Publicatiedatum : 02/01/2024

Opleiding : Cybercriminaliteit en cyberoorlog, problemen en uitdagingen

seminarie - 2d - 14u00 - Ref. BYR
Prijs : 1850 € V.B.

3,9 / 5

Cybercriminaliteit vormt een groeiende bedreiging voor de samenleving. Cybercriminelen handelen overal vandaan om bedrijfsinfrastructuren aan te vallen. De vraag die in deze cursus wordt behandeld is niet of uw organisatie zal worden aangevallen, maar hoe u zich kunt voorbereiden op cybercrises en hoe u deze kunt detecteren, anticiperen en beheren.

Pedagogische doelstellingen

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

- De gevaren kennen en de bronnen van bedreigingen identificeren
- Inzicht in veiligheidsrisico's en -kwesties
- Inbraak detecteren en reageren op kwaadaardige handelingen
- Weten hoe je een effectieve, nuttige en gefaseerde reactie organiseert
- Crisisplanning voor cyberoorlogvoering

Doelgroep

CISO, IB-functie, algemeen management, IT-afdeling, juristen.

Voorafgaande vereisten

Geen speciale kennis vereist.

Praktische modaliteiten

Leer methodes

Meesterlijke presentatie met echte en recente veiligheidsfeiten en -incidenten en jurisprudentie in Frankrijk en Europa.

Opleidingsprogramma

DEELNEMERS

CISO, IB-functie, algemeen management, IT-afdeling, juristen.

VOORAFGAANDE VEREISTEN

Geen speciale kennis vereist.

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.

1 Cybercriminaliteit in het nieuws

- Gevoelige gegevens: cyberdiefstal, spionage.
- Nieuwe koude oorlog tussen Oost en West, VS/China.
- Denial of service op wereldwijde schaal.
- Georganiseerde hackers en de rol van inlichtingendiensten.
- Laatste nieuws: malware, bots/botnets, ransomware.
- APT (Advanced Persistant treat), CB-inbreuken, skimming.

2 Indringers detecteren

- Beheer van sporen, bewijsmateriaal en opnames.
- Detecteer abnormale activiteit, rapporteer een incident.
- Analyse en correlatie van beveiligingsgebeurtenissen (SIEM).
- Relevantie van het SOC (Security Operation Centre).
- Incidentbeheer automatiseren.
- Inbraaktesten, een essentiële anticiperende maatregel.
- Maak gebruik van een gespecialiseerd bedrijf voor incidentdetectie.

3 De respons organiseren

- Onderzoek en verzamelen van bewijs.
- Een incident melden, je crisiscommunicatie voorbereiden.
- Rol van CERT's.
- Crisiseenheid: de crisis organiseren en beheren.
- Kwetsbaarheid en patchbeheer.

4 Staatsorde tegenover cybercriminaliteit

- Cybercriminaliteit (Frankrijk, Europa): welke repressieve maatregelen zijn nodig?
- Rol van ANSSI (Frankrijk) en ENISA (Europa).
- Bewijsbeheer: ontvankelijkheid, verzamelen op het internet.
- Europese richtlijn inzake netwerk- en informatiebeveiliging (2018).
- Europese Cyber Security Act (2019).
- Militaire planningswet (2016).
- Rol van staten en Europa: wetten, richtlijnen en verordeningen.

5 OIV / OSE goede praktijken

- Cyberbeveiligingsbeheer: rollen, verantwoordelijkheden, betrokkenheid van bedrijfslijnen bij risicobeheer.
- Verdediging in de diepte: toegangscontrolebeleid, beheer van geprivilegieerde accounts.
- Cyberbeveiligingsincidentbeheer: detectiebeleid, reactie.

6 Veiligheid handhaven

- Beleid voor kwetsbaarheidsbeheer, behandeling (patchen).
- Kwetsbare gebieden: beheer bijwerken.
- Verklaring van geleden aanvallen.
- Verplichte gecertificeerde dienstverleners (PDIS, PRIS).
- Beveiligingsaudit door ANSSI, gebruik van gecertificeerde auditors (PASSI, LPM).

Data en plaats

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.

KLAS OP AFSTAND
2026 : 17 maa., 8 juni, 15 sep., 10 dec.

PARIS LA DÉFENSE
2026 : 17 maa., 8 juni, 15 sep., 10 dec.