CYBERSECURITE (A DESTINATION DES IT-MANAGERS)

Pôle d'activité

PREVENTION ET SECURITE

Formule

Présentiel

Prix/participant

200,00 €
Gratuité possible : consultez les conditions sur notre site.

Nombre max. de participants/session

12

Durée de la formation

2 jours (8h30-16h30)

Personne de contact

Lamia MALLOULI Responsable du service Secrétariat

lmallouli@erap-gsob.brussels

Détail de la formation

Le domaine de la cyber sécurité évolue très rapidement et de nouveaux défis ne cessent d'émerger. Les cas de piratage informatique, de violation de données, de fraude électronique, d'interruption de services administratifs ou de perturbation de leurs infrastructures arrivent encore trop régulièrement. Pour faire face à cette problématique et afin de répondre aux besoins des administrations locales et régionales, l'ERAP a élaboré un programme visant à apporter davantage de clarté ainsi qu'à donner des outils afin de lutter contre la cybercriminalité. Ce programme est décliné en deux modules de formations, adapté au niveau de responsabilité de chacun.

Le présent module se propose donc d'offrir une base de référence cohérente, qui permettra aux IT managers (éventuellement les IT business analysts et chefs de projets) issus des administrations locales et (para)régionales, d'élaborer une stratégie, de l'implémenter et de savoir comment réagir en cas d'attaques ou d'incidents dans son organisation.

Ces programmes s'inscrivent dans le cadre du Plan Global de Sécurité et de Prévention (PGSP) et de Brusafe.

Vous êtes collaborateur au sein d'un service IT ? Un second module de 3 journées vous est proposé afin d'intégrer les notions communes, faciliter la communication avec votre respon¬sable et acquérir les connaissances nécessaires pour lutter contre la cybercriminalité.

Objectifs

A minima, la formation poursuivra les objectifs suivants :

- Élaborer une stratégie cyber-sécurité ;
- Implémenter une stratégie cyber-sécurité ;
- Savoir réagir en cas d'attaques/d'incidents dans son organisation.

Public cible

La formation est destinée à tous les IT managers des pouvoirs locaux ou régionaux bruxellois et des organismes d'intérêt public bruxellois ci-dessous.

Institutions visées (non-exhaustif) :
- Communes
- CPAS
- Centre d'Informatique pour la Région Bruxelloise
- Bruxelles Propreté
- Bruxelles Environnement
- Zones de Police Bruxelloises
- Service Public Régional de Bruxelles
- Bruxelles Prévention Sécurité
- Ecole Régionale des Métiers de la Sécurité, de la Prévention et du Secours
- Société du Logement de la Région Bruxelloise
- …

Méthodes pédagogiques

Résolument axée sur la pratique, illustrée d'exemples adéquats et animée par des intervenants spécialistes de la matière traitée, cette formation se veut très interactive et basée sur des cas concrets. Pour ce faire, le formateur / la formatrice alterne les styles pédagogiques et les thèmes sont abordés via des méthodologies pratiques et actives permettant de mettre les bénéficiaires au centre de la formation et d'être régulièrement en interaction à l'aide d'exercices en groupe.

Contenu

Sensibilisation au piratage

- Présentation de la méthodologie d'un piratage
- Présentation d'outils utilisés lors d'un piratage
- Démonstration d'un piratage sur un système d'information contrôlé

→ Objectif : sensibiliser les participants à l'importance de la sécurité de l'information, attirer leur attention sur la facilité que représente un piratage ainsi que présenter les outils et les méthodes de piratage permettant de tester les infrastructures pour déceler les failles.

Gestion du risque en cyber-sécurité

- Identification du risque
  - Identifier les risques/menaces
  - Identifier les vulnérabilités et les failles systèmes
  - Déceler les avantages et gains pour un pirate
- Mitigation du risque
  - Prioriser les risques
  - S'exercer à établir une priorité
  - Découverte de la méthode EBIOS – Analyse de risque de l'ANSSI

→ Objectif : permettre aux participants de déceler facilement et rapidement les risques que représentent les systèmes dont ils ont la charge. Livrer des outils leur permettant de continuer à se former sur la détection des risques après la formation.

Sécuriser l'environnement

- La gouvernance
  - Aspect financier
  - Les inventaires
- Hygiène et uniformisation de la sécurité de l'information
  - Exercice de réflexion collective sur l'hygiène actuelle et l'uniformisation des politiques de sécurités de son administration
  - Construction en groupe d'une hygiène de la sécurité de l'information portant sur :
    - Une politique des mots de passe
    - Une politique de création des comptes
    - Une politique de partage d'informations et de fichiers
    - Une politique de gestion des périphériques personnels
    - Une politique de communication
  - Les risques en cas de non-uniformisation de la cyber-sécurité
  - Présentation et exercice sur la sécurisation des systèmes informatiques :
    - Serveurs
    - Postes de travail
    - Réseaux (LAN/WAN/WI-FI)
    - Communications

→ Objectif : présenter l'intérêt d'établir une gouvernance, de l'appuyer avec un inventaire et s'exercer afin de comprendre la sécurisation des différents systèmes.

Gestion des incidents

- Gestion des incidents
- Implémentation

→ Objectif : permettre aux participants de comprendre l'intérêt de la planification pour la gestion des incidents ainsi que les aider à trouver des moyens de les implémenter.

Détection de vulnérabilité et d'intrusion

- Outils de détection de vulnérabilité
- Outils de détection d'intrusions

→ Objectif : permettre aux participants de faire des audits de vulnérabilités sans avoir recours à des consultants externes, montrer des outils permettant d'opérer de la détection d'intrusions sur leurs systèmes avec un exercice pratique sur un SIEM Open-Source.

Solutions social engineering

- Limiter les droits des utilisateurs
- Construire des formations/sensibilisations pour les collaborateurs

→ Objectif : permettre aux participants d'envisager des solutions IAM pour limiter les risques de social Engineering et permettre de former les collaborateurs pour éviter des attaques.

Construction d'une politique de sécurité

- Révision sur l'uniformisation de la sécurité informatique
- Point sur l'ISO 27001

→ Objectif : rappeler l'intérêt de l'uniformisation de la sécurité et mettre les participants face à l'ISO 27001.

Défendre ses propositions en matière de cyber-sécurité face à un comité de direction/ d'administration

→ Objectif : donner les arguments nécessaires aux participants afin de défendre leur politique en matière de sécurité informatique.

Informations complémentaires

Veuillez noter qu'afin de poursuivre les échanges, un lunch est inclus pour cette formation. Un assortiment de sandwiches sera proposé. Merci de nous communiquer, par email (secretariat@erap-gsob.brussels), vos intolérances et/ou régime alimentaire particulier au minimum une semaine avant le début de la session afin que nous puissions éventuellement prendre les mesures adéquates.