

VEILLE TECHNOLOGIQUE

HAMED JAWED SIO2 SLAM



L'Informatique et la Santé : La cybersécurité dans le Secteur Médical

L'informatique dans le domaine de la santé a connu une évolution significative au fil des années, s'appuyant sur des infrastructures technologiques complexes. Cependant, cette transformation numérique a également exposé le secteur de la santé en France à des menaces croissantes en matière de cybersécurité. Dans cette veille technologique, nous explorerons l'évolution de l'informatique dans le domaine de la santé, les cyberattaques ciblant les établissements de santé, et les mesures de protection basées sur des concepts informatiques avancés.

I. L'évolution de l'informatique dans la santé et l'e-santé en France :

L'informatique dans le domaine de la santé en France a connu une transformation majeure, notamment grâce à l'e-santé. L'e-santé englobe l'utilisation de technologies de l'information pour améliorer la prestation des soins de santé, la gestion des données médicales et la communication entre les professionnels de santé et les patients.

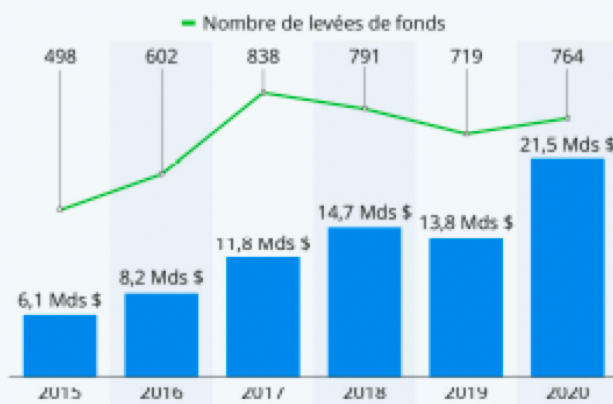
Par exemple, les Dossiers Médicaux Partagés (DMP) ont été introduits pour permettre un accès électronique aux informations médicales essentielles, facilitant la coordination des soins et améliorant la continuité des soins.

De plus, la télémédecine qui repose sur des infrastructures de réseaux sécurisées, permet aux médecins de consulter à distance, ce qui favorise l'accès aux soins dans tout le pays (téléconsultations durant la crise sanitaire du Covid-19).

Les dispositifs médicaux connectés utilisent des protocoles de communication cryptés pour transmettre les données des patients aux systèmes de santé, améliorant ainsi le suivi à distance.

L'e-santé en plein boom

Montant et nombre de levées de fonds des start-ups du secteur de la santé dans le monde



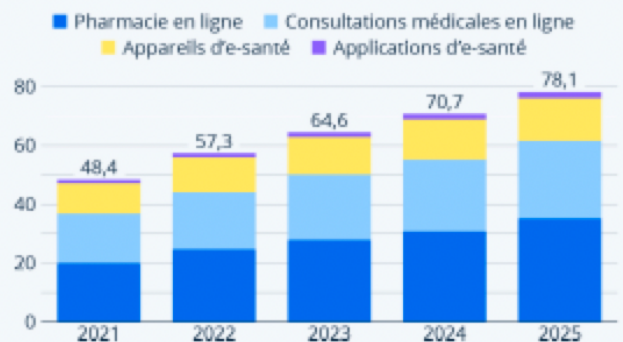
Source : StartUp Health



statista

E-santé : un marché gigantesque

Ventes mondiales estimées dans le secteur de l'e-santé, en milliards d'euros *



* marché B2C uniquement

Source : Statista Health Market Outlook



statista

II. Pourquoi les hôpitaux sont visés par ces cyberattaques en France :

Les hôpitaux et les services médicaux en France sont devenus des cibles privilégiées pour les cyberattaques en raison de plusieurs facteurs. Tout d'abord, les établissements de santé détiennent une quantité considérable de données médicales sensibles, telles que les antécédents des patients, les résultats de tests, les informations sur les traitements, et les données personnelles. Ces informations ont une grande valeur sur le marché noir et peuvent être utilisées à des fins de fraude, d'extorsion ou de vol d'identité.

De plus, les hôpitaux sont souvent mal préparés en matière de cybersécurité, ce qui les rend vulnérables. Ils ont des budgets limités et sont souvent en retard dans l'adoption de mesures de sécurité avancées. Les systèmes informatiques des hôpitaux sont souvent diversifiés et hétérogènes, ce qui complique la gestion de la sécurité. De plus, les attaquants profitent parfois de la dépendance des hôpitaux à l'égard de leurs systèmes informatiques pour demander des rançons, sachant que la disponibilité des données est cruciale pour la prestation de soins de santé.



III. L'importance de la cybersécurité pour la sécurité des données de santé en France:

La cybersécurité est d'une importance vitale pour protéger les données médicales sensibles en France. Les données de santé sont parmi les informations les plus personnelles et sensibles, et leur divulgation non autorisée peut avoir des conséquences graves pour les patients. Une faille de sécurité peut entraîner la divulgation de dossiers médicaux confidentiels, compromettre l'intégrité des données ou entraîner la suppression des informations médicales essentielles. La sécurité des données de santé est une préoccupation majeure, à la fois pour la confidentialité des patients et pour la qualité des soins.

En outre, conformément au Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne, les établissements de santé en France sont tenus de mettre en place des mesures de protection des données médicales, sous peine de sanctions sévères en cas de violation. La perte de données de santé peut entraîner des amendes substantielles, des pertes de confiance des patients, et des impacts juridiques et financiers considérables.



En conclusion,

la cybersécurité est essentielle pour garantir la sécurité des données de santé en France. Les établissements de santé doivent investir dans des mesures de sécurité avancées pour protéger les données sensibles et garantir la confidentialité des patients. La sensibilisation, la formation du personnel et la conformité aux réglementations en vigueur, telles que le RGPD, sont des éléments clés pour maintenir la sécurité des données médicales dans un environnement informatique en constante évolution. La cybersécurité demeure une priorité absolue pour garantir un secteur de la santé moderne, sûr et efficace en France.