Dossier réalisé par Elsa Ferreira et Dominique Deveaux

# Cybersécurité : *les hôpitaux sous haute tension*

**À l'hôpital, un virus peut en cacher un autre. Les établissements de santé sont des cibles privilégiées pour des cybercriminels attirés par des données sensibles et un secteur très dépendant de son système informatique.**

*Vincent Trely, président de l'Association pour la sécurité des systèmes d'information de santé (APSSIS)*

©DR

*« Est-ce que le numérique est une menace ? Le numérique induit des risques. Le papier en avait aussi beaucoup »*, pose Vincent Trely, président de l'Association pour la sécurité des systèmes d'information de santé (APSSIS) lorsqu'on lui parle de la généralisation des dossiers médicaux partagés, carnet de santé numérique qui vous permet de coordonner les soins. Mais il reconnaît : *« À partir du moment où l'on produit des données qui sont stockées et circulent, on s'expose à un certain nombre de vulnérabilités. »*

## Précieuses données

D'autant que les données sont pour la plupart non anonymisées. *« C'est tout l'enjeu de leur confidentialité,* souligne Vincent Trely. *On a le nom, l'adresse, le numéro de sécurité sociale, les pathologies, les comptes-rendus. Tout ceci est nominatif. »* Sur le marché noir, les données médicales valent cher. Entre 22 et 150 € le dossier médical, selon le président de l'APSSIS qui base ce prix sur une dizaine d'estimations en vigueur. Ces dossiers sont vendus par milliers – certaines bases de données regroupent les informations de plus de 300 000 patients. De quoi faire monter les enchères. *« Les données volées peuvent servir à des escroqueries,* détaille Vincent Trely. *Les escrocs récupèrent les infos puis appellent les patients et se font passer pour l'hôpital : "Bonjour, c'est tel hôpital, on a besoin de mettre à jour votre dossier." »* Ils endorment la vigilance des patients en demandant des informations médicales et arrivent aux numéros de carte bleue, trigrammes visuels et dates d'expiration. Une technique d'autant plus efficace chez les personnes âgées, *« habituées à respecter l'autorité »*, explique Vincent Trely.

Autre menace : le chantage. *« L'hôpital a la responsabilité de l'absolue confidentialité des données*, rappelle le directeur de l'APSSIS. *On peut lui extirper des données de santé et le menacer de tout mettre sur Internet, avec à la clé autant de procès que vous avez de patients. »*

## Ransonmware, l'autre grande menace

Au-delà du vol de données, les hôpitaux sont menacés par les rançongiciels (aussi appelés cryptolockers ou ransomwares), virus qui chiffrent vos données et les rendent inutilisables. Les cybercriminels demandent alors une rançon pour débloquer les informations. Comme Wannacry, déployé en mai 2017 dans une attaque mondiale et qui

a touché plus de 300 000 ordinateurs. Le Royaume-Uni a été particulièrement affecté avec 80 hôpitaux publics britanniques touchés directement ou indirectement par le virus et près de 600 cabinets de médecins généralistes, pour un coût de 92 millions de livres (soit un peu plus de 107 millions d'euros), notamment en mise à jour des systèmes après l'attaque, selon un rapport du ministère de la Santé. En six jours, plus de 19 000 rendez-vous avaient dû être annulés. En mars 2016, un hôpital de Boulogne a été victime du virus Locky, qui a rendu inaccessibles près de 10 000 fichiers. Si les attaques concernent particulièrement les hôpitaux, les plus petites structures, moins bien préparées, pourraient devenir des cibles intéressantes, alerte Vincent Trely.

### Et les objets connectés en santé ?

*« Les objets connectés se développent à vitesse grand V,* répond Vincent Trely. *50 milliards d'entre eux sont attendus en 2020 dans tous les secteurs. »* La santé n'est pas épargnée, avec des tétines ou des fourchettes reliées à internet mais aussi des pompes à insuline, des pacemakers, des neurostimulateurs, et même des rotules connectées pour les personnes âgées. *« Forcément, quand on a un objet communicant, il y a des failles »*, déclare Vincent Trely. En 2017, l'agence de santé américaine FDA a rappelé 500 000 pacemakers à cause d'une faille de sécurité qui permettait d'en prendre le contrôle à distance, tandis qu'en juin 2018 des chercheurs belges ont pris le contrôle d'un neurostimulateur et déclaré possible d'*« empêcher le patient de parler ou de se déplacer, de provoquer des dommages irréversibles sur son cerveau, et même de l'exposer à une atteinte mortelle »*. En août 2018, des chercheurs en sécurité démontraient qu'il était possible d'envoyer une décharge électrique à travers un pacemaker ou de retenir une dose d'insuline à distance. *« La plupart du temps, les failles sont découvertes par des équipes de chercheurs éthiques qui vont prévenir la communauté »,* rassure Vincent Trely. *Mais certaines failles de sécurité sont inacceptables*, déplore-t-il. *« Toutes les entreprises ne sont pas sérieuses. »*
Quant aux blocs opératoires de plus en plus numérisés, l'enjeu est le même. Pour s'assurer que l'hôpital puisse fonctionner correctement même en cas de panne, les hôpitaux doivent anticiper des plans de continuité d'activité. *« Plus on va vers du tout numérique, plus ça devient compliqué. Il y a une forte dépendance,* déplore Vincent Trely. *C'est tout l'enjeu d'assurer sa sécurité au sens large. »*

## Las Vegas, au rendez-vous des hackers !


© ArnoldReinhold / CC
*Def Con, une des conventions de hackers les plus connues au monde.*

Août 2018. Las Vegas, Etats-Unis. Deux conventions majeures sur la sécurité informatique se sont enchainées : la Black Hat USA 2018 du 4 au 9 au casino Mandalay Bay, et la 26e édition de la DEF CON du 9 au 12, dans les Caesars Palace et Flamingo. La DEF CON doit son nom au niveau d'alerte américain (DEFense Readiness CONdition) allant de 5 (situation normale) à 1 (plus haut niveau). Au programme : plus d'une centaine de conférences, des ateliers « hacking » organisés sur place et des villages thématiques : machines à voter, biohacking, objets connectés, crypto et vie privée, réseaux sans fil, « r00tz Asylum » pour les enfants, hardware hacking, intelligence artificielle, drones, voitures… Un rendez-vous incontournable pour les chercheurs qui présentent leurs trouvailles en matière de sécurité et planchent sur les nouveaux exploits dans la découverte de défauts de sécurité.

## 80 hôpitaux, 600 cabinets de médecins généralistes

***En mai 2017, suite à l'attaque mondiale déclenchée par le virus WannaCry, 300.000 ordinateurs ont été infectés : 80 hôpitaux et près de 600 cabinets de médecins généralistes ont été affectés au Royaume-Uni !***

© CC
*Capture d'écran du message de rançon laissé sur un ordinateur infecté par le virus WannaCry.*