Publicatiedatum : 07/08/2024

Opleiding : Cyberbeveiliging, gebruikersbewustzijn

Synthese cursus - 1d - 7u00 - Ref. SES
Prijs : 860 € V.B.

4,4 / 5

BEST

Deze cursus stelt u in staat om de risico's en gevolgen te identificeren van een gebruikersactie die de beveiliging van het informatiesysteem ondermijnt, om de beperkingen opgelegd door het beveiligingsbeleid uit te leggen en te rechtvaardigen, en om de belangrijkste tegenmaatregelen te begrijpen die in het bedrijf worden toegepast.

Pedagogische doelstellingen

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

- De soorten IS-beveiligingsrisico's en hun mogelijke gevolgen begrijpen
- Maatregelen identificeren voor het beschermen van informatie en het beveiligen van werkstations
- De implementatie van het IS-beveiligingsbeleid van het bedrijf bevorderen

Doelgroep

Alle gebruikers met toegang tot het informatiesysteem via een computerwerkstation.

Voorafgaande vereisten

Geen.

Opleidingsprogramma

DEELNEMERS

Alle gebruikers met toegang tot het informatiesysteem via een computerwerkstation.

VOORAFGAANDE VEREISTEN

Geen.

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 IT-beveiliging: de bedreigingen en risico's begrijpen

- Inleiding: algemeen kader, wat wordt bedoeld met IT-beveiliging (bedreigingen, risico's, bescherming)?
- Hoe kan nalatigheid een ramp veroorzaken? Hier zijn een paar voorbeelden. Aansprakelijkheid.
- IS-componenten en hun kwetsbaarheden. Client- en serverbesturingssystemen.
- Bedrijfsnetwerken (lokaal, site-to-site, internettoegang).
- Draadloze netwerken en mobiliteit. Toepassingen met een hoog risico: web, e-mail, enz.
- Database en bestandssysteem. Bedreigingen en risico's.
- Sociologie van piraten. Ondergrondse netwerken. Motivaties.
- Typologie van risico's. Cybercriminaliteit in Frankrijk. Woordenschat (sniffing, spoofing, smurfing, hijacking, enz.).

2 Informatiebeveiliging en werkplekbeveiliging

- Woordenschat. Vertrouwelijkheid, handtekening en integriteit. De beperkingen van encryptie begrijpen.
- Algemeen schema van cryptografische elementen. Windows, Linux of macOS: wat is het veiligst?
- Beheer van gevoelige gegevens. Laptopproblemen.
- Wat is de bedreiging op het werkstation van de client? Begrijpen wat kwaadaardige code is.
- Hoe beheer u zwakke plekken in de beveiliging? De USB-poort. De rol van de client firewall.

3 Gebruikersauthenticatie en externe toegang

- Toegangscontrole: authenticatie en autorisatie.
- Waarom is authenticatie zo belangrijk?
- Het traditionele wachtwoord.
- Authenticatie met behulp van certificaten en tokens.
- Toegang op afstand via het internet. VPN's begrijpen.
- De voordelen van sterke authenticatie.

4 Hoe kunt u betrokken raken bij IS-beveiliging?

- Analyse van risico's, kwetsbaarheden en bedreigingen.
- Wettelijke en regelgevende beperkingen.
- Waarom moet mijn organisatie aan deze veiligheidseisen voldoen?
- De sleutelpersonen in beveiliging: inzicht in de rol van de CISO en de risicomanager.
- Actie ondernemen om de veiligheid te verbeteren: sociale en juridische aspecten. CNIL en wetgeving.
- Cybersurveillance en de bescherming van de privacy.
- Het handvest voor het gebruik van IT-middelen.
- Alledaagse veiligheid. De juiste reflexen. Conclusie.

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 : 2 juni, 11 juni, 11 juni, 11 juni, 15 sep., 24 sep., 24 sep., 26 nov., 3 dec., 3 dec., 3 dec.

PARIS LA DÉFENSE

2026 : 11 juni, 24 sep., 3 dec.