Informatiesysteembeveiliging, samenvatting

Seminar van 3 dagen - 21u
Ref : SSI - Prijs 2024 : € 2 890 excl. BTW

Met de explosie van de digitale technologie die de ontwikkelingsmogelijkheden heeft verveelvoudigd, is informatiesysteembeveiligingsbeheer een grote uitdaging geworden voor alle bedrijven. Dit zeer uitgebreide seminarie stelt u alle acties en oplossingen voor om de veiligheid van uw IS te verzekeren: van risicoanalyse tot de optimale implementatie van beveiligingsoplossingen.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

Het beveiligingsgovernanceproces beheersen

Gebruikmaken van de bedrijfsraamwerken en de bijbehorende normen van de ISO 27K-serie

Het Franse en Europese rechtskader kennen (LPM, NIS, AVG ...)

Een actieplan plannen om de doelstellingen van het beveiligingsbeleid te verwezenlijken

Een adequate en evenredige respons ontwikkelen om cyberrisico's te beperken

HET PROGRAMMA

laatste update: 01/2022

1) Grondbeginselen van de informatiesysteembeveiliging

- Definitie van proces-/informatieactiva en ondersteunende activa (IT).
- DICT/P-classificatie: Beschikbaarheid, integriteit, vertrouwelijkheid en traceerbaarheid/bewijzen.
- Definitie van het ISS-risico en de specifieke eigenschappen ervan (kwetsbaarheden, bedreigingen).
- De verschillende soorten risico's: ongeluk, fout, kwaad opzet.
- Ontstaan van het cyberrisico, APT's, u voorbereiden op een cybercrisis.
- Essentiële externe informatiebronnen (ANSSI, CLUSIF, ENISA, enz.).

2) ISS task force: verschillende beroepsprofielen

- Rol en verantwoordelijkheden van de CISO, relatie met de IS-afdeling.
- Naar een gestructureerde en beschreven beveiligingsorganisatie, vaardigheden identificeren.
- Rol van de "Assets Owners" en de noodzakelijke betrokkenheid van het management.
- Profielen van architecten, integrators, auditors, pentesters, supervisors, risk managers, enz.
- Een competent team samenstellen dat is opgeleid en kan reageren op veranderingen in de cyberruimte.

3) Normatieve en regelgevende kaders

- Bedrijfs-, wettelijke en contractuele eisen integreren. De conformiteitsbenadering.
- Een voorbeeld van bedrijfsregelgeving: PCI DSS om uw gevoelige gegevens te beschermen.
- Beveiligingsmaatregelen om vertrouwelijkheid en gegevensintegriteit te bereiken.
- Een voorbeeld van juridische regelgeving: NIS-richtlijn / Loi Programmation Militaire.
- De 4 pijlers van beveiliging, zoals gezien door Europa en het ANSSI: governance, bescherming, verdediging en veerkracht.

DEELNEMERS

Ingenieurs die de functies op zich nemen van CISO's, IT-directeurs of -managers, beveiligingsingenieurs of veiligheidscorrespondenten, projectleiders die veiligheidsbeperkingen integreren.

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.

- Beveiligingsmaatregelen om beschikbaarheid en procesintegriteit te bereiken.
- De ISO 27001-norm in een managementsysteembenadering (Deming-/PDCA-cirkel).
- De universele best practices van de ISO 27002-norm, de essentiële minimumkennis.
- Veiligheidsgebieden: van beleid via IT-beveiliging tot conformiteit.
- Een veiligheidsgarantieplan binnen uw relatie tussen klant en leverancier opstellen.

4) Risicoanalyseproces

- Integratie van risicoanalyse in het beveiligingsgovernanceproces.
- Identificatie en classificatie van risico's, ongevalsrisico's en cyberrisico's.
- De normen ISO 31000 en 27005 en de relatie van het risicoproces tot het ISO 27001-ISMS.
- Van risicobeoordeling tot het risicobehandelingsplan: de juiste procesactiviteiten.
- Vooraf gedefinieerde methoden kennen: FR/EBIOS RM-benadering, US/NIST-benadering, enz.

5) Veiligheidsaudits en bewustmaking van gebruikers

- Auditcategorieën, van de organisatieaudit tot de penetratietest.
- Op de beveiliging toegepaste best practices van de 19011-norm.
- Hoe uw auditors te kwalificeren? - voorbeeld met de PASSI's (PASSI = 'Prestataire d'audit de la sécurité des systèmes d'information') in Frankrijk.
- Bewustmaking voor beveiliging: Wie? Wat? Hoe?
- De noodzaak van geprogrammeerde en gebudgetteerde bewustmaking.
- De verschillende vormen van bewustmaking, face to face of virtueel?
- Het veiligheidshandvest, het legaal bestaan en de inhoud ervan, de sancties.
- Tests en serious games, voorbeeld met de MOOC van het ANSSI.

6) Kosten van beveiliging en noodplannen

- Veiligheidsbudgetten, beschikbare statistieken.
- De definitie van Return On Security Investment (ROSI).
- Kostenevaluatietechnieken, verschillende berekeningsmethoden, TCO-berekening.
- Risicodekking en continuïteitsstrategie.
- Nood-, continuïteits-, herstel- en crisisbeheerplannen, PCA/PRA, PSI, RTO/RPO.
- Een continuïteitsplan ontwikkelen en integreren in een beveiligingsbenadering.

7) Optimale technische oplossingen ontwikkelen

- Uw logische en fysieke beveiliging structureren. Een diepteverdediging kunnen uitwerken.
- De drie grote pijlers van IT-beveiliging (netwerken, gegevens, software).
- Uw gevoelige netwerken, netwerk- en toepassingsfirewalltechnologieën verdelen.
- Uw gegevens onleesbaar maken tijdens opslag en transport, cryptografische technieken.
- Uw software beveiligen door harding en veilig ontwerp.
- Beheer van softwarekwetsbaarheden, CVE's/CVSS'en kunnen gebruiken.

8) Supervisie van de beveiliging

- Operationele governance- en beveiligingsindicatoren.
- Cyberbeheer: ISO-conform dashboard.
- Uw verdediging voorbereiden (IDS, incidentdetectie, enz.).
- Verwerking van waarschuwingen en cyber forensics, de rol van CERT's.

9) Wettelijke inbreuken op het systeem voor automatische gegevensverwerking

- Herhaling, definitie van het systeem voor automatische gegevensverwerking (ADPS).
- Soorten inbreuken, Europese context, de LCEN-wet. De AVG-verordening
- Wat zijn de juridische risico's voor het bedrijf, zijn bestuurders en de CISO?

10) Aanbevelingen voor een "wettelijke" beveiliging van het IS

- De bescherming van persoonsgegevens, sancties bij niet-naleving.
- Het gebruik van biometrie in Frankrijk.

- Cybersurveillance van werknemers: grenzen en wettelijke beperkingen.
- De rechten van werknemers en de sancties die de werkgever riskeert.

DATA

Neem contact met ons op