Cybercriminalité pour les managers maîtriser les enjeux techniques et juridiques

★★★★★

PL-46 **2 Jours (14 Heures)**

Description

La cybercriminalité est une menace grandissante sur la société. Les cybercriminels agissent de n'importe où pour s'attaquer aux infrastructures critiques des entreprises. La question abordée dans ce cours ne sera pas de savoir si votre organisme sera attaqué mais de savoir comment répondre efficacement à ces attaques.

À qui s'adresse cette formation ?

Pour qui

Managers métiers ou SI, direction générale, DSI, experts sécurité SI, juristes.

Prérequis

Aucune

Les objectifs de la formation

- Connaître les dangers et identifier les sources de menaces
- Comprendre les risques et les enjeux de sécurité
- Lutter et réagir face aux malveillances
- Savoir organiser une riposte efficace, utile et graduée

Programme de la formation

La cybercriminalité dans l'actualité

- Arnaques au président ? FOVI (Faux Ordre de Virement International).
- Ingénierie sociale, Spear Phishing.
- Vol de données sensibles, intrusion réseaux en tout genre : quelle actualité ? Le darknet, les malwares, les bots/botnets, les ransomwares.
- Infractions aux cartes bancaires, skimming, le darknet.

Enjeux techniques - Bien anticiper

- La gestion des traces, preuves et enregistrements.
- Comment détecter puis caractériser une activité "anormale" ? Les bons réflexes en cas d'intrusion (copie disque, sauvegarde logs.
-).
- Les bonnes pratiques internes : sonde IDS, analyse et corrélation d'évènements (SIEM).

La lutte contre la cybercriminalité

- OCLCTIC, BEFTI ,DGSI, Gendarmerie Nationale/C3N : à chacun sa compétence.
- La SDLC et les investigateurs en cybercriminalité (ICC).
- Signaler tout événement anormal : PHAROS, signal-spam, CERT.
- La LPM, les Opérateurs Importance Vitale, bonnes pratiques et exigences sur les SIIV.
- Les offres de services spécialisés, le rôle de l'ANSSI, les prestataires qualifiés.

Enjeux juridiques - Bien comprendre les risques

- Dualité de la responsabilité juridique : les principes de la responsabilité pénale et civile.
- Cyberdélits en France et à l'international : quel dispositif répressif ? Définitions/jurisprudences sur le "vol" ou la fuite de données, atteinte et maintien frauduleux dans un SI/Réseau.
- Définitions/jurisprudences sur le cyber harcèlement, happy slaping, e-réputation, atteinte à l'image sur le Web.

Cybercriminalité : quels moyens juridiques ?

- Moyens d'investigation et de contrôle des pouvoirs publics : LCEN, LOPPSI 2, Loi de Programmation Militaire.
- Gestion de la preuve : licéité, recevabilité, différence procédure pénale/civile, collecte de la preuve sur le Web.
- Moyens de cryptologie : biens à double usage, régime juridique.
- Illustrations/cas : hacking du SI d'un hôpital/d'un défibrillateur, atteinte d'un SI par un administrateur.
- Illustrations/cas : affaire Jérôme Kerviel, cyberattaque de la messagerie bancaire Swift.