Avis d'expert : la mobilité sécurisée au service de la santé

Un service de santé de qualité dépend grandement des technologies mises en places par les différentes structures pour rapprocher les médecins, les infirmières et les équipes médicales de leurs patients afin de pouvoir enregistrer des données de façon précise en temps réel et donc apporter les soins nécessaires et fournir les traitements et/ou les médicaments appropriés.

Le réseau est au cœur de tout, depuis les communications, en passant par les données relatives au patient, jusqu'aux choses les plus basiques comme la construction et la gestion de l'infrastructure des bâtiments (des portes d'entrée aux parkings).

Un réseau Ethernet mobile « intelligent » est capable de supporter des éléments critiques comme les DMP (dossiers médicaux informatisés qui contiennent de nombreuses informations sur les soins pratiqués), les CPOE (décisions prises par les médecins et transmises via le réseau aux différents services médicaux d'un hôpital comme la pharmacie, le laboratoire ou le service de radiologie par exemple), ou encore les données relatives aux traitements et aux médicaments administrés, les antécédents médicaux et les allergies dont souffrent les patients, etc.

Par ailleurs, les technologies d'imagerie médicale comme le DICOM (gestion des données issues de l'imagerie médicale) et le PACS (système d'archivage et de transmission d'images) produisent, archivent et fournissent des images haute-résolution, en 3D, animées et colorées : le réseau à hautes performances sur lequel s'appuient ces technologies se doit donc d'être à la fois résilient, intelligent et sécurisé.

La question de l'identité

Lorsqu'il s'agit de conserver en toute sécurité les informations relatives au patient et de répondre aux exigences de conformité, les cliniques ne peuvent pas se permettre d'expliquer à leurs clients qu'une intrusion a eu lieu sur le réseau. Le droit à la confidentialité des données est fortement réglementé et contrôlé en Europe. Les dossiers des patients doivent donc être sécurisés en accord avec la directive européenne sur la protection des données.

Le rapport d'enquête intitulé *"2012 HIMSS Analytics Report: Security of Patient Data"* (Rapport d'Analyses HIMSS 2012 : sécurité des données relatives aux patients) a été effectué par la société de conseil Kroll Advisory Solutions.

Au cours de cette étude, il a été demandé aux directeurs responsables de la gestion de la sécurité informatique, aux responsables des technologies de l'information et de la communication, aux gestionnaires des informations relatives à la santé et aux responsables des données à caractère privé travaillant dans 250 hôpitaux et centre médicaux de citer le nombre d'intrusions dont ils avaient eu connaissance ces douze derniers mois : 27% d'entre eux avaient eu connaissance d'au minimum une intrusion durant l'année, contre 19% en 2010 et 13% en 2008.

L'étude a mis en évidence que 79% de ces intrusions avaient pour origine les employés,

tandis que la plupart des autres étaient dues à des sous-traitants ou des prestataires de service. Plus de la moitié des problèmes ont été identifiés comme étant des « accès non autorisés à des informations » de la part de personnes individuelles.

Pour que les équipes informatiques des services médicaux puissent gérer efficacement des menaces à la fois internes et externes comme celles que nous venons de décrire, un certain nombre de nouveaux mécanismes de sécurité ont émergé, comme par exemple les solutions de gestion des identités (Identity Management/IM) permettant aux administrateurs des services informatiques de savoir de quelle manière, depuis quel lieu et sous quelle identité un utilisateur ou un équipement accède au réseau et à ses ressources.

L'une des parties clés d'une politique globale de gestion de l'identité basée sur la fonction de chaque individu au sein d'une entreprise est un mécanisme permettant l'enregistrement sécurisé des différents utilisateurs et équipements et l'assignement des bonnes fonctions occupées et des bonnes politiques à ces utilisateurs et équipements.

Au fur et à mesure que les utilisateurs et les équipements se connectent au réseau, leur identité est d'abord enregistrée puis conservée pour pouvoir être ensuite l'objet d'un réel suivi. Cela se traduit notamment par une absence d'interruption du flux de travail de l'utilisateur et aide à fournir une meilleure expérience d'utilisation.

Avec l'intégration du protocole LDAP aux commutateurs réseaux (ne nécessitant pas d'appareil externe ou la superposition de modèles de sécurité), le réseau peut exploiter les profils et les attributs utilisateurs déjà existants dans le LDAP/Serveur Active Directory. Alors que les utilisateurs et/ou les équipements parcourent le réseau, la Gestion d'Identité (IM) peut fournir des politiques simplifiées de « suivi personnalisé » basées sur la fonction de chaque utilisateur pour assurer la productivité à la demande tout en améliorant la sécurité.

L'IM identifie les équipements et peut allouer des ressources réseaux ou définir des politiques de sécurité en fonction de ces derniers, s'assurant par exemple qu'un port d'accès situé à l'accueil et qui ne devrait être utilisé que pour une caméra vidéo, n'est pas utilisé pour fournir une connexion à un ordinateur portable en dehors des heures d'ouverture ou permettre l'accès à des applications sans fil clandestines depuis le parking, protégeant de manière efficace contre les connexions non autorisées ou imprévues.

Les solutions réseau mobiles choisies par les services de santé doivent être conçues pour inclure plusieurs niveaux de protection, sur les segments sans fil comme sur les segments câblés du réseau. Les fonctionnalités de sécurité doivent fonctionner de façon automatique – ou nécessiter très peu d'interventions – et être automatisées pour permettre une gestion proactive des évènements ayant trait à la sécurité, comme les ajouts, les déplacements ou les modifications.

La mobilité : une prescription pour le succès

Un réseau local sans fil fournit aux services de santé un fort potentiel de mobilité leur permettant de mieux atteindre leur but premier : apporter un suivi médical de qualité à leurs patients.

Avec un mélange de connectivité avec et sans fil, les personnels soignants ne sont plus contraints d'être enchainés à leurs bureaux pour rechercher des données ou saisir des renseignements, donner des conseils ou encore communiquer entre eux.

Désormais, ils peuvent travailler au chevet de leurs patients et profiter de la facilité d'utilisation et de la précision du système Point Of Care (POC) en accédant aux fichiers d'images PACS, aux données EMR et à tous les services de téléphonie et de gestion des données disponibles sur le système du service de santé auquel ils appartiennent via le réseau et depuis n'importe quel endroit sur le campus.

Ils peuvent également travailler de manière collaborative, en accédant à des fichiers provenant de n'importe quelle origine et en les regardant/analysant ensemble. En plus de faciliter grandement la mobilité, les accès sans fil réduisent significativement le nombre d'erreurs humaines puisque les données du patient sont désormais saisies en temps réel dans le système depuis le chevet du patient, plutôt que d'être d'abord transcrites par écrit pour ensuite être saisies dans le système bien plus tard, ce qui se traduisait par des erreurs d'interprétation ou de compréhension beaucoup plus nombreuses.

La voix sur réseau local sans fil (VoWLAN) améliore encore davantage la mobilité en permettant aux médecins et aux autres membres de l'équipe de se déplacer d'un endroit à l'autre de l'hôpital ou de la clinique tout en continuant à parler via un kit mains libres VoIP adapté ou via leur badge équipé d'un système de communication vocale.

Les téléphones mobiles souffrent régulièrement d'une perte de signal due aux barrières structurelles (interférences physiques ou électroniques) lorsque le personnel de santé se déplace entre les différents bâtiments ou depuis le garage sous terrain jusqu'à l'entrée et l'étage de leur patient, alors que la technologie VoWLAN est bien plus fiable, permettant de maintenir la conversation à travers tous les bâtiments et toutes les pièces du campus, ce qui est crucial dans les situations d'urgence.

Fonctionnalités indispensables pour une solution mobile destinée aux services de santé :

- Mise en réseau basée sur l'identité pour segmenter de manière logique les utilisateurs (accès différenciés pour les médecins, infirmiers, patients…).
- Performances permettant de fournir un accès en continu et depuis n'importe quel lieu aux DMP (EMR) et aux CPOE.
- Réseau fiable et disponible 24h/24, 7 jours sur 7.
- Capacité à sécuriser des points d'accès pour les services destinés aux visiteurs.
- Conformité avec la sécurité HIPAA et les standards EMI.
- Accès rapide aux images médicales PACS et DICOM.
- Mises à l'échelle et mises à jour faciles à mettre en place.
- Gestion du réseau et résolution de problèmes centralisées.

La résilience répond aux exigences essentielles

Un réseau sans fil est souvent bien plus résilient qu'un réseau câblé indépendant en raison de la nature même de son déploiement. Les appareils de contrôle et les points d'accès peuvent être

distribués dans des zones de couvertures se chevauchant, éliminant ainsi les zones blanches et les points de déconnexion ponctuelle.

Lorsqu'ils sont configurés sur des serveurs redondants et en grappe, ces équipements fonctionnent comme un domaine unifié à haute densité capable de supporter une répartition des charges agrégées, le basculement automatique en cas de panne et la gestion à distance. Cela n'augmente pas uniquement la résilience et la fiabilité, mais facilite également la gestion, réduit l'encombrement et lorsque les équipements supportent le PoE, permet de réaliser d'importantes économies d'argent et d'énergie et de limiter l'émission de carbone dans l'atmosphère.

Lorsque les solutions sans fil sont évaluées consciencieusement à la fois en termes de compatibilité HIPPA et d'extensibilité et lorsqu'elles sont déployées pour s'intégrer de manière homogène à l'infrastructure câblée, les services de santé peuvent alors profiter d'une importante sécurité, d'une grande résilience et d'une mobilité totale au sein d'un réseau convergent.

Prendre soin de créer des fondations solides permettra de rationaliser l'installation, la maintenance et les mises à jour tout au long du cycle de vie du réseau, pour améliorer le coût total de propriété et le retour sur investissement.

Crédit photos : © Extreme Networks

Voir aussi

Quiz Silicon.fr – La fibre optique en dix questions