PACA
Axe 3 : FONCTIONS SUPPORT

Module n°9 : SERVICES TECHNIQUES - mise en situation d'une cyberattaque [DEMETER SANTE]

Contexte

L’écosystème du secteur de la santé évolue considérablement avec le développement de nouveaux outils numériques, leur lot d’avantages et de risques numériques. Ces risques numériques ne sont plus aujourd’hui à prendre à la légère, s’il y a 10 ans une panne informatique pouvait engendrer des désagréments passagers, elle peut aujourd'hui mettre à l’arrêt des services complets et impacter la continuité des soins. Le service technique gère un grand nombre d’appareils et de systèmes connectés ayant des fonctions de support et de sécurité. Il est donc indispensable que ce service soit capable de mettre en place une politique de sécurisation de ses appareils connectés. Les appareils support étant également plus répandus et plus nombreux il est important de mettre en place une politique de gestion des risques et de réponse sur incident.

Objectifs

- Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l’établissement, continuité des soins)
- Comprendre les interactions entre les différents appareils connectés et le service sécurité informatique
- Connaître le risque de piratage des appareils
- Être confronté à des scénarii d’attaque mettant en cause ces appareils connectés.
- Apprendre à réagir efficacement en cas de cyberattaque

Renseignements complémentaires

Pour plus d'informations :

- Audrey DAVID - 04.91.17.71.28 - a.david@anfh.fr

Programme

Comprendre à quoi sert la SSI dans un établissement de santé et plus particulièrement dans son service

- Quelle est aujourd’hui l’état de la menace cyber ?
- Les principes de base de la SSI
- L’intégration des personnels techniques dans la SSI

Comprendre les interactions entre les différents appareils connectés et le service sécurité informatique

- Le rôle de la SSI au sein d’un établissement (la confidentialité, l'intégrité, la disponibilité et la traçabilité)
- La SSI garante de la sécurité des périphériques et des données

Connaître le risque de piratage des appareils

- Diagnostiquer son SI et évaluer les risques dans son environnement
- Méthode d’évaluation des risques équipement par équipement
- Mise en situation, évaluation de plusieurs objets connecté de l’établissement
- Debriefing discussion et partage de connaissance sur la méthode AMDEC et le scoring des objets

Être confronté à des scénarii d’attaque mettant en cause ces appareils connectés

- A l’aide des résultats de l’évaluation des risques le formateur proposera différents scénarii d’attaque
- Chaque scenarii sera présenté par le formateur d’un point de vue technique avant de laisser au sous-groupe le soin d’évaluer la menace

Apprendre à réagir efficacement en cas de cyberattaque

- Quels environnements techniques pour quel type de menaces
- Reconnaitre les cyberattaques les plus courantes
- Réagir à une cyberattaque
- Mise en situation d’une réponse à une cyberattaque
- Debriefing sur les simulation et mise en place d’un plan d’action pour la mise en place du mode dégradé

Exercice
2025

Code de formation
3.09

Nature
AFR

Organisé par
ASCENT FORMATION / CRISALYDE / DEMETER SANTE

Durée
7 heures