Publicatiedatum : 09/07/2024

Opleiding : De grondbeginselen van IS-beveiliging

seminarie - 3d - 21u00 - Ref. FTS
Prijs : 2330 € V.B.

4,3 / 5

BEST

Met de explosie van het internet, die de mogelijkheden voor ontwikkeling heeft verveelvoudigd, is de beveiliging van informatiesystemen een belangrijk onderwerp geworden voor alle bedrijven. In deze uitgebreide cursus maakt u kennis met alle acties en oplossingen die u kunt ondernemen om de beveiliging van uw informatiesystemen te garanderen en te verbeteren. U leert wat een risicoanalyse is, hoe u beveiligingsoplossingen kunt implementeren en welke verzekeringstechnische en juridische kwesties nauw verbonden zijn met de toepassing van een beveiligingsbeleid.

Pedagogische doelstellingen

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

- Inzicht in het IS-risicobeheerproces
- De referentiesystemen en bijbehorende standaarden kennen
- Het wettelijke kader leren kennen
- De implementatie van oplossingen beheren

Doelgroep

Iedereen die de grondbeginselen van IS-beveiliging wil leren.

Voorafgaande vereisten

De training "Inleiding tot computerbeveiliging" hebben afgerond.

Opleidingsprogramma

1 Risicobeheer en veiligheidsdoelstellingen

- De definitie van risico en de kenmerken ervan: potentieel, impact, ernst.
- De verschillende soorten risico's: ongeluk, fout, kwaad opzet.
- DIC-classificatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie.
- Tegenmaatregelen voor risicobeheer: preventie, bescherming, risico-overdracht, uitbesteding.

DEELNEMERS

Iedereen die de grondbeginselen van IS-beveiliging wil leren.

VOORAFGAANDE VEREISTEN

De training "Inleiding tot computerbeveiliging" hebben afgerond.

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.

2 De taak van de CISO

- Wat zijn de rol en verantwoordelijkheden van de IS Security Manager?
- Naar een veiligheidsorganisatie, de rol van de Assets Owners.
- Hoe een optimaal beheer van de toegewezen middelen en hulpbronnen te implementeren.
- De risicomanager in het bedrijf, zijn rol in relatie tot de IS Security Manager.

3 Normen en voorschriften

- SOX, COSO en COBIT voorschriften. Waarvoor? Voor wie?
- Governance van informatiesystemen. Verbanden met ITIL en CMMI.
- De ISO 27001-norm in een beheersysteem voor informatiebeveiliging.
- Koppelingen met ISO 15408: gemeenschappelijke criteria, ITSEC, TCSEC.
- De voordelen van ISO 27001 certificering voor organisaties.

4 Analyse van IT-risico's

- Hoe een proces voor risico-identificatie en -classificatie op te zetten.
- Operationele, fysieke en logische risico's.
- Hoe kun je je eigen kennis over bedreigingen en kwetsbaarheden opbouwen?
- Methoden en normen: EBIOS (Expression of Requirements and Identification of Security Objectives)/FEROS, MEHARI.
- De risicoanalyse-aanpak binnen het kader van ISO 27001, de PDCA (Plan, Do, Check, Act) aanpak.
- Wat zijn de bijdragen van de ISO 27005-norm en veranderingen aan Franse methoden?
- Van risicobeoordeling tot risicomanagement: beste praktijken.

5 Het veiligheidsauditproces

- Een continu en uitgebreid proces.
- Auditcategorieën, van organisatorische audits tot penetratietests.
- 19011 beste praktijk toegepast op veiligheid.
- Hoe stel je een intern auditprogramma op? Hoe kwalificeer je je auditors?
- Vergelijkende bijdragen, recursieve benadering, menselijke implicaties.
- Veiligheidsbewustzijn: wie? Wie? Wat? Hoe?
- Definities van moraliteit/Deontologie/Ethiek.
- Het veiligheidshandvest, het juridische bestaan, de inhoud en de validatie ervan.

6 Het noodplan en de kosten van veiligheid

- Risicodekking en continuïteitsstrategie.
- Het belang van rampen-, continuïteits-, herstel- en crisismanagementplannen, PCA/PRA, PSI, RTO/RPO.
- Een continuïteitsplan ontwikkelen en integreren in een kwaliteitsaanpak.
- Hoe veiligheidsbudgetten te definiëren.
- De definitie van ROSI (Return On Security Investment).
- Wat zijn de kostenevaluatietechnieken, de verschillende berekeningsmethoden en de Total Cost of Ownership (TCO)?
- Het Angelsaksische concept van de "Terugverdientijd".

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.

7 Beveiligingsoplossingen en -architecturen

- Selectieproces voor geschikte beveiligingsoplossingen voor elke actie.
- Definitie van een doelarchitectuur.
- ISO 15408 als selectiecriterium.
- Kiezen tussen IDS en IPS, inhoudscontrole als noodzaak.
- Hoe implementeer je een PKI-project? Te vermijden valkuilen.
- Authenticatietechnieken, SSO-projecten, identiteitsfederatie.
- De beveiligingsaanpak in IB-projecten, de ideale PDCA-cyclus.

8 Veiligheidstoezicht

- Hoe zet je een risicomanagementaanpak op: feiten, zekerheden...
- Wat zijn de belangrijkste indicatoren en dashboards? Op weg naar een ISO- en PDCA-aanpak.
- Outsourcing: wat zijn de voordelen en wat zijn de beperkingen?

9 Juridische aspecten

- Herinnering, definitie van het Automatic Data Processing System (ADPS).
- Soorten inbreuken, de Europese context, de LCEN-wetgeving.
- Wat zijn de juridische risico's voor het bedrijf, de managers en de CISO?

10 Goede praktijken

- Bescherming van persoonsgegevens, sancties bij niet-naleving.
- Het gebruik van biometrische gegevens in Frankrijk.
- Cybersurveillance van werknemers: grenzen en wettelijke beperkingen.
- Rechten van werknemers en sancties voor werkgevers.

Data en plaats

KLAS OP AFSTAND
2026 : 9 maa., 8 juni, 21 sep., 23 nov.

PARIS LA DÉFENSE
2026 : 9 maa., 8 juni, 21 sep., 23 nov.