Publicatiedatum : 06/05/2024

Opleiding : Inleiding tot IT-beveiliging

Synthese cursus - 1d - 7u00 - Ref. ISI
Prijs : 850 € V.B.

4,6 / 5

Met de ontwikkeling van het internet wordt de beveiliging van informatiesystemen steeds belangrijker in zowel privé- als professionele omgevingen. Deze inleiding in de beveiliging van informatiesystemen laat je kennismaken met de risico's en bedreigingen voor de beveiliging van informatiesystemen.

Pedagogische doelstellingen

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

- De risico's en bedreigingen begrijpen die van invloed kunnen zijn op de IB
- De mogelijke gevolgen van een computeraanval
- Informatiebeveiligingsmaatregelen identificeren
- Leer hoe u uw werkplek veiliger kunt maken
- De implementatie van het IS-beveiligingsbeleid van het bedrijf bevorderen

Doelgroep

Alle gebruikers die de basisprincipes van IT-beveiliging willen leren.

Voorafgaande vereisten

Wees bekend met de ANSSI-gids voor veiligheidshygiëne.

Opleidingsprogramma

DEELNEMERS

Alle gebruikers die de basisprincipes van IT-beveiliging willen leren.

VOORAFGAANDE VEREISTEN

Wees bekend met de ANSSI-gids voor veiligheidshygiëne.

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 Bedreigingen en risico's

- Wat is IT-beveiliging?
- Hoe kan nalatigheid een ramp veroorzaken?
- Ieders verantwoordelijkheden.
- IS-architectuur en potentiële kwetsbaarheden.
- Bedrijfsnetwerken (lokaal, extern, internet).
- Draadloze netwerken en mobiliteit. Toepassingen met een hoog risico: web, berichtenverkeer, enz.
- De database en het bestandssysteem. Bedreigingen en risico's.
- De sociologie van piraten. Ondergrondse netwerken. Motivaties.

2 Veiligheid op de werkplek

- Vertrouwelijkheid, handtekening en integriteit. Encryptiebeperkingen.
- De verschillende cryptografische elementen. Windows, Linux of MAC OS: wat is het veiligst?
- Beheer van gevoelige gegevens. Laptopproblemen.
- De verschillende bedreigingen voor het clientwerkstation? Kwaadaardige code begrijpen.
- Hoe ga je om met beveiligingslekken?
- USB-poorten. De rol van de client firewall.

3 Het verificatieproces

- Toegangscontrole: authenticatie en autorisatie.
- Het belang van authenticatie.
- Het traditionele wachtwoord.
- Authenticatie met behulp van certificaten en tokens.
- Verbinding op afstand via het internet.
- Wat is een VPN?
- Waarom sterke authenticatie gebruiken?

4 Het wettelijke kader en de juiste reflexen om te hebben

- Wat zijn de wettelijke en juridische beperkingen?
- Waarom moeten we aan deze veiligheidseisen voldoen?
- Actie ondernemen om de veiligheid te verbeteren: de sociale en juridische aspecten.
- De CNIL (Commission Nationale de l'Informatique et des Libertés) en wetgeving.
- Wat is een risico-, kwetsbaarheids- en bedreigingsanalyse?
- Inzicht in de rol van de CISO en de risicomanager.
- Cybersurveillance en de bescherming van de privacy.
- Het handvest voor het gebruik van IT-middelen. Dagelijkse beveiliging en goede gewoonten.

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.

Data en plaats

KLAS OP AFSTAND
2026 : 5 maa., 4 juni, 17 sep., 19 nov.

PARIS LA DÉFENSE
2026 : 4 juni, 17 sep., 19 nov.