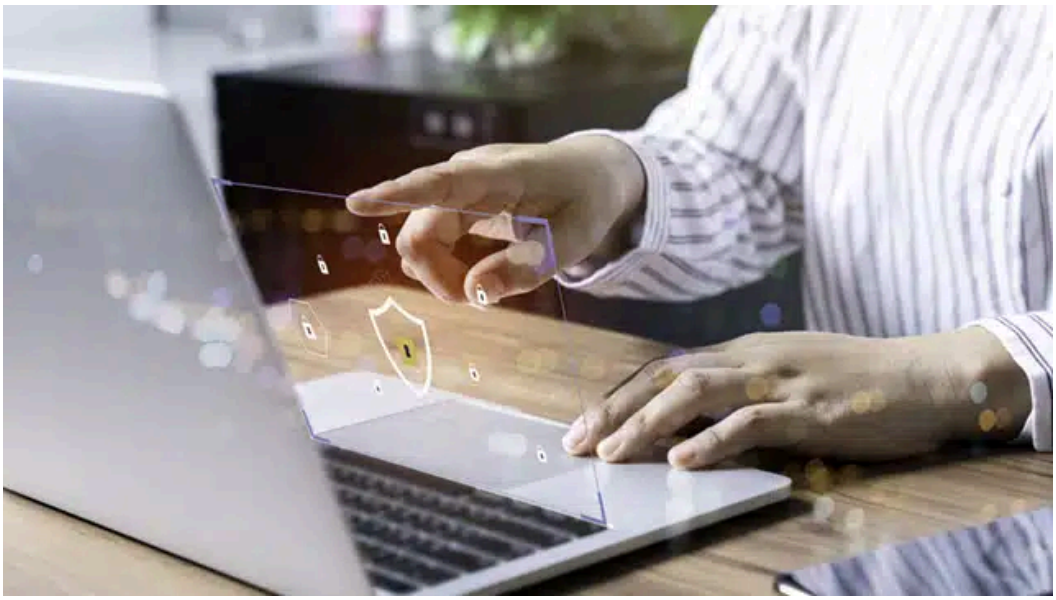
SANTÉ / SANTÉ

Cybersécurité et RGPD, les oubliés de la crise sanitaire !

Cyberattaque | Cybersécurité | Établissements de santé, sociaux et médico-sociaux | Piratage | Protection des données personnelles | RGPD | Sécurité informatique

Publié le 8 juillet 2020 à 7h40 - par Rédaction Weka

La crise sanitaire que nous venons de vivre, sans pouvoir d'ailleurs évoquer avec assurance son achèvement, a relégué au second rang une autre menace, également souvent virale, celle liée aux attaques informatiques.



Dans un contexte où les établissements de santé ont fait face à des défis opérationnels et budgétaires sans précédent, les tentatives de cyberattaques ont été très importantes et exacerbées. Au-delà du nombre et de l'impact encore difficile à chiffrer, c'est la nature même de la menace qui évolue avec des attaquants, qui exploitent aussi désormais les impacts organisationnels : mise en place du télétravail, diminution de la disponibilité des compétences en cyber et vigilance des collaborateurs orientée vers d'autres enjeux.

Même si la crise sanitaire tend à se résorber, tout le monde s'accorde à dire que beaucoup d'établissements de santé vont devoir de manière durable transformer leurs organisations et les pratiques associées.

Les établissements de santé en première ligne en termes d'exposition et de risques !

Parmi les acteurs, les établissements de santé tant d'ailleurs hospitaliers que médico-sociaux sont ainsi fortement exposés. Ceci pour plusieurs raisons : forte digitalisation des processus et des parcours, diversité et mobilité des personnels, connexions multiples au système d'information, diversité de ce dernier (HIS, RIS…), valeur financière de la donnée médicale, impact très important et attractif pour les dispositifs de ransomware.

Les chiffres suivants rappellent l'importance de cette menace :

- 81 % des établissements de santé français ont déjà été attaqués, sans autant le savoir obligatoirement.
- 41 % des cabinets médicaux (de 0 à 9 salariés) ont déjà subi une ou plusieurs intrusions dans leurs systèmes.
- 44 % des établissements de petite taille (de 9 à 49 salariés) ont déjà subi une ou plusieurs attaques. 120 établissements de santé d'un grand groupe privé ont par exemple été victimes en août 2019 d'une cyberattaque de masse.

Des situations qui ont, en premier lieu, un impact économique estimé à 90 000 € en moyenne par jour pour un établissement de santé (perte d'activité, désorganisation, implication de prestataires…). Ces impacts financiers sont certes significatifs mais in fine peut-être pas les plus importants !

Les risques juridiques, réglementaires… et réputationnels

La direction d'un établissement de santé induit de nombreuses obligations telles que :

- Garantir le maintien en conditions opérationnelles des outils assurant le parcours de soins ou de vie.
- Assurer à l'ensemble des personnels la mise à disposition d'un environnement sécurisé.
- Concourir au respect des obligations liées au statut d'opérateur de service essentiel (OSE).
- Déployer en cas de crise un plan de continuité d'activité avec une partie communication interne et externe associée.

Est associée à ces missions, et à différents degrés, une responsabilité civile voire pénale. Au-delà, il faut également tenir compte du risque d'image inhérent à toute médiatisation d'une telle situation.

Les impacts en matière de réputation peuvent être de différents ordres:

- Vis-à-vis des patients (ex : perte de données).
- Attractivité de l'établissement vis-à-vis des personnels.
- Positionnement vis-à-vis des acteurs institutionnels (ARS) et assurantiels (hausse des primes).

De nombreuses sanctions ont d'ailleurs déjà été mises en œuvre par la Cnil que ce soit en matière d'insuffisance dans le respect des obligations de sécurité et de confidentialité des données de santé, de manque de protection des données personnelles sur un site internet (sanction de 180 000 € le 18 juillet 2019) ou pour non-respect des durées de conservation (sanction de 400 000 € le 28 mai 2019).

Comment se protéger de manière réaliste, raisonnable et pérenne ?

Tous les établissements de santé ne disposent pas des mêmes compétences et budgets pour se doter d'une solution de sécurisation à la fois adaptée, efficiente et surtout pérenne. En effet, ne pas adapter sa stratégie de cybersécurité aux évolutions de son établissement revient à rendre quasi-nulle cette protection. Le faille étant par définition toujours dans les détails.

Les offreurs de solutions de cybersécurité sont nombreux et s'appuient sur différentes stratégies : matériels, logiciels et/ou prestations. La plupart des acteurs du marché fonctionnent en audit ou mise en œuvre sur des interventions ponctuelles, forfaitaires ou sur un nombre de jours étroits. Dès la première évolution, à la fin de la mission, les rapports d'audit, préconisations, ou mises en œuvre deviennent parfois obsolètes.

La sensation d'abandon ressentie par l'établissement, surtout sur ce thème devient vite anxiogène. Une approche pertinente pour les offreurs mais naturellement source de éconvenues notamment budgétaires pour les établissements de santé.

L'émergence d'un modèle de type assurantiel !

Comme dans beaucoup de domaines de la vie professionnelle ou personnelle, les derniers acteurs arrivés sur le marché sont souvent les plus pertinents tant en termes de compréhension des usages que de proposition de modèles économiques disruptifs. Ces acteurs ne disposent d'aucune « base installée », d'aucune certitude de « rentes » et ont pour vocation première de pénétrer le marché en se rapprochant au plus près des besoins actuels et à venir.

Si l'audit de démarrage demeure indispensable afin de connaître la situation exacte de l'infrastructure physique et logique de l'établissement, le plus important réside dans la mise en place croissante d'abonnements annuels assurant une approche tout compris, un suivi personnalisé et un accompagnement sur la durée. Le principe même d'une assurance ! L'adaptation du contrat aux évolutions techniques, réglementaires et organisationnelles (ex : télétravail, télémédecine…) de l'établissement se fait ensuite de manière forfaitisée et connue dès le début. Aucune surprise, aucune mauvaise surprise.

En conclusion

La question n'est pas de savoir si vous avez déjà été victime d'une cyberattaque ou à quel moment, mais plutôt de la rapidité à laquelle vous serez en mesure de l'identifier et ainsi de limiter l'impact sur votre établissement, votre responsabilité juridique, votre budget et votre image. La question est aussi de s'assurer de pas générer d'autres risques en recourant à un prestataire quelconque. Les enjeux liés notamment aux données (et à leur hébergement !), à la réalité des compétences exposées et à la pérennité de la société sont des éléments majeurs à regarder.

Le modèle déployé notamment par la société 123 CS, filiale récemment créée au sein du groupe Verso Healthcare, acteur 100 % français et indépendant des constructeurs, semble ainsi montrer la voie de ce que sera demain une approche responsable et durable de la cybersécurité dans le secteur de la santé.

Sébastien Taupiac
Directeur du développement / Verso Healthcare

On vous accompagne

Retrouvez les dernières fiches sur la thématique « Santé »

Le document individuel de prise en charge
#Document de procédure administrative #Information du patient
04/09/24

Fin de vie des mineurs
#Mineur #Soins palliatifs
04/09/24

Guide de préparation aux situations sanitaires exceptionnelles
#Gestion de crise #Établissement de santé
02/09/24

Les acteurs du secteur
#Personnel médico-social #Professionnel de santé
02/09/24

Désamorcer la violence en psychiatrie
#Violence #HAS #Patient
02/09/24

Les agences régionales de santé face aux situations sanitaires exceptionnelles
02/09/24 #ARS #Risque sanitaire #Gestion de crise

La gestion des situations sanitaires exceptionnelles au prisme du référentiel de certification des établissements de santé
02/09/24 #Certification #Gestion de crise #Établissement de santé

Organisation des études médicales

#Interne #Praticien hospitalier

28/08/24

Voir toutes les ressources numériques Santé

On vous recommande

Santé **02/03/21**

Cybersécurité : 375 millions d'euros pour renforcer la sécurité informatique ...

Administration **18/02/21**

Cyberattaques : Emmanuel Macron promet une riposte à un milliard après le piratage ...

Administration **16/02/21**

Le rançongiciel, quand la foudre tombe sur une organisation

Santé **22/01/21**

Cyberattaques et Covid-19 : attention à renforcer la sécurité informatique des ...

Administration **16/07/20**

Les collectivités se préoccupent encore peu de cybersécurité, selon le Clusif

Administration **14/03/24**

La menace cyber en forte hausse en 2023 pour les collectivités, selon ...

Offres d’emploi
Institutions et administration territoriale

OPERATEUR DE REPROGRAPHIE
Mairie de Guyancourt
Publiée Il y a 3 jours **Voir l'annonce**

Agent polyvalent des espaces verts (h/f)
Mairie du Blanc-Mesnil
Publiée Il y a 3 jours **Voir l'annonce**

Chargé de l'animation du patrimoine (h/f)
Mairie du Blanc-Mesnil
Publiée Il y a 3 jours **Voir l'annonce**

Manager de commerces (h/f)
Mairie du Blanc-Mesnil
Publiée Le 18 sept. **Voir l'annonce**

Voir toutes les offres sur weka.jobs

Les + Vus

16/09/24
Les emplois territoriaux sont plus attractifs, selon le baromètre RH ...

02/09/24
GIPA 2024 : les agents publics veulent bénéficier d’un nouveau ...

17/09/24
Petite enfance : à trois mois de l'entrée en vigueur de la ...

11/09/24
Arrêts de travail pour raisons de santé : un rapport préconise de ...

17/09/24
Finances : les départements dans la tourmente

Voir tous les articles publiés