Formation « Gestion de crise cyber »

Réf : SECUCRISE

Les méthodes proactives demeurent limitées et tout un chacun est confronté un jour à une crise due à des incidents informatiques ou un problème de sécurité. Il faut donc maîtriser cette réaction d'urgence et savoir y faire face.

Objectifs

- Apprendre à mettre en place une organisation adaptée pour répondre efficacement aux situations de crise
- Apprendre à élaborer une communication cohérente en période de crise
- Apprendre à éviter les pièges induits par les situations de crise
- Tester votre gestion de crise SSI.

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Directeur ou responsable des systèmes d'information
- Responsable de la sécurité des systèmes d'information
- Responsable de la gestion de crise
- Responsable des astreintes
- Responsable de la gestion des incidents

Pré-requis

- Cette formation ne demande pas de pré-requis particuliers.

Méthode pédagogique

- Cours magistral avec des exemples basés sur le retour d'expérience des formateurs.

Supports

- Support de cours en français au format papier en présentiel et au format numérique en distanciel
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- Cette formation n'est pas certifiante.

Programme

Module 1 : Gestion de crise cyber

- Exemple de crises cyber
- Cas concret détaillé d'une crise cyber "rançongiciel"
  - Pourquoi est-ce la principale crainte des organisations ?
  - Quel est l'état d'un système d'information et d'une organisation après le déclenchement d'un rançongiciel ?
  - Description d'une chronologie classique : l'attaque, le constat, la réaction, le suivi et la sortie de crise

Module 2 : Dispositif de crise et les spécificités d'une cyber-attaque

- Vocabulaire : Investigation/Inforensic, Plan de défense, Assainissement, Durcissement, Reconstruction, Main courante, etc.
- Les spécificités d'une crise cyber
- Qu'est-ce qu'un dispositif de gestion de crise cyber ?
- Organisations types
- Processus de la crise : la montée en crise, le lancement, les points de situation, la sortie de crise
- Outillage
- Facteurs humains et gestion du stress
- Logistique et communication
- Cyber-assurance
- Mise en situation : qualification et premier plan d'actions

Module 3 : Observation & Investigation

- Comprendre pour mieux agir
- Plan d'investigation : vecteurs d'intrusion/patient 0, de propagation, mécanismes de persistance
- Responsabilité de l'investigation
- Posture d'observation
- Actions clefs de l'investigation
- Outillage du plan d'investigation
- Interactions inter et intra cellules de crise
- Mises en situations : définir une posture, mobiliser les ressources, établir un plan d'investigation

Module 4 : Défense & Surveillance

- Plan de défense
- Responsabilité de la défense
- Remédiation
- Reconstruction
- Durcissement
- Surveillance de circonstance et surveillance long terme
- Mises en situation : évaluer les impacts, établir un plan de défense, construire l'organisation nécessaire

Module 5 : Sortie de crise… et l'après crise

- Critères de sortie de crise
- Analyse de la cause primaire ("root cause analysis")
- Construction du RETEX
- Plan d'actions post-crise
- Retour en mode projet et en "RUN"
- S'entraîner / exercices de crise
- Mises en situation : construction un plan d'actions post-crise, acter une sortie de crise, établir un RETEX

Synthèse : les clefs de la gestion de crise cyber

Mise en situation complète