Résilience des établissements de santé en cas de cyberattaque

Face à l'explosion de la cybercriminalité, les établissements de santé sont de plus en plus exposés à des risques critiques pouvant perturber gravement leurs activités. Assurer la résilience des établissements en cas de cyberattaque est essentiel pour garantir la continuité des soins et préserver la sécurité des données des patients. Formavenir Performances propose un accompagnement stratégique et opérationnel pour renforcer votre préparation à la gestion de crise, protéger vos infrastructures numériques et garantir la continuité des activités dans toutes les situations critiques.

Objectifs

- **Évaluer la vulnérabilité des infrastructures :**
  - Identifier les points faibles des systèmes et des processus face aux cyberattaques.
  - Analyser les risques pour établir un diagnostic précis.
- **Mettre en place un plan de continuité d'activité :**
  - Définir une stratégie de gestion de crise adaptée aux besoins spécifiques de l'établissement.
  - Structurer un management efficace de la continuité d'activité pour minimiser les impacts.
- **Constituer une cellule de crise opérationnelle :**
  - Former une équipe dédiée pour réagir rapidement et efficacement en cas d'incident.
  - Organiser des rôles et responsabilités clairs au sein de cette cellule.
- **Simuler des cyberattaques pour tester la résilience :**
  - Réaliser des exercices pratiques pour évaluer les capacités de réponse.
  - Identifier les axes d'amélioration pour renforcer les processus existants.
- **Renforcer la sécurité et la sensibilisation :**
  - Former les professionnels aux bonnes pratiques de cybersécurité.
  - Développer une culture organisationnelle axée sur la prévention et la résilience.

Le + de la formation

Le + de l'accompagnement :

Public concerné et pré-requis

Public concerné :

- Directions générales des établissements sanitaires et médico-sociaux.
- Corps médical, comité de direction, direction des soins.
- Directions des ressources humaines, des services numériques, techniques et biomédicaux.

Prérequis :

- Connaissance des systèmes d'information et des enjeux liés à la continuité d'activité.
- Volonté de renforcer la sécurité organisationnelle et numérique.

Programme

1. Diagnostic initial

- Analyse des infrastructures et processus existants.
- Identification des vulnérabilités et des priorités de sécurisation.

2. Organisation et planification

- Définition des objectifs et périmètre d'intervention.
- Identification des acteurs clés et constitution d'un comité de pilotage.
- Planification des actions et des livrables.

3. Élaboration de la cible

- Construction d'une vision stratégique et partagée de la résilience numérique.
- Développement d'objectifs clairs pour renforcer les capacités de réaction.

4. Mise en œuvre de la continuité d'activité

- Définition des procédures de gestion de crise.
- Constitution d'une cellule de crise et formation des membres.

5. Exercices de simulation

- Organisation d'exercices pour tester les capacités de réponse aux cyberattaques.
- Analyse des résultats et ajustement des processus en conséquence.

6. Suivi et évaluation

- Suivi des indicateurs de performance et retour d'expérience.
- Production de rapports pour mesurer les progrès réalisés et identifier les prochaines étapes.

Votre intervenant

Notre intervenante est une experte reconnue dans le domaine de la résilience numérique avec plus de 20 ans d'expérience comme Directrice des Services Numériques dans un établissement de plus de 800 lits. Membre du Conseil d'Administration du GRADeS PACA pendant 5 ans, elle combine une expertise stratégique, opérationnelle et pédagogique, avec une expérience significative en consulting (Accenture, Capgemini, Formavenir).

Notre démarche pédagogique

- **Approche personnalisée :** Analyse des besoins spécifiques et des risques propres à chaque établissement.
- **Méthodologie structurée :** Diagnostic, élaboration et mise en œuvre des plans d'action.
- **Formation et sensibilisation :** Développement des compétences internes pour pérenniser les bonnes pratiques.
- **Suivi rigoureux :** Évaluation continue des actions mises en place pour garantir leur efficacité.

Livrables

- Rapport de diagnostic des vulnérabilités numériques.
- Plan de continuité d'activité et de gestion de crise.
- Documentation des procédures et formations réalisées.
- Rapports d'évaluation des simulations et axes d'amélioration.

Evaluation

- Analyse des performances des simulations de crise.
- Feedback des équipes sur les actions et processus mis en œuvre.

- Bilan final avec recommandations pour optimiser la résilience.

Intra

Durée : À définir selon vos besoins

Tarif : Devis personnalisé sur demande

Demande de contact

Dernière modification le 28 mars 2025 à 10h57

FORMAVENIR PERFORMANCES
139 avenue Jean Jaurès - 75019 PARIS
01 53 19 80 30
contact@formavenir-performances.fr