USCB18 - Réagir à une attaque cyber

Mis à jour le 22-04-2022

Code : USCB18

Unité spécifique de type mixte

4 crédits

Responsabilité nationale :
EPN05 - Informatique / 1

Contact national :

Cnam Centre Régional de Bretagne

Zoopôle Les Croix
2 rue Camille Guérin
22440 Ploufragan
0 972 311 312
Isabelle Guée
bzh_master_cybersecurite@lecnam.

Présentation

Objectifs pédagogiques

Description :

Les spécificités liées à la problématique cyber démontrent la nécessité de se préparer à une attaque en formalisant les attaques passées afin d'en reconnaître des « patterns » et en organisant des exercices afin que chaque auditeur puisse en comprendre les enjeux ainsi que le rôle qu'il va devoir jouer sur l'ensemble de la chaîne de sécurité dans le cadre d'une crise cyber.

Objectifs pédagogiques :

Cette formation introduit tout d'abord différents formalismes de modélisation de la menace afin capitaliser les attaques et faciliter le maintien en condition de sécurité. Dans une seconde partie, elle organise, prépare et entraîne la gouvernance dans la constitution d'une cellule de crise pour faire face à un incident cyber majeur.

Compétences

Compétences acquises :

- Savoir mettre en place une organisation de prévention et de gestion de crise
- Savoir modéliser la menace afin de pouvoir réaliser les documentations (plan de défense, PRA, PCA, PCI, PRI, fiches réflexes, etc.)
- Identifier les compétences utiles à la gestion de crise et savoir les mobiliser, utiliser au mieux les plans élaborés au fur et à mesure du déroulement du scénario,
- S'approprier la nécessaire coordination entre les équipes techniques, managériales et de planification et faire converger les efforts en vue de maîtriser et réduire la crise,
- Savoir présenter les enjeux liés à la crise, les prioriser et proposer des modes opératoires à une autorité,
- Accompagner les équipes dans la mise en place des règles de sécurité pour prévenir les risques humains et techniques,
- Rendre compte aux instances étatiques (déclaration d'incident, couverture médiatique) et internes (ensemble des équipes, gouvernance et membres d'autres cellules),
- Comprendre, appliquer les règles juridiques en vigueur au niveau national et international et en anticiper les effets sur la diffusion et l'accessibilité des informations sensibles,
- Savoir tracer, documenter la gestion de crise pour préparer une analyse post-mortem et rassembler des éléments légaux,
- Savoir organiser un retour d'expérience en vue de l'amélioration de la procédure de gestion de crise.

Savoirs :

- Utiliser le logiciel OpenCTI. Connaissance de STIX, plan de défense, plan de continuité d'activité.

Programme

Contenu

- Introduction à la modélisation de la menace
- Formalisme de modélisation
  - CybOX (Cyber Observable eXpression)
  - Le langage STIX (Structured Thread Information Expression)
  - Modèle de diffusion TAXII (Trusted Automated eXchange of Indicator Information)
  - Modélisation d'un rapport de sécurité dans le langage STIX
- Cycle de la Threat Intelligence
- Organisation d'une cellule de crise
  - Planifications

        - Politique de sécurité, plans de défense, SMCA
        - Continuité d'activité (PCA, PCO, PGC, PRA) et continuité informatique (PCI, PRI)
    - Méthodologie de gestion de crise
        - Qu'est-ce qu'une crise ? Typologies de crises
        - Gestion d'incidents et gestion de crise
        - Mécanismes de prise de décision
    - Décision en situation de crise
        - Etude d'une crise pour en tirer des enseignements
        - Passage en crise : réunion et ordres de déclenchement, mise en configuration de crise, décision

- Coordonner la communication crise

- Exercice de crise
    - Coordonner les équipes
    - Réaliser les déclarations légales nécessaires en fonction de la situation simulée et de la législation applicable,
    - Gérer les phases de réaction immédiates et d'investigation
- Rétrospective sur le déroulé de l'exercice :
    - « Déconfliction » : facteurs, conduite, compte-rendu
    - Compte rendu et modélisation de l'attaque effectuée
    - Adaptation de l'organisation et des procédures dans un processus d'amélioration continue

Modalités de validation

- Projet(s)

Description des modalités de validation

L'évaluation est réalisée sur la mise en situation individuelle à différentes fonctions, l'organisation de l'exercice étant basée sur une rotation des acteurs. Chaque auditeur devra remettre un dossier individuel sur l'ensemble de l'exercice.

Celui-ci devra rédiger un rapport d'incident qui comprendra :

- Les éléments de la phase préparatoire
- Une modélisation de l'attaque subie,
- La trace des événements et actions réalisées pendant l'exercice
- Ainsi qu'une description des adaptations à prendre en compte pour améliorer le processus.