Publicatiedatum : 12/04/2024

Opleiding : EBIOS Risk Manager, voorbereiding op LSTI-certificering

Cyber APT-risicoanalyse en ecosysteem

seminarie - 2d - 14u - Ref. IVH

Prijs : 1850 € V.B.

De EBIOS RM (2018) methode stelt u in staat om veiligheidsrisico's van IS te beoordelen en aan te pakken, in het bijzonder cyberrisico's, gebaseerd op bewezen ervaring in IS consulting en project management assistentie. Dit seminar biedt je alle kennis die je nodig hebt om de methode in een echte situatie toe te passen.

Pedagogische doelstellingen

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

- Inzicht in cyberrisico's: cyberdefensie door risico's
- Beoordelen hoe het nieuwe EBIOS past (of niet past) bij de huidige beveiligingsuitdagingen
- Inzicht in de voorgestelde risicobeheerbenadering
- De woordenschat en concepten begrijpen die door ANSSI zijn ontwikkeld
- Voer een volledig onderzoek uit met behulp van alle aangeboden workshops

Doelgroep

CISO's of beveiligingscorrespondenten, beveiligingsarchitecten, IT-directeuren of -managers, ingenieurs, projectmanagers (projectbeheer, contractbeheer) die beveiligingsvereisten moeten integreren.

Voorafgaande vereisten

Basiskennis van risicobeheer en cyberbeveiliging, of kennis die gelijkwaardig is aan die van de BYR- en ASE- of BYR- en AIR-cursussen.

DEELNEMERS

CISO's of beveiligingscorrespondenten, beveiligingsarchitecten, IT-directeuren of -managers, ingenieurs, projectmanagers (projectbeheer, contractbeheer) die beveiligingsvereisten moeten integreren.

VOORAFGAANDE VEREISTEN

Basiskennis van risicobeheer en cyberbeveiliging, of kennis die gelijkwaardig is aan die van de BYR- en ASE- of BYR- en AIR-cursussen.

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.

Certificatie

Overgang naar certificaties op afstand

Raadpleeg de officiële documentatie van de certificerende instantie om de voorafgaande vereisten voor het afleggen van het online certificatie-examen te raadplegen.

Praktische modaliteiten

Voorbeeld

Casestudies in een industriële en tertiaire context zullen je helpen om de methode te begrijpen en te oefenen.

Opleidingsprogramma

1 De cyberdreiging in het nieuws

- Cyberdiefstal en cyberspionage van gevoelige gegevens.
- Naar een nieuwe Oost-West Koude Oorlog, VS-China.
- Dienstweigering op wereldwijde schaal.
- Georganiseerde hackersgroepen en de rol van inlichtingendiensten.
- Phishing/social engineering, Spear phishing: beproefde scenario's.
- APT's: persistentie en diepte van aanvallen.
- Diefstal van gevoelige gegevens, netwerkinbraak, malware, bots/botnets en ransomware.

2 Identificatie en analyse van de cyberdreiging

- De militaire aanpak toegepast op de cyberwereld.
- De Amerikaanse aanpak met Find, Fix, Track, Target, Engage, Assess.
- De cyber kill chain als basis voor beschrijving. Typisch voorbeeld: Lockheed Martin.
- Fasen van verkenning, bewapening, aflevering, exploitatie, installatie, controle (C2). Acties op doelstellingen.
- De schets van een gerichte aanval volgens ANSSI.
- De fasen van het proces (Weten, Invoeren, Vinden, Uitbuiten).
- Identificatie van directe en indirecte aanvalspaden.

3 De EBIOS-methode

- Rol van ANSSI en de EBIOS-club.
- EBIOS en de uitdagingen van de LPM.
- Bijdrage van de nieuwe EBIOS RM-methode (2018) en EBIOS 2010.
- RM EBIOS-compatibiliteit versus ISO 31000 en ISO 27005.

4 De grondbeginselen van de methode

- Zakelijke waarde, goed ondersteund, ecosysteem, belanghebbenden.
- Compliance-benadering versus risicoscenario-benadering.
- Houdt rekening met geavanceerde opzettelijke APT-bedreigingen.
- Beoordeling van het ecosysteem en kritische niveau 1-, 2- en 3-stakeholders.
- EBIOS RM in het goedkeuringsproces voor de LPM en de NIS-richtlijn.
- Veiligheidsregels voor de nalevingsaanpak (hygiënegids, LPM/NIS-maatregelen, enz.).
- Risicobeheerproces als maatstaf voor ISS-governance.

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 De doelstellingen van RM EBIOS

- Identificeer de beveiligingsstichting die het meest geschikt is voor het doel van het onderzoek.
- Voldoe aan de veiligheidsvoorschriften (handels-/juridisch/contractueel).
- Scenario's op hoog niveau identificeren en analyseren door het ecosysteem en belanghebbenden te integreren.
- Identificeren en implementeren van beveiligingsmaatregelen voor kritieke belanghebbenden.
- Voer een voorlopige risicobeoordeling uit om prioriteitsgebieden voor verbetering te identificeren.
- Prioriteitsgebieden voor verbetering: beveiliging en zwakke punten die door aanvallers kunnen worden uitgebuit.
- Voer een gedetailleerde risicobeoordeling uit, bijvoorbeeld met het oog op ANSSI-certificering.

6 Methode-activiteiten (1 en 2)

- 1. Workshop - Kader en basis voor beveiliging :
- Welke bedrijfswaarden, activa en media moeten in kaart worden gebracht?
- Welke gebeurtenissen moeten worden gevreesd vanuit zakelijk oogpunt?
- Welke beveiligingsbasis moet worden geïntegreerd? ANSSI, interne PSSI, etc.?
- Welke regelgevende normen moeten als verplicht worden geïdentificeerd?
- 2. Workshop - Risicobronnen en doelstellingen :
- Hoe aantrekkelijk zijn de zakelijke waarden van cyberaanvallers?
- Hoe kunnen de business lines betrokken worden bij het identificeren van risicobronnen?
- Welke criteria moeten gebruikt worden om SR-OV paren te beoordelen? De middelen en motivatie van aanvallende groepen beoordelen.

Casestudy

Presentatie van workshops 1 en 2.

7 Methode-activiteiten (3, 4 en 5)

- 3.4. Workshop - Strategische en operationele scenario's :
- Wie zijn de belanghebbenden in het ecosysteem?
- Wat zijn de scenario's gezien vanuit de zakelijke kant en vervolgens vanuit de technische kant?
- Welke directe en indirecte aanvalsroutes moeten worden beschreven?
- Hoe scenariowaarschijnlijkheden te berekenen: van de expresmethode tot de geavanceerde methode.
- 5. Workshop - Risicobeheer :
- Welke risico's moeten in de huidige context als onaanvaardbaar worden beschouwd?
- Wat zijn de deliverables voor een RM EBIOS-onderzoek?
- ISO 27001-verklaring van toepasselijkheid, LPM/NIS-risicobeoordelingsrapport, enz.

Casestudy

Presentatie van workshops 3, 4 en 5.

8 Casestudie EBIOS

- 1 De context van het onderzoek: betrokkenheid van de business lines bij de identificatie van bedrijfswaarden en waargenomen effecten.
- Risicobronnen en potentiële aanvalsdoelen identificeren.
- Bepaling van regelgevende en wettelijke verplichtingen en identificatie van kritische belanghebbenden van niveau 1.
- De digitale dreigingskaart van het ecosysteem in context opbouwen.
- 2. De workshopactiviteiten die nodig zijn om de strategische en vervolgens operationele scenario's op te stellen.
- Risicobeoordeling in termen van ernst en waarschijnlijkheid.
- Ontwikkeling van een methode voor het berekenen van cybervolwassenheid en afhankelijkheid van belanghebbenden.
- 3. Opstellen van een risicomanagementplan.
- Een actieplan opstellen.
- Technische (bescherming, verdediging) en organisatorische (bestuur, veerkracht) beveiligingsmaatregelen.
- De keuze van maatregelen uit de beveiligingsregels van het LPM/NIS of ISO of andere referentiekaders.
- De keuze uit ANSSI-gecertificeerde software (momenteel gecertificeerd: ARIMES, EGERIE, AGILE RM, FENCE, IBM OpenPages, etc.).
- De voorlopige constructie van zijn spreadsheet-gebaseerde "software".

Data en plaats

KLAS OP AFSTAND
2026 : 2 apr., 23 juni, 29 sep., 15 dec.

PARIS LA DÉFENSE
2026 : 2 apr., 23 juni, 29 sep., 15 dec.