Piratage informatique

Comment protéger les données de santé des Réunionnais ?

Les établissements de santé sont aujourd'hui particulièrement dépendants du bon fonctionnement de leurs systèmes numériques. Toute défaillance, qu'elle relève d'un dysfonctionnement technique ou d'une attaque ciblée, risque de perturber les services de soins, et, en conséquence, d'impacter la prise en charge des patients.

Comme l'a souligné le Président de la République dans la présentation de la stratégie nationale pour la cybersécurité le 18 février 2021, le niveau de menace cyber auquel notre pays est actuellement confronté nous impose une réaction supplémentaire à la hauteur des enjeux, sous peine d'assister à une désorganisation de notre système de santé. L'ARS La Réunion prend très au sérieux cette menace et soutient les établissements de santé dans leur mise en sécurité numérique.

INTERVIEW **GÉRARD COTELLON,** Directeur général de l'ARS La Réunion

Quelles seraient les conséquences d'une cyberattaque pour la prise en charge des patients ?

En raison de notre insularité, et suivant la nature des attaques et de leurs impacts sur les systèmes d'information des établissements de santé, les conséquences pourraient être graves. Contrairement à la métropole, nous ne disposons pas de capacités de repli vers d'autres régions proches. Nous serions alors dans une situation assez similaire à celle que nous avons pu connaître pendant les pics épidémiques de la COVID. Les établissements seraient dans l'obligation de déprogrammer les interventions non-prioritaires afin de traiter l'urgence vitale. Nous serions aussi contraints de mobiliser des moyens humains supplémentaires notamment en faisant appel à la réserve sanitaire ainsi qu'à des volontaires. Cette situation pourrait durer car l'expérience des précédentes cyber attaques sur des établissements de santé a montré que le retour à la normale était long.

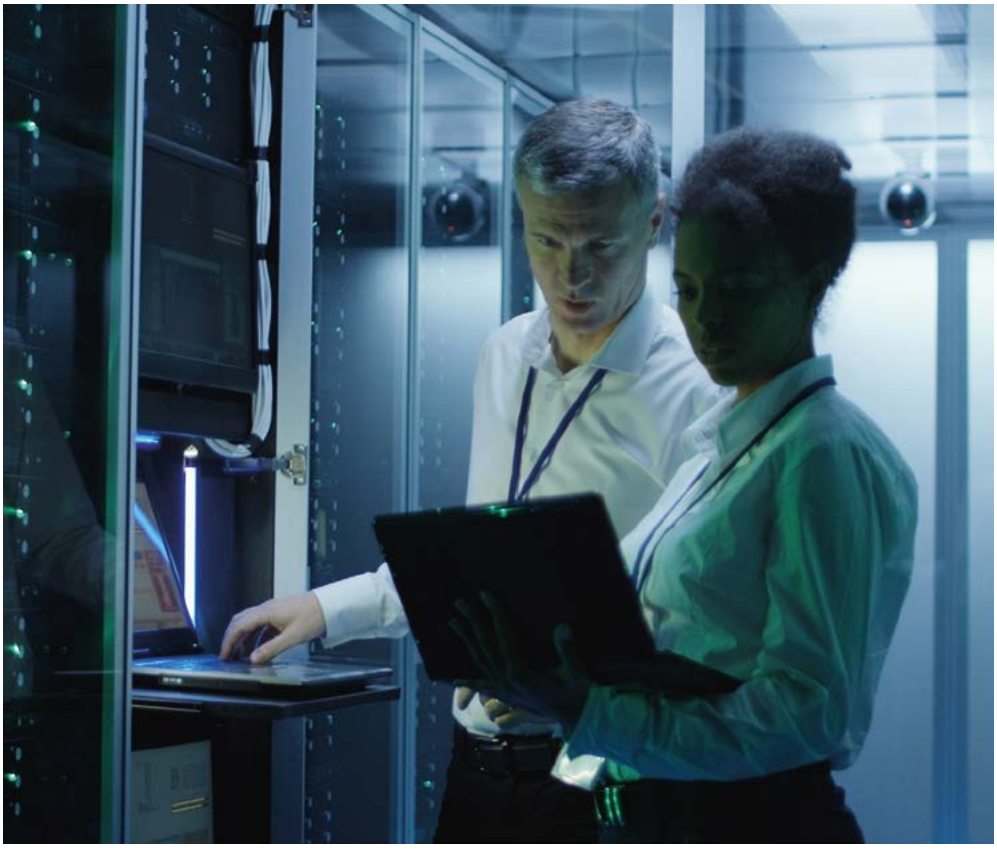
Comment l'ARS agit-elle pour protéger le système de santé d'une cyberattaque ?

L'ARS a soutenu le recrutement de compétences spécialisées en cybersécurité depuis 2012. Elle a également demandé au CHU de La Réunion, de recruter un Responsable de la Sécurité des Systèmes d'Information (RSSI) pour le

Groupement Hospitalier de Territoire.
Dans le cadre de sa démarche d'évaluation et d'accompagnement de la sécurisation des systèmes d'information de l'offre de soin publique, nous avons aussi financé un audit exhaustif de sécurité. Suite à cet audit, l'agence a financé la mise en œuvre d'un plan d'actions prioritaires pour sécuriser les systèmes d'information des établissements publics, qui s'étale de 2021 à 2024.
À ce jour, les acteurs de santé peuvent, en cas de cyberattaque, contacter un support disponible 24H/24 et 7 jours/7 pour demander de l'aide et savoir réagir face aux incidents mineurs ou majeurs.
Enfin, conscient que les ressources spécialisées en cybersécurité et en protection des données sont rares et chères, nous avons souhaité que le GCS TESIS propose, une offre de service d'accompagnement à tous les acteurs sanitaires et médico-sociaux :
• la mise en conformité légale et réglementaire de leur système d'information;
• l'anticipation et la gestion de crise en cas de potentielles attaques d'origine interne ou externe;
• la préparation au maintien.

Comment sensibilisez-vous les professionnels de la santé à cette problématique ?
Nous avons soutenu l'acquisition, par le GCS TESIS, de solutions de sensibilisation ludiques. Parmi elles, nous proposons notamment un jeu d'évasion ou " escape game " construit spécifiquement pour les professionnels de la santé et qui rencontre un franc succès : Médiscape est à la disposition des d'établissements sanitaires et médico-sociaux désireux de sensibiliser leurs équipes aux sujet de cybersécurité.
Nous fédérons et finançons au niveau régional, les initiatives de sensibilisation à la cybersécurité portées par les établissements afin de les mettre à disposition du plus grand nombre. C'est ainsi qu'est né NOUVEY, le label régional de cybersécurité que nous avons officiellement lancé le 8 novembre au cours du forum e-NOV et dont les premières affiches et film ont été dévoilés aux professionnels présents.

La Réunion est-elle en retard sur les sujets de cybersécurité en santé ?
La Réunion est une région pilote qui alimente aujourd'hui les groupes de travail nationaux et partage son expérience. ■



NOUVEY QU'EST-CE QUE C'EST ?

"En informatique comme en médecine, il y a des règles d'hygiène à respecter !" C'est le message principal que souhaite faire passer NOUVEY, le label régional dédié à la cybersécurité dans la santé. Piloté par l'ARS La Réunion et les acteurs de santé puis mis en œuvre par TESIS, NOUVEY souhaite fédérer les initiatives des professionnels autour de deux objectifs :
• atténuer les risques d'attaques informatiques en rendant les acteurs plus vigilants;
• protéger les données de santé des Réunionnais au travers d'une offre de confiance.
Pour y parvenir, NOUVEY regroupe des outils pratiques à disposition de tous les acteurs de la santé de La Réunion : kit de sensibilisation pédagogique, site internet ressource, offre de service dédiée à la cybersécurité portée par le GCS TESIS avec le soutien de l'ARS La Réunion (accompagnement, formation, jeux sérieux).

Pour exemple, le GHT, très impliqué dans la démarche, a choisi de lancer une première campagne de sensibilisation à destination de ses 9000 agents en s'appuyant sur différents supports (affiches, vidéo, flyers…).

Témoignages

KARINE GERNELLE

Directrice qualité gestion des risques ASFA & Eric Lesigne, RSSI de l'ASFA

L'Association Saint François d'Assise, qui compte environ 700 salariés et une douzaine d'établissements dont un hôpital d'enfant, un EHPAD, des établissements pour personnes en situation de handicap et un pôle formation.

Pour les patients et les usagers de l'ASFA, quels seraient les impacts d'une cyberattaque ?

En cas de cyberattaque, tout ou une bonne partie du réseau informatique est coupé soit par les pirates eux-mêmes soit par mesure de protection. Aujourd'hui, le dossier des patients et usagers, le matériel biomédical, les badges d'entrée et de sortie, la climatisation, la téléphonie, l'imprimante, les fax : tout est branché sur un réseau informatique ! Si ça coupe, il faudra impérativement et rapidement nous réorganiser pour assurer la continuité minimale des soins et des accompagnements.

Comment l'ASFA se prépare-t-elle aux cyberattaques ?

Nous restons en alerte et nous réfléchissons à des solutions palliatives, pour assurer la prise en charge de nos usagers même dans des conditions dégradées (dossiers patients prêts à être imprimés…). Accompagnés par le GCS TESIS, nous bâtissons un cadre de sécurité solide grâce à des solutions techniques et des actions de sensibilisation tels que des exercices de simulation très efficaces ! Pouvoir faire appel à TESIS est un énorme atout car on ne sent pas seuls face à ces défis !

STÉPHANE DUCHESNE

Responsable de la Sécurité des Systèmes d'Information du Groupement Hospitalier du Territoire (GHT), délégué à la Protection des Données (DPD) des quatre établissements du GHT*

Comment le CHU agit-il pour se protéger des cyberattaques ?

Au CHU nous travaillons notamment à :

- mettre en place des systèmes de protection efficaces sur l'ensemble des outils informatiques, biomédicaux ou numériques ;
- mieux détecter les cyberattaques, plus tôt, pour réagir plus vite ;
- assurer le fonctionnement en continu des outils informatiques même en cas de panne ou de sinistre majeur ;
- accompagner le personnel dans la prise en charge des patients même dans des conditions dégradées en cas d'attaques.

Tout cela est complété par la sensibilisation de nos agents à l'hygiène informatique, qui sont la première barrière de sécurité puisqu'ils sont les premiers utilisateurs de la donnée de la santé.

Si une cyberattaque avait lieu demain, le CHU serait-il prêt ?

La question n'est pas de savoir s'il est probable qu'on se fasse cyberattaquer mais plutôt de savoir comment se préparer pour le jour où cela va arriver ! On parle ici de cyber résilience.

Face à la complexité des attaques, personne ne peut garantir une protection totalement efficace. Cependant, au CHU, nous nous préparons à subir une attaque comme il y a eu dans d'autres hôpitaux de métropole, à travers nos projets de sécurisation mais aussi par une bonne gestion des incidents et des crises en s'appuyant sur de la formation et des exercices de simulation. Notre objectif est avant tout d'éviter qu'une attaque se propage, d'en minimiser les impacts et de continuer d'assurer la prise en charge de nos patients. ■

**CHU de La Réunion, CHOR, EPSMR et GHER.*

FRÉDÉRIC BROQUIER ET MATHIAS LAURENT (GCS TESIS)

Qu'est-ce que TESIS ?

TESIS est un Groupement de Coopération Sanitaire (GCS) financée par des fonds publics. Sa mission ? Accompagner les professionnels de la santé vers la transition numérique.

Depuis combien de temps et comment TESIS agit en matière de cybersécurité ?

Comme on le ferait pour protéger sa maison des intrusions, des incidents ou des intempéries (fermer ses portes et fenêtres en partant, vérifier l'étanchéité du toit en cas de fuite, surveiller ses doubles des clés…). Nous bâtissons avec les acteurs de santé de La Réunion et depuis 10 ans, un environnement solide, sécurisé et fonctionnel en cas d'attaques ou d'incidents dans leur système.

Notre objectif est double :

• Permettre aux acteurs de santé de continuer à exercer leur métier dans les meilleures conditions. Grâce à un plan d'accompagnement complet, nous diagnostiquons, définissons et assurons le suivi d'une politique de sécurité au sein de toutes les structures médico-sociales et établissements sanitaires qui en font la demande.

• Protéger les données de santé des patients (dossiers médicaux, examens, ordonnances…) grâce à la mise en place d'un datacenter sécurisé, véritable coffre-fort numérique 100% péï ! Mis en place avec avec le soutien financier de l'ARS, les établissements de santé et TESIS, il contribue à préserver la confidentialité des informations de santé des Réunionnais depuis 2012.

Au-delà de notre devoir de conseil et des mesures techniques pour anticiper les risques et les atténuer, tout un volet est consacré, à travers le label régional NOUVEY, à la sensibilisation des professionnels aux usages de l'informatique.

À gauche : Frédéric Broquier, administrateur du GCS TESIS. À droite : Mathias Laurent, Responsable de la Sécurité des Systèmes d'Information (RSSI) et Délégué à la Protection des Données (DPD).