CYBERSECURITY (VOOR IT-MEDEWERKERS)

Activiteitspool

PREVENTIE EN VEILIGHEID

Formule

Face-to-face

Prijs/deelnemer

300,00 €
Mogelijk gratis: bekijk de voorwaarden op onze website.

Max. aantal deelnemers/sessie

12

Duur van de opleiding

3 dagen (8u30-16u30)

Contactpersoon

Lamia MALLOULI Verantwoordelijke voor het Secretariaat

lmallouli@erap-gsob.brussels

Beschrijving van de opleiding

Het cybersecuritydomein evolueert razendsnel en er duiken voortdurend nieuwe problemen op. Computerhacking, datalekken, elektronische fraude, onderbreking van administratieve diensten of verstoring van hun infrastructuur komen nog steeds al te vaak voor. Om al die problemen aan te pakken en tegelijk tegemoet te komen aan de behoeften van de lokale en gewestelijke besturen heeft de GSOB een programma ontwikkeld dat meer klaarheid schept en tools aanreikt om cybercriminaliteit te bestrijden. Dit programma bestaat uit twee opleidingsmodules, op maat van de verantwoordelijkheden van iedere deelnemer.

Deze module biedt een coherente referentiebasis die medewerkers van de IT-diensten (IS Engineers, Analysts, Developers, ...) van lokale en (para)gewestelijke besturen in staat stelt om IT beveiligingsmaatregelen en -systemen uit te rollen.

Dit programma is onderdeel van het Globaal Veiligheids- en Preventieplan (GVPP) en Brusafe.

U bent IT Manager en/of stuurt een team aan? Dan kunt u een tweede 2-daagse module volgen waarbij u leert hoe u een cyberse curitystrategie binnen uw organisatie kunt uittekenen en uitvoeren.

Doelstellingen

- De deelnemers in staat stellen om samen met de IT Managers gemeenschappelijke begrippen te hanteren om de communicatie vlotter te laten verlopen en versterking te geven aan de teams.
- De deelnemers in staat stellen om kwetsbaarheden in een server op te sporen en een effectieve en in het cybersecuritymilieu erkende beveiliging te bieden.
- De deelnemers helpen om aanvallen vanaf het internet te begrijpen en samen met hen een oplossing vinden om een beveiliging op te bouwen die geschikt is voor hun infrastructuren.
- De deelnemers in staat stellen om na de opleiding verder te leren en om zelfstandig training te volgen.
- De deelnemers voorstellen doen voor het verbeteren van hun infrastructuren om een regelmatige bescherming van hun bestuur/organisatie te garanderen op het vlak van cybersecurity.
- De deelnemers in staat stellen om de veiligheid van de webapplicaties van hun bestuur/ organisatie te controleren en oplossingen voor te stellen aan de personen die verantwoordelijk zijn voor de ontwikkeling van deze platformen.
- De deelnemers helpen om «de oplossing» te begrijpen, zodat ze deze of een soortgelijke oplossing in hun infrastructuren kunnen integreren.

Doelgroep

De opdleiding is bestemd voor de IT-medewerkers van de Brusselse plaatselijke of gewestelijke besturen en van de hierna genoemde Brusselse instellingen van openbaar nut.

Bedoelde instellingen (niet-exhaustieve lijst):
- Gemeenten
- OCMW's
- Centrum voor Informatica voor het Brusselse Gewest
- Net Brussel
- Leefmilieu Brussel
- Brusselse politiezones
- Gewestelijke Overheidsdienst Brussel
- Brussel Preventie en Veiligheid
- Gewestelijke school voor Veiligheids-, Preventie- en Urgentieberoepen
- Brusselse Gewestelijke Huisvestingsmaatschappij
- ...

Pedagogische methoden

Deze bijzonder interactieve, praktijkgerichte opleiding wordt aan de hand van concrete en herkenbare voorbeelden geïllustreerd en begeleid door lesgevers die gespecialiseerd zijn in de behandelde leerstof. De lesgever wisselt verschillende leerstijlen af en behandelt de thema’s aan de hand van praktische en actieve methodieken die de deelnemers centraal stellen en die een regelmatige interactie moge lijk maken door middel van groepsoefeningen.

Inhoud

Beheer van cybersecurity

- De hackwaarde bepalen
- Het risico beperken
- Cybersecurityhygiëne beheren
- Incidenten beheren

Voorstelling van hackingtools

- Hackingmethoden
- Voorstelling en oefeningen op Kali Linux
- Voorstelling en oefeningen op NMAP
- Voorstelling en oefeningen op Metasploit

Beveiliging van de werkposten

- Metasploit en NMAP: aanval op een werkpost
- Een werkpost beveiligen
    - Anti-Virus/Anti-Malware
    - Versleuteling van disks
    - Beheer van de programma's
- Governance
    - Gebruikersbeheer
    - Scheiding van gebruikers- en administratoraccounts
    - Gebruik van multifactorauthenticatie

Beveiliging van de servers

- Metasploit en NMAP: aanval op een server
- Een server beveiligen
    - Beveiliging van een webserver (Apache en NGINX)
    - Beheer van databases (SQL en No-SQL)
    - Beheer van rechten
- Governance
    - Beheer van toegang en rechten
    - VPN

Beveiliging van netwerken (LAN)

- Lokaal netwerk (LAN)
    - Verkenning door het gebruik van NMAP
    - Aanval op een netwerk via NMAP
    - Beveiliging van het netwerk d.m.v. VLAN

    - Beveiliging van de netwerktoegang (wifi + fysieke toegang)
    - Oefening met het opzetten van een IDS/IPS (Intrusion Detection)
- Lokaal netwerk (WAN)
    - Aanval op een firewall
    - Hoe een firewall instellen
    - Beheer van belasting

Theorie van cybersecurity

- Versleuteling
- Tools in de Cloud
    - Azure Active Directory
    - Online scanners
    - Online hulpmiddelen
- Online training
    - Voorstelling van platformen voor online training op het gebied van IT-beveiliging
    - Voorstelling van websites om de verworven kennis te verdiepen

Geavanceerde beveiliging

- Hyperconnection en informatiebeveiliging
- Beheer van toegang en rechten (IAM)
- Werking van een SIEM (Security Information and Event Manager)
- Werking van een SOC (Security Operations Center)

Beveiliging van een webapplicatie

- Aanval van een webapplicatie via Kali Linux
- Voorstelling van OWASP
- Beveiligingsonderzoek voor webapplicatie

Oefening: uitrol van een SIEM-oplossing

- Voorstelling van de Open Source ELK-oplossing
- Praktische oefening