Opleiding : Veiligheid in cyberspace

seminarie - 3d - 21u00 - Ref. SCE
Prijs : 2550 € V.B.

4,4 / 5

Cybercriminaliteit is een groeiende bedreiging voor de samenleving en cybercriminelen handelen vanaf elke plek om bedrijfsinfrastructuren aan te vallen via cyberspace. Deze cursus laat zien hoe je kunt voldoen aan de beveiligingseisen van bedrijven en hoe je beveiliging kunt integreren in de architectuur van een informatiesysteem. Je krijgt een gedetailleerde analyse van bedreigingen en indringingsmiddelen, evenals een overzicht van de belangrijkste beveiligingsmaatregelen die op de markt verkrijgbaar zijn.

Pedagogische doelstellingen

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

- Inzicht in de evolutie van criminelen in cyberspace
- Inzicht in beveiliging in de cloud
- Weten hoe je clientwerkstations en -toepassingen moet beveiligen
- De principes van cryptografie begrijpen
- Leren hoe je IS-beveiligingstoezicht beheert

Doelgroep

Iedereen die de grondbeginselen van IS-beveiliging wil leren.

Voorafgaande vereisten

Afronding van de training "Grondbeginselen van IB-beveiliging".

Opleidingsprogramma

1 Cyberspace en informatiebeveiliging

- Principes van veiligheid: verdediging in de diepte, veiligheidsbeleid.
- Fundamentele concepten: risico, vermogen, bedreiging, enz.
- Methoden voor risicobeheer (ISO 27005, EBIOS, MEHARI). Overzicht van ISO 2700x-normen.
- De evolutie van cybercriminaliteit. Identificeren van dreigers.
- Nieuwe bedreigingen (APT, spear phishing, watering hole, exploit kit, etc.).
- Onvolkomenheden in de beveiliging van software.
- Het verloop van een cyberaanval (NIST).
- 0day-kwetsbaarheden, 0day-exploits en exploitatiekits.

DEELNEMERS

Iedereen die de grondbeginselen van IS-beveiliging wil leren.

VOORAFGAANDE VEREISTEN

Afronding van de training "Grondbeginselen van IB-beveiliging".

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 Firewalls, virtualisatie en cloud computing

- Proxyservers, reverse proxy, adresmaskering.
- Firewall-gebaseerde perimeterbescherming.
- De verschillen tussen UTM, enterprise, NG en NG-v2 firewalls.
- Intrusion Prevention System (IPS)-producten en IPS NG.
- DMZ-oplossingen (gedemilitariseerde zone).
- Kwetsbaarheden in virtualisatie.
- De risico's van Cloud Computing volgens ANSSI, ENISA en CSA.
- De cloudcontrolematrix en het gebruik ervan bij het evalueren van cloudaanbieders.

3 Beveiliging client-werkstation

- Bedreigingen voor clientwerkstations.
- De rol van de persoonlijke firewall en zijn beperkingen.
- Anti-virus/anti-spyware software.
- Beveiligingspatches op clientwerkstations.
- Beveilig verwijderbare apparaten.
- Controleren of klanten voldoen aan de NAC-oplossingen.
- Kwetsbaarheden in browsers en plug-ins.

4 De basis van cryptografie

- De belangrijkste gebruiksbeperkingen en wetgeving in Frankrijk en de rest van de wereld.
- Cryptografische technieken.
- Openbare sleutel en symmetrische algoritmen.
- Hashfuncties.
- Openbare sleutelarchitecturen.
- Programma's voor cryptoanalyse van NSA en GCHQ.

5 Het verificatieproces voor gebruikers

- Biometrische authenticatie en de juridische aspecten.
- Challenge/response verificatie.
- Technieken om wachtwoorden te stelen, brute kracht, entropie van geheimen.
- Sterke verificatie.
- Smartcard- en X509-clientcertificaatverificatie.
- De "3A" architectuur: concept van SSO, Kerberos.
- IAM-platforms.
- Identiteitsfederatie via API's van sociale netwerken.
- Identiteitsfederatie voor de onderneming en de cloud.

6 Handelsveiligheid

- SSL Crypto API en ontwikkelingen van SSL v2 naar TLS v1.3.
- Aanvallen op SSL/TLS-protocollen en HTTPS-stromen.
- Hardwarematige insluiting van sleutels, FIPS-140-3 certificering.
- Beoordeel eenvoudig de beveiliging van een HTTPS-server.
- De IPsec standaard, AH en ESP modi, IKE en sleutelbeheer.
- De problemen tussen IPSec en NAT oplossen.
- SSL VPN's. Wat is het voordeel ten opzichte van IPSec?
- Gebruik van SSH en OpenSSH voor veilig beheer op afstand.
- On-the-fly ontcijfering van gegevensstromen: juridische aspecten.

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 De beveiliging van draadloze netwerken en mobiele apparaten

- Specifieke WiFi-aanvallen. Hoe kunnen Rogue AP's worden gedetecteerd?
- Beveiligingsmechanismen voor terminals.
- Kwetsbaarheden in WEP. Zwakke plekken in het RC4-algoritme.
- Beschrijving van risico's.
- De beveiligingsstandaard IEEE 802.11i. WLAN-architectuur.
- Verificatie van gebruikers en terminals.
- WiFi-authenticatie in de onderneming.
- Audittools, gratis software, aircrack-ng, Netstumbler, WifiScanner...
- Bedreigingen en aanvallen op mobiliteit.
- iOS, Android, Windows mobile: sterke en zwakke punten.
- Virussen en kwaadaardige code op mobiele telefoons.
- MDM- en EMM-oplossingen voor wagenparkbeheer.

8 Software beveiliging

- Webapplicaties en mobiele applicaties: wat zijn de verschillen op het gebied van beveiliging?
- De belangrijkste risico's volgens OWASP.
- Richt je op XSS-, CSRF-, SQL-injectie- en sessiekapingaanvallen.
- De belangrijkste veilige ontwikkelingsmethoden.
- Beveiligingsclausules in ontwikkelingscontracten.
- De applicatiefirewall of WAF.
- Hoe beoordeel je het beveiligingsniveau van een applicatie?

9 De concepten van Security by Design en Privacy by Design

- Veiligheid in ontwerp.
- De Security by Design-benadering van beveiligingsgarantie.
- De 7 fundamentele principes van ingebouwde privacy.
- Tijdens het hele proces wordt rekening gehouden met privacy.

10 Veiligheidstoezicht

- Veiligheidsdashboards.
- Beveiligingsaudits en penetratietests.
- De juridische aspecten van penetratietesten.
- IDS sondes, VDS scanner, WASS.
- Hoe reageer je effectief op aanvallen?
- Leg het bewijs vast.
- Een SIEM-oplossing implementeren.
- ANSSI-labels (PASSI, PDIS & PRIS) voor uitbesteding.
- Hoe reageer je in het geval van een indringer?
- Gerechtelijke expertise: de rol van een gerechtelijk deskundige (in straf- of civiele zaken).
- Particuliere juridische expertise.

Data en plaats

KLAS OP AFSTAND
2026 : 16 maa., 15 juni, 28 sep., 30 nov.

PARIS LA DÉFENSE
2026 : 16 maa., 15 juni, 28 sep., 30 nov.