Netwerk-/internetcyberbeveiliging, samenvatting
bescherming van het IS en de bedrijfscommunicatie

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

Dit seminarie laat zien hoe u aan de beveiligingseisen van bedrijven kunt voldoen, en beveiliging in de architectuur van een informatiesysteem kunt integreren. Het omvat een gedetailleerde analyse van bedreigingen en middelen om in te breken, evenals een overzicht van de belangrijkste beveiligingsmaatregelen die op de markt beschikbaar zijn. U zult over de technische en juridische elementen beschikken om de beveiliging van uw IS te waarborgen en te superviseren.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

De evolutie van cybercriminaliteit en de uitdagingen ervan kennen

De beveiliging van de cloud, toepassingen en clientwerkstations onder de knie krijgen

De principes van cryptografie begrijpen

Het IS-beveiligingssupervisieproces beheren

HET PROGRAMMA

laatste update: 11/2021

1) Informatiebeveiliging en cybercriminaliteit

- Beveiligingsprincipes: diepteverdediging, cyberrisicomodellering.
- Risicobeheermethoden (ISO 27005, EBIOS RM).
- Overzicht van de ISO 2700x-normen.
- Evolutie van cybercriminaliteit.
- Nieuwe bedreigingen (APT's, spear phishing, watering hole, Crypto-jacking ...).
- Beveiligingsproblemen in software.
- Het verloop van een cyberaanval (Kill Chain).
- 0day-gebreken, 0day Exploit en exploitatiekit.

2) Firewall, virtualisatie en cloud computing

- Perimeterbescherming op basis van firewalls en DMZ-zones.
- Verschillen tussen UTM-, bedrijfs-, NG- en NG-v2-firewalls.
- IPS-producten (IPS = 'Intrusion Prevention System') en NG IPS-producten.
- Kwetsbaarheden in de virtualisatie.
- Risico's verbonden met cloud computing volgens het CESIN, het ENISA en de CSA.
- CASB-oplossingen voor de beveiliging van gegevens en toepassingen in de cloud.
- De Cloud Controls Matrix en het gebruik ervan bij de evaluatie van cloudleveranciers.

3) Beveiliging van clientwerkstations

- Clientwerkstationgerichte bedreigingen begrijpen.
- Antivirus-/antispywaresoftware.
- Hoe om te gaan met beveiligingspatches op clientwerkstations.
- Ransomware: preventieve en corrigerende maatregelen.
- Hoe verwijderbare apparaten te beveiligen?
- Kwetsbaarheden van browsers en plug-ins.

DEELNEMERS

CISO's, IS-afdelingen, architecten, ontwikkelaars, projectleiders, pre-sales vertegenwoordigers, systeem- en netwerkbeheerders.

VOORAFGAANDE VEREISTEN

Algemene kennis van IT en het internet is vereist.

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.

- De Drive-by-downloadaanval.
- Bedreigingen via USB-sticks (BadUSB, rubber ducky ...).

4) Grondbeginselen van de cryptografie
- Cryptografische technieken.
- Openbaresleutel- en symmetrische algoritmen.
- Gewone, salted en keyed hashing-functies (HMAC).
- Openbare-sleutelarchitecturen (PKI).
- CC-certificering en ANSSI-kwalificatie van cryptografische producten.

5) Authenticatie en machtiging van gebruikers
- Biometrische authenticatie en juridische aspecten.
- Authenticatie door antwoord op verificatievraag.
- De verschillende aanvalstechnieken (brute force, keylogger, credential stuffing ...).
- Sterke multifactorauthenticatie (MFA).
- Authenticatie met smartcard en X509-clientcertificaat.
- HOTP- en TOTP-standaarden van de OATH.
- UAF- en U2F-standaarden van de FIDO-alliantie (FIDO = ‘Fast ID Online’).

6) Beveiliging van netwerkstromen
- SSL Crypto API en evolutie van SSL v2 naar TLS v1.3.
- Aanvallen op SSL-/TLS-protocollen.
- Aanvallen op HTTPS-stromen.
- Confinement hardware van sleutels, FIPS-140-2-certificeringen.
- IPsec-standaard, AH- en ESP-modi, IKE en sleutelbeheer.
- De problemen tussen IPSec en NAT overwinnen.
- SSL VPN's. Welk belang ten opzichte van IPSec?
- Gebruik van SSH en OpenSSH voor beveiligd beheer op afstand.
- Snelle ontcijfering van stromen: juridische aspecten.
- De beveiliging van een HTTPS-server gemakkelijk beoordelen.

7) Wifi-beveiliging
- Specifieke wifi-aanvallen.
- Hoe Rogue AP’s te detecteren?
- Terminalbeveiligingsmechanismen.
- KRACK-aanval op WPA en WPA2.
- Beschrijving van de risico's.
- De IEEE 802.11i-beveiligingsstandaard.
- De bijdragen van WPA3 en de DragonBlood-kwetsbaarheden.
- Authenticatie van gebruikers en terminals.
- Wifi-authenticatie in het bedrijf.
- Audithulpmiddelen, open software, aircrack-ng, Netstumbler, WiFiScanner ...

8) Smartphonebeveiliging
- Bedreigingen en aanvallen op de mobiliteit.
- iOS en Android: sterke en zwakke punten.
- Virussen en schadelijke code op mobiele apparaten.
- MDM- en EMM-oplossingen voor wagenparkbeheer.

9) Toepassingsbeveiliging
- Toepassing van het diepteverdedigingsprincipe.
- Web- en mobiele toepassingen: wat zijn de beveiligingsverschillen?
- De belangrijkste risico's volgens OWASP.
- Focus op XSS-, CSRF-, SQL injection- en session hijacking-aanvallen.
- De belangrijkste methoden voor beveiligde ontwikkeling.
- Welke beveiligingsclausule in ontwikkelingscontracten?

- De toepassingsfirewall of WAF.
- Het beveiligingsniveau van een toepassing beoordelen.

10) Actief beveiligingsbeheer en actieve beveiligingssupervisie

- Beveiligingsaudits (scope en raamwerken: ISO 27001, AVG ....).
- Penetratietests (black box, gray box en white box).
- Hoe doeltreffend op aanvallen te reageren?
- Een SIEM-oplossing implementeren.
- Uw Security Operation Center (SOC) implementeren of uitbesteden?
- SOC 2.0-technologieën (CASB, UEBA, Deceptive Security, EDR, SOAR, machine learning ...).
- ANSSI-labels (PASSI, PDIS en PRIS) voor uitbesteding.
- Procedures voor reactie op incidenten (ISO 27035 en NIST SP 800-61 R2).
- “Bug Bounty"-platforms.

DATA

Neem contact met ons op