Anfh Association nationale pour la formation permanente du personnel hospitalier

Projet cybersécurité

Simuler une attaque/défense pour les services informatiques hospitaliers

Les professionnels des services informatiques sont au coeur de la cybersécurité d'un établissement et seront les premiers sollicités en cas d'attaque. Si beaucoup est déjà fait sur le travail de renforcement de la sécurité des systèmes, il faut également être en mesure de réagir ou d'agir efficacement lorsque les systèmes sont interrompus. A l'instar des entraînements à la sécurité incendie, la sécurité des SI doit aussi appréhender la gestion de crise lorsque le risque survient.

PUBLIC VISÉ :
- Professionnel des SI
- Équipe SSI
- Administrateur

ORGANISÉ PAR :
- Ascent Formation

NOMBRE DE PARTICIPANTS :
- Jusqu'à 20 participants

DURÉE :
- 2 jours (14 heures)

PRÉREQUIS :
- Maîtrise de l'environnement informatique

CONTACT :
- contact@ascent-formation.fr

OBJECTIFS

- Appréhender les méthodes d'attaques et prévoir les mécanismes de défenses adaptés
- Mettre en place les premières actions pour limiter les dégâts
- Informer / dialoguer efficacement avec la Direction
- Solliciter les bons acteurs extérieurs
- Faciliter le fonctionnement de l'établissement en mode dégradé
- Spécifier les procédures de gestion de crise et de communication
- Assurer et anticiper la reprise

MODALITÉS PÉDAGOGIQUES

- Présentiel
- Distanciel
- Cas pratiques
- Mise en pratiques

PROGRAMME

JOUR 1 :

▪ **Compréhension des mécanismes d'attaques**

- Reconnaissance
- Découverte de vulnérabilités
- Écriture/Exploit de failles
- Exfiltration
- Couverture des traces
- Répartition travaux pratiques : 70% / 30%

JOUR 2 :

▪ **Simulation réelle**

- Mise en pratique : avec un laboratoire comprenant un Système d'Information virtualise (comprenant des serveurs, site web, système de messagerie, partage de fichiers, imprimantes, routeurs, postes de travail avec des OS reprenant ceux de l'environnement actuel du centre hospitalier...). Le but étant de mettre en pratique en situation « réelle » une phase d'attaque et une phase défense en simultanée permettant d'activer ainsi les différents Protocoles. Division en deux groupes : attaquants & défenseurs, inversement
- Répartition travaux pratiques : 90% / 10%