

Opleiding : Cloud computing, bestuur en beveiliging

seminarie - 3d - 21u00 - Ref. CCG

Prijs : 2550 € V.B.



4,6 / 5

BEST

Cloud computing stelt bedrijven in staat om het IT-beheer te vereenvoudigen en geld te besparen, maar het brengt ook zorgen over de beveiliging met zich mee. In deze uitgebreide cursus wordt uitgelegd hoe u de risico's kunt inschatten (met name regelgevingsrisico's) en welke oplossingen u moet implementeren om de cyberbeveiligingsuitdaging het hoofd te bieden.



Pedagogische doelstellingen

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

- ✓ Leer hoe je virtuele omgevingen en netwerktoegang tot de cloud kunt beveiligen
- ✓ Risico's van cloud computing beoordelen en beheren in overeenstemming met ISO 27005
- ✓ Controle en toezicht op cloudbeveiliging
- ✓ Leer over juridische aspecten en naleving van regelgeving

Doelgroep

IT-directeuren, CISO's, IS-architecten, netwerk-/opslag-/systeemingenieurs, beveiligingsmanagers, projectmanagers, consultants.

Voorafgaande vereisten

Basiskennis van Cloud SaaS, PaaS, IaaS-modellen en IT-beveiliging. Begrippen van projectmanagement.

Opleidingsprogramma

1 Inleiding tot beveiliging van cloud computing

- Definitie van Cloud Computing (NIST) en ISO 17788-norm.
- De belangrijkste leveranciers en de belangrijkste mislukkingen die al zijn waargenomen.
- SecaaS (Security as a Service) biedt.
- De sleutels tot een veilige architectuur in de cloud.

DEELNEMERS

IT-directeuren, CISO's, IS-architecten, netwerk-/opslag-/systeemingenieurs, beveiligingsmanagers, projectmanagers, consultants.

VOORAFGAANDE VEREISTEN

Basiskennis van Cloud SaaS, PaaS, IaaS-modellen en IT-beveiliging. Begrippen van projectmanagement.

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 veiligheid van virtuele omgevingen

- Risico's verbonden aan servervirtualisatie (VM Escape, VM Hopping, VM Theft en VM Sprawl).
- Het probleem van anti-malwarebescherming in een gevirtualiseerde infrastructuur.
- De risico's van kwetsbaarheden, API's en software (Openstack, Docker, VmWare, enz.).

3 Beveiliging voor toegang tot cloudnetwerken

- Beveiligde toegang via IPsec, VPN, https en SSH.
- Specifieke oplossingen voor cloud-toegang (Intercloud, AWS Direct connect, enz.).
- CASB-oplossingen (Cloud Access Security Broker).
- Kwetsbaarheden in Cloud clients (pc's, tablets, smartphones) en browsers.

4 Het werk van de Cloud Security Alliance (CSA)

- Beveiligingsrichtlijnen voor kritieke aandachtsgebieden in cloud computing.
- De twaalf belangrijkste bedreigingen die in de Cloud zijn geïdentificeerd.
- Het OCF raamwerk en de STAR (Security, Trust & Assurance Registry) directory.
- Hoe gebruik ik de Cloud Controls Matrix (CCM) en de CAIQ-vragenlijst?
- Certificaat van kennis over cloudbeveiliging (CCSK).

5 Beveiliging van cloud computing volgens ENISA

- Risicobeoordeling en -beheer in de cloud met behulp van de ISO 27005-norm.
- De vijfendertig risico's die door ENISA zijn geïdentificeerd.
- ENISA-aanbevelingen voor de beveiliging van overheidsclouds.

6 Controle over cloudbeveiliging

- Hoe kan de beveiliging in de cloud worden gecontroleerd: audit, inbraaktest, kwalificatie, certificering?
- Wat is de waarde van de beveiligingslabels Secure Cloud, CSA STAR en Cloud confidence?
- Hoe kan tijdens de hele duur van het contract een continue veiligheidsmonitoring worden uitgevoerd?
- Hoe worden beveiligingsincidenten gedetecteerd en gerapporteerd in de cloud?

7 Het cloudcontract

- De essentiële beveiligingsclausules die in een Cloud-contract moeten worden opgenomen (toezichtcomité, vertrouwelijkheid, enz.).
- Omkeerbaarheidsclausules (upstream & downstream) om te voorkomen dat je door een leverancier in de val wordt gelokt.
- De security audit clausule: kan er nog over onderhandeld worden? Wat moet u doen in een publieke cloud?
- Het belang van gegevenslocatie en jurisdictie.
- Cloud Service Level Agreements (SLA's).
- Sancties en schadeloosstellingen: de verschillen begrijpen.

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.

8 Juridische aspecten en naleving van regelgeving

- Wat zijn de wettelijke verantwoordelijkheden van de leverancier? Hoe zit het met de onderaannemers van de leverancier?
- De nationaliteit van de leverancier en de locatie van de datacenters.
- Het wettelijke kader voor persoonlijke gegevens (Richtlijn 95/46 EG, GDPR, CCT, BCR, enz.).
- Wat zijn de nieuwe garanties van het Privacy Shield na de opzegging van de Safe Harbour-overeenkomst?
- Een update over de USA Patriot Act. Vormt het een bedreiging voor gegevens in de cloud buiten de VS?
- Het wettelijke kader voor persoonlijke gezondheidsgegevens (wet van 26 januari 2016).
- Hosts van gezondheidsgegevens (ASIP-accreditatie, beveiligingsverplichtingen, lokalisatie van gegevens, enz.)

9 Cloudbeveiligingsstandaarden

- Wat is de waarde van de ISO 27001-beveiligingscertificering die leveranciers laten zien?
- ISO/IEC 17788:2014 (woordenschat) en ISO/IEC 17789:2014 (referentiearchitectuur).
- De nieuwe ISO/IEC standaarden (27017 & 27018) gewijd aan beveiliging in de Cloud.
- Welke bijdrage levert ISO 27018 aan de bescherming van persoonlijke gegevens in de cloud?
- De ISO 27017-norm en zijn ideale aanvulling CSA Cloud Control Matrix.

10 Licenties beheren in de cloud

- Begrijp waarom licentiebeheer complexer is in de cloud.
- Hoe zorg je voor naleving?
- De grenzen van Software Asset Management-tools in de cloud.
- Inventarisatie en reconciliatie van geïnstalleerde, aangeschafte en gebruikte licenties in de Cloud.

Data en plaats

KLAS OP AFSTAND

2026 : 24 maa., 19 mei, 13 okt., 15 dec.

PARIS LA DÉFENSE

2026 : 24 maa., 19 mei, 13 okt., 15 dec.