoffen en ingrediënten:
- **Suikerleveranciers**
- **Cacao- en chocoladeleveranciers**
- **Zuivelproductenleveranciers**
- **Noten- en vruchtenleveranciers**
- **Aroma- en smaakstoffenleveranciers**
- **Verpakkingsmateriaal:**

Plastic verpakkingsleveranciers
- **Karton- en papierleveranciers**
- **Glas- en metalen verpakkingsleveranciers**
- **Etiketten en drukwerkleveranciers**

Productieapparatuur:
- **Meng- en kneedmachines**
- **Tempermachines voor chocolade**
- **Verpakkingsmachines**
- **Koel- en vriesapparatuur**
- **Automatiseringssystemen**

Hulpmaterialen en Additieven:
- **Emulgatoren en stabilisatoren**
- **Conserveringsmiddelen**
- **Kleurstoffen**
- **Verdikkingsmiddelen**

Transport en logistiek:
- **Distributiecentra en magazijnen**
- **Transportbedrijven**
- **Koel- en vriestransportdiensten**
- **Kwaliteitscontrole en Laboratoriumdiensten:**

Laboratoriumapparatuur
- **Test- en analysebedrijven**
- **Certificeringsdiensten**
- **Energie en Nutsvoorzieningen:**

Elektriciteitsleveranciers
- **Gasleveranciers**
- **Waterzuiveringsdiensten**
- **Onderhoud en technische Diensten:**

Onderhoudsbedrijven voor apparatuur
- **Kalibratie- en validatiediensten**
- **IT en Softwareoplossingen:**

ERP-systemen
- **Productieplanning en -beheer software**
- **Supply chain management systemen**

Samen Digitaal Veilig

Welke leveranciers? (Voorbeelden)

Bouwmaterialen:
- Cement en beton
- Staal en metaalproducten
- Hout en houtproducten
- Asfalt en bitumen
- Aggregaten en steenslag
- Water- en gasleidingen

Afwerkingsmaterialen:
- Dakbedekking
- Vloeren en tegels
- Verf en coatings
- Scheidingswanden en plafondsystemen
- Verwarmings- en koelsystemen

Installatiematerialen:
- Sanitair
- HVAC: *Leveranciers van verwarmings-, ventilatie- en airconditioningsystemen*
- Elektrische installaties

Bouwchemie:
- Lijmen en afdichtmiddelen
- Isolatiematerialen
- Markeeringsmaterialen

Heavy equipment en gereedschappen:
- Bouwmachines
- Handgereedschap en elektrisch gereedschap
- Asfaltmachines en walsen
- Graafmachines en laadschoppen

Prefab en modulaire bouw:
- Prefab elementen
- Modulaire systemen: *Leveranciers van modulaire bouwsystemen en containerunits*

Dienstverleners:
- Architecten en ingenieursbureaus
- Logistieke dienstverleners
- Duurzame bouwmaterialen
- Recycling en hergebruik
- Adviesbureaus/projecten bureaus
- Engineering & ontwerp

Samen Digitaal Veilig

Welke leveranciers? (Voorbeelden)

- Leveranciers van koel- en vriesunits voor vrachtwagens en bestelwagens
- Technologie en software: Fleet management, routeplanning, logistieke optimalisatie etc.
- Voertuigfabrikanten en distributeurs
- Carrosserie leveranciers
- Banden leveranciers
- Koeling (componenten) leveranciers
- Brandstofleveranciers
- Reserve-onderdelen en onderhoud
- Veiligheids- en/of beschermingsmiddelen
- Verpakking en containerleveranciers.
- Software & Data leveranciers
- Bedrijven die temperatuurmonitoring en tracking oplossingen bieden om de omstandigheden in het laadruim in de gaten te houden.
- Leveranciers van verpakkingsmaterialen voor gekoelde goederen
- Inspectie, service en onderhoudsbedrijven
- Inhuur: bijv. Chauffeurs

Samen Digitaal Veilig

Stelling 3

Ik ben mij bewust van de verantwoordelijkheid richting mijn toeleveringsketen en heb een compleet overzicht van al mijn klanten en leveranciers (incl. contactpersonen)

Antwoord:

Eens	42%
Oneens	57%

NIS2 inkoop en je leveranciers

Artikel 21.2d van de zorgplicht

1. Risico-inventarisatie van al je leveranciers maken (samen met je cybersecurityspecialist).
2. Bepaal het risiconiveau
3. Leg de passende cybersecurity standaard op
4. Zet die standaard in je inkoopvoorwaarden / contracten
5. Ontvang het bewijs van de audit dat de leverancier er aan voldoet

NB

IT kent vaak niet alle details van een leverancierscontract, evt. maatwerk of just in time? IT kan dus zonder input van inkoop of legal een veel te zware norm kiezen voor een toeleverancier! Afstemming tussen inkoop, IT en legal is derhalve van groot belang

Samen Digitaal Veilig

Voorbeeld: Risico inventarisatie vragen

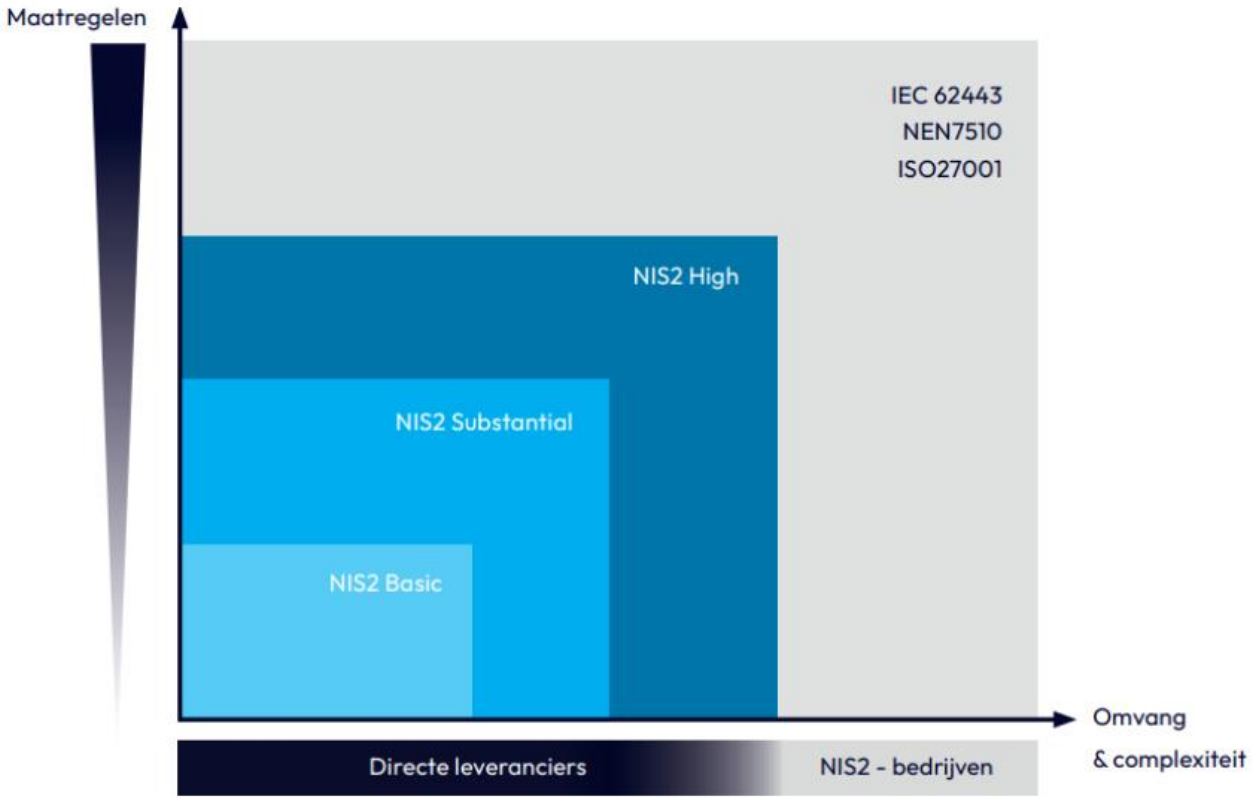
- ❑ Is er e-mailverkeer met de leverancier door één of meerdere van je medewerkers en één of meerdere medewerkers van de leverancier?
- ❑ Gebruik je digitale systemen van deze leverancier binnen de bedrijfsvoering?
- ❑ Hoe lang kun je zonder de producten en/of dienstverlening van deze leverancier zonder dat de bedrijfsvoering wordt verstoord?

Volledige risico-inventarisatie op **www.samendigitaalveilig.nl**

Geen risico is natuurlijk ook een uitkomst

Samen Digitaal Veilig

Optimale normen voor alle bedrijven



NIS2 QUALITY MARK

NB (1): Met ISO27001/NEN7510 ben je (nog) niet NIS2 Compliant

NB (2): NIS2 Quality Mark High is de 1e norm die aansluit op de communicatie van de overheid en past als je geen ISO27001 of andere cybersecurity norm hebt*

** Sluit aan bij de huidige NIS2 EU-Richtlijn*

Samen Digitaal Veilig

Niks mis met ISO of NEN of andere normen.

Pas de juiste normen toe obv het Risico Profiel

Toeleveringsketen beveiligen en passende maatregelen afspreken

Kennispartners

Basic

Dit niveau is vergelijkbaar met wat de overheid hanteert als basis voor cybersecurity. Uitermate geschikt voor veel mkb-bedrijven.

Substantial

Dit niveau is geschikt voor bedrijven die een substantieel risico vormen voor hun klant. Een hack geeft last maar de impact is gemiddeld.

High

Dit niveau is voor leveranciers die een hoog risico vormen voor hun klant als ze niet meer leveren. Een hack heeft een stevige impact op de organisatie.

ISO - NEN

ISO en/of NEN normering is raadzaam als er met een leverancier gewerkt wordt die een extreem hoog risico vormt. Bij een hack ligt het bedrijf direct stil.

Samen Digitaal Veilig

Werk aan de winkel …

Advies: Begin er nu aan

- ✔ Het is veel werk
- ✔ Groot tekort aan cyberspecialisten
- ✔ Je bent verantwoordelijk voor de hele keten

Samen Digitaal Veilig

Wij ondersteunen via SDV platform en bieden ondersteuning bij het halen van het NIS2 Quality Mark samen met partners, w.o.

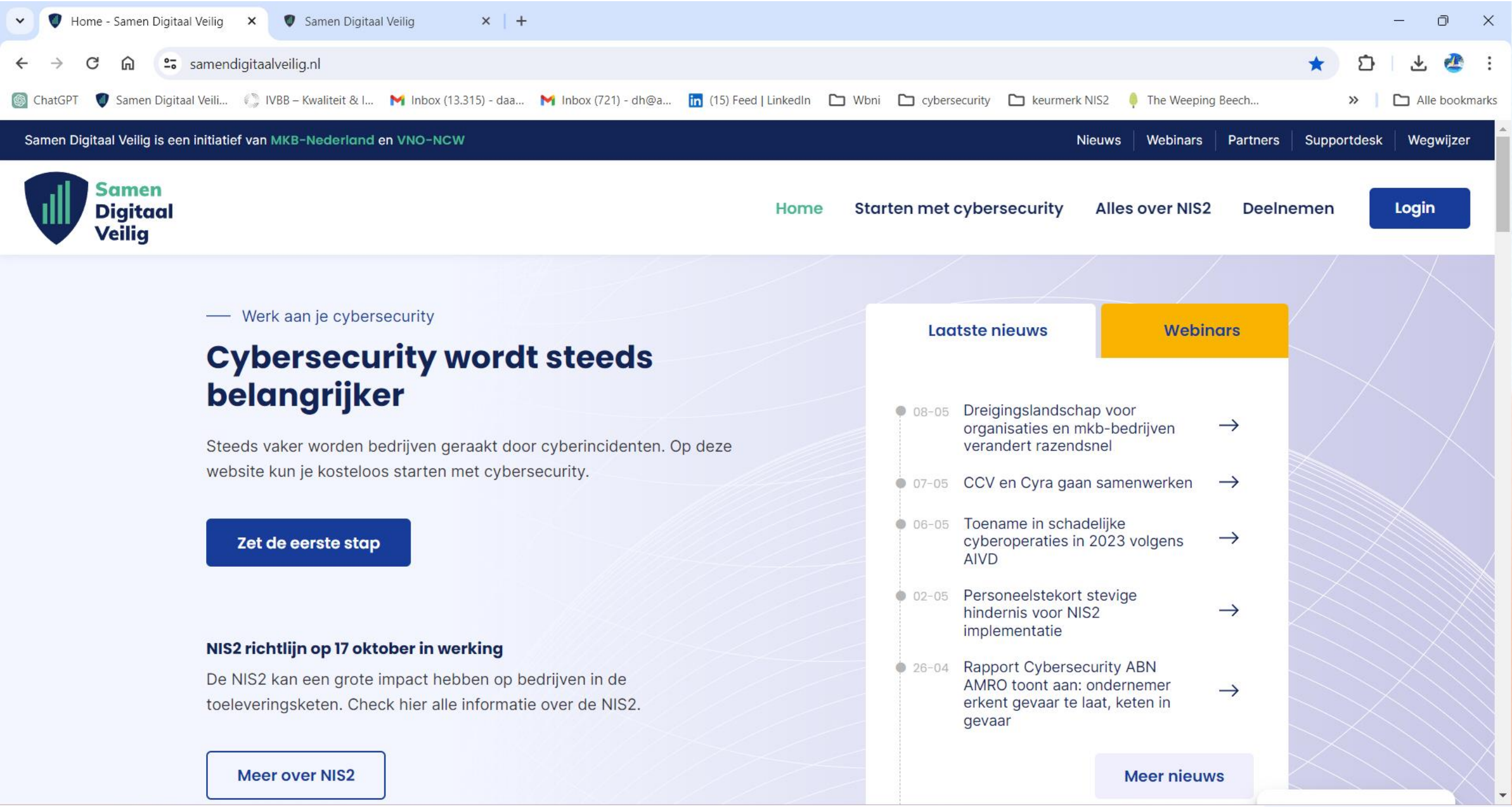
- Online omgeving
- Begrijpelijke taal
- Goed haalbaar

EKCO

Samen Digitaal Veilig

DEMO NIS2 OPLOSSING SDV

- ✓ Waarom moeilijk doen als het makkelijk kan?
- ✓ Zelf controle nemen over de NIS2.
- ✓ Alle stappen doorlopen.
- ✓ Cyber van moeilijk naar tastbaar.
- ✓ Inclusief voorbeelddocumenten


Home - Samen Digitaal Veilig
Samen Digitaal Veilig
samendigitaalveilig.nl
ChatGPT
Samen Digitaal Veili...
IVBB – Kwaliteit & I...
Inbox (13.315) - daa...
Inbox (721) - dh@a...
(15) Feed | LinkedIn
Wbni
cybersecurity
keurmerk NIS2
The Weeping Beech...
Alle bookmarks
Samen Digitaal Veilig is een initiatief van MKB-Nederland en VNO-NCW
Nieuws
Webinars
Partners
Supportdesk
Wegwijzer
Samen Digitaal Veilig
Home
Starten met cybersecurity
Alles over NIS2
Deelnemen
Login
Werk aan je cybersecurity
Cybersecurity wordt steeds belangrijker
Steeds vaker worden bedrijven geraakt door cyberincidenten. Op deze website kun je kosteloos starten met cybersecurity.
Zet de eerste stap
NIS2 richtlijn op 17 oktober in werking
De NIS2 kan een grote impact hebben op bedrijven in de toeleveringsketen. Check hier alle informatie over de NIS2.
Meer over NIS2
Laatste nieuws
Webinars
08-05 Dreigingslandschap voor organisaties en mkb-bedrijven verandert razendsnel
07-05 CCV en Cyra gaan samenwerken
06-05 Toename in schadelijke cyberoperaties in 2023 volgens AIVD
02-05 Personeelstekort stevige hindernis voor NIS2 implementatie
26-04 Rapport Cybersecurity ABN AMRO toont aan: ondernemer erkent gevaar te laat, keten in gevaar
Meer nieuws

Home - Samen Digitaal Veilig | Samen Digitaal Veilig

portal.samendigitaalveilig.nl/?_gl=1*glat3c*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ4Nzk2LjAuMC4w#/inloggen

ChatGPT | Samen Digitaal Veili... | IVBB – Kwaliteit & I... | Inbox (13.315) - daa... | Inbox (721) - dh@a... | (15) Feed | LinkedIn | Wbni | cybersecurity | keurmerk NIS2 | The Weeping Beech... | Alle bookmarks

Samen Digitaal Veilig

Inloggen

NL

E-mailadres

*****@*******.nl

Wachtwoord

••••••••••••••

Wachtwoord vergeten?

Inloggen

Nieuw bij Samen Digitaal Veilig?

Wil je deelnemen aan Samen Digitaal Veilig maar heb je nog geen account?

Nieuw account aanmaken

Startpagina
Dashboard NIS2
Ontvangen vragenlijsten
Mijn training
NIS2 Quality Mark
Organisatie
Medewerkers
Leveranciers
Meldplicht
Beheer
Supportdesk

Startpagina Samen Digitaal Veilig

Op deze pagina vind je alle informatie en links voor het gebruik van Samen Digitaal Veilig. Kies het juiste blokje en volg de instructies. Daarnaast kun je webinars volgen voor begeleiding en uitleg.

NIS2 Quality Mark halen
Voldoe aan de cybersecurityeisen van grote bedrijven of als onderdeel van je groeistrategie deze noodzakelijk is.

Abonnementen
Welke versie van SDV-abonnementen is voor mijn organisatie het meest geschikt?

Ketenzorgplicht
Zorg dat jij voldoet aan de ketenzorgplicht. Zo kunnen wij je hierbij helpen.

Medewerkers & training
Medewerkers zijn cruciaal voor de veiligheid van jouw organisatie.

Beheerders
Je bedient namens jouw organisatie dit platform en deelt taken uit.

Dashboarding
Inzicht in jouw keten. Verschillende dashboards voor jouw organisatie.

Vragenlijsten
Controleer jouw organisatie en keten door middel van vragenlijsten.

Alerts en meldingen
Wat moet je doen bij welk datalek? Welke meldingen kan ik van leveranciers verwachten.

Ben jij een NIS2 bedrijf?

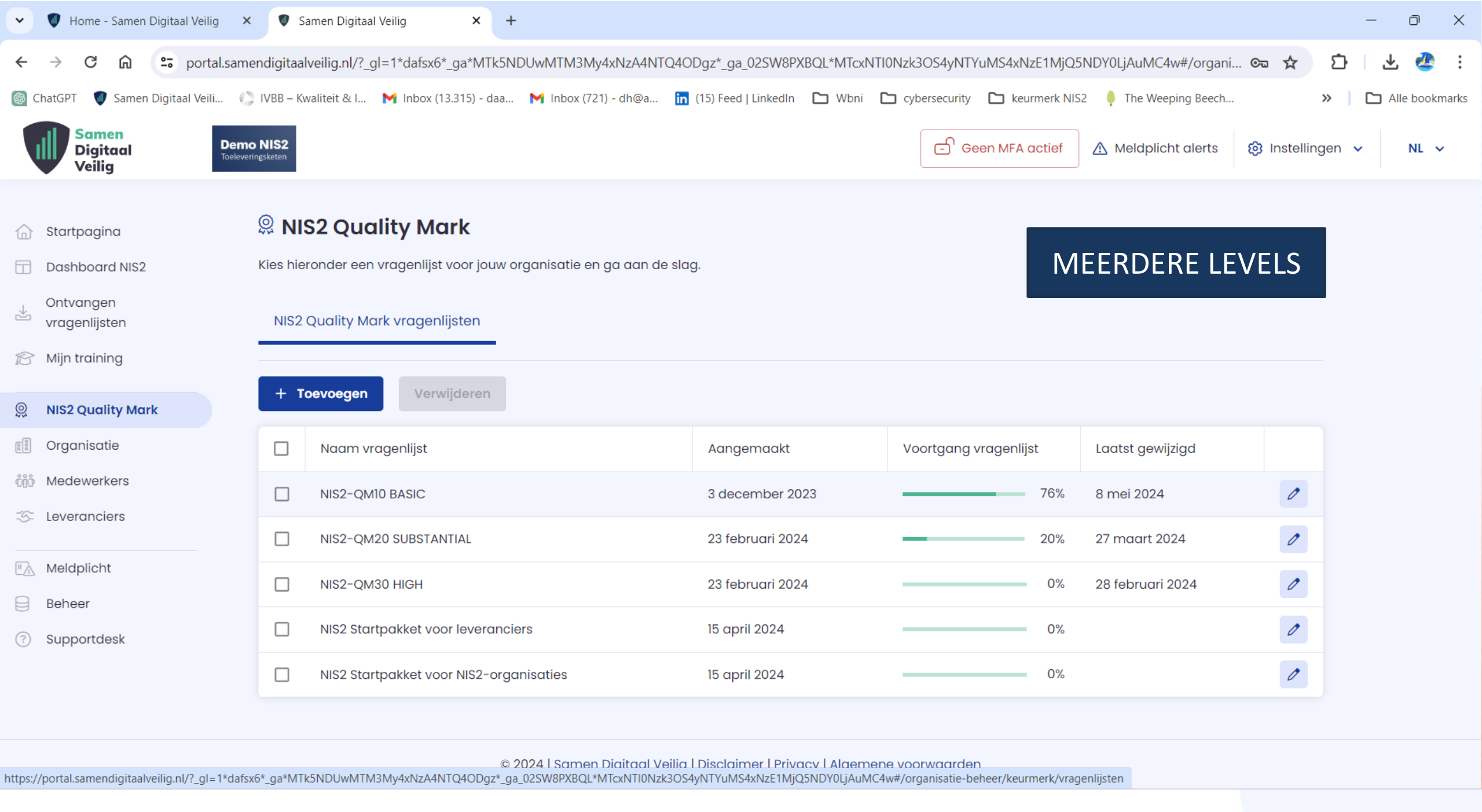
Controleer hier of jij een NIS2 bedrijf bent. Kijk wat je dan allemaal moet doen en hoe wij jou hierbij kunnen helpen.

Nu controleren

Zoek je ondersteuning?

Voldoen aan NIS2 is niet altijd gemakkelijk. Wij staan klaar om je te helpen te voldoen aan de cybersecurityeisen.

Ik wil ondersteuning


Home - Samen Digitaal Veilig
Samen Digitaal Veilig
portal.samendigitaalveilig.nl/?_gl=1*dafsx6*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ5NDY0LjAuMC4w#/organi...
ChatGPT
Samen Digitaal Veili...
IVBB – Kwaliteit & I...
Inbox (13.315) - daa...
Inbox (721) - dh@a...
(15) Feed | LinkedIn
Wbni
cybersecurity
keurmerk NIS2
The Weeping Beech...
Alle bookmarks
Samen Digitaal Veilig
Demo NIS2
Toeleveringsketen
Geen MFA actief
Meldplicht alerts
Instellingen
NL
Startpagina
Dashboard NIS2
Ontvangen vragenlijsten
Mijn training
NIS2 Quality Mark
Organisatie
Medewerkers
Leveranciers
Meldplicht
Beheer
Supportdesk
NIS2 Quality Mark
Kies hieronder een vragenlijst voor jouw organisatie en ga aan de slag.
MEERDERE LEVELS
NIS2 Quality Mark vragenlijsten
+ Toevoegen
Verwijderen
Naam vragenlijst
Aangemaakt
Voortgang vragenlijst
Laatst gewijzigd
NIS2-QM10 BASIC
3 december 2023
76%
8 mei 2024
NIS2-QM20 SUBSTANTIAL
23 februari 2024
20%
27 maart 2024
NIS2-QM30 HIGH
23 februari 2024
0%
28 februari 2024
NIS2 Startpakket voor leveranciers
15 april 2024
0%
NIS2 Startpakket voor NIS2-organisaties
15 april 2024
0%
© 2024 | Samen Digitaal Veilig | Disclaimer | Privacy | Algemene voorwaarden
https://portal.samendigitaalveilig.nl/?_gl=1*dafsx6*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ5NDY0LjAuMC4w#/organisatie-beheer/keurmerk/vragenlijsten

Home - Samen Digitaal Veilig | Samen Digitaal Veilig

portal.samendigitaalveilig.nl/?_gl=1*dafsx6*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ5NDY0LjAuMC4w#/organi...

ChatGPT | Samen Digitaal Veili... | IVBB – Kwaliteit & I... | Inbox (13.315) - daa... | Inbox (721) - dh@a... | (15) Feed | LinkedIn | Wbni | cybersecurity | keurmerk NIS2 | The Weeping Beech... | Alle bookmarks

Samen Digitaal Veilig

Demo NIS2 Toeleveringsketen

Geen MFA actief | Meldplicht alerts | Instellingen | NL

- Startpagina
- Dashboard NIS2
- Ontvangen vragenlijsten
- Mijn training
- NIS2 Quality Mark
- Organisatie
- Medewerkers
- Leveranciers
- Meldplicht
- Beheer
- Supportdesk

← NIS2 Quality Mark

NIS2-QM10 BASIC

LIJST MET NIS2 ONDERWERPEN

Overzicht antwoorden

VOORTGANG 76%

- Organisatorische beheersmaatregelen
  - Beleidsvorming
  - Verantwoordelijk
  - Informatie
  - ICT-bedrijfsmiddelen
  - Bedrijfsmiddelen
  - Bepalen van toegangsrechten
  - Voorbereiding en optimalisati...
  - Samen de toeleveringsketen ...
- Mensgerichte beheersmaatregelen
- Fysieke beheersmaatregelen
- Technologische beheersmaatregelen

Beleidsvorming

Opslaan en volgende

Beleidsvorming voor informatiebeveiliging (cyberhygiëne) en bestuurlijke goedkeuring

Om aan de beheersmaatregel **Beleidsvorming voor informatiebeveiliging (cyberhygiëne) en bestuurlijke goedkeuring** te voldoen, is er minimaal een goed cyberhygiënebeleid nodig dat is goedgekeurd door het management en gedeeld met alle betrokkenen (personeel en andere relevante belanghebbenden).

Je hebt een door het management goedgekeurd plan nodig voor je cybersecurity

Je gaat een plan (het cyberhygïenebeleid) opstellen. In dit beleid leg je d.m.v. richtlijnen vast hoe de informatie van de organisatie beschermd wordt. Ook vermeld je wie contactpersonen zijn en zorg je voor trainingen voor bestuurders en personeel. Formele bestuurlijke goedkeuring voor je plan is een must.

In de toelichtingsdocumenten aan de rechterkant krijg je een voorbeeld van een plan, uitleg over welke regels je hierin kunt opnemen en hoe je je plan periodiek kunt beoordelen.

HULPMIDDELEN

- Cyberhygiënebeleid
- Onderwerp- specifieke beleidsregels
- Cyberhygiënebeleid beoordelen

https://portal.samendigitaalveilig.nl/?_gl=1*dafsx6*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ5NDY0LjAuMC4w#/organisatie-beheer/keurmerk/424/beantwoorden/41

Home - Samen Digitaal Veilig | Samen Digitaal Veilig

portal.samendigitaalveilig.nl/?_gl=1*dafsx6*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ5NDY0LjAuMC4w#/organi...

ChatGPT | Samen Digitaal Veili... | IVBB – Kwaliteit & I... | Inbox (13.315) - daa... | Inbox (721) - dh@a... | (15) Feed | LinkedIn | Wbni | cybersecurity | keurmerk NIS2 | The Weeping Beech... | Alle bookmarks

Samen Digitaal Veilig

Demo NIS2 Toeleveringsketen

Geen MFA actief | Meldplicht alerts | Instellingen | NL

- Startpagina
- Dashboard NIS2
- Ontvangen vragenlijsten
- Mijn training
- NIS2 Quality Mark
- Organisatie
- Medewerkers
- Leveranciers
- Meldplicht
- Beheer
- Supportdesk

← NIS2 Quality Mark

NIS2-QM10 BASIC

LIJST MET NIS2 ONDERWERPEN

Overzicht antwoorden

VOORTGANG 76%

- Organisatorische beheersmaatregelen
  - Beleidsvorming
  - Verantwoordelijk
  - Informatie
  - ICT-bedrijfsmiddelen
  - **Bedrijfsmiddelen**
  - Bepalen van toegangsrechten
  - Voorbereiding en optimalisati...
  - Samen de toeleveringsketen ...
- Mensgerichte beheersmaatregelen
- Fysieke beheersmaatregelen
- Technologische beheersmaatregelen

Bedrijfsmiddelen

Inleveren bedrijfsmiddelen na gebruik

Opslaan en volgende

Om te voldoen aan de beheersmaatregel **Het inleveren van bedrijfsmiddelen na gebruik,** heeft de organisatie een duidelijk beleid nodig rondom het teruggeven van bedrijfsmiddelen. Simpel gezegd: iedereen die de organisatie verlaat, moet alle spullen die ze van de zaak hebben, weer netjes inleveren. Hiervoor zijn een vastgestelde procedure en checklist nodig.

Als werknemers vertrekken, moeten ze computers, smartphones etc. van de zaak inleveren.

Om vertrouwelijke informatie niet in verkeerde handen te laten vallen, is het belangrijk dat als iemand de organisatie verlaat, diegene ook zijn bedrijfsmiddelen inlevert.

Je stelt een procedure en checklist op voor het inleveren van bedrijfsmiddelen.

Kijk in de toelichtingsdocumenten aan de rechterkant voor voorbeelden van procedures en checklists.

HULPMIDDELEN

- Procedures
- Checklist

Samen Digitaal Veilig

KANT-EN –KLARE TEMPLATES

HET INLEVEREN VAN BEDRIJFSMIDDELEN NA GEBRUIK

Checklist

VOORBEELD VAN EEN UITGEWERKTE CHECKLIST

Een checklist voor het inleveren van bedrijfsmiddelen na gebruik kan dienen als een handige tool voor zowel de medewerker die vertrekt als de organisatie. Hieronder zie je een voorbeeld van een uitgewerkte checklist voor het inleveren van bedrijfsmiddelen na gebruik bij een IT-bedrijf.

Checklist voor het inleveren van bedrijfsmiddelen na gebruik bij [IT-bedrijf]

Checklist voor het inleveren van bedrijfsmiddelen na gebruik bij [IT-bedrijf]

Persoonlijke gegevens

- ❑ Naam van de medewerker
- ❑ Afdeling
- ❑ Laatste werkdag

Apparatuur en elektronica

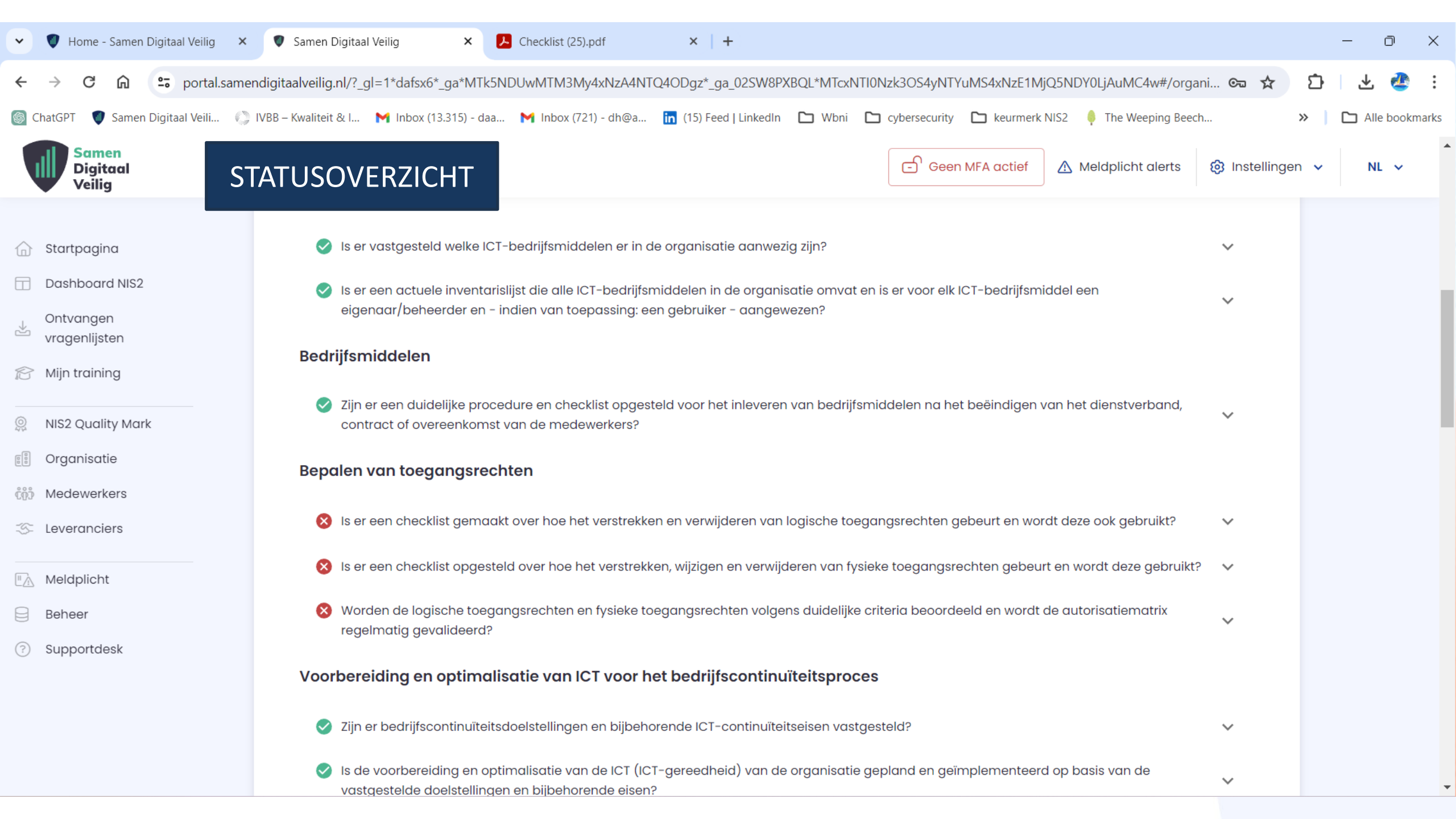
- ❑ Laptop (inclusief lader en eventuele extra's zoals muizen of toetsenborden)
- ❑ Mobiele telefoon (inclusief oplader)
- ❑ Externe harde schijven of USB-sticks
- ❑ Headset / Oortjes

Toegangsmiddelen

- ❑ Toegangspas / ID-kaart
- ❑ Parkeerkaart
- ❑ Sleutels (gebouw, kluis, kantoor)

Software en data

- ❑ Terugzetten van alle bedrijfsgegevens naar het bedrijfsnetwerk
- ❑ Verwijdering van persoonlijke bestanden
- ❑ Uitloggen uit bedrijfsaccounts (e-mail, projectmanagementtools, etc.)
- ❑ Verwijderen medewerker uit toegangsbeheersysteem


Home - Samen Digitaal Veilig
Samen Digitaal Veilig
Checklist (25).pdf
portal.samendigitaalveilig.nl/?_gl=1*dafsx6*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ5NDY0LjAuMC4w#/organi...
ChatGPT
Samen Digitaal Veili...
IVBB – Kwaliteit & I...
Inbox (13.315) - daa...
Inbox (721) - dh@a...
(15) Feed | LinkedIn
Wbni
cybersecurity
keurmerk NIS2
The Weeping Beech...
Alle bookmarks
Samen Digitaal Veilig
STATUSOVERZICHT
Geen MFA actief
Meldplicht alerts
Instellingen
NL
Startpagina
Dashboard NIS2
Ontvangen vragenlijsten
Mijn training
NIS2 Quality Mark
Organisatie
Medewerkers
Leveranciers
Meldplicht
Beheer
Supportdesk
Is er vastgesteld welke ICT-bedrijfsmiddelen er in de organisatie aanwezig zijn?
Is er een actuele inventarislijst die alle ICT-bedrijfsmiddelen in de organisatie omvat en is er voor elk ICT-bedrijfsmiddel een eigenaar/beheerder en - indien van toepassing: een gebruiker - aangewezen?
Bedrijfsmiddelen
Zijn er een duidelijke procedure en checklist opgesteld voor het inleveren van bedrijfsmiddelen na het beëindigen van het dienstverband, contract of overeenkomst van de medewerkers?
Bepalen van toegangsrechten
Is er een checklist gemaakt over hoe het verstrekken en verwijderen van logische toegangsrechten gebeurt en wordt deze ook gebruikt?
Is er een checklist opgesteld over hoe het verstrekken, wijzigen en verwijderen van fysieke toegangsrechten gebeurt en wordt deze gebruikt?
Worden de logische toegangsrechten en fysieke toegangsrechten volgens duidelijke criteria beoordeeld en wordt de autorisatiematrix regelmatig gevalideerd?
Voorbereiding en optimalisatie van ICT voor het bedrijfscontinuïteitsproces
Zijn er bedrijfscontinuïteitsdoelstellingen en bijbehorende ICT-continuïteitseisen vastgesteld?
Is de voorbereiding en optimalisatie van de ICT (ICT-gereedheid) van de organisatie gepland en geïmplementeerd op basis van de vastgestelde doelstellingen en bijbehorende eisen?

Startpagina
Dashboard NIS2
Ontvangen vragenlijsten
Mijn training
NIS2 Quality Mark
Organisatie
Medewerkers
Leveranciers
Meldplicht
Beheer
Supportdesk

Leveranciers 50 Trucks bv

Leveranciers spelen een belangrijke rol in de beveiliging van jouw organisatie. Maak hieronder je leveranciers bekend. Eerst je ICT-leveranciers daarna de andere leveranciers.

5
Leveranciers

+ Toevoegen | Risicoprofiel instellen | Verwijderen

Zoeken

Leverancier	Risico-inventarisatie	Risicoprofiel	Notitie	Alert
ABC Truck chemicals cleaning	RI bezig	Hoog		
A-B Fast Routeplanning software	RI gereed (Advies: Hoog)	Hoog		
Webmedia works	RI gereed (Advies: Substantieel)	Substantieel		
Accountantcy Alex & Co	RI bezig	Basis		
ASPA International	RI bezig	Geen		

Home - Samen Digitaal Veilig | Samen Digitaal Veilig | Checklist (25).pdf

portal.samendigitaalveilig.nl/?_gl=1*dafsx6*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ5NDY0LjAuMC4w#/...

ChatGPT | Samen Digitaal Veili... | IVBB – Kwaliteit & I... | Inbox (13.315) - daa... | Inbox (721) - dh@a... | (15) Feed | LinkedIn | Wbni | cybersecurity | keurmerk NIS2 | The Weeping Beech... | Alle bookmarks

Samen Digitaal Veilig

Demo NIS2
Toeleveringsketen

Geen MFA actief | Meldplicht alerts | Instellingen | NL

- Startpagina
- Dashboard NIS2
- Ontvangen vragenlijsten
- Mijn training
- NIS2 Quality Mark
- Organisatie
- Medewerkers
- Leveranciers
- Meldplicht
- Beheer
- Supportdesk

Level 1

Maak kennis met Dennis de internetcrimineel

Level 1 | 2 min.

De top 3 grootste fouten die we allemaal maken

Level 1 | 2 min.

Gebruik nooit hetzelfde wachtwoord

Level 1 | 1 min.

Voelt het niet goed? Vraag het voordat je iets doet

Level 1 | 1 min.

Level 2

De top 3 gevaren op internet

Level 2 | 2 min.

Tips voor een topwachtwoord!

Level 2 | 1 min.

Herken de nepmail

Level 2 | 2 min.

Zet een slot op al je apparaten

Level 2 | 2 min.

https://portal.samendigitaalveilig.nl/?_gl=1*dafsx6*_ga*MTk5NDUwMTM3My4xNzA4NTQ4ODgz*_ga_02SW8PXBQL*MTcxNTI0Nzk3OS4yNTYuMS4xNzE1MjQ5NDY0LjAuMC4w#/medewerkers/vragen

Resumé

“Het is niet de bedoeling dat heel MKB Nederland extreem hoge normen gaat halen“

Voordelen NIS2 Quality Mark

- **Jaag je leveranciers niet weg**
- **Raak je grote klant niet kwijt**
- **Je gebruikt een haalbare norm**
- **Groeit in de loop der jaren**
- **Aan de wet voldoen is voldoende**
- **Verhoging van vertrouwen bij klanten en partners**
- **Verbetering van bedrijfsreputatie**

Samen Digitaal Veilig

Belangrijke websites

1. Zelfevaluatie NIS2: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/
2. NIS2 Quickscan: https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/
3. Alles over NIS2: https://www.samendigitaalveilig.nl/allesovernis2/
4. NIS2 Quality Mark informatie: https://nis2qualitymark.eu/keurmerk/
5. Cyber Oefeningen: https://www.digitaltrustcenter.nl/nieuws/dtc-stimuleert-cyberoefenen-met-crisisgame
6. Internet Consultatie wettekst: https://www.internetconsultatie.nl/cyberbeveiligingswet/b1

Samen Digitaal Veilig

Aandachtspunten voor een bestuurder

- **Aandachtspunten irt. toeleveringsketen, controleer:**
  - **Zorgdragen voor risicoanalyse voorwaarden**
  - **Inkoopvoorwaarden voor toeleveranciers aanpassen aan NIS2 richtlijn**
    - **Risico's mitigeren ism juridische zaken**
  - **Compliance voorwaarden afspreken met toeleveranciers**
  - **Vastleggen technische standaarden met gebruikmaking van marktstandaarden, w.o. NIS2 Quality Mark audit**
  - **Regelmatige updates om continuïteit te laten zien**
  - **Meldplicht: afspraken maken over incidenten en meldingen**
  - **Incident Response in place?**

Samen Digitaal Veilig

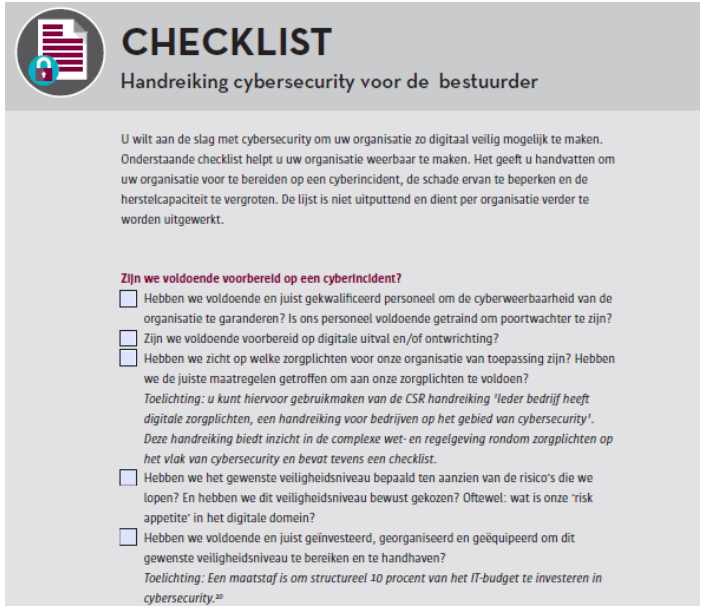
Handreiking voor een bestuurder

Het belang van cybersecurity in de vitale processen en digitale diensten

Welke afwegingen maakt u in het kader van cybersecurity?

Hoe belegt u cybersecurity in uw organisatie?

Hoe bouwt u structureel aan digitale veiligheid?



CHECKLIST

Handreiking cybersecurity voor de bestuurder

U wilt aan de slag met cybersecurity om uw organisatie zo digitaal veilig mogelijk te maken. Onderstaande checklist helpt u uw organisatie weerbaar te maken. Het geeft u handvatten om uw organisatie voor te bereiden op een cyberincident, de schade ervan te beperken en de herstelcapaciteit te vergroten. De lijst is niet uitputtend en dient per organisatie verder te worden uitgewerkt.

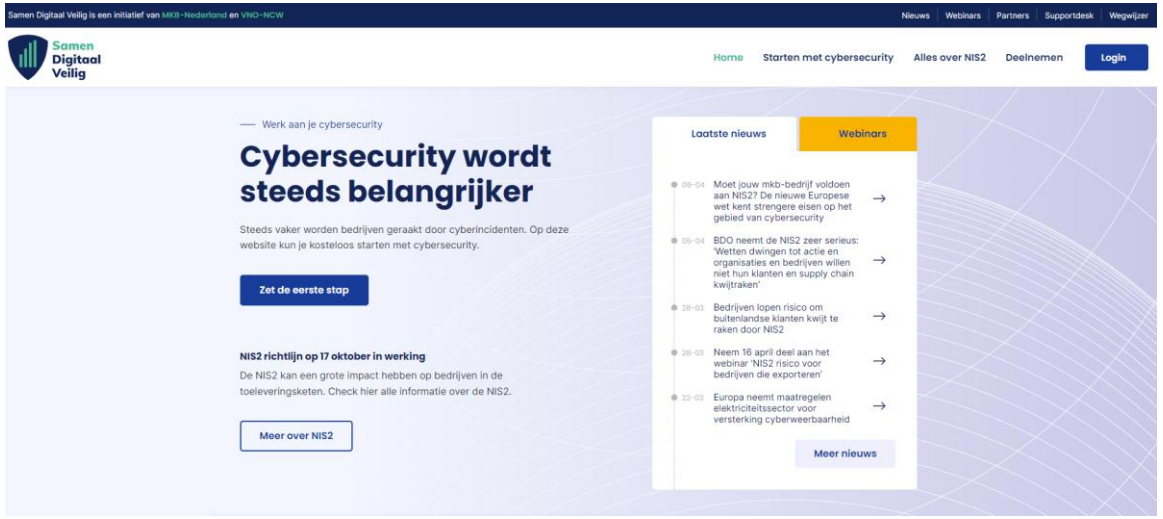
Zijn we voldoende voorbereid op een cyberincident?

- ☐ Hebben we voldoende en juist gekwalificeerd personeel om de cyberweerbaarheid van de organisatie te garanderen? Is ons personeel voldoende getraind om poortwachter te zijn?
- ☐ Zijn we voldoende voorbereid op digitale uitval en/of ontwrichting?
- ☐ Hebben we zicht op welke zorgplichten voor onze organisatie van toepassing zijn? Hebben we de juiste maatregelen getroffen om aan onze zorgplichten te voldoen?
  Toelichting: u kunt hiervoor gebruikmaken van de CSR handreiking 'Ieder bedrijf heeft digitale zorgplichten, een handreiking voor bedrijven op het gebied van cybersecurity'. Deze handreiking biedt inzicht in de complexe wet- en regelgeving rondom zorgplichten op het vlak van cybersecurity en bevat tevens een checklist.
- ☐ Hebben we het gewenste veiligheidsniveau bepaald ten aanzien van de risico's die we lopen? En hebben we dit veiligheidsniveau bewust gekozen? Oftewel: wat is onze 'risk appetite' in het digitale domein?
- ☐ Hebben we voldoende en juist geïnvesteerd, georganiseerd en geëquipeerd om dit gewenste veiligheidsniveau te bereiken en te handhaven?
  Toelichting: Een maatstaf is om structureel 10 procent van het IT-budget te investeren in cybersecurity.[20]

Samen Digitaal Veilig

Wat bieden SDV & Ekco

- Dagelijks NIS2 nieuws
- Website samendigitaalveilig.nl (button: Alles over NIS2)
- Informatieve webinars
- e-Book & Video’s
- Voorbeelddocumenten en brieftemplates
- Inkoopvoorwaarden voor je leveranciers
- Tooling voor leveranciersbeheer
- Risico-inventarisatie tooling
- NIS2-QM30 lijst met alle maatregelen en ISO27001 mapping op www.nis2qualitymark.eu



NIS2 QUALITY MARK

Ik wil aan de slag, en nu?

Advies: www.samendigitaalveilig.nl

Stap 1: Volg Orientatie webinars
(https://www.samendigitaalveilig.nl/webinars/)

- Hoe bereidt je je voor op NIS2
- Veiligheid in de toeleverings keten

Stap 2: Maak een account aan

Stap3: Maak keuze uit een pakket
Gratis; Plus; NIS2; NIS2 Corp.

Stap 4: Bekijk de video's

Stap 5: Ga aan de slag met invullen
(e/o maak gebruik van de supportdesk)

Voor cybersecurity normeringen:
www.nis2qualitymark.eu/keurmerk/
en download de 3 normeringen (Basic, Substantial, High)

Samen Digitaal Veilig

Afsluiting

- Wij hebben een checklist en kunnen jullie helpen
- Werkgroep samenstellen
- Samen een webinar houden voor jullie klanten en toeleveranciers

EKCO NIS2 checklist voor mkb-leveranciers 1/2

Als mkb-leverancier is het waarschijnlijk dat jouw grote klanten eisen dat j
Hier zijn de stappen om te volgen:

Maatregel	Uitleg
Wijs een projectmanager of team aan	Stel een projectmanager aan (of als c projectteam) die verantwoordelijk is v ervoor dat de directie dit project steu bestuur of de directie is eindverantwo
Stel een projectplan op	• **Risico-inventarisatie:** Voer same uitgebreide risicoanalyse uit, voor als voor jouw leveranciers. • **Normering:** Bepaal aan welke nor cybersecurity te verbeteren. In de QM10 voldoende zijn. • **Communicatie leveranciers:** Info leveranciers direct over de vereis voldoen. Zij hebben ook tijd nodig beginnen. Als zij niet klaar zijn kur halen. Om dit te voorkomen moet het project informeren.
Bepaal het budget	Stel een realistisch budget vast dat al dekt.
Stel een bedrijfscontinuïteitsplan op	Ontwikkel een robuust plan om de be waarborgen.
Implementeer risicobeheersmaatregelen	Start de implementatie van beveiligin geïdentificeerde kritieke risico's.
Houd je aan de ketenzorgplicht	Implementeer noodzakelijke back-up zorgplicht onderdelen.
Opleiding medewerkers	Zorg dat medewerkers opgeleid zijn i
Ontwikkel een leveranciersbeleid	Stel duidelijke beveiligingseisen aan l in contracten. Verwijs naar Samen Dig ondersteuning.

EKCO NIS2 checklist voor NIS2 bedrijven 1/2

Volg deze stappen om ervoor te zorgen dat jouw bedrijf NIS2 proof wordt:

Maatregel	Uitleg	Check
Stel een projectteam op	Stel een gespecialiseerd team samen dat verantwoordelijk is voor het NIS2 project. Zorg ervoor dat de directie dit project steunt en prioriteit geeft. Het bestuur of de directie is eindverantwoordelijk voor de NIS2.	☐
Bepaal het budget	Stel een realistisch budget vast dat alle aspecten van het project dekt.	☐
Stel een projectplan op	• **Normering:** Bepaal aan welke norm je wilt voldoen om aan te tonen dat jouw bedrijf voldoet aan NIS2. • **Risico-inventarisatie:** Voer een uitgebreide risicoanalyse uit voor zowel de eigen organisatie als de leveranciers. • **Communicatie leveranciers:** Informeer je leveranciers direct over de vereisten om knelpunten in tijd te voorkomen.	☐ ☐ ☐
Stel een bedrijfscontinuïteitsplan op	Ontwikkel een robuust plan om de bedrijfscontinuïteit te waarborgen.	☐
Implementeer risicobeheersmaatregelen	Start de implementatie van beveiligingsmaatregelen voor de geïdentificeerde kritieke risico's.	☐
Houd je aan de ketenzorgplicht	Implementeer noodzakelijke back-ups en andere cruciale zorgplicht onderdelen.	☐
Opleiding bestuur/directie	Zorg dat het bestuur/de directie grondig opgeleid is in de NIS2 vereisten.	☐
Opleiding medewerkers	Zorg dat medewerkers opgeleid zijn in de NIS2 vereisten.	☐
Ontwikkel een leveranciersbeleid	Stel duidelijke beveiligingseisen aan leveranciers en leg deze vast in contracten. Verwijs naar Samen Digitaal Veilig voor ondersteuning.	☐

NIS2 QUALITY MARK

EKCO NIS2 checklist voor mkb-leveranciers

EKCO NIS2 checklist voor NIS2 bedrijven 2/2