

La cyber-sécurité dans les services de santé: il est temps de se faire examiner

L'ENISA publie quelques recommandations clefs pour protéger les services de télésanté et les infrastructures

Les répercussions potentielles d'une coupure des réseaux peuvent être d'une grande gravité pour un hôpital. L'interruption du service ou les pannes d'appareils médicaux causées par un piratage à distance (par exemple à travers la force brute ou une attaque DoS) peuvent être significatives. De tels incidents de cyber sécurité ont sérieusement affecté les services hospitaliers, mettant en danger des vies humaines et exposant les institutions et systèmes de santé à des risques de réputation. Le thème de la santé prend une plus grande importance dans les agendas politiques et est souvent considéré par les Etats Membres comme une infrastructure critique. L'ENISA a impliqué plus de quinze Etats Membres et deux pays de l'AELE dans une étude visant à identifier les mesures que les secteurs public et privé devraient prendre pour améliorer la sécurité et la résilience des systèmes de télésanté. Cette étude se concentre sur trois cas communs : les fichiers électroniques de santé, les services nationaux de télésanté (par exemple ePrescription) et les services cloud soutenant les systèmes de télésanté.

Udo Helmbrecht, Directeur Exécutif de l'ENISA, a commenté ce rapport en déclarant « la complexité et les interdépendances des systèmes de télésanté se sont amplifiés. Assurer la disponibilité, l'intégrité et la confidentialité de la télésanté est un défi pour les fournisseurs et les bénéficiaires. L'ENISA cherche à coopérer avec toutes les parties prenantes pour améliorer la sécurité et la confidentialité de tous les services et infrastructures de télésanté. »

Le rapport recommande, entre autre, que:

- Les autorités nationales de cyber sécurité identifient les actifs de télésanté et mènent des évaluations des risques en vue de prévenir ces derniers.
- Les responsables politiques introduisent des recommandations basiques de cyber sécurité pour les infrastructures et services de télésanté.
- Les opérateurs de télésanté, avec les acteurs du secteur public, installent des mécanismes de partage de l'information pour échanger les bonnes pratiques et l'expertise sur les menaces et vulnérabilités.

Ces conclusions ont été validées par de nombreux experts des secteurs public et privé dans un atelier public organisé avec la Commission Européenne le 30 octobre 2015.

Les nouvelles technologies, telles que le cloud computing, les appareils intelligents et l'internet des objets fournissent déjà l'innovation dont la télésanté a besoin. Alors que les défis de cyber-sécurité croissent, l'ENISA se concentrera en 2016 sur l'adoption du cloud computing par les opérateurs de santé et effectuera une analyse des hôpitaux intelligents.

Pour le rapport intégral

Pour de plus amples informations techniques: Dimitra Liveri, NIS expert, Dimitra.liveri@enisa.europa.eu

Pour les demandes de presse et les interviews, merci de contacter press@enisa.europa.eu, Tel. +30 2814 409576