Publicatiedatum : 12/03/2024

Opleiding : VPN, draadloze en mobiliteitsbeveiliging, samenvatting

seminarie - 2d - 14u00 - Ref. VPN
Prijs : 1850 € V.B.

5 / 5

Draadloze communicatietechnologieën en mobiele terminals maken het tegenwoordig veel gemakkelijker om toegang te krijgen tot bedrijfsapplicaties. Dit seminar biedt een uitgebreid overzicht van de bedreigingen en kwetsbaarheden en praktische oplossingen om je hiertegen te beschermen.

Pedagogische doelstellingen

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

- Veiligheidsrisico's beoordelen in een mobiele context
- De aanvalstypen kennen
- De VPN-oplossing begrijpen
- Draadloze netwerken en smartphones beveiligen

Doelgroep

IT-directeuren, CISO's, beveiligingsmanagers, projectmanagers, consultants, beheerders.

Voorafgaande vereisten

Basis computervaardigheden.

Praktische modaliteiten

Voorbeeld

Approche théorique et pratique avec démonstration, avantages et inconvénients des solutions, retours d'expérience.

Opleidingsprogramma

DEELNEMERS

IT-directeuren, CISO's, beveiligingsmanagers, projectmanagers, consultants, beheerders.

VOORAFGAANDE VEREISTEN

Basis computervaardigheden.

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 Bedreigingen en kwetsbaarheden

- Ontwikkelingen in cybercriminaliteit in Frankrijk.
- Statistieken en trends in aanvallen.
- Risicobeoordeling in een mobiele context.

2 Aanvallen op de gebruiker

- Gebruikersgeoriënteerde aanvalstechnieken.
- Technieken voor social engineering.
- Kwaadaardige code en sociale netwerken.
- De specifieke gevaren van Web 2.0.
- Aanval op wachtwoorden.
- Aanval "Man in het midden".

3 Aanvallen op clientwerkstations

- Specifieke risico's voor clientwerkstations (wormen, virussen, enz.).
- De veiligste browser.
- Rootkitbrowser en werkstation van de gebruiker.
- Hoe effectief is antivirussoftware eigenlijk?
- De risico's van verwijderbare randapparatuur.
- De rol van de persoonlijke firewall.
- Beveiliging USB-sleutel.
- Client-werkstations en virtualisatie.

4 Beveiliging van een virtueel privénetwerk (VPN)

- Tunnelingtechnieken. Toegang op afstand via het internet: overzicht van het aanbod.
- PPT, LTP en L2F protocollen voor VPN's.
- De IPsec standaard en de AH, ESP en IKE protocollen.
- VPN-oplossingen voor 3G-toegang.
- Welke oplossingen voor Blackberry, iPhone... ?
- SSL VPN: de technologie en haar beperkingen.
- Overzicht van het SSL VPN aanbod. Selectiecriteria.
- IPsec of SSL VPN: wat is de juiste keuze voor mobiele werkstations?

5 Draadloze netwerkbeveiliging

- Beveiliging toegangspunt (SSID, MAC-filtering, enz.).
- Waarom is WEP gevaarlijk? Wat zijn de voordelen van WPA, WPA2 en de 802.11i-standaard?
- Authenticatie in zakelijke Wi-Fi-netwerken.
- VPN-technologieën (IPsec) voor Wi-Fi-netwerken.
- Hoe wordt de beveiliging van een Wi-Fi-hotspot gegarandeerd?
- Aanvaltechnieken op WPA en WPA2.
- Rogue AP.
- Specifieke aanvallen op Bluetooth.

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.

6 Smartphone beveiliging

- Mobiele beveiliging (Edge, 3G, 3G+...).
- De specifieke risico's van smartphones.
- Inbreuken op de beveiliging: de top tien per platform.
- Virussen en kwaadaardige code: wat is het echte risico?
- Bescherm je gegevens bij verlies of diefstal.

Demonstratie

Implementatie van een zeer veilige Wi-Fi-toegang met IPsec en EAP-TLS.
Man in the Middle" aanval op een HTTPS-webtoepassing via een smartphone (sslsnif en sslstrip).

Data en plaats

KLAS OP AFSTAND
2026 : 9 juni, 24 sep., 15 dec.

PARIS LA DÉFENSE
2026 : 9 juni, 24 sep., 15 dec.