

Cyberattaque : La santé impactée

Internet

Posté par : JulieM

Publié le : 2/11/2022 13:00:00

Ce secteur est ainsi deux fois plus vulnérable aux conséquences de violations des données que les autres secteurs

Netwrix, fournisseur de cybersécurité qui simplifie la sécurité des données, dévoile de nouvelles conclusions pour le secteur de la santé issues de son rapport mondial 2022 sur la sécurité du cloud.

61 % des organismes interrogés dans le secteur de la santé ont subi une cyberattaque ciblant leur infrastructure cloud au cours des 12 derniers mois, contre 53 % pour les autres secteurs. Le phishing est le type d'attaque le plus courant.

« Les établissements de soins de santé sont une cible lucrative pour les attaquants, car les chances de réussite y sont plus élevées. En effet, les deux premières années de la pandémie ont épuisés les équipes ; et la santé des patients demeurant la priorité absolue, les ressources de cybersécurité ont été très sollicitées.

Les efforts se sont donc concentrés sur le maintien des fonctions essentielles, observe Dirk Schrader, VP of security research chez Netwrix. De plus, la valeur élevée des données offre aux cybercriminels de meilleures opportunités de gains financiers : ils ont le choix entre la vente sur le Dark Web des informations médicales sensibles volées et la demande d'une rançon en échange de l'accès rendu aux systèmes indispensables à la survie des patients. »

Il est également plus probable qu'une attaque dans le secteur de la santé entraîne des conséquences financières. 32 % des organisations interrogées dans d'autres secteurs déclarent avoir subi une attaque sans impact sur leur activité, alors que ce n'était le cas que pour 14 % dans la santé.

Les dépenses imprévues pour couvrir les failles de sécurité, ainsi que les amendes pour non-conformité, sont les types de dommages les plus courants auxquels ce secteur fait face après une cyberattaque.

« Les établissements de santé prévoient d'augmenter leur workload dans le cloud de 38 % à 54 % d'ici la fin 2023, poursuit Dirk Schrader. Or, l'adoption rapide du cloud doit s'accompagner de mesures de sécurité appropriées et d'une attention particulière aux dispositifs et systèmes liés à l'Internet des objets (IoT).

La segmentation du réseau contribuera à protéger l'ensemble du système si l'un de ses appareils est compromis. Les équipes IT doivent également limiter strictement qui a accès humain comme machine - peut accéder à quelles données et à quels systèmes, conformément au principe du moindre privilège, et réexaminer régulièrement ces droits d'accès pour les ajuster si besoin. »