Publicatiedatum : 06/06/2024

Opleiding : Jezelf beschermen tegen virussen en malware in de Microsoft-omgeving

Praktijkcursus - 2d - 14u00 - Ref. MAL
Prijs : 1370 € V.B.

5 / 5

Deze cursus geeft informatie over computervirussen en malware die de prestaties van computers verminderen en bedrijfsactiviteiten verstoren. Aan het einde van de cursus ben je in staat om een aanpak te ontwikkelen, de beste technieken te kiezen en de juiste tools te gebruiken om ze op te sporen en uit te roeien.

Pedagogische doelstellingen

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

- Malware of virussen identificeren en neutraliseren
- Onderscheid maken tussen een infectie en een storing
- Gebruik de juiste hulpmiddelen om ze op te sporen en uit te roeien
- Een actieplan opstellen in overeenstemming met de behoeften van het bedrijf

Doelgroep

Technici, beheerders en ingenieurs op het gebied van systemen/netwerken/beveiliging.

Voorafgaande vereisten

Goede kennis van het beheren van Windows werkstations in een netwerk.

Praktische modaliteiten

Praktisch werk

Werkstations met Windows 10 en Windows Server 2016 worden gebruikt om de gepresenteerde concepten in de praktijk te brengen.

Opleidingsprogramma

DEELNEMERS

Technici, beheerders en ingenieurs op het gebied van systemen/netwerken/beveiliging.

VOORAFGAANDE VEREISTEN

Goede kennis van het beheren van Windows werkstations in een netwerk.

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 Basisconcepten

- Wat zijn virale infecties?
- Definitie van het virusconcept. De juiste hulpmiddelen.
- De jungle van namen (backdoor, worm, Trojaans paard, bot/botnet...).
- Algemene principes van hoe bedreigingen werken.
- De meest voorkomende infectievectoren.
- Beveiliging uitschakelen en omzeilen.

Praktisch werk

Analyse van een infectie (backdoor, rootkit, enz.). Spyware en phishing.

2 Hoe kan ik mezelf beschermen? Antivirus en firewall

- Werkingsprincipes.
- Soorten detectie (door handtekening, heuristiek, gedrag, enz.).
- De Packers (UPX, FSG, Upack, Armadillo, Themida...).
- Vals alarm.
- Overzicht firewalls. De juiste tools.
- Wat kan het detecteren?
- Wat zijn de grenzen?

Praktisch werk

Detectietests met de verschillende typen en bypasses van een firewall.

3 Mechanismen van infectie

- Hoe programma's werken.
- De relatie met DLL's.
- Code injecties.
- Hoe detecteer je een infectie bij het opstarten? De juiste hulpmiddelen.
- Windows opstartherinnering.
- Het juiste gereedschap.
- Infecties en het register.

Praktisch werk

Voorbeeld van een virale injectie. Simulatie van kwaadaardige code in de opstartfase en uitroeiingstechnieken.

4 Identificeren voor betere uitroeiing

- Het belang van het correct identificeren van de bedreiging.
- Gebruik het meest geschikte hulpprogramma: Windows Defender, concurrerende tools.
- Uitroeien "de eeuwige terugkeer".
- Verwijder inactieve residuen.

Praktisch werk

Scripts gebruiken om infecties tegen te gaan. Hoe infectiebronnen identificeren? Uitroeien zonder opmaak.

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.

5 Liever voorkomen dan genezen

- Bewustmaking van gebruikers.
- De in te voeren procedures.
- Je beveiligingssystemen kiezen.
- Back-ups en herstelpunten.
- Het juiste gereedschap kiezen.
- Marktoplossingen en het antivirusprogramma.

Praktisch werk
De fasen in een actieplan voor een bedrijf identificeren.

Data en plaats

KLAS OP AFSTAND
2026 : 11 juni, 22 okt.

PARIS LA DÉFENSE
2026 : 11 juni, 22 okt.