

La sécurité des identités au service du secteur de la santé

La France a connu 27 attaques majeures d'hôpitaux durant l'année 2020. Saviez-vous que la deuxième cause de ces violations était l'accès non autorisé ?

L'année 2020 fut si chaotique et inattendue qu'elle nous a appris que la vie peut parfois être imprévisible et que nous sommes alors obligés d'être particulièrement réactifs. Tristement, cette année a aussi connu une forte croissance des cyberattaques à destination des organismes de santé, qui forme pourtant l'un des secteurs les plus réglementés.

Alors que le gouvernement Français a annoncé la mise en place la stratégie Cyber en février dernier à destination des hôpitaux, comment le secteur de la santé, peut-il s'adapter pour prévenir les failles de sécurité tout en stimulant l'innovation pour la modernisation de leur structure ?

À mesure que les organismes de santé passent à des solutions basées sur le Cloud et à la collaboration à distance, la gestion des informations d'identification dans l'ensemble de l'entreprise devient plus complexe et plus longue. Les professionnels de l'IT dans le domaine de la santé doivent être en mesure de répondre rapidement à certaines questions. Qui a accès à quels systèmes et applications ? Leur niveau d'accès est-il approprié à leur rôle ? Ou encore, utilisent-ils leur accès de manière responsable ?

Malheureusement, comme la plupart des équipes informatiques du secteur de la santé manquent cruellement de personnel, les processus manuels de gestion des informations d'identification ne fonctionnent tout simplement pas. Une solution automatisée rend alors le provisioning, le transfert et le retrait des comptes plus rapide, plus facile et plus sûr, réduisant ainsi la charge sur les précieuses ressources informatiques.

Il est à noter que les organismes de santé peuvent compter des milliers d'employés travaillant sur plusieurs sites. Pour que tout se passe bien, les gestionnaires doivent être en mesure d'intégrer rapidement les nouveaux soignants afin qu'ils aient accès aux outils dont ils ont besoin pour servir les patients dès le premier jour et gérer les besoins d'accès dynamiques des employés qui assument plusieurs rôles sur différents sites. Ils doivent également être en mesure d'aisément résilier et ajuster l'accès lorsqu'un employé est muté ou quitte l'organisation, de manière immédiate.

Une solution automatisée permet ainsi des intégrations sécurisées entre les principales applications cliniques et administratives en un seul flux de travail complet qui peut rationaliser ces tâches importantes.

Le rythme rapide et l'évolution constante de la fourniture d'accès dans un établissement de santé sont une problématique majeure pour les responsables de la conformité. Pour aider à répondre aux exigences réglementaires de manière efficace et cohérente, une solution de sécurité de l'identité fournit une visibilité sur qui a accès à quelles applications et plateformes.

Les hôpitaux et cabinets de santé doivent donc s'équiper de solutions de sécurité d'identités pour sécuriser leurs données et les dossiers médicaux des Français. La santé est un domaine d'importance vitale et se doit d'être mis à l'abri des cyberattaques pour le bien de tous.