DISPOSITIF CYBERDÉFENSE

Depuis plusieurs années, les cyberattaques contre les établissements de santé se multiplient. En 2021, le nombre d'attaques cyber a par exemple doublé par rapport à l'année précédente.

Dans la plupart des cas, les centres hospitaliers font face à des pirates informatiques qui réussissent à s'infiltrer dans leur système informatique, pour y voler les données sensibles et en bloquer l'accès. Une rançon est alors exigée pour espérer un retour à la normale.

Les établissements attaqués se retrouvent alors souvent totalement paralysé et les conséquences peuvent être lourdes, aussi bien pour les patients pris en charge que pour les agents qui se retrouvent à devoir œuvrer en mode dégradé. La politique étant bien sûr de ne jamais payer la rançon, le retour à la normale n'arrive qu'après plusieurs mois d'un lourd travail de reconstruction et de sécurisation du système informatique.

Si les conséquences peuvent être aussi impactantes, il semble pourtant que la connaissance de la menace que représente une cyberattaque, de ses différentes formes, n'est peu voire pas connue des agents hospitaliers. De la même manière, connaître le risque implique que l'on se prépare à y faire face.

C'est dans ce contexte que s'inscrit le dispositif Cyberdéfense de l'ANFH. Il s'agira dans un premier temps de sensibiliser et de former le plus grand nombre au risque de cyberattaque et à ses différentes formes. Cela passe notamment par la connaissance des bons gestes pour limiter les possibilités qu'ont les pirates informatiques de s'infiltrer.

Dans un second temps, l'axe majeur de se dispositif est de permettre à des publics cibles, de se préparer à une cyberattaque en se formant, via des mises en situation, à la définition de process permettant de poursuivre le travail en mode dégradé.

Contribuer à la cyber vigilance, connaître les bons gestes pour participer à la sécurité informatique de son établissement, être en mesure de détecter les menaces, alerter, et appliquer les premières mesures réflexes ; se préparer à la gestion de crise ; piloter un plan de continuité d'activité, seront autant de thématiques proposer par ce dispositif.

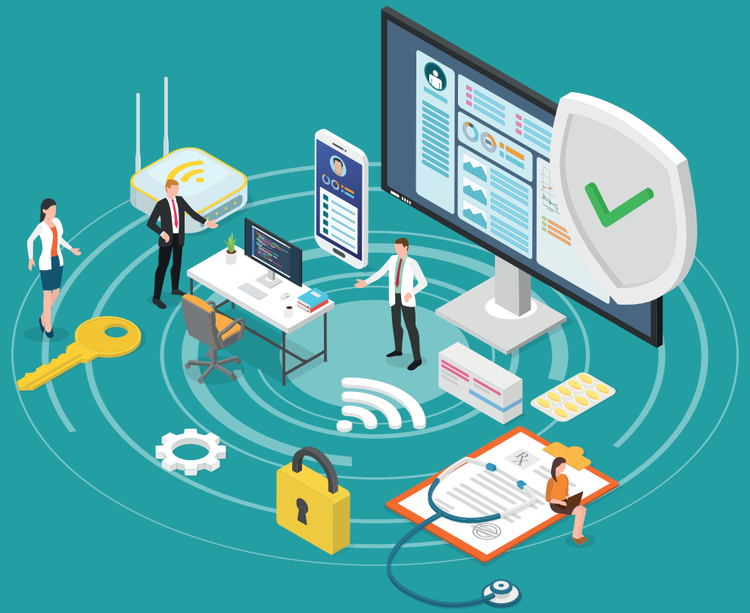
Anfh
Association nationale pour la formation permanente du personnel hospitalier

www.anfh.fr

Création graphique : LPJ HYPPOCAMPE - 04 67 42 78 09 - Document non contractuel sous réserve d'erreurs typographique.

Anfh
Association nationale pour la formation permanente du personnel hospitalier

DISPOSITIF CYBERDÉFENSE



Cyberattaque : connaître les risques, réagir efficacement en cas de piratage

1. WEBINAIRE SENSIBILISATION À LA CYBERSÉCURITÉ

Tous publics

- Sensibiliser les agents aux risques de piratage informatique
- Acquérir les bons réflexes face à une cybermenace
- Connaître les principaux types d'attaques possibles
- Comprendre son rôle dans la chaîne de sécurité du système d'information
- Présenter le reste du dispositif ANFH

2. MISE EN SITUATION CYBERATTAQUE

BUREAU DES ENTRÉES

Tout personnel des bureaux des entrées et admissions

- Lister les outils SI utilisés dans son service ;
- Reconnaître une situation de cyberattaque ;
- Concevoir l'activité du service sans ces outils ;
- Etablir quels documents papier, supports, outils, peuvent pallier l'absence de système SI opérationnel ;
- Définir une procédure d'activité en mode dégradé spécifique à son service/pôle.

GÉNIE BIOMÉDICAL

Ingénieurs et techniciens des services biomédicaux

- Comprendre les interactions entre le service biomédical et le service sécurité informatique ;
- Connaître le risque de piratage des appareils médicaux ;
- Communiquer efficacement avec le SSI ;
- Savoir être vigilant lors de la maintenance des appareils médicaux (en présentiel ou à distance) ;
- Définir un protocole de mise au rebus des disques durs contenant des données de santé ;
- Etablir des protocoles d'action en cas de cyberattaque

SERVICES TECHNIQUES

Tout personnel des services techniques

- 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.

DIRECTION

Tout personnel des services de direction

- Communiquer efficacement avec le SSI ;
- Repérer les acteurs
- Mettre en place une chaîne décisionnelle efficace ;
- Connaître les prérogatives de chaque secteur d'activité ;
- Déployer un plan d'action prédéfini.
- Mettre en place un plan de de communication adapté en interne et en externe

3. COMMENT PILOTER UN PLAN DE CONTINUITÉ DES ACTIVITÉS

Directions et toute personne en charge d'un PCA (qualité, SI...)

- Acquérir la méthodologie d'élaboration du Plan de Continuité des Activités spécifiques à son domaine ;
- Assurer le lien entre les services de soins et le service informatique.
- Définir le contexte et les objectifs de l'organisation ;
- Identifier et formaliser les besoins de continuité ;
- Identifier et gérer les risques prioritaires ;
- Choisir les scénarii à prendre en compte ;
- Formaliser les moyens et procédures (outils, reporting...) ;
- Définir la stratégie de continuité ;
- Spécifier les procédures de gestion de crise et de communication ;
- Assurer et anticiper la reprise

4. SIMULER UNE ATTAQUE/DÉFENSE CYBER POUR LES AGENTS DES SERVICES INFORMATIQUES

Administrateur du réseau SI et tout personnel du service SI

- Entraîner les administrateurs et techniciens des SI à faire face à différents scénarii de cyberattaque, en fonction d'environnements types.
- 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.