Pourquoi les systèmes informatiques de santé sont-ils si difficiles à sécuriser ?

Par Leif Nixon,
Expert sécurité chez Sectra Communications

Les questions de sécurité des systèmes informatiques dans le monde de la santé soulèvent de plus en plus d'inquiétudes, chez les professionnels du secteur comme dans les organismes réglementaires. Ces six derniers mois, le FBI, le Ministère américain de la sécurité intérieure et d'autres organisations de sécurité n'ont cessé d'alerter, par des messages flash, contre le renforcement de la menace visant les systèmes des établissements de santé. Parmi les acteurs de la santé, on ne compte plus les victimes de rançongiciels qui mettent en danger la vie des patients et causent des pertes financières énormes. Pourquoi une telle recrudescence des attaques spécifiquement dans ce secteur ? Le domaine de la santé aurait-il des spécificités qui rendraient particulièrement difficile la sécurisation de ses données ? La réponse est clairement oui.

Sûreté versus sécurité

Bien que très proches, sûreté et sécurité sont considérées comme des activités distinctes. La première consiste à lutter contre les défaillances et les erreurs, alors que la seconde vise les attaques délibérées. Or, on constate que dans le domaine de la santé, ces deux concepts sont très étroitement liés. Ajoutez à cela le caractère souvent très confidentiel des données traitées par les systèmes informatiques de santé, et vous obtenez des problématiques sans fin pour lesquelles, faute de solutions idéales, il faut bien se contenter de compromis imparfaits.

En voici un exemple concret : Les textes réglementant la confidentialité des données, tels que la loi HIPAA aux Etats-Unis ou le RGPD, indiquent que les archives médicales sont des données extrêmement sensibles nécessitant une protection avancée. Cette affirmation a suscité des exigences de sécurité limitant strictement les accès aux bases de données aux seules personnes authentifiées via une procédure sécurisée. Cependant, on peut comprendre que du strict point de vue de la sécurité, l'accès rapide aux archives médicales peut être une question de vie ou de mort. L'urgence médicale s'accommode très mal des verrouillages d'écrans et autres mots de passe oubliés.

En, pratique, les compromis permettant de résoudre le conflit entre sécurité et sûreté vont des dispositifs de type “bris de glace” avancés, où il est possible de contourner le contrôle d'accès normal en cas d'urgence, jusqu'aux solutions plus pragmatiques consistant à placer la souris d'ordinateur à l'intérieur d'un agitateur de poches de sang basculant d'un côté à l'autre afin d'empêcher l'activation du verrouillage d'écran.

Des systèmes informatiques superposés sur trois niveaux

La structure tripartite caractéristique des systèmes informatiques de santé, complexifie encore ces problématiques. Tous les prestataires d’établissement de santé possèdent évidemment des systèmes pour assurer leurs tâches bureautiques quotidiennes comme la messagerie ou la gestion de feuilles de calcul. Cette catégorie informatique est commune à toutes les grandes structures, et non spécifique à la santé.

Bien que la protection de ces systèmes ne soit pas encore parfaite, elle peut néanmoins s'appuyer, pour la résolution des problèmes, sur un socle commun de connaissances et de bonnes pratiques.

Les acteurs de la santé les plus importants utilisent aussi de nombreux dispositifs médicaux connectés, depuis les pompes à perfusion ou moniteurs de glucose jusqu'aux appareils d'IRM ultra-sophistiqués, tous raccordés au réseau informatique à des fins de suivi, de partage de données et d'accès distant. Ces instruments sont soumis à des procédures de sécurité très strictes souvent incompatibles avec les pratiques de sécurité informatique classiques comme les mises à jour régulières des logiciels. De fait, beaucoup d'appareils médicaux contiennent des ordinateurs intégrés exécutant des systèmes d'exploitation qui ne sont plus supportés par le fabricant. Or un ingénieur de sécurité informatique décidant classiquement de placer des systèmes aussi peu sécurisés dans des réseaux entièrement isolés, peut se trouver dans l'incapacité de réaliser une telle opération car elle empêcherait les personnels d'accéder à leurs données médicales depuis un poste de travail distant. En outre, beaucoup d'hôpitaux s'adressent à des prestataires spécialisés, comme des sociétés de téléradiologie, basés dans des territoires éloignés afin de faciliter le service en dehors des heures d'ouverture des établissements, d'où la nécessité de transférer les données d'IRM à des spécialistes travaillant à l'autre bout du monde.

Au-dessous des systèmes administratifs et des instruments médicaux des prestataires de santé se trouve un troisième type de système, souvent méconnu : le système de contrôle et d'acquisition de données (SCADA) qui gère l'infrastructure des établissements.
Tous les services fondamentaux intégrés aux bâtiments modernes — chauffage, ventilation, eau, électricité, éclairage — sont gérés par des systèmes informatiques spécialisés. Toutefois, bien que leur rôle soit absolument vital pour le bon fonctionnement des hôpitaux, ils sont rarement pris en compte dans les questions de sécurité informatique. Les scénarios catastrophes susceptibles de devenir réalité sont pourtant nombreux et parfaitement crédibles.

Par exemple, un rançongiciel qui parviendrait à pénétrer dans un ordinateur chargé de la gestion du système de chauffage et de ventilation d'un hôpital pourrait stopper toutes les opérations importantes en cours en arrêtant la ventilation des blocs opératoires puis en désactivant l'ordinateur. De même un cybercriminel qui pénétrerait dans les systèmes d'alimentation électrique de l'établissement pourrait tout à fait couper l'alimentation principale et de secours et donc mettre en danger la vie des patients en quelques minutes. Et ceci n'est qu'un exemple parmi une longue liste de désastres possibles.

Un paysage réglementaire complexe

Au-delà de leur propre complexité technique, les systèmes informatiques de santé sont confrontés à un véritable dédale réglementaire. Prenons l'exemple d'un système typique chargé de la distribution d'oxygène médical, dans lequel le gaz est acheminé dans l'ensemble de l'hôpital à l'intérieur de conduits pressurisés. Dans un contexte normal, la canalisation physique est sous la responsabilité du personnel en charge des installations, tandis que le gaz est un produit médical dont la responsabilité revient à une infirmière ou un médecin spécifique. De plus, il existe des codes de sécurité de l'industrie encadrant la prise en charge des gaz sous pression, et imposant la mise en place d'un service interne de sécurité des gaz. Or, il est extrêmement difficile d'identifier, parmi les nombreuses parties prenantes concernées, celle à qui incombe en dernier ressort la responsabilité de la sécurité informatique du système de contrôle de la distribution de gaz.

Le manque de clarté dans les chaînes de responsabilités augmente le risque de voir une menace passer entre les mailles du filet de protection, et rend plus difficile la mise en œuvre d'une politique de sécurité informatique cohérente.

Comment échapper au fléau des rançongiciels ?

Au vu de ce que nous venons de décrire, il est peu surprenant de constater que beaucoup d'établissements médicaux sont des cibles assez faciles pour des cybercriminels déterminés. La plupart d'entre eux cherchent naturellement à retirer un avantage financier de leurs attaques. Si les archives médicales volées ont toujours eu une certaine "valeur de marché", c'est avec la généralisation des attaques par rançongiciels que la menace sur la sécurité informatique des établissements de santé a véritablement décollé ces dernières années.

En refusant purement et simplement de payer la rançon exigée, une entreprise classique frappée par une attaque de rançongiciel peut — par simple civisme ou par malveillance — ruiner l'investissement investi par le pirate. Au contraire, face à l'enjeu capital de la sécurité des patients, un établissement de santé sera plus enclin à vouloir rétablir ses systèmes. Pour les cybercriminels les plus endurcis, les acteurs de la santé sont donc des cibles particulièrement rentables financièrement, car ils sont plus susceptibles que d'autres de céder au chantage.

« Un rançongiciel qui parviendrait à pénétrer dans un ordinateur chargé de la gestion du système de chauffage et de ventilation d'un hôpital pourrait stopper toutes les opérations importantes en cours en arrêtant la ventilation des blocs opératoires puis en désactivant l'ordinateur. »

Si de nombreux cybercriminels se sont engagés publiquement à ne pas rançonner les établissements de santé pendant la pandémie de COVID-19, d'autres groupes ont, au contraire, renforcé leurs attaques, profitant du fait qu'une victime déjà fragilisée par la pandémie sera plus susceptible de payer une rançon. La plus connue de ces organisations est sans doute le groupe Ryuk, basé en Russie et qui figure en bonne place dans les bulletins d'alerte diffusés par les pouvoirs publics.

Comment trouver la solution ?

Il n'existe malheureusement pas de solution universelle à la crise de sécurité informatique que connaissent les établissements de santé ; pas de boîtier magique qu'il suffirait d'installer sur le réseau ; pas de procédure en 5 étapes qui résoudrait tous les problèmes. Quant à l'idée de mettre tous ces pirates en prison, elle est tout aussi irréaliste : ces gens agissent depuis des états voyous comme l'Iran ou la Russie où ils sont hors d'atteinte de la justice.

Les vraies solutions seront longues à trouver et nécessiteront une étroite collaboration entre toutes les parties prenantes.

Les fabricants d'équipements médicaux doivent s'efforcer d'améliorer la sécurité de leurs produits, et les organismes chargés de faire respecter la loi doivent se demander comment établir une coopération internationale efficace — les établissements de santé, de leur côté, doivent s'attacher à renforcer leur sécurité de manière continue et progressive

Car s'il n'existe pas de solutions toutes faites, des axes d'amélioration de la sécurité ont au moins été identifiés.

La première des prises de conscience est que le combat contre la cybercriminalité est sans fin. Nous avons affaire à des adversaires intelligents et déterminés qui ne cessent d'inventer de nouveaux artifices pour nous tromper. L'expression “la sécurité est un processus, pas un produit” n'a jamais été aussi vraie.

N'oublions pas, non plus, que le renforcement de la sécurité doit être mis en œuvre de manière équilibrée. Si vous consacrez la totalité de votre budget à l'amélioration de la sécurité de vos instruments médicaux, les pirates, toujours prompts à identifier vos points faibles, se rabattront sur votre réseau local.

Et pour finir, pensez à protéger vos systèmes SCADA !

Sectra AB • communications@sectra.com • communications.sectra.com

SECTRA
Knowledge and passion