TechTarget | Custom Media

Les 3 étapes critiques de **la continuité d'activité dans le secteur des services de santé**

Pour les établissements de santé, répondre aux fortes attentes numériques des soins de nouvelle génération représente un défi redoutable. Les médecins, le personnel soignant et les patients exigent un accès de tous les instants aux dossiers médicaux, depuis n'importe quel périphérique. Les données médicales sensibles et critiques se multiplient jour après jour et suscitent des cauchemars de stockage, de sauvegarde et de partage pour le personnel informatique. Pendant ce temps, les exigences de conformité réglementaire et les sanctions continuent à augmenter.

Les temps d'arrêt, les pertes de données et les violations de sécurité des données font courir aux établissements de santé le risque d'amendes réglementaires, sans parler des dommages infligés à la marque et de la perte de confiance des patients. La vie des patients peut également être menacée en raison des temps d'arrêt. Entre les budgets restreints, les attentes fortes et la dépendance numérique croissante, la concurrence et l'ampleur des enjeux, aucun établissement ne peut se permettre de faire un faux pas sur le marché actuel des services de santé.

Ce document analyse l'importance critique de la disponibilité dans le secteur des services de santé et les trois étapes que vous pouvez suivre pour améliorer la continuité de votre activité.

Sponsorisé par
Veeam Software
VEEAM

Chapitre 1 : La numérisation du secteur des services de santé

Comprendre le lien direct entre la technologie et les soins dispensés aux patients est essentiel, mais peut s'avérer accablant. Les médecins comptent sur des informations actualisées pour prendre des décisions pertinentes quant aux meilleurs traitements pour leurs patients. L'accès aux données des patients est essentiel pour les soins et parfois, il peut faire la différence entre la vie et la mort. Les dossiers de santé électroniques (DSE) passent d'un système à l'autre, d'un hôpital à l'autre, de l'enregistrement initial du patient à sa sortie en passant par les données recueillies dans les différents services tels que les laboratoires, la radiologie ou la cardiologie. Ajoutez cela aux données financières et d'assurance recueillies et on comprend mieux l'importance de la disponibilité dans le secteur des services de santé.

De plus, chaque acteur des services de santé a une « expérience numérique » ou une façon spécifique de travailler et de vivre avec la technologie.

- **Médecins, personnel soignant et hospitalier :** L'expérience numérique s'articule sur les données recueillies auprès des patients et de diverses autres sources. Sans elles, leur travail serait sérieusement compromis.
- **Patients :** L'expérience numérique est centrée sur la capacité à accéder à leurs données médicales, à les partager à tout instant et depuis n'importe quel périphérique. Cette capacité leur permet de se faire un avis sur leurs propres soins.
- **Actionnaires et institutions de services de santé :** L'expérience numérique porte sur les données requises pour la productivité, la transparence, la conformité, le paiement et les meilleures pratiques relatives aux soins.

Chapitre 2 : Continuité d'activité — maintenir l'expérience numérique

Les temps d'arrêt peuvent avoir des conséquences catastrophiques sur l'expérience numérique du personnel soignant, des administratifs, des parties prenantes et des patients.

Dans une étude publiée par le *Journal of Biometrics*, les chercheurs ont indiqué que 96 % des incidents de sécurité concernant les patients signalés à la Food and Drug Administration des États-Unis était dus à des problèmes techniques.[1] Certains incidents ont entraîné des recherches inutiles de résultats de tests, l'incapacité à lire les résultats de tests et des commandes de procédures dupliquées.

À grande échelle, l'attaque du ransomware WannaCry de mai 2017 a affecté 230 000 ordinateurs et a fait trembler les fondations du National Health Service britannique. WannaCry est un virus qui exploite certaines faiblesses connues de Microsoft Windows, une plateforme largement utilisée dans les hôpitaux à travers le monde. Le virus bloque toutes les données des systèmes informatiques jusqu'au paiement d'une rançon. Ainsi, chaque aspect de l'expérience numérique du personnel soignant, des administratifs et des patients est affecté.

Dans le cas mentionné, le virus a infecté les périphériques médicaux et provoqué le détournement d'ambulances et l'arrêt de 16 hôpitaux du Royaume-Uni.[2] Les autres hôpitaux dont les systèmes étaient arrêtés ont dû annuler les opérations prévues et les services d'urgence ont été bloqués. De plus, les dossiers médicaux des patients étaient inaccessibles.

Un panorama des menaces en évolution

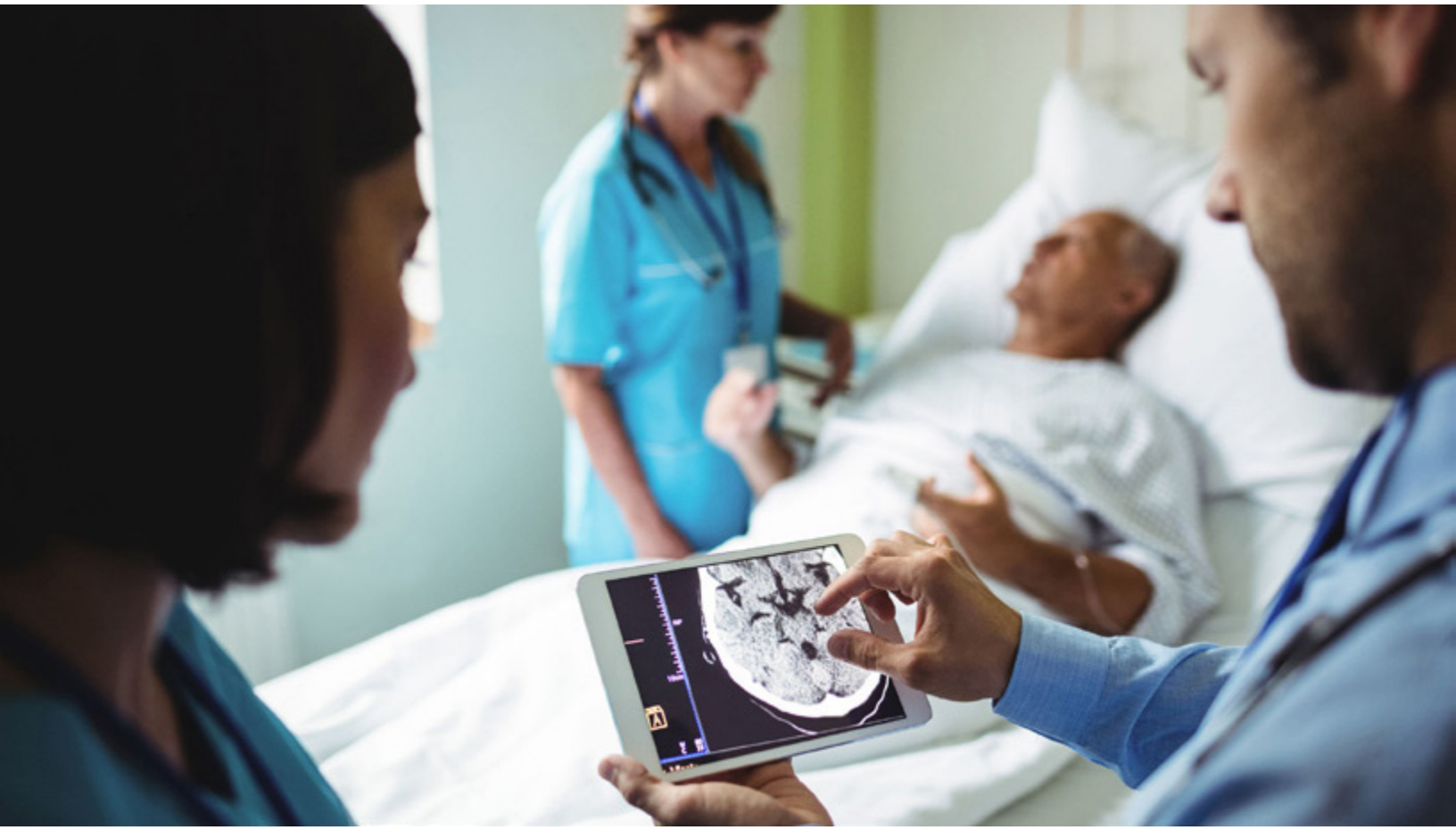
Les cybermenaces visant les services de santé comprennent les pirates, les attaques par botnet, l'exfiltration (le vol d'informations médicales) et les logiciels malveillants tels que les ransomware. Selon l'avis général, une cyberattaque sur un établissement de santé n'est pas une éventualité mais une certitude. Les cyberattaques peuvent paralyser les établissements de santé et compromettre gravement les soins dispensés aux patients. Elles peuvent également causer un préjudice majeur à leur image et entraîner de lourdes pénalités réglementaires.

Les workloads numériques vitaux et complexes des services de santé

Les établissements de santé possèdent des workloads parmi les plus volumineux, les plus complexes, les plus sensibles et les plus précieux de tous les secteurs d'activité confondus. L'équipement de diagnostic et l'internet des objets médical génèrent d'énormes fichiers numériques 24 heures sur 24. Ces données doivent être partageables, récupérables, stockées et archivées en toute sécurité. La loi fédérale protège les dossiers médicaux électroniques (DME) et les DSE.

1 « Measuring the effects of computer downtime on hospital pathology processes », Journal of Biomedical Information, Wang, Ying, et al., février 2016

2 « NHS seeks to recover from global cyber-attack as security concerns resurface », *The Guardian*, 13 mai 2017



Tout temps d'arrêt affecte les patients, le personnel soignant et l'activité en cercles concentriques :

- Lorsque les patients ne peuvent pas accéder à leurs données médicales ou aux canaux de communication en ligne, la dynamique de maintien ou de rétablissement de leur bonne santé est cassée. Dans le marché hautement concurrentiel d'aujourd'hui, les patients frustrés sont également des consommateurs frustrés qui peuvent facilement choisir un autre fournisseur.
- Lorsque les médecins, le personnel soignant et le personnel administratif ne peuvent pas accéder aux données, ils ne peuvent pas être productifs ni prendre des décisions dans le meilleur intérêt de leurs patients.
- Pour un établissement de santé, les pertes de productivité, les erreurs et les insuffisances ont des conséquences négatives sur la conformité, la réputation, la marque et le chiffre d'affaires.

Chapitre 3 : Assurer la disponibilité et la continuité d'activité dans le secteur des services de santé

Les hôpitaux et les centres de soins comprennent des services critiques qui ne tolèrent aucun temps d'arrêt. Certaines procédures chirurgicales reposent sur les données en temps réel fournies par les équipements de diagnostic numériques. Hélas, il existe des cas de décès de patients dus à des temps d'arrêt. Selon un rapport récent, un temps d'arrêt a retardé un traitement postopératoire et a entraîné un handicap permanent pour un patient et la mort d'un autre en raison de l'impossibilité de transmettre des images pour diagnostic.[3]

En plus de décès tragiques, si un établissement de santé n'est pas capable de restaurer un accès immédiat à ses données, il subit des amendes réglementaires, une perte de confiance du public et une dégradation du moral des employés. La clé pour survivre et s'épanouir dans le nouveau paysage des services de santé tient dans un plan de continuité d'activité fiable et complet. La disponibilité est la pierre angulaire d'un tel plan de continuité d'activité dans le contexte de la transformation numérique.

L'écart de disponibilité

Selon une récente étude d'Enterprise Strategy Group (ESG),[4] la moitié des 1 000 entreprises interrogées estiment que les problèmes de disponibilité ont abouti à une perte de confiance des consommateurs, à des conséquences négatives sur l'intégrité de la marque et à la révocation de licences et d'accréditations.

De nombreuses entreprises ont également indiqué que les problèmes de disponibilité ont entraîné une perte de confiance des employés et la réaffectation de ressources qui se consacraient aux projets stratégiques.

Il est important d'évaluer votre propre écart de disponibilité avant qu'une catastrophe ne se produise :

- **Quantifiez les accords de niveaux de services (SLAs) :** Faites-le pour chaque unité opérationnelle et de soins dans votre établissement.
- **Évaluez les mécanismes de protection existants :** En comparant vos besoins de disponibilité aux métriques réelles, vous pourrez identifier les écarts dans votre plan de continuité d'activité.
- **Convertissez les écarts en analyses de conséquences :** Pour chaque unité opérationnelle ou de soins, déterminez les conséquences de la panne d'un système pour les patients, le personnel et l'activité.
- **Communiquez les conclusions de l'analyse de conséquences aux décideurs :** Illustrez la mesure dans laquelle une indisponibilité affecterait l'expérience numérique des patients, du personnel soignant et de l'établissement.

3 Op. cit., *Journal of Biomedical Information*

4 « Pourquoi les entreprises éprouvent encore des difficultés à effectuer leur transformation digitale et à innover », Veeam Availability Report 2017, Veeam et Enterprise Strategy Group, 2017

Chapitre 4 : Les 3 étapes critiques de la continuité d'activité dans le secteur des services de santé

Face à des enjeux aussi considérables, les entreprises de services de santé doivent se préoccuper de la continuité de leur activité et elles doivent le faire rapidement et de façon réfléchie. Les trois étapes les plus critiques de la continuité d'activité dans le secteur des services de santé sont :

1. Assurer la continuité et la disponibilité

- **Stratégie de sauvegarde et de restauration optimisée :** Les institutions médicales ont besoin d'outils de sauvegarde et de restauration fiables, rapides et évolutifs conçus spécialement pour les grandes entreprises. Elles doivent être capables de restaurer rapidement leurs sauvegardes pour répondre aux obligations légales sur l'assurance maladie (HIPAA) et à d'autres exigences réglementaires. Une bonne recommandation de sauvegarde est la règle du 3-2-1 :
  - 3 : Disposez de trois copies de vos données au moins.
  - 2 : Stockez vos copies sur deux supports différents.
  - 1 : Conservez une copie de vos sauvegardes hors site.
- **Assurez-vous de pouvoir restaurer rapidement des machines entières au niveau des applications :** La vérification permanente de la restauration de chaque fichier, application ou serveur virtuel est essentielle.
- **Assurez la prévention des pertes de données :** Votre solution de disponibilité doit vous permettre des améliorations majeures, avec des temps de restauration et des délais optimaux de reprise d'activité (RTPO™) inférieurs à 15 minutes pour toutes les applications et toutes les données.

2. Assurer l'agilité de la transformation numérique

- **Mobilité des workloads cloud :** Pour vous assurer que vous pouvez rapidement restaurer des machines entières, déployez la mobilité des workloads cloud afin de mieux vous adapter aux changements et administrer vos données plus facilement. Vous devez également avoir la capacité à tester toutes vos applications et vos mises à niveau avant leur déploiement en production. Pour la mobilité des workloads cloud, tirez parti d'Azure ou d'autres clouds publics pour vos environnements de test et de développement. Cela vous permettra de monter des serveurs et des workloads rapidement et facilement.
- **Mobilité des workloads :** L'infrastructure complexe d'une grande entreprise comprend des machines physiques et virtuelles, ainsi que des clouds privés, publics ou hybrides. Pour parvenir à une configuration optimale et gérer ou migrer vos données facilement, il vous faut une solution d'administration et de disponibilité des données qui offre une certaine flexibilité.

3. Profiter des analyses et de la visibilité

- **Visibilité et conformité pour empêcher les pannes et les temps d'arrêt :** L'outil de visibilité que vous choisissez doit permettre la supervision et le reporting en temps réel de tous les environnements virtualisés de votre infrastructure.
- **Visibilité de bout en bout des machines physiques et virtuelles :** Pour être efficace, il doit également offrir la visibilité de bout en bout des machines virtuelles et physiques pour prévenir tous les types de défaillances éventuelles des applications ou du système.
- **Création de procédures de gestion d'incidents en fonction des événements qui se produisent dans votre environnement :** Enfin, il doit générer des rapports d'incidents en fonction des événements qui se produisent dans votre environnement afin que vous puissiez apporter les corrections et les modifications nécessaires.

Conclusion

Pour l'informatique des services de santé, répondre aux fortes attentes numériques des soins de nouvelle génération revient à viser une cible mobile. Les temps d'arrêt, les pertes de données et les violations de sécurité des données exposent au risque tout ce qui est important pour un établissement de santé. Les périodes d'indisponibilité peuvent même mettre la vie des patients en danger. En fait, aucun établissement de services de santé ne peut se permettre d'improviser sur le marché des services de santé modernes.

Pour réussir dans ce nouveau contexte, les établissements de santé doivent avoir confiance en leur stratégie de continuité d'activité. Une stratégie de disponibilité holistique peut comprendre le déploiement de la mobilité des workloads cloud, l'augmentation de la visibilité et de la conformité et l'optimisation des stratégies de sauvegarde et de restauration.

Toutes les solutions de disponibilité ne sont pas identiques. Pour plus d'informations sur la manière d'implémenter une solution de sauvegarde, de restauration et de disponibilité holistique, veuillez consulter le site de Veeam à l'adresse www.veeam.com/fr.