CYBERSECURITY (VOOR IT-MANAGERS)

Activiteitspool

PREVENTIE EN VEILIGHEID

Formule

Face-to-face

Prijs/deelnemer

200,00 €
Mogelijk gratis: bekijk de voorwaarden op onze website.

Max. aantal deelnemers/sessie

12

Duur van de opleiding

2 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.

Het doel van deze module is om een coherente referentiebasis te bieden die IT Managers (eventueel ook IT Business Analysts en projectleiders) van de lokale en (para)gewestelijke besturen in staat stelt om een strategie uit te tekenen, te implementeren en te weten hoe ze moeten reageren bij aanvallen of incidenten in hun organisatie.

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

U werkt op een IT-dienst? Dan kunt u een tweede 3-daagse module volgen om u een aantal gemeenschappelijke begrippen eigen te maken, de communicatie met uw verantwoordelijke vlotter te laten verlopen en de nodige kennis te verwerven om cybercriminaliteit effectief te bestrijden.

Doelstellingen

De opleiding heeft de volgende doelstellingen :

- Een strategie van cybersecurity uitwerken ;
- Een strategie van cybersecurity implementeren ;
- Weten hoe te reageren op aanvallen / incidenten binnen de eigen organisatie.

Doelgroep

De opleiding is bestemd voor alle IT-managers 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

Sensibilisering rond hacking

- Voorstelling van hackingmethoden
- Voorstelling van hackingtools
- Demonstratie van een hack op een gecontroleerd informatiesysteem

→ Doel: de deelnemers bewust maken van het belang van informatiebeveiliging, hun aandacht vestigen op het gemak waarmee hackers systemen kunnen aanvallen en de hackingmethoden en -tools toelichten, zodat ze kwetsbaarheden in infrastructuren kunnen opsporen.

Beheer van risico's op het vlak van cybersecurity

- Risico's identificeren
    - Risico's/bedreigingen identificeren
    - Kwetsbaarheden en system failures identificeren
    - De voordelen/winst voor een hacker bepalen
- Het risico beperken
    - Risico's prioriteren
    - Oefenen in het bepalen van prioriteiten
    - Verkenning van de EBIOS-methode - ANSSI-risicoanalyse

→ Doel: de deelnemers in staat te stellen om de risico's waaraan de systemen onder hun controle zijn bloot¬gesteld gemakkelijk en snel te identificeren. De tools aanreiken waarmee ze zich ook na de opleiding verder kunnen bekwamen in het detecteren van risico's.

Beveiliging van de omgeving

- Governance
    - Financieel aspect
    - Inventarissen
- Hygiëne en standaardisatie van informatiebeveiliging
    - Gezamenlijke brainstorm over de huidige hygiëne en standaardisering van het beveiligingsbeleid van het eigen bestuur
    - Ontwikkeling van een informatiebeveiligingshygiëne in groep, meer bepaald :
        - Een beleid i.v.m. wachtwoorden
        - Een beleid voor het aanmaken van accounts
        - Een beleid voor het delen van informatie en bestanden
        - Een beleid voor het beheren van persoonlijke randapparatuur
        - Een communicatiebeleid
    - Risico's bij niet-standaardisering van cybersecurity
    - Voorstelling en oefening in het beveiligen van IT-systemen :
        - Servers
        - Werkposten
        - Netwerken (LAN/WAN/WI-FI)
        - Communicatie

→ Doel: het belang van goed governance benadrukken, ondersteunen met een inventa¬ris en oefenen om inzicht te krijgen in de beveiliging van de verschillende systemen.

Incidentbeheer

- Incidenten beheren

- Implementeren

→ Doel: de deelnemers in staat stellen om het belang van een planning voor het beheren van inci¬denten te begrijpen en hen helpen bij het vinden van manieren om dit te implementeren.

Opsporing van kwetsbaarheden en indringing

- Tools voor het opsporen van kwetsbaarheden
- Tools voor het detecteren van indringing

→ Doel: de deelnemers in staat stellen om kwetsbaarheidscontroles uit te voeren zonder een beroep te doen op externe consultants, tools demonstreren die het mogelijk maken om indringing in hun systemen te detecteren aan de hand van een praktische oefening op een Open Source SIEM-oplossing.

Social engineering-oplossingen

- De rechten van gebruikers beperken
- Medewerkers opleiden/bewustmaken

→ Doel: de deelnemers in staat stellen om IAM-oplossingen te bedenken om de risico's van social en¬gineering te beperken en medewerkers op te leiden zodat aanvallen worden voorkomen.

Opstelling van een beveiligingsbeleid

- De standaardisatie van de IT-beveiliging herbekijken
- Stand van zaken i.v.m. ISO 27001

→ Doel: de deelnemers herinneren aan het belang van de standaardise¬ring van de beveiliging en hen confronteren met ISO 27001.

De eigen voorstellen in verband met cybersecurity verdedigen voor een directiecomité/bestuurscomité

→ Doel: de deelnemers de nodige argumenten aanreiken om hun IT-beveiligingsbeleid te verdedigen.

Aanvullende informatie

Houd er rekening mee dat een lunch in deze opleiding is begrepen om de uitwisselingen voort te zetten. Er zal een assortiment broodjes worden aangeboden. Gelieve ons via e-mail (secretariat@erap-gsob.brussels) uw intoleranties en/of specifiek dieet mee te delen, ten laatste een week voor het begin van de sessie zodat we eventueel gepaste maatregelen kunnen nemen.