We zetten ons in voor een optimaal ondernemingsklimaat voor cybersecurity bedrijven in Nederland. We brengen transparantie aan in de sector door de ontwikkeling van een gedragscode en keurmerk. We nemen actief deel aan het publieke debat en zien cybersecurity niet alleen als een risico, maar juist ook als een kans om Nederland te positioneren als een land dat veilige producten en diensten voortbrengt.

We gaan het gesprek aan met de overheid en andere strategische partners om onze kennis en kunde van het cybersecurity werkveld voor het grotere belang in te zetten. We brengen verbindingen tot stand, tussen cybersecurity bedrijven onderling, maar ook brengen we vragers en aanbieders samen. We praten met de overheid en politiek om (toekomstige) knelpunten weg te nemen die de digitale weerbaarheid van Nederland in de weg staan. Dit alles zorgt ervoor dat we de zichtbaarheid en impact van onze sector vergroten.

DOOR LID TE WORDEN VAN CYBERVEILIG NL:

1. Draag je bij aan de verbetering van de cybersecuritysector, aan de weerbaarheid van de Nederlandse samenleving en aan het imago van Nederland als land dat veilige producten en diensten voortbrengt.
2. Versterk je de eigen positie in de markt dankzij het toepassen van de Cyberveilig NL gedragscode en het mogen voeren van de (nog te ontwikkelen) kwaliteitskeurmerk(en). Je kunt invloed uitoefenen op het tot stand komen hiervan.
3. Profiteer je van voor de cybersecuritybranche belangrijke belangenbehartiging bij de overheid en andere stakeholders. Daarmee heb je toegang tot eerstelijns informatie en oefen je invloed uit op relevante ontwikkelingen, bijvoorbeeld op wet- en regelgeving die een impact hebben op de cybersecuritysector.
4. Heb je directe invloed op de strategie, standpunten en activiteiten van Cyberveilig NL.
5. Krijg je toegang tot een cybersecuritynetwerk bij de overheid, industrie en overige relevante sectoren.

CONTRIBUTIE

- Leden betalen jaarlijks contributie waarvan de hoogte wordt bepaald op basis van het totale aantal medewerkers van de desbetreffende organisatie.
- Indien de cybersecurity-dienstverlening slechts een deel van de totale dienstverlening van het lid betreft, wordt het aantal medewerkers berekend op basis van het aantal medewerkers dat betrokken is bij het leveren van cybersecurity-dienstverlening. Betreffende leden dienen over het aantal medewerkers én de dienstverlening een goede onderbouwing te geven, zulks ter beoordeling van het bestuurd van Cyberveilig NL.
- Het aantal medewerkers wordt jaarlijks opnieuw vastgesteld met peildatum 31/12 van het voorgaande jaar. Leden ontvangen in de eerste week van december het verzoek de gegevens aan te leveren.
- Leden die in de loop van het jaar zich als lid aansluiten ontvangen een factuur naar rato van het verstreken jaar, met minimum van 4 maanden.
- De facturen voor het lidmaatschap worden in de maand januari verstuurd. Indien de contributie niet of niet tijdig wordt betaald kan dit opzegging van het lidmaatschap tot gevolg hebben.

#MEDEWERKERS	CONTRIBUTIE
2-10	€ 1.000
11-20	€ 2.000
21-50	€ 3.000
51-100	€ 6.000
101-250	€ 10.000
250-400	€ 17.000
400+	€ 25.000

De genoemde bedragen zijn exclusief 21% BTW

GEDRAGSCODE

Het gedrag van de leden van Cyberveilig NL moet in al het doen en laten, binnen de kaders van de doelstelling van de branchevereniging Cyberveilig NL passen en de toets der kritiek in het openbaar kunnen doorstaan. De gedragscode functioneert als visitekaartje van Cyberveilig NL. Als brancheorganisatie hanteren we de algemene beginselen van behoorlijk bestuur, ook wel genoemd 'good corporate governance'.

Alle leden van Cyberveilig NL conformeren zich aan onderstaande beginselen en regels van de gedragscode. De mogelijkheid bestaat dat de gedragscode nog met nieuwe regels zal worden aangevuld.

PROCEDURE AANMELDEN EN TOELATING

Een bedrijf dat lid wil worden van de Vereniging kan zich aanmelden bij het secretariaat van Cyberveilig NL via **www.cyberveilignederland.nl**, telefonisch **088-1182510** of via **info@cyberveilignederland.nl**.
De aanmelding dient te worden begeleid met een onderbouwing onder welke voorwaarden men lid wil worden, waarna de aanvraagprocedure in gang wordt gezet. De eventuele toelating zal worden beoordeeld door het bestuur van Cyberveilig NL. De toelatingsuitslag is bindend en kan niet over worden gecorrespondeerd. Onderdeel van de procedure is dat aspirant leden de gedragscode van Cyberveilig NL ondertekenen. Indien twijfel/onduidelijkheid bestaat of ontstaat over het voldoen aan de in de gedragscode gestelde eisen, kan aanvullende motivatie en/of bewijslast worden opgevraagd.

VOORWAARDEN LIDMAATSCHAP

- Het lidmaatschapsjaar van de vereniging loopt van 1 januari tot en met 31 december.
- De leden van de vereniging zijn rechtspersonen die ingeschreven zijn bij het handelsregister (KvK) en dienen permanent een vestiging te hebben in Nederland.
- Leden dienen een substantieel deel aan cybersecuritydiensten en/of producten te leveren (vanaf nu te noemen: cybersecurity-dienstverlening) ten behoeve van de totale bedrijfsvoering.
- Betreffende leden dienen over het aantal medewerkers in cybersecurity én de geassocieerde dienstverlening een goede onderbouwing te geven, zulks ter beoordeling van het bestuur van Cyberveilig NL.
- De onderneming die een lidmaatschap aanvraagt bestaat uit minimaal 2 medewerkers in cybersecurity dienstverlening en moet aantoonbaar deze diensten verlenen aan in Nederland gevestigde organisaties.
- ZZP-ers zijn vooralsnog uitgesloten van een lidmaatschap.[1]
- Ondernemingen waarvan de dienstverlening hoofdzakelijk op privacy is gericht vanuit juridisch oogpunt, worden uitgesloten van lidmaatschap.
- Leden onderschrijven de gedragscode(s) van Cyberveilig NL en handelen hiernaar.

LEDEN

1. zullen zich ten opzichte van de opdrachtgever te allen tijde professioneel en integer opstellen, dat wil zeggen met inzet van alle kwalitatieve deskundigheid.
2. zullen zich zodanig gedragen dat de reputatie van Cyberveilig NL niet in diskrediet wordt gebracht.
3. zullen voor zover nodig maatregelen nemen die het naleven van de gedragscode waarborgt.
4. onderschrijven het beleid van Responsible Disclosure (**responsibledisclosure.nl** en **https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html**)
5. hebben de eigen informatiebeveiliging op hoog niveau gerealiseerd, bij voorkeur mede blijkend uit bijvoorbeeld het voldoen aan de ISO 27001 norm en/of het mogen voeren van een bedrijfsrecherchevergunning.
6. voldoen aan de van toepassing zijnde wetgeving, waaronder de Algemene Verordening Gegevensbescherming.
7. moeten op professionele en integere wijze omgaan met computernetwerken en gevoelige informatie van de organisaties die gebruik maken van hun diensten.
8. waarborgen actief het kennisniveau van hun medewerkers, zodat zij de beschikken over actuele kennis en kunde binnen het cybersecuritydomein.
9. leveren cybersecurity-dienstverlening van hoge kwaliteit en maken dit inzichtelijk, bijvoorbeeld middels een kwaliteitsmanagementsysteem zoals beschreven in ISO 9001.
10. voeren werkzaamheden op gebied van security testen alleen uit onder juridische vrijwaring met betrekking tot de betreffende systemen.

1 Hoewel de bijdrage die ZZP'ers leveren aan de cyberweerbaarheid van Nederland en onze branche specifiek significant is, richt de branchevereniging zich vooralsnog primair op de belangen van ondernemingen.