Actualité > Action Sociale

Cybersécurité et RGPD, les oubliés de la crise sanitaire !

Santé

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 _____, 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 (_____) ou pour non-respect des durées de conservation (_____).

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 /

Posté le 08/07/20 par Rédaction Weka

ENVOYER | IMPRIMER |

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

POUR TOUT COMPRENDRE

Télétravail : les collectivités doivent renforcer la cybersécurité

Maîtrise des risques et de la qualité

ON VOUS RECOMMANDE

Lutte contre les exclusions — 09/07/20

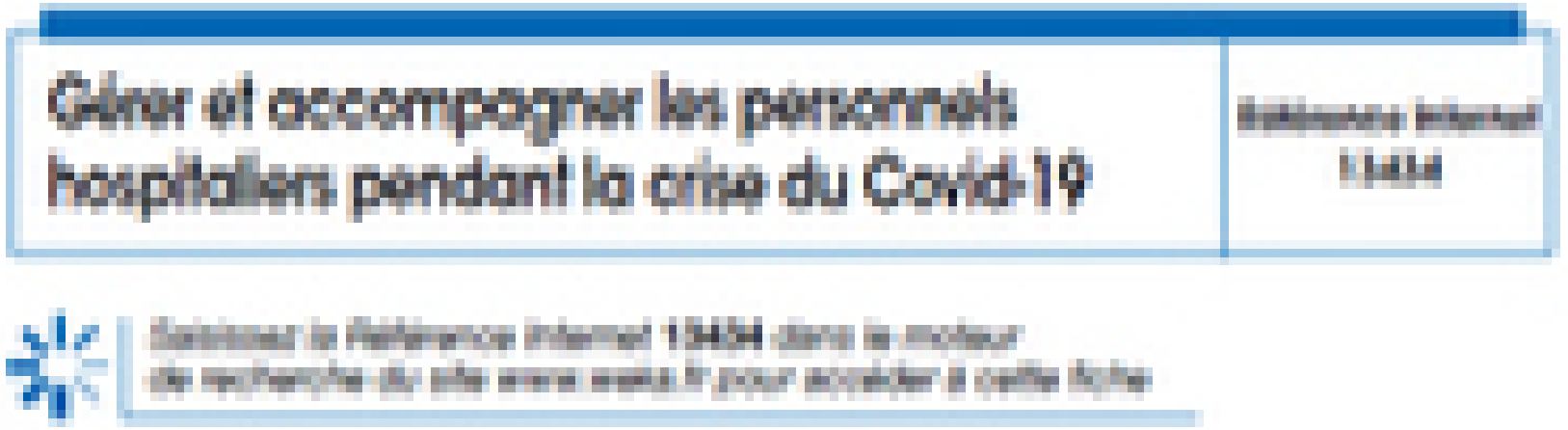
Lutte contre les exclusions — 09/07/20

Santé — 08/07/20

Santé — 08/07/20

Santé — 07/07/20

Enfance et famille — 07/07/20



Gérer et accompagner les personnels hospitaliers pendant la crise du Covid-19

Référence Internet 1345

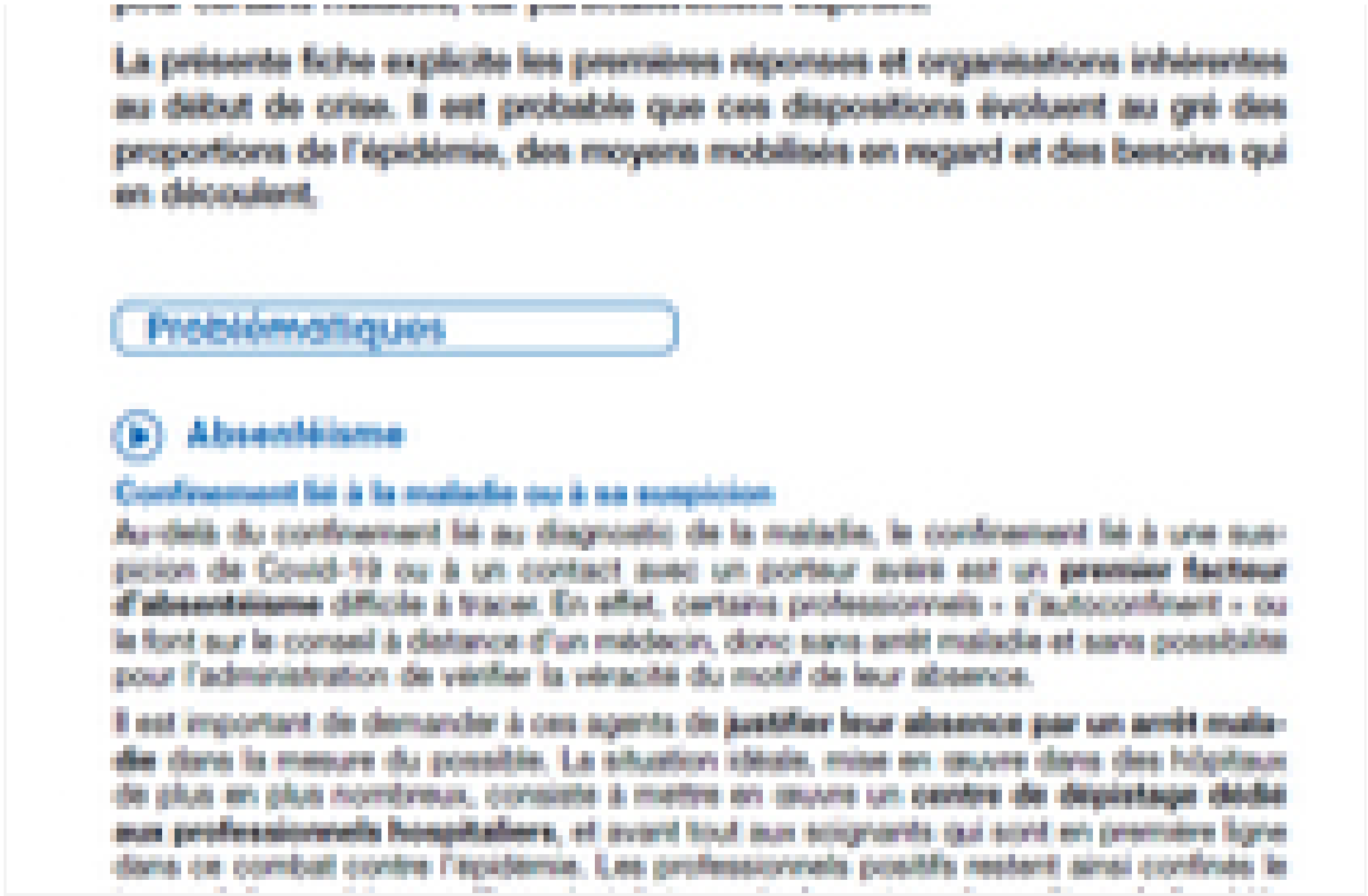
Saisissez la Référence Internet 1345 dans le moteur de recherche du site www.weka.fr pour accéder à cette fiche

La crise sanitaire comme à la pandémie de Covid-19 bouleverse, en peu de temps, tous les repères de notre organisation sanitaire, et tout particulièrement celle des établissements publics hospitaliers situés aux avant-postes de ce que beaucoup qualifient aujourd'hui de « guerre » contre le virus.

Ainsi, les réorganisations de l'environnement professionnel, inhérentes à la crise, impactent au premier chef les ressources humaines de l'hôpital : médecins, soignants, mais aussi techniciens, logisticiens ou encore administratifs, soit, sans pouvoir être exhaustif, l'ensemble des professionnels qui soutiennent directement ou indirectement les soins.

Ce sont les mêmes, en outre, qui subissent comme tout un chacun les modifications de leur environnement personnel (régulation des déplacements notamment).

Ce sont les mêmes, enfin, qui subissent les impacts directs du virus et tombent pour certains malades, car particulièrement exposés.


La présente fiche explicite les premières réponses et organisations inhérentes au début de crise. Il est probable que ces dispositions évoluent au gré des proportions de l'épidémie, des moyens mobilisés en regard et des besoins qui en découlent.

Problématiques

Absentéisme

Confinement lié à la maladie ou à sa suspicion

Au-delà du confinement lié au diagnostic de la maladie, le confinement lié à une suspicion de Covid-19 ou à un contact avec un porteur avéré est un **premier facteur d'absentéisme** difficile à tracer. En effet, certains professionnels « s'autoconfinent » ou le font sur le conseil à distance d'un médecin, donc sans arrêt maladie et sans possibilité pour l'administration de vérifier la véracité du motif de leur absence.

Il est important de demander à ces agents de **justifier leur absence par un arrêt maladie** dans la mesure du possible. La situation idéale, mise en œuvre dans des hôpitaux de plus en plus nombreux, consiste à mettre en œuvre un **centre de dépistage dédié aux professionnels hospitaliers**, et avant tout aux soignants qui sont en première ligne dans ce combat contre l'épidémie. Les professionnels positifs restent ainsi confinés le

Télécharger