Cyberbeveiliging, sensibilisering van de gebruikers

Synthèsecursus van 1 dag - 7u
Ref : SES - Prijs 2024 : € 950 excl. BTW

Deze opleiding maakt u vertrouwd met de risico's en gevolgen van een handeling van de gebruiker die van invloed is op de veiligheid van het informatiesysteem, zodat u de door het beveiligingsbeleid opgelegde eisen kunt uitleggen en rechtvaardigen, en de belangrijkste tegenmaatregelen begrijpt die in de onderneming zijn ingevoerd.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

Begrijpen van de typologie van de risico's in verband met de IS-beveiliging en de mogelijke gevolgen ervan

Identificeren van de maatregelen ter bescherming van de informatie en voor de beveiliging van uw werkstation

Bevorderen van de uitvoering van het IS-beveiligingsbeleid van de onderneming

HET PROGRAMMA

laatste update: 11/2021

1) Computerbeveiliging: kennis van de bedreigingen en risico's

- Inleiding: algemeen kader, wat wordt bedoeld met IT-beveiliging (bedreigingen, risico's, bescherming)?
- Hoe kan nalatigheid een ramp veroorzaken? Enkele voorbeelden. Verantwoordelijkheid.
- De componenten van een IS en hun kwetsbare plekken. Client- en serverbesturingssystemen.
- Bedrijfsnetwerken (lokaal, site-to-site, internettoegang).
- Draadloze netwerken en mobiliteit. Risicotoepassingen: web, e-mail...
- Database en bestandssysteem. Bedreigingen en risico's.
- Sociologie van hackers. Ondergrondse netwerken. Motieven.
- Typologie van de risico's. Cybercriminaliteit in Frankrijk. Terminologie (sniffing, spoofing, smurfing, hijacking...).

2) Informatiebeveiliging en beveiliging van werkstations

- Terminologie. Vertrouwelijkheid, handtekening en integriteit. Begrijpen van de eisen in verband met encryptie.
- Algemeen schema van de cryptografische elementen. Windows, Linux of MAC OS: wat is het veiligst?
- Beheer van gevoelige gegevens. De problematiek van laptops.
- Wat is de dreiging op het client werkstation? Begrijpen wat kwaadaardige code is.
- Hoe omgaan met zwakke plekken in de beveiliging? De USB-poort. De rol van de client firewall.

3) Authenticatie van de gebruiker en toegang van buitenaf

- Toegangscontrole: authenticatie en autorisatie.
- Waarom is authenticatie belangrijk?
- Het klassieke wachtwoord.
- Authenticatie door certificaten en token.
- Toegang op afstand via internet. Kennis van VPN's.

DEELNEMERS

Alle gebruikers die via een computer toegang hebben tot het informatiesysteem.

VOORAFGAANDE VEREISTEN

Aucune connaissance particulière.

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.

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.

- Over het belang van versterkte authenticatie.

4) Hoe zich toeleggen op IS-beveiliging?

- Analyse van de risico's, kwetsbare plekken en bedreigingen.
- Wettelijke en juridische voorschriften.
- Waarom moet mijn organisatie aan deze beveiligingseisen voldoen?
- De sleutelfiguren in de beveiliging: kennis van de rol van de CISO en de Risk manager.
- Werken aan een betere beveiliging: sociale en juridische aspecten. De CNIL, de wetgeving.
- Cyber-surveillance en bescherming van de privacy.
- Het gebruikscharter van computerhulpmiddelen.
- Beveiliging in het dagelijks leven. De juiste reflexen. Conclusie.

DATA

KLAS OP AFSTAND
2024 : 06 sep, 09 dec

BRUSSEL
2024 : 06 sep, 09 dec