Publicatiedatum : 17/02/2025

Opleiding : Een NIS 2-project implementeren, besturen en certificeren

NIS v2-compliance met succes bereiken

seminarie - 2d - 14u00 - Ref. NIS

Prijs : 1850 € V.B.

4,6 / 5

Het doel van de NIS 1 (Network and Information System 1)-richtlijn was het ontwikkelen van cyberveiligheid in de hele Europese Unie, het beperken van bedreigingen voor netwerken en informatiesystemen die worden gebruikt om essentiële diensten in belangrijke sectoren te leveren en het waarborgen van de continuïteit van deze diensten in het geval van incidenten. Op die manier draagt de richtlijn bij aan de veiligheid van de Unie en aan de goede werking van haar economie en samenleving. De NIS 2-richtlijn maakt deel uit van een versterkte en noodzakelijke continuïteit met het oog op een zich uitbreidend cyberdreigingslandschap en het ontstaan van nieuwe uitdagingen.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- Inzicht in de uitdagingen van cyberrisico's en de reactie van Europa hierop
- Het door de Franse overheid gedefinieerde beveiligingskader voor de richtlijn inzake netwerk- en informatiebeveiliging integreren.
- De veranderingen tussen NIS 1 en NIS 2 begrijpen
- Ontdek aan de hand van casestudy's hoe je ze kunt implementeren en inzetten
- Inzicht in het ANSSI-certificeringsproces
- De kosten van de implementatie van een project evalueren

Doelgroep

ISSM's en beveiligingsadviseurs, beveiligingsarchitecten, IT-directeuren en -managers, IT-ingenieurs, projectmanagers, beveiligingsauditors en juristen op het gebied van IT-regelgeving.

Voorafgaande vereisten

Basiskennis van cyberbeveiliging of kennis die gelijkwaardig is aan de kennis die is opgedaan tijdens de BYR- en SSI-seminars.

DEELNEMERS

ISSM's en beveiligingsadviseurs, beveiligingsarchitecten, IT-directeuren en -managers, IT-ingenieurs, projectmanagers, beveiligingsauditors en juristen op het gebied van IT-regelgeving.

VOORAFGAANDE VEREISTEN

Basiskennis van cyberbeveiliging of kennis die gelijkwaardig is aan de kennis die is opgedaan tijdens de BYR- en SSI-seminars.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

Opleidingsprogramma

1 Inleiding: de uitdagingen van Europese cyberbeveiliging

- Gevoelige gegevens: cyberdiefstal, spionage, sabotage...
- Een nieuwe Koude Oorlog, Oost/West, VS/China, West/Rusland.
- Georganiseerde hackers en de rol van inlichtingendiensten.
- APT (Advanced Persistent Threat), ransomware, gerichte risico's.
- De aanpak van cyberbedreigingen: naar een "cyber-Schengen"?

2 De essentie voor CISO's

- Voor wie: essentiële entiteiten en belangrijke entiteiten, nieuwe geschiktheids- en uitsluitingscriteria.
- Voor welke ecosystemen? Nieuwe bedrijfssectoren en betrokken ESN's.
- Welke regels? Van de 23 regels van NIS 1 plus "wat ontbrak".
- Wanneer zal het plaatsvinden? Van 2024 tot 2026...
- Hoe kunnen we dit doen? Met een gecontroleerd bestuurs- en certificeringsproces.
- Wat zijn de sancties? Gegradueerd op basis van omzet, naar het voorbeeld van de RGPD.

3 Veiligheidsmaatregelen

- Regels voor governance, bescherming, verdediging en veerkracht van netwerk- en informatiebeveiliging 1.
- Beleid met betrekking tot risicoanalyse en beveiliging van informatiesystemen.
- Incidentbeheer.
- Bedrijfscontinuïteit en herstel, crisismanagement.
- Veiligheid van de toeleveringsketen.
- Beveiliging bij de aanschaf, ontwikkeling en het onderhoud van netwerken en informatiesystemen.
- Beoordeling van de effectiviteit van maatregelen voor risicobeheer op het gebied van cyberbeveiliging.
- Basis cyberhygiënepraktijken en cyberbeveiligingstraining.
- Beleid en procedures met betrekking tot het gebruik van cryptografie en, indien van toepassing, encryptie.
- Personeelsbeveiliging, toegangscontrolebeleid en activabeheer.
- Het gebruik van multifactorauthenticatie of oplossingen voor continue authenticatie.

4 Het nalevingsproject beheren

- Van kloofanalyse tot naleving.
- Risicogovernance: relevantie van EBIOS RM in een NIS-project.
- Herhaling van bestaande beveiligingsmaatregelen en NIS 1-regels waar van toepassing.
- Het goedkeuringsproces van de ANSSI is aangepast aan de NIS 2-richtlijn.
- De belangrijkste mijlpalen in het NIS 2-project en de benodigde middelen.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

5 Conclusie: op weg naar certificering

- Sterke ISO 27K inspiratie: link met ISO 27001 en nieuwe ISO 27002:2022 best practices.
- Consistente cyberweerbaarheid: koppeling met DORA- en CER-richtlijnen en -verordeningen.
- Franse omzetting: de parallelle ontwikkeling van de LPM en de OIV.
- Gedifferentieerde staatscontroles (ex ante of ex post regulering).
- Een boeteprocedure die vergelijkbaar is met de RGPD, met regels voor de gradatie van boetes.
- De veiligheid van zijn ecosysteem en kritische belanghebbenden.

Data en plaats

KLAS OP AFSTAND
2026 : 26 maa., 16 juni, 1 okt., 8 dec.

PARIS LA DÉFENSE
2026 : 16 juni, 1 okt., 8 dec.