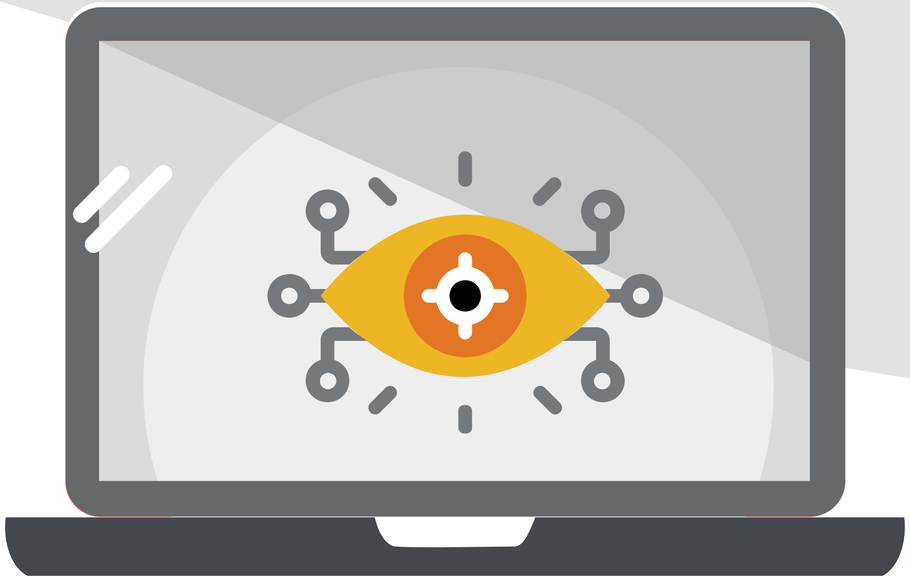
CYBERVEILIG NEDERLAND



Strategische Agenda 2026 -2028

Over deze agenda

Deze strategische agenda 2026–2028 beschrijft de pijlers waarop Cyberveilig Nederland de komende jaren haar inzet richt. Het document vormt, samen met het Strategisch Kader, de basis voor de koers van de vereniging.

Deze agenda is een herijking van de vorige strategische agenda (2023–2025) en wordt jaarlijks geactualiseerd door de werkgroep Strategie, met een driejarige horizon.

Per pijler benoemen we de kernactiviteiten, beoogde impact en de mate van inzet waarmee Cyberveilig Nederland bijdraagt aan de digitale weerbaarheid van Nederland. Tevens zijn de eigenschappen uit het strategisch kader opgenomen waartegen de specifieke activiteiten getoetst worden.

Deze eigenschappen zijn:

EIGENSCHAPPEN VAN DE BIJDRAGE VAN DE SECTOR AAN DE MAATSCHAPPIJ

1. **Kwaliteit.** Wat een klant krijgt is voorspelbaar en heeft het beloofde effect.
2. **Transparantie.** Van een product of dienst is duidelijk wat het is, wat het bijdraagt en waarom het in de prijs-range valt waar het valt. Dit helpt potentiële klanten van onze leden om producten en diensten te begrijpen en te vergelijken en zo beter geholpen te worden.

EIGENSCHAPPEN VAN DE RELATIE MET ONZE BELANGHEBBENDEN

3. **Toegankelijkheid.** De vertegenwoordiging van onze sector en dwarsdoorsnedes daarvan is bekend, vindbaar, benaderbaar en inhoudelijk deskundig.
4. **Invloed.** We spannen ons in voor zinvolle security-gerelateerde wet- en regelgeving en voor een gunstig economisch klimaat en werken samen met overheidspartijen als dit de weerbaarheid van de maatschappij ten goede komt. Wij richten ons primair op Nederland maar kunnen ook internationaal activiteiten ontplooien als dat effectief is.

EIGENSCHAPPEN VAN ONZE LEDEN

5. **Samenwerking.** We delen kennis, tijd en (operationele) informatie om onze gezamenlijke bijdrage (security-effect) te vergroten.
6. **Integriteit.** Integriteit is de basis van al onze activiteiten waarbij wij ons gedragen op een wijze die onze strategie ondersteunt, om ons gezamenlijk effect te vergroten. Wij zijn eerlijk, oprecht en niet omkoopbaar. We zijn transparant, volgen geldende wet- en regelgeving en leggen verantwoording af over ons eigen gedrag en keuzes.

EIGENSCHAPPEN VAN DE VERENIGING

7. **Representatie.** De vereniging vertegenwoordigt een voldoende groot deel van de sector en de samenstelling van het ledenbestand is een representatieve afspiegeling van de sector.
8. **Toekomstbestendigheid.** De vereniging is dusdanig vormgegeven dat ze deze strategie op lange termijn kan blijven uitvoeren.

Onze pijlers

PIJLER 1
VERSTERKEN KWALITEIT EN TRANSPARANTIE VAN DE CYBERSECURITYSECTOR

Doel: Cyberveilig Nederland bouwt aan een gedeeld kompas voor vakmanschap. Dit kwaliteitskader biedt een gemeenschappelijke standaard voor professionele dienstverlening in de cybersecuritysector.

Eigenschappen:
- Kwaliteit
- Transparantie
- Toegankelijkheid

PIJLER 2
VERSTERKEN BIJDRAGE AAN BELEID, STRATEGIE EN POLITIEK IN NEDERLAND ÉN EUROPA OP GEBIED VAN CYBERSECURITY

Doel: Cyberveilig Nederland is een gezaghebbende gesprekspartner in de beleidsvorming rond digitale veiligheid. De sector wordt hierdoor zichtbaar en invloedrijk via strategische communicatie en consultaties.

Eigenschappen:
- Toegankelijkheid
- Invloed

PIJLER 3
STIMULEREN VAN ÉN ACTIEF DEELNEMEN AAN INFORMATIEDELING IN PRIVAAT-PRIVAAT EN PRIVAAT-PUBLIEK VERBAND IN HET CYBERDOMEIN

Doel: Cyberveilig Nederland verbindt leden en publieke partners in een ecosysteem van vertrouwen. Via projecten wordt praktijkkennis en informatie gedeeld, samenwerking versterkt en maatschappelijke meerwaarde gecreëerd.

Eigenschappen:
- Toegankelijkheid
- Transparantie

7. HUMAN CAPITAL

PIJLER 4
STIMULEREN VAN INTEGRATIE VAN OT-SECURITY ALS VOLWAARDIG ONDERDEEL VAN IT-CYBERSECURITY

Doel: Cyberveilig Nederland zet zich in om OT-security (Operational Technology) niet als een losstaand of aanvullend thema te behandelen, maar als een volwaardig en geïntegreerd onderdeel van IT-cybersecurity.

Eigenschappen:
- Kwaliteit
- Toegankelijkheid

PIJLER 5
VERDIEPEN VAN THEMA DIGITALE SOEVEREINITEIT

Doel: Cyberveilig Nederland signaleert en verdiept het thema digitale soevereiniteit als strategisch vraagstuk voor Nederland. Door technologische afhankelijkheden en beleidskeuzes in kaart te brengen, draagt de vereniging bij aan het versterken van de autonomie en weerbaarheid van de digitale infrastructuur.

Eigenschappen:
- Kwaliteit
- Toegankelijkheid
- Invloed

PIJLER 6
VERDIEPEN VAN STRATEGISCH THEMA AI IN CYBERSECURITY

Doel: Cyberveilig Nederland verkent de rol van kunstmatige intelligentie (AI) binnen cybersecurity, zowel als kans als risico. Door het thema te verdiepen en te duiden, draagt de vereniging bij aan verantwoorde inzet van AI in de sector.

Eigenschappen:
- Kwaliteit
- Toegankelijkheid
- Invloed

Pijler 1

VERSTERKEN KWALITEIT EN TRANSPARANTIE VAN DE CYBERSECURITYSECTOR

Doel: Cyberveilig Nederland bouwt aan een gedeeld kompas voor vakmanschap. Dit kwaliteitskader biedt een gemeenschappelijke standaard voor professionele dienstverlening in de cybersecuritysector. Het versterkt transparantie, betrouwbaarheid en vakmanschap — en vergroot het vertrouwen van opdrachtgevers, beleidsmakers, toezichthouders en de maatschappij.

Eigenschappen:

- Kwaliteit
- Transparantie
- Toegankelijkheid

Kernactiviteiten:

- Onderhouden bestaande keurmerken en bijdrage aan ontwikkeling nieuwe keurmerken via het CCV
- Inzetten op het positioneren van het Cybersecurity Woordenboek binnen Europa als dé standaard voor terminologie en vaktaal
- Verkennen “woordenboek” voor samenwerkingsverbanden en overheidsjargon
- Inzetten op leveren van inhoudelijke input op standaardisatie projecten. Voorbeelden zijn ENISA en wet- en regelgeving zoals de Cyber Security Act, gericht op certificering.
- Organiseren kennisbijeenkomsten gericht op kwaliteit en transparantie voor en/of door leden

Impact:

Leden
Verhoogde professionalisering, duidelijkheid over normen, versterkte marktpositie

Maatschappij
Meer vertrouwen in cybersecuritydiensten, transparantie van de sector

Stakeholders
Transparantie in toezicht, beleidsverankering van kwaliteit, minder interpretatieverschillen

Mate van Inzet:

Proactief
Co-creatie met leden en andere experts, publicaties

Reactief
Ondersteuning bij implementatie, doorontwikkeling op basis van feedback

Pijler 2

VERSTERKEN BIJDRAGE AAN BELEID, STRATEGIE EN POLITIEK IN NEDERLAND ÉN EUROPA OP GEBIED VAN CYBERSECURITY

Cyberveilig Nederland is een gezaghebbende gesprekspartner in de beleidsvorming rond digitale veiligheid. De sector is zichtbaar en invloedrijk via strategische communicatie, stakeholdermanagement en consultaties. Door actieve betrokkenheid bij trajecten zoals o.a. bij NIS2, CER, CRA, AI-verordeningen, draagt de vereniging bij aan uitvoerbare, effectieve en toekomstbestendige wet- en regelgeving.

Eigenschappen:

- Toegankelijkheid
- Invloed

Kernactiviteiten:

- Organiseren van strategische sessies, beleidsdialogen en kennisbijeenkomsten voor en/of door leden over Nederlandse en Europese (beleids)initiatieven en wet- en regelgeving
- Inbrengen van inhoudelijke input in wetgevings- en beleidstrajecten binnen Nederland én Europa
- Deelnemen aan en inhoudelijke inbreng geven in strategisch overleggen zoals de Cyber Security Raad en NIS2 PPS overleg
- Standpunten inbrengen bij Nederlandse politici – nieuwe Kamerleden en Tweede Kamer Commissie Digitale Zaken

Impact:

Leden
Beleidskaders sluiten beter aan op praktijk, meer invloed op toekomstige regelgeving, verkrijgen van inzichten in lopende wet- en regelgeving

Maatschappij
Effectiever beleid dat maatschappelijke belangen en digitale veiligheid versterkt

Stakeholders
Constructieve dialoog, betere uitvoerbaarheid van wetgeving

Mate van Inzet:

Proactief
Initiëren van dialogen, actieve communicatie richting beleid en politiek en beïnvloeden van beleid vanuit inhoud

Reactief
Reageren op consultaties, duiden van knelpunten en actuele debatten

Pijler 3

STIMULEREN VAN ÉN ACTIEF DEELNEMEN AAN INFORMATIEDELING IN PRIVAAT-PRIVAAT EN PRIVAAT-PUBLIEK VERBAND IN HET CYBERDOMEIN

Cyberveilig Nederland verbindt leden en publieke partners in een ecosysteem van vertrouwen. Praktijkkennis en informatie wordt pro-actief gedeeld, samenwerking versterkt en maatschappelijke meerwaarde gecreëerd. Als verbindende kracht binnen de sector brengt Cyberveilig Nederland publieke en private partijen samen om de digitale weerbaarheid te vergroten. Door het delen van (praktijk)kennis, het opzetten van gezamenlijke initiatieven en het versterken van relaties, bouwt de vereniging aan een veerkrachtig ecosysteem met maatschappelijke impact.

Eigenschappen:

- Toegankelijkheid
- Transparantie

Kernactiviteiten:

- Stimuleren van informatie-uitwisseling vanuit de leden van Cyberveilig Nederland in de Nederlandse aanpak van ransomwarebestrijding (Project Melissa)
- Stimuleren van deelname en informatie-uitwisseling vanuit de leden van Cyberveilig Nederland in belangrijke overheidsprogramma's en samenwerkingen rondom informatie-uitwisseling, zoals Programma Cyclotron en het Cyberweerbaarheidsnetwerk
- Gezamenlijke inzichten delen door het publiceren van whitepapers of door het organiseren van (digitale) kennissessies

Impact:

Leden
Snellere toegang tot relevante kennis, versterking van expertise, peer learning, maatschappelijke bijdrage vergroten

Maatschappij
Bredere toepassing van best practices, verhoogde weerbaarheid van Nederland

Stakeholders
Betere samenwerking in ketens, gedeeld inzicht in dreigingen en oplossingen, versterking publiek-private relaties

Mate van Inzet:

Proactief
Deelnemen en opzetten van platforms, initiëren en stimuleren van actieve uitwisseling

Reactief
Reageren op samenwerkingsverzoeken, duiden van sectorstandpunten

Pijler 4

STIMULEREN VAN INTEGRATIE VAN OT-SECURITY ALS VOLWAARDIG ONDERDEEL VAN CYBERSECURITY

Doel: Cyberveilig Nederland onderkent en duidt strategische thema's en vertaalt deze naar handelingsperspectieven die bijdragen aan de digitale weerbaarheid van Nederland.
Daarbij richten we ons op OT-security (Operational Technology). Cyberveilig Nederland zet zich in om OT-security niet als een losstaand of aanvullend thema te behandelen, maar als een volwaardig en geïntegreerd onderdeel van het brede cybersecurity perspectief.

Eigenschappen:

- Kwaliteit
- Toegankelijkheid

Kernactiviteiten:

- Zichtbare rol en inzet van Cyberveilig Nederland en leden in de IACS-Coalitie
- Inzetten en uitdragen dat OT en IT een totaalpakket is

Impact:

Leden
Vroegtijdige duiding van trends, strategische positionering, innovatiekracht

Maatschappij
Bewustwording van opkomende risico's en kansen, betere beleidskeuzes

Stakeholders
Inhoudelijke input voor beleid, versterking van publiek-private samenwerking, anticipatie op technologische ontwikkelingen

Mate van Inzet:

Proactief
Deelname aan IACS-coalitie

Reactief
Aansluiten bij externe initiatieven

Pijler 5

VERDIEPEN VAN STRATEGISCH THEMA “DIGITALE SOEVEREINITEIT”

Doel: Cyberveilig Nederland signaleert en verdiept het thema digitale soevereiniteit als strategisch vraagstuk voor Nederland. Het resultaat van de verkenning zal bepalen wat de inzet van Cyberveilig Nederland op het thema digitale soevereiniteit zal zijn. Mogelijke uitkomsten zijn het in kaart brengen van technologische afhankelijkheden en beleidskeuzes. De uitkomsten moeten bijdragen aan het versterken van de autonomie en weerbaarheid van de digitale infrastructuur.

Eigenschappen:

- Kwaliteit
- Toegankelijkheid
- Invloed

Kernactiviteiten:

- Opzetten van projectgroep “digitale soevereiniteit”
- Opleveren voorstel van rol Cyberveilig Nederland binnen thema “digitale soevereiniteit” gebaseerd op analyses, trends en beleidsontwikkeling

Impact:

Leden
Strategische positionering, inzicht in afhankelijkheden

Maatschappij
Verhoogd bewustzijn, betere bescherming van publieke waarden

Stakeholders
Beleidsinput, versterking van strategische autonomie, samenwerking met sector

Mate van Inzet:

Proactief
Opzetten van en deelnemen aan projectgroep, publiceren van analyses en aanbevelingen en agenderen van het thema in beleidsdialogen

Reactief
Reageren op politieke en maatschappelijke debatten en aansluiten bij externe initiatieven rond digitale soevereiniteit

Pijler 6

VERDIEPEN VAN STRATEGISCH THEMA ARTIFICIAL INTELLIGENCE

Doel: Cyberveilig Nederland verkent de rol van kunstmatige intelligentie (AI) binnen cybersecurity — zowel als kans (detectie, respons, automatisering) als risico (deepfakes, autonome aanvallen). Door het thema te verdiepen en te duiden, draagt de vereniging bij aan verantwoorde inzet van AI in de sector en tegen AI-gerelateerde dreigingen. De focus ligt op het verbinden van technologische ontwikkelingen binnen dit domein met ethiek, beleid en sectorpraktijk.

Eigenschappen:

- Kwaliteit
- Toegankelijkheid
- Invloed

Kernactiviteiten:

- Opzetten van projectgroep “AI”
- Kennisdeling en analyses over AI in cybersecurity, gericht op innovatie, toepassing, ethiek en beleid

Impact:

Leden
Inzicht in AI-toepassingen, versterking van innovatiekracht

Maatschappij
Verantwoorde inzet van AI, bescherming tegen misbruik

Stakeholders
Beleidsinput, ethische kaders, samenwerking met sector

Mate van Inzet:

Proactief
Opzetten van en deelnemen aan werkgroep, publiceren van whitepapers en ethische richtlijnen

Reactief
Reageren op incidenten of maatschappelijke zorgen rond AI en aansluiten bij externe AI-initiatieven en/of kennisproducten van overheid of kennisinstellingen

Pijler 7

HUMAN CAPITAL CYBERSECURITY

Doel: De inzet van Cyberveilig Nederland op het onderwerp Human Capital zal binnen de pijlers worden uitgevoerd. Toch wordt het apart benoemd om voldoende aandacht te hebben voor dit onderwerp.
Human capital vormt de personele ruggengraat van digitale weerbaarheid. Het raakt álle strategische pijlers van Cyberveilig Nederland: van kwaliteit en transparantie tot beleidsbeïnvloeding, informatiedeling en technologische verkenning. Vakmanschap, ethiek, instroom en ontwikkeling zijn bepalend voor de slagkracht van de sector — en voor het vertrouwen van opdrachtgevers, toezichthouders en de maatschappij. Human capital is daarmee niet alleen een HR-vraagstuk, maar een strategisch fundament.

Eigenschappen:

- Toegankelijkheid
- Samenwerken

Kernactiviteiten:

- Aansluiten bij initiatieven die bijdragen aan de ontwikkeling van meer en kwalitatief beter human capital voor de cybersecuritysector

Impact:

Leden
Verhoogde vakbekwaamheid en positionering.

Maatschappij
Verhoogde beschikbaarheid van deskundige professionals

Stakeholders
Inzicht in capaciteitsvraagstukken; input voor onderwijs, beleid en arbeidsmarktinstrumenten

Mate van Inzet:

Proactief
Voorzitten werkgroep 2 (Aanbod – vraag versterken) Human Capital Agenda Cybersecurity

Reactief
Reageren op verzoeken tot geven van gastcolleges, verbinden van netwerk bij (bestaande) HC initiatieven zoals Hackshield

Colofon

Dit is een uitgave van Cyberveilig Nederland. De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. Cyberveilig Nederland kan daarvoor niet aansprakelijk worden gesteld.

Dit Strategisch Kader is mede tot stand gekomen met input van de leden van Cyberveilig Nederland, in het bijzonder de werkgroep Strategie.

Meer informatie over de activiteiten van Cyberveilig Nederland vindt u op **cyberveilignederland.nl**

Contactgegevens
E-mail: **info@cyberveilignederland.nl**
Telefoon: **088 - 118 25 10**