CBW/NIS2 TRAININGEN VOOR CYBERSECURITY COMPLIANCE

Met de goedkeuring van de NIS2 richtlijn is een belangrijke Europese stap gezet op het gebied van een meer uniforme cybersecurity. Het doel van deze nog naar Nederlandse wetgeving te vertalen richtlijn, is om een hoger niveau van gemeenschappelijke beveiliging van netwerk- en informatiesystemen in de hele EU te waarborgen en zo de weerbaarheid tegen cyberdreigingen te vergroten.

Momenteel werken we in Nederland nog met de Wet beveiliging netwerk- en informatiesystemen (Wbni). Zodra het Nederlandse wetsvoorstel is goedgekeurd, vervalt de Wbni en geldt voor een breed scala aan organisaties de nieuwe regels van de NIS2.

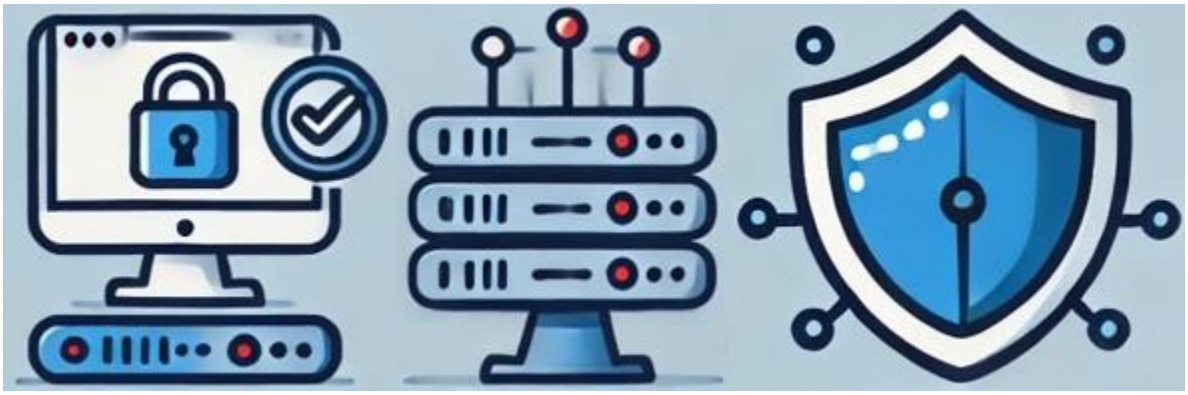
Houd er rekening mee dat uw organisatie eerder wellicht niet onder de Wbni viel, maar wel onder de nieuwe Cyberbeveiligingswet (Cbw). In dat geval is er waarschijnlijk best veel werk aan de winkel. Maar ook als u wel al onder de Wbni valt, verandert er veel.

In dit document krijgt u een globaal beeld van de eisen van de NIS2 en welke trainingen u kunnen helpen zo snel mogelijk compliant te zijn.

VALT MIJN ORGANISATIE ONDER DE NIS2-RICHTLIJN OF NIET?

Een 100% sluitend antwoord hierop is pas te geven zodra de Nederlandse wet is goedgekeurd. In de tussentijd geeft de NIS2 (met name in bijlage I en II) zelf wel al enige duidelijkheid. Ook als toeleverancier van een ‘NIS2 organisatie’ is de impact groot, zelfs al valt u zelf niet direct onder de noemer ‘essentiële’ of ‘belangrijke’ entiteit.

De Rijksoverheid heeft een tool ontwikkeld waarmee u een zelf-evaluatie kunt doen. U vindt deze hier: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/



Bestuurlijke aansprakelijkheid

Een belangrijke verandering met consequenties is de bestuurlijke aansprakelijkheid in de NIS2. Het doel is ervoor te zorgen dat cybersecurity prioriteit krijgt op het hoogste niveau van organisaties die onder de NIS2-richtlijn vallen.

Leidinggevenden van organisaties worden persoonlijk verantwoordelijk gehouden voor de naleving van de cybersecurityvereisten die de richtlijn stelt. Dit betekent dat bedrijfsleiders, zoals CEO's en bestuursleden, proactief betrokken moeten zijn bij de implementatie en het handhaven van adequate cybersecuritymaatregelen binnen hun organisatie.

Om hieraan te voldoen is één van de NIS2-eisen dat deze leidinggevenden verplicht trainingen volgen om (zoals NIS2 letterlijk aangeeft):

"voldoende kennis en vaardigheden te verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen."

TSTC heeft diverse oplossingen die u kunnen helpen aan deze eis te voldoen. Vaak is maatwerk in een training/workshop op locatie gewenst, waarin bijvoorbeeld een compleet managementteam of bestuur wordt bijgepraat over informatiebeveiliging, specifieke risico's, maatregelen en de omgang met incidenten. Neem gerust contact met ons op om de mogelijkheden te bespreken.

Een voorbeeld van een dergelijke incompany training is de training **Cbw/NIS2 Governance voor Bestuurders** die in een dagdeel op locatie of online kan worden verzorgd. Met deze training sluit u in de basis aan op de genoemde NIS2-eis dat ieder lid van het bestuur van organisaties die onder de richtlijn vallen, een gerichte opleiding over cyberbeveiliging dient te volgen.

Via ons open rooster volgt u ook de uitgebreidere 2-daagse **Certified NIS2 Professional (CNIS2) - Managing NIS2** training, waarin u dieper kennismaakt met de NIS2 en alle bijbehorende eisen. Deze training wordt afgesloten met een begeleide GAP-analyse waarin u inzichtelijk krijgt waar nog actie ondernomen moet worden. De bijbehorende te behalen certificering is een tastbaar bewijs dat u geïnvesteerd hebt in kennis over de Cbw/NIS2, wat bijvoorbeeld van pas komt wanneer er onverhoopt toch een incident plaatsvindt en de toezichthouder onderzoekt wat u hebt gedaan om aan de gestelde richtlijnen te voldoen.

Ditzelfde geldt ook voor de uitgebreidere 5-daagse **NIS2 Lead Implementer** training die minder geschikt is voor bestuurders, maar security managers en -professionals helpt bij de daadwerkelijke implementatie van de gestelde eisen.

Welke verplichtingen schrijft de NIS2-richtlijn voor?

De NIS2-richtlijn schrijft zowel verplichtingen voor die gelden op nationaal niveau, als op bedrijfsniveau. Op nationaal niveau zijn dat onder andere:

- Ondersteuningsplicht
- Toezichthoudersplicht

Op bedrijfsniveau zijn dat onder andere:

- Registratieplicht
- Zorgplicht
- Meldplicht

Met name de Zorg- en Meldplicht bevatten eisen waarbij onze trainingen u kunnen helpen. Zowel de hierboven benoemde **CNIS2 Professional** training, als **NIS2 Lead Implementer** training gaan uitgebreid in op hoe u invulling kunt geven aan deze plichten en waar u specifiek aan moet denken. Daarnaast zijn er op allerlei deelvlakken andere trainingen die u op meer specialistisch gebied kunnen helpen bij de implementatie van de cybersecurity eisen van de NIS2.

HIERONDER VOLGEN EEN AANTAL MAATREGELEN EN BIJPASSENDE TRAININGEN:

Zorgplicht

Essentiële en belangrijke entiteiten moeten maatregelen nemen om hun netwerk- en informatiesystemen tegen incidenten te beschermen. Hetzelfde geldt voor de fysieke omgeving waarin deze systemen zich bevinden.

1. Risicoanalyse en beveiliging van informatiesystemen
   - **ISO 27005 Certified Risk Manager**
   - **ISO 27001 Lead Implementer**
   - **Certified BIO Professional - Foundation**
   - **Certified BIO Professional - Practitioner**
   - **CRISC - Certified in Risk and Information System Control**

2. (Beleid en procedures over) incidentenbehandeling
   - **ECIH - Certified Incident Handler**
   - **CSA - Certified SOC Analyst**
   - **CISM - Certified Information Security Manager**
   - **CCISO - Certified Chief Information Security Officer**

3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen

- **EDRP - Disaster Recovery Professional inclusief ISO 22301**
- **CCISO - Certified Chief Information Security Officer**

4. Beveiliging van de toeleverancierskеten

- **CSSLP - Certified Secure Software Lifecycle Professional**
- **CCSP - Certified Cloud Security Professional**
- **CCISO - Certified Chief Information Security Officer**
- **CRISC - Certified in Risk and Information System Control**

5. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden

- **Security+**
- **CISSP**
- **ECIH - Certified Incident Handler**
- **CND - Certified Network Defender**

6. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen

- **CISM - Certified Information Security Manager**
- **CCISO - Certified Chief Information Security Officer**
- **Lead Cybersecurity Manager**

7. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging

- **Cyber & IT Security Foundation**
- **CEH - Certified Ethical Hacker**
- **CCISO - Certified Chief Information Security Officer**
- **Awareness oplossingen**

8. Beleid en procedures over het gebruik van cryptografie en encryptie

- **ECES - Certified Encryption Specialist**

9. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa

- **CCISO - Certified Chief Information Security Officer**

10. Het gebruik van multifactor-authenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit

- **CND - Certified Network Defender**

Meldplicht

De NIS2-richtlijn schrijft voor dat entiteiten potentieel significante incidenten binnen 24 uur moeten melden bij de toezichthouder. Hier vloeien een aantal verantwoordelijkheden uit voort die te maken hebben met incident management/handling en monitoring processen:

1. Monitoring - worden incidenten gedetecteerd?

- **CSA - Certified SOC Analyst**
- **CySA+ - CompTIA CyberSecurity Analyst**

2. Incident Management / Handling - ligt er een plan klaar hoe te handelen bij incidenten?

- **ECIH - Certified Incident Handler**

3. Threat Intelligence - op de hoogte zijn van nieuwe bedreigingen, weten waarop alert te zijn?

- **CTIA - Certified Threat Intelligence Analyst**

4. Pentesting - Incidenten voorkomen door te testen op mogelijke kwetsbaarheden

- **CEH - Certified Ethical Hacker**
- **OSCP - OffSec Certified Professional**
- **CPENT - Certified Penetration Testing Professional**
- **WASA - (Web)Application Security Assessment**

GENERIEKE NIS2 WORKSHOPS & TRAININGEN

We adviseren u in alle gevallen te starten met één van de eerder benoemde, specifieke NIS2 trainingen. Aangezien er vaak meerdere rollen met de richtlijn te maken krijgen, kan het prettig zijn om een training samen met collega's te volgen zodat de neuzen naderhand dezelfde kant op staan.

Een andere strategie kan zijn om medewerkers afhankelijk van hun rol verschillende trainingen te laten volgen, zodat de juiste kennis op de juiste plekken terecht komt.

- **Cbw/NIS2 Governance voor Bestuurders (incompany)**
- **CNIS2 - Certified NIS2 Professional / Managing NIS2**
- **NIS2 Lead Implementer**

WAAROM TRAINEN?

Het volgen van security trainingen speelt een cruciale rol in het voldoen aan NIS2-compliance. De in dit document benoemde trainingen brengen bedrijven en organisaties de kennis en vaardigheden bij om zélf actief hun beveiligingsniveaus te waarborgen. Als alternatief voor of aanvullend op het inschakelen van consultancy waarbij organisaties vaak afhankelijk zijn van externe experts, zorgen trainingen ervoor dat interne medewerkers of teams zelfstandig en proactief risico's kunnen identificeren en beheersen.

Dit bevordert een cultuur van continue verbetering en een security bewustzijn binnen de organisatie. Door medewerkers zelf te trainen, ontstaat daarnaast een diepere betrokkenheid bij het naleven van de richtlijnen. Hiermee groeit een security cultuur waarmee problemen effectief intern kunnen worden aangepakt zonder voortdurend externe hulp in te hoeven schakelen. Buiten dat dit op de langere termijn kostenbesparend werkt, draagt het ook bij aan een toekomstbestendige organisatie die strategisch voordeel haalt uit het aantoonbaar in-control zijn op het gebied van informatie- en cyberbeveiliging.

TSTC ICT & Security trainingen is al sinds 2006 gespecialiseerd in het verzorgen van (cyber)security trainingen. Mocht bovengenoemde informatie nog onvoldoende duidelijk zijn of wanneer u zoekt naar een opleidingsadvies op maat, dan helpen we u graag persoonlijk verder. Of het nu een individuele aanvraag betreft, een opleidingsplan voor een team of een workshop op maat - wij zijn graag uw opleider voor het Cbw/NIS2 vraagstuk.

TSTC ICT & Security Trainingen

Plesmanstraat 62

3905 KZ Veenendaal

WWW.TSTC.NL / 0318-581480 / info@tstc.nl