Cellule Régionale Cyber Santé

Présentation de la stratégie et des premières actions de la cellule

Cellule composée

Les enjeux

Prendre en compte le risque numérique pour renforcer la sécurité

L’essor du numérique en santé expose à des risques accrus l’ensemble des acteurs du système de santé (structures de santé et médico-sociales, professionnels libéraux, éditeurs de solutions) avec un impact potentiel majeur sur la santé et la vie des patients

La résilience de chaque établissement de santé face à la menace est devenue une priorité nationale. Un effort important est demandé à chaque structure et professionnel

Stratégie nationale de cybersécurité

Au niveau territorial

Animation portée par les ARS sur leurs territoires, avec le soutien de leur GRADeS, pour accompagner le volet cyber du virage numérique des territoires :

- Sensibilisation des acteurs
- Partages de pratiques
- Appui aux mutualisations, accompagnement
- Organisation de la réponse à incident

Montée en puissance des GHT comme accélérateur des nouveaux usages numérique organisé autour de la sécurisation des SI partagés, de la mutualisation des moyens cyber et des capacités de réponses à incident

Au niveau de chaque structure de santé

Stratégie nationale de cybersécurité

Au niveau des établissements de santé

Chaque établissement de Santé doit réaliser, de manière régulière, et au moins une fois par an, un exercice de crise cyber dont le retour d'expérience sera présenté au comité de direction de l'établissement et pris en compte dans le PCA.

Plan de Renforcement Cyber du 30/07/21

En cas d'incident, vous pouvez vous informer et trouver de l'assistance à cette adresse:

https://esante.gouv.fr/securite/cert-sante

Stratégie régionale de cybersécurité

La stratégie régionale s'articule autour d'axes majeurs:

- Sensibilisation
- Animation régionale pour les acteurs SSI santé
- Appui et accompagnement des structures et des professionnels de santé

avec pour objectifs prioritaires de :

- Favoriser l'acculturation des acteurs aux enjeux et aux problématiques de la cybersécurité
- Proposer des outils opérationnels pour accompagner les structures dans la diffusion auprès des équipes internes (kits de communication, campagnes de sensibilisation...)
- Construire avec les acteurs de terrain un espace de partage et de mutualisation au bénéfice de tous
- Mettre en place une offre de cybersécurité répondant aux attentes des acteurs de terrain

Mise en œuvre de la stratégie régionale

La démarche de mise en œuvre est progressive et collaborative avec un objectif de mutualisation

Progressive : Les premières actions sont lancées en 2021 (cellule régionale cybersanté, espace d'information cyber régional, contacts avec les partenaires de l'écosystème cyber santé) et vont se poursuivre et s'enrichir tout au long de 2022 et au-delà

Collaborative : Une concertation régionale permettra la définition des actions opérationnelles à prioriser et d'évaluer leur pertinence dans le temps

Notre démarche

Ecouter

Accompagner

Etablir la confiance par la transparence

Rester le plus factuel possible: volonté claire d'analyser mais ne pas juger

Développer la résilience par le partage des connaissances, des méthodes et des outils

Notre approche 1/2

Afin de favoriser les conditions d'émergence ou d'amélioration de la résilience du microcosme régional de la santé, certains piliers nous semblent essentiels:

1- Faire progresser le niveau d'acculturation des professionnels du milieu concernant les problématiques de cybersécurité, mais plus généralement sur la sécurité et le management de l'information.

2- Développer le partage des savoirs, la mutualisation et l'harmonisation des environnements et pratiques afin de faciliter l'identification, le redéploiement et le « prêt » de ressources en cas d'incident majeur

Notre approche 2/2

Pour comprendre vos besoins, et adapter au mieux les actions futures de la Cellule, nous avons rédigé une enquête, volontairement anonyme.

Elle balaie des problématiques diverses (état d'esprit, freins, analyse des besoins et contextes,…).

Cette enquête est en cours d'évaluation

actions de formation en cours

D’autres actions de formation sont actuellement portées par la Cellule.

Les objectifs pédagogiques principaux de ces webinaires ou conférences sont:

1- L’acculturation aux problématiques de la sécurité de l’information

(management de l’information et du risque, prédation, …)

2- Faire découvrir des enjeux parfois cachés de la cybersécurité et en général de la sécurité de l’information

3- Approcher différemment un public parfois en difficulté: direction / responsable de structure des ES/ ESMS afin de favoriser ou renforcer la résilience cyber, tout en créant de nouveaux axes d’échanges entre la direction/le personnel et les DSI/RSSI.

A noter : Pour connaitre les prochains évènements de ce type, contactez: cybersecurite@esea-na.fr

Les CyberMardi (information mensuelle)

les 3 objectifs du CyberMardi (1er mardi de chaque mois) :

Durée: 30 minutes

1- Partager l'information cyber en santé du moment

2- Echanger sur des problématiques ou proposer une interview, un partage d'expérience

3- Présenter un outil (remédiation, audit,…)

Le CyberMardi peut être bien entendu évoluer en fonction des retours, des envies et besoins des professionnels.

A noter : Pour connaitre les prochains évènements de ce type, contactez: cybersecurite@esea-na.fr

Nous contacter

cybersecurite@esea-na.fr

Damien Teyssier - 06 16 01 29 37