Acronis

5 étapes pour renforcer la cyberrésilience dans le secteur de la santé

Le secteur de la santé est une cible lucrative pour les cyberattaques, et les coûts de récupération ne cessent d'augmenter, atteignant des dizaines de milliards de dollars chaque année. Pourquoi les frais associés à la restauration augmentent-ils ? Les écosystèmes de santé d'aujourd'hui sont largement interconnectés, ce qui amplifie l'impact et les dégâts des attaques. Les cybercriminels ont besoin de moins de temps et de ressources pour causer davantage de dommages.

De la salle de réunion au bloc opératoire : Les interruptions d'activités affectent tous les acteurs du secteur de la santé

92 %
des organisations de santé ont signalé au moins une attaque en 2024[1].

300 %
d'attaques par ransomware en plus ont frappé le secteur de la santé depuis 2015[2].

41 %
des RSSI considèrent les ransomwares comme l'une des trois menaces les plus préoccupantes[3].

56 %
des organisations de santé signalent de mauvais résultats pour les patients en raison des attaques[4].

53 %
des établissements de santé ont constaté une hausse des complications médicales à la suite d'une cyberattaque[5].

28 %
des établissements de santé victimes de cyberattaques déclarent une hausse du taux de mortalité[6].

5 étapes pour renforcer la cyberrésilience dans le secteur de la santé : Défense et restauration

Donner la priorité à une cybersécurité robuste

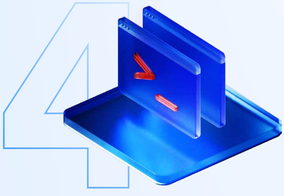
Investissez dans des solutions avancées de détection, de prévention et de réponse aux menaces. Mettez régulièrement à jour vos logiciels et appliquez les correctifs sans délai.

Mettre en place une segmentation efficace

Limitez les déplacements latéraux des cybercriminels sur votre réseau. Isolez les systèmes critiques pour éviter une propagation massive.

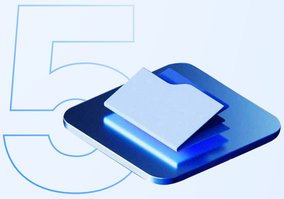
Élaborer des plans de reprise d'activité après sinistre et de continuité des activités

Définissez et testez des plans solides pour assurer la poursuite ou la restauration rapide des opérations en cas d'attaque.



Renforcer la gestion des risques liés aux tiers

Évaluez rigoureusement les pratiques de sécurité de tous vos fournisseurs et partenaires, et surveillez-les en continu, en particulier ceux ayant un accès étendu à vos systèmes.



Améliorer les capacités de réponse aux incidents

Mettez en place des protocoles clairs pour détecter, contenir et corriger les incidents. Organisez régulièrement des exercices et des formations.

En savoir plus sur Acronis Cyber Protect pour le secteur de la santé

↘ En savoir plus

[1] **The HIPAA Journal. "92% of U.S. Healthcare Organizations Experienced a Cyberattack in the Past Year." Posté le 9 octobre 2024.** https://www.hipaajournal.com/92pc-us-healthcare-organizations-cyberattack-past-year/

[2] **IBM. "When ransomware kills: Attacks on healthcare facilities." Posté le 30 janvier 2025.** https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities

[3] **Statista. "Most significant cybersecurity threats in organizations worldwide according to Chief Information Security Officers (CISOs) as of February 2024." Publié le 10 mars 2025.** https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/

[4, 5, 6] **Healthcare Dive. "Nearly 70% of healthcare organizations hit by cyberattacks report patient care disruptions: survey." Publié le 8 octobre 2024.** https://www.healthcaredive.com/news/healthcare-cyberattacks-patient-care-disruption-ponemon-proofpoint-survey/729251/