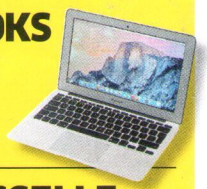
QUE CHOISIR
N°550 • SEPTEMBRE 2016
WWW.QUECHOISIR.ORG EXPERT • INDÉPENDANT • SANS PUBLICITÉ

GRANDES SURFACES
Où acheter moins cher P. 16

TESTS LABO

SMARTPHONES
DE 130 À 969 €
P. 35

ULTRABOOKS
P. 42



LAVE-VAISSELLE
P. 32

IMPRIMANTES MULTIFONCTIONS
P. 40

RENTRÉE SCOLAIRE
P. 44

Du poison dans nos cartables

TEST **LABO**
Crayons, stylos, feutres, colles, encres...

GAZ ÉLECTRICITÉ
Comment faire baisser votre facture
P. 12

ASSURANCE VIE
Faut-il souscrire aux fonds euro-croissance?
P. 52

L 12260 - 550 - F: 4,60 € - RD

Mal protégés, les établissements de santé sont des proies faciles pour les pirates informatiques. Les cyberattaques sont devenues quotidiennes et leurs conséquences peuvent être graves. Pourtant, les dirigeants hospitaliers ne prennent toujours pas la mesure de la menace.

ECHO/GETTY IMAGES - FOTOLIA

ÉTABLISSEMENTS DE SANTÉ

Cyberattaques, les virus se répandent

MORGAN **BOURVEN**

Pour les organisations du monde de la santé, la question n'est pas de savoir si elles seront attaquées, mais quand. Plus une journée ne passe en France sans qu'un établissement de soins ne soit confronté à une cyberattaque. Et pourtant, la sécurité informatique n'est toujours pas considérée comme une priorité des dirigeants hospitaliers. «*Le niveau de prise de conscience est catastrophique*», a alerté Philippe Loudenot, fonctionnaire de sécurité des systèmes d'information (FSSI) pour les ministères des Affaires sociales et de la Santé, en avril dernier, lors du 4e congrès national de l'Apssis (Association pour la promotion de la sécurité des systèmes d'information de santé). Il s'exprimait juste après la démonstration d'un hacker qui, en quelques minutes, avait pris le contrôle de l'informatique d'un hôpital en usurpant l'identité d'un utilisateur.

Un hacker peut pirater le système d'un hôpital en quelques minutes

La sécurité numérique négligée

Pour Philippe Loudenot, les responsables de la sécurité des hôpitaux n'ont «*pas vu arriver la révolution numérique*». Tout, aujourd'hui, est connecté : le dossier du patient, les appareils biomédicaux et même la climatisation des blocs opératoires. Ce n'était pas un problème lorsque les victimes les plus rentables pour les pirates étaient les institutions financières ou les magasins en ligne. Mais les autres secteurs ayant su développer des stratégies de protection efficaces, les cybercriminels se tournent dorénavant vers des cibles plus vulnérables… comme les hôpitaux.

Des établissements rançonnés

Rien qu'en 2015, plus de 1 300 incidents ont été signalés aux autorités par les établissements de santé. Volontaires, ces remontées ne constituent pas une liste exhaustive. Sur ce total, 816 étaient des attaques par opportunisme, autrement dit le système était si poreux que les pirates ont décidé d'y pénétrer. Cette faiblesse est en partie due au manque d'investissement dans les systèmes d'information hospitaliers : ils ne représentent que 2 % des dépenses des établissements. Les experts préconisent d'atteindre 5 %.

L'année dernière, 18 des incidents signalés à Philippe Loudenot étaient des attaques ciblées «*avec une réelle volonté de nuire*». Si l'on ne déplore pas encore d'hôpitaux français évacués à la suite d'une malveillance, comme ce fut le cas à six reprises en >>>

GLOSSAIRE

LES TYPES DE MENACES

Le rançongiciel (ransomware)
Il s'agit d'un « virus » qui verrouille le réseau et les fichiers du système informatique. La seule solution pour en retrouver l'accès : payer une rançon pour récupérer la clé de déchiffrement. Les experts estiment que le taux de réussite de ces attaques dépasse celui d'autres actions cybercriminelles, d'où leur développement.

Le « défaçage » du site Internet
La page d'accueil est remplacée par des images ou messages de propagande ou de revendication. Impressionnante, cette attaque reste anodine. Mais le site visé peut être une porte d'entrée vers le système informatique de l'hôpital.

Le vol ou la perte de données
Dans ce domaine, la moitié des sinistres est liée à une erreur humaine (perte d'un ordinateur portable, négligence…) mais les cyberattaques existent également. Les voleurs s'introduisent dans le système et récupèrent les données des patients, soit pour les revendre, soit pour exercer un chantage sur l'établissement.

Le sabotage
Objectif : s'introduire dans le système informatique et compromettre le fonctionnement des machines médicales ou manipuler les données médicales pour qu'un mauvais traitement soit donné à un patient, voire falsifier les inventaires de médicaments…
Ces scénarios d'attaques ont été menés avec succès, excepté la phase finale d'action, par des sociétés de sécurité mandatées pour tester la sécurité d'hôpitaux.

février et mars aux États-Unis, chaque attaque a des conséquences au minimum financières. Le 1er avril, un établissement de soixante lits a subi cinq jours d'interruption de son système d'information. Coût de la remise à niveau : 50 000 €. À Valence, dans la Drôme, un centre de radiothérapie ayant vu l'ensemble de ses paramétrages effacés, il a fallu reporter tous les rendez-vous. Autre exemple : un hôpital a récemment perdu son « plan blanc », c'est-à-dire le protocole prévu pour faire face à des situations exceptionnelles. Il n'en existait pas de copie. L'inquiétude actuelle la plus forte est liée aux « ransomwares ». Après avoir chiffré les données d'un établissement, ces logiciels malveillants réclament une rançon en échange de la clé de déchiffrement. « *Chaque jour, un hôpital français est touché* », confie Vincent Trely, président de l'Apssis. « *Nous sommes contactés chaque semaine par l'un de nos clients* », confirme un grand éditeur de logiciels hospitaliers. La demande de rançon peut également faire suite à un vol de données. Des pirates ont ainsi rendu public, le 17 mars 2015, les données médicales de 15 000 patients après avoir tenté d'extorquer 20 000 euros au groupe de laboratoires de biologie médicale Labio. « *Accepter de payer constituerait une véritable incitation au renouvellement de telles pratiques* », avait alors expliqué la société pour justifier son refus. Qu'il s'agisse de logiciels de cryptage ou de vol de données, les demandes de rançon sont généralement de quelques dizaines de milliers d'euros. Les pirates font le pari que les établissements paieront rapidement des sommes abordables, afin de reprendre la main sur leur informatique, de préférence avant que leur mésaventure ne s'ébruite.

Les dossiers médicaux des patients valent de l'or pour les cybercriminels

L'assureur Beazley, spécialiste de la gestion des risques, note que si le monde de la santé représente moins d'un tiers de ses clients, il concentre 69 % des incidents liés à la cybersécurité. Les institutions financières arrivent très loin derrière avec seulement 8 % des incidents. Explication : les données de santé sont celles qui ont le plus de valeur sur le marché noir, bien plus que des numéros de carte bancaire, promptement bloqués par les banques. Pirater des dossiers médicaux, c'est disposer d'informations fiables et complètes extrêmement intéressantes pour les arnaqueurs ou faussaires. Le 29 juin, un pirate a annoncé la mise en vente de 9,2 millions de dossiers médicaux volés à une institution américaine, au prix de 750 bitcoins (430 000 euros).

Un petit air de ligne Maginot…

Alors que les établissements sont de plus en plus connectés, on compte, dans l'Hexagone, moins de 600 personnes formées à la sécurité informatique. C'est peu en comparaison des 3 000 établissements de santé recensés sur le territoire. « *90 % d'entre eux disent avoir un référent sécurité, mais il s'agit beaucoup trop souvent de temps partiel ou de sous-traitance* », regrette Michel Raux, de la Direction générale de l'offre de soins (DGOS). Selon ses données, seulement 8 % des établissements ont un référent sécurité à temps complet. Les CHU (centres hospitaliers universitaires) et CHR (centres hospitaliers régionaux) se distinguent : 42 % en possèdent un.
Pour les épauler, plusieurs agences de l'État sont chargées de définir les orientations en matière de sécurité des systèmes d'information en santé. Le gros problème, c'est qu'entre les exigences de la DGOS, les préconisations de la Délégation à la stratégie des systèmes d'information de santé (DSSIS) du ministère de la Santé ou les recommandations de l'Agence des systèmes d'information partagés de santé (Asip santé), les hôpitaux se perdent dans un véritable maquis réglementaire. « *Mais si tout le monde appliquait notre mémento de quatre pages, on serait déjà plus en sécurité* », glisse Christophe Jodry, chargé de mission sécurité à l'Asip santé. Venu du secteur bancaire, il réalise un important travail de pédagogie auprès des responsables d'établissements, qui commencent à être moins nombreux à se dire que ça n'arrive qu'aux autres. Aux États-Unis, on n'en est plus là : 90 % des hôpitaux ont été attaqués ces deux dernières années. ◆

Elles sont vaccinées

Contrairement à l'informatique hospitalière, les applications mobiles sont vaccinées contre les attaques. En effet, leurs données ont peu de valeur pour les pirates.

N. ALLIARD/PHOTONONSTOP

ALERTER
ÉTABLISSEMENTS DE SANTÉ

C'est un véritable tsunami : il existe plus de 165 000 applications mobiles liées à la santé ou au bien-être sur les plateformes Apple et Android ! Chaque jour, de nouvelles apparaissent, qui vont du compteur de calories jusqu'au carnet de suivi glycémique, en passant par le calculateur du risque cardio-vasculaire. Mais ces applis arrivent sur les stores (les plateformes de téléchargement) d'Apple et de Google sans contrôle de leur contenu. Face à l'ampleur de la tâche, même l'État a renoncé. La Haute autorité de santé (HAS) a toujours en tête sa tentative ratée de certification (le HONcode) des sites diffusant de l'information de santé, abandonnée en 2013.

Un besoin d'évaluation

Des entreprises ont pris le relais pour répondre aux attentes des médecins et des mutuelles, qui aimeraient connaître les applications qu'ils peuvent recommander sans risque. *« Ces applications doivent répondre à trois défis : la sécurité, le respect de la réglementation et la qualité du contenu médical »*, explique David Sainati, docteur en pharmacie et fondateur de Medappcare. Cette start-up a développé une méthodologie d'évaluation fondée sur 80 critères, dont plusieurs ont trait à la sécurité. L'application envoie-t-elle des données personnelles sur le réseau ? Peut-elle engendrer des pertes financières ? Contient-elle un virus ? *« Nous avons déjà vu une application vérolée à l'insu de son éditeur »*, indique David Sainati. Le rapport envoyé par Medappcare aux éditeurs leur sert à régler les éventuels soucis avant la mise sur le marché de leur produit. *« Il s'agit surtout de problèmes de réglementation (pas de conditions générales d'utilisation, pas d'identité de l'éditeur…) »*, précise-t-il.

Des données sans intérêt financier

Même observation du côté de dmd Santé, qui vient de lancer son label mHealth Quality. *« Il faut réfléchir à la cybersécurité pour demain, mais ce n'est pas le problème numéro 1 aujourd'hui »*, estime Guillaume Marchand, interne de psychiatrie au CHU de Rouen et fondateur de dmd Santé. *« Le risque de vol des données de santé est minime, car elles n'ont pas de valeur »*, poursuit-il. Que ferait un pirate du poids ou des données de jogging de boubou75 ? Guillaume Marchand note que le principal problème est l'absence de mentions légales sur *« 71 % des applications »* et leur manque de suivi de la part des éditeurs. Pour autant, *« le marché avance vite vers la qualité »*, relève-t-il. Avec un bémol : sans modèle économique, les applications rentables sont très rares. Leurs éditeurs ne peuvent donc se permettre de payer une société pour les faire évaluer. Seuls quelques dizaines d'entre eux l'ont fait. ◆

CONSEILS

Choisir une bonne appli

Face à l'offre abondante et de qualité inégale, ayez les bons réflexes !

Optez pour une application labellisée
Medappcare et mHealth Quality garantissent que les applis respectent la réglementation, la déontologie médicale et, surtout, qu'elles sont utiles ! Avant de télécharger une appli non labellisée, lisez les avis des utilisateurs.

Intéressez-vous à l'éditeur
Si l'auteur est un inconnu ou n'a qu'une seule application à son actif, méfiance. À l'inverse, vous pouvez vous fier aux éditeurs reconnus du milieu médical (Elsevier Masson, Vidal, Lavoisier, etc.), les institutions, voire les mutuelles ou les labos pharmaceutiques : leur réputation est vitale et ils ne se risqueront pas à proposer du contenu suspect.

Cherchez la caution médicale
Les éditeurs d'applis mobiles signent fréquemment des partenariats avec des sociétés savantes, des associations de médecins ou de patients, ou encore des établissements de santé qui contrôlent le contenu médical et le respect de la déontologie.

Testez l'ergonomie
Téléchargez plusieurs applis avant de choisir la plus agréable à utiliser. L'objectif est que vous ne l'abandonniez pas au bout de quelques jours !