Entretien avec Pierre-François Regamey, directeur des systèmes d'information du Centre hospitalier universitaire vaudois (CHUV)

«Les cyberattaques peuvent être extrêmement dommageables»

Entretien: Bruno Kesseli

Dr méd. et lic. phil., rédacteur en chef

La numérisation croissante du secteur de la santé augmente le risque de cyberattaques. Directeur des systèmes d'information du Centre hospitalier universitaire vaudois (CHUV), Pierre-François Regamey est presque quotidiennement confronté à des attaques venant d'Internet. L'entretien qui suit a été réalisé en octobre 2017 à l'occasion de l'exposé qu'il a donné sur le sujet à la Chambre médicale.

Vous avez parlé de cybercriminalité dans le secteur hospitalier. Quelle est la gravité du problème dans les hôpitaux suisses?

Il s'agit d'un problème sérieux à l'échelle mondiale, et donc en Suisse aussi. Dans le secteur hospitalier suisse, nous sommes toutefois privilégiés, car nous disposons de bonnes infrastructures techniques. Si l'on compare notre situation à celle des hôpitaux de Grande-Bretagne, par exemple, qui ont été paralysés au printemps 2017 par une cyberattaque au rançongiciel «WannaCry», nous sommes mieux lotis.

Pierre-François Regamey lors de son exposé à la Chambre médicale d'octobre 2017.

Pourquoi cette attaque n'a pas frappé les hôpitaux suisses?

Les systèmes informatiques des hôpitaux britanniques touchés étaient obsolètes et présentaient des failles de sécurité. Pas assez d'argent n'avait été investi dans le renouvellement des systèmes, tout simplement. En Suisse, il y a eu jusqu'ici suffisamment de moyens à disposition pour mettre à jour les systèmes et ainsi singulièrement compliquer la tâche des malfaiteurs.

A quelle fréquence le CHUV, dont vous êtes responsable, est-il exposé à des attaques?

Les cyberattaques se jouent des frontières nationales. Le CHUV est ainsi confronté tous les jours à des attaques visant, par exemple, à introduire des virus dans le système. Pas plus tard qu'hier, une de nos collaboratrices a reçu un courriel avec une pièce jointe, qu'elle n'a heureusement pas ouverte. Cette pièce jointe contenait un virus extrêmement dangereux, qui nous aurait créé d'énormes problèmes. Nous subissons ce genre d'incident quasi quotidiennement.

«Les cyberattaques se jouent des frontières nationales. Le CHUV est ainsi confronté tous les jours à des attaques visant, par exemple, à introduire des virus dans le système.»

Les hôpitaux sont-ils des cibles privilégiées pour les cybercriminels?

En Europe, pour le moment, les cybercriminels ne visent pas particulièrement les hôpitaux. Aux USA, c'est différent, parce qu'il y a beaucoup plus d'hôpitaux privés et que les hackers s'intéressent surtout à deux types de données personnelles: le numéro de sécurité sociale, qui joue un rôle central aux USA en tant qu'identificateur unique d'une personne dans maints domaines, et les numéros de cartes de crédit des «clients de l'hôpital», c'est-à-dire des patients. Aux USA, les hôpitaux sont ainsi régulièrement victimes d'attaques visant à obtenir ces informations.

Portrait

Depuis 2006, Pierre-François Regamey est à la tête de la Direction des systèmes d'information du Centre hospitalier universitaire vaudois (CHUV), un service qui compte 170 personnes. Auparavant, il a été cadre dirigeant dans le département informatique d'une grande compagnie d'assurance ainsi que dans différentes entreprises de conseil en informatique suisses et internationales, pour le compte de clients issus des secteurs de la santé, de l'assurance, des finances et de l'armée.

Pierre-François Regamey est ingénieur diplômé de l'EPFL et possède une vaste expérience en matière de développement de logiciels et d'applications.

En quoi réside la menace pour les hôpitaux européens?

Ici, je la vois surtout dans ce que l'on appelle les «attaques collatérales». La cybercriminalité se distingue par ses structures mafieuses. Le but est d'extorquer le plus d'argent possible: une des attaques les plus courantes est le cryptage des données, les victimes devant ensuite verser une «rançon» pour les récupérer. Ces attaques aux rançongiciels ne visent pas spécialement les hôpitaux. Mais leurs conséquences sont désastreuses dans le secteur hospitalier, car des données hautement sensibles y sont enregistrées, et le traitement des patients peut être fortement compromis lorsque l'accès à ces informations est bloqué pendant un certain temps.

Il paraît qu'aujourd'hui il est plus facile d'empocher beaucoup d'argent en lançant des cyberattaques qu'en dévalisant une banque. Cela s'applique-t-il aussi au secteur hospitalier?

Oui et non. Il est vrai que par le passé beaucoup d'hôpitaux n'étaient pas suffisamment protégés dans le domaine informatique. D'énormes progrès ont cependant été réalisés ces dernières années. Aujourd'hui, les hôpitaux me semblent plutôt bien armés contre les attaques, et ce particulièrement en Suisse. A cet égard, ils n'ont plus grand chose à envier aux banques ou aux assurances.

Est-ce qu'en Suisse des hôpitaux ont déjà été rançonnés?

J'ignore si cela est déjà arrivé en Europe. Ici, comme nous l'avons dit, les attaques aux rançongiciels ne sont pas spécialement dirigées contre les hôpitaux, contrairement à ce qui est le cas aux USA. Le risque est tout de même considérable, car si une cyberattaque réussit, il faut ensuite des heures de travail jusqu'à ce que le système fonctionne de nouveau normalement. Par exemple, si vous devez réduire les activités des urgences ou que vous ne pouvez réaliser aucune opération parce que vous n'avez pas accès aux données requises, c'est la catastrophe.

Comment se passe la récupération des données bloquées après un rançonnement?

Au CHUV, nous sommes bien préparés à ce type de cas, puisque nous faisons une copie de sauvegarde de nos données au moins une fois par heure. Il y a trois ans, nous avons subi une attaque et quelques fichiers administratifs ont été cryptés. Mais nous ne les avons pas perdus. Nous avons pu les récupérer grâce aux copies de sauvegarde dès que le virus a été extirpé du système. De leur côté, les données cliniques sensibles (dossier patient) sont stockées dans des bases de données sécurisées et sont donc à l'abri des rançongiciels courants. Ces multiples niveaux de sécurité sont la clef de la protection contre ce type d'attaques.

Les hôpitaux ont-ils des points faibles spécifiques, profitables aux malfaiteurs?

Malheureusement, les hôpitaux sont très vulnérables, car ils sont très ouverts. Un hôpital est par essence bien plus ouvert qu'une banque ou qu'une caserne. Les banques peuvent établir des normes de sécurité très sévères sans grande difficulté, y compris au niveau de l'informatique. Dans les hôpitaux, cela n'est pas si simple, pour diverses raisons. Ainsi, il faut par exemple que les médecins puissent accéder très rapidement aux données des patients pour leur dispenser les meilleurs soins. Il en va d'ailleurs de même sur le plan physique. Dans les banques privées de Genève, on doit franchir plusieurs sas de sécurité jusqu'à ce que l'on soit «à l'intérieur», alors qu'à l'hôpital, on peut entrer presque partout avec une blouse blanche…

Comment les cybercriminels parviennent-ils à déjouer les systèmes de sécurité des hôpitaux?

La méthode la plus courante consiste à envoyer aux collaborateurs des courriels contenant des liens ou des pièces jointes. Il suffit alors d'un clic pour qu'un logiciel malveillant s'installe. Il existe encore d'autres moyens, par exemple une sorte de «scanner» d'Internet, qui recherche systématiquement les brèches permettant de pénétrer dans les systèmes protégés. Il est possible de s'en prémunir, mais c'est un peu comme dans un immense hôtel: si vous y parcourez les couloirs toute la journée en essayant chaque porte, vous finirez bien par en trouver une qui est ouverte. Alors vous pourrez entrer et voler ce que vous voulez. Des milliers de tentatives de ce type ont lieu chaque jour.

«C'est un peu comme dans un immense hôtel: si vous y parcourez les couloirs toute la journée en essayant chaque porte, vous finirez bien par en trouver une qui est ouverte.»

Peut-on garder toutes les portes fermées?
Nous nous y attelons, en tentant constamment de nous améliorer. Un des moyens que nous utilisons pour y parvenir est d'embaucher des «hackers éthiques». Il s'agit de spécialistes qui, à notre demande, essaient de s'introduire dans nos systèmes. Au début, il y a quinze ans, ils réussissaient plutôt bien à détecter des portes ouvertes. Depuis, nous avons verrouillé nos systèmes, mais nous continuons de réaliser ces tests régulièrement, et avec profit, parce que de nouvelles menaces apparaissent quotidiennement, et parce que nos systèmes évoluent continuellement, ce qui peut créer de nouvelles failles.

La sécurité informatique est surtout l'affaire de spécialistes comme vous. Dans quelle mesure les questions de sécurité concernent également les médecins qui travaillent à l'hôpital?
En fait, les questions techniques dont s'occupent les spécialistes ne sont qu'un aspect. La sensibilisation des collaborateurs s'avère primordiale, particulièrement en cas d'attaques de type ingénierie sociale. Celles-ci consistent notamment à recueillir des données personnelles via les réseaux sociaux et à les utiliser pour s'adresser à des personnes précises de manière crédible.

Comment cela se passe concrètement?
Si vous êtes médecin et que vous recevez un courriel qui vous semble digne de foi, parce qu'il contient des détails vous concernant, mais que le contexte vous paraît étrange, vous devriez entendre la sonnette d'alarme. Par exemple, il n'est pas normal qu'un chef de clinique reçoive une facture de Swisscom à l'hôpital – ce qui est réellement arrivé chez nous. Dans ce cas, il ne faut pas cliquer sur les liens ou les pièces jointes, même par curiosité. L'une des tâches des responsables informatiques est d'établir une culture d'entreprise en la matière.

«La sensibilisation des collaborateurs s'avère primordiale, particulièrement en cas d'attaques de type ingénierie sociale.»

Arrive-t-il souvent au CHUV que des collaborateurs causent des problèmes de sécurité, voire des dommages, par négligence?
Il n'est pas rare que des collaborateurs commettent des erreurs. Après tout, le CHUV compte 12 000 postes de travail informatisés. Le fait que les droits d'administrateur soient octroyés avec une extrême parcimonie permet cependant de limiter les dommages: si dans l'agitation quotidienne un médecin active d'un clic un logiciel malveillant, celui-ci ne peut pas s'installer sur le PC, car ce collaborateur ne dispose pas des droits d'administrateur. Le risque de subir des dommages est en revanche bien plus élevé à la maison, où nous détenons les droits d'administrateur sur notre propre PC.

Est-ce que les collaborateurs du CHUV doivent tous respecter les mêmes normes de sécurité?
Il y a bien quelques différences. Pour les chercheurs, il est capital de travailler en réseau, d'échanger avec des collègues du monde entier, voire d'essayer un nouveau logiciel fourni par un collègue de San Diego ou de Londres. Nous devons leur en donner les moyens – alors que cela n'est pas indispensable pour le personnel soignant, par exemple. C'est pourquoi le CHUV dispose de deux réseaux: le premier, extrêmement sécurisé, pour les données cliniques, et le second, plus ouvert, pour les données des chercheurs. Mais évidemment, cela a un coût.

«Dans le secteur hospitalier tout spécialement, il faudra toujours trouver un compromis entre les solutions techniques et les besoins opérationnels.»

A votre avis, faudrait-il prévoir une formation spéciale en cybercriminalité pour le personnel (médical)?
Absolument – c'est capital. Nous travaillons à l'établissement d'une nouvelle culture de sécurité. Depuis longtemps, nous sensibilisons nos nouveaux collaborateurs par diverses mesures. Au cours des prochains mois, nous les compléterons par des programmes spécifiques à destination de différents groupes de collaborateurs, tels que le personnel infirmier ou le corps médical.

Sera-t-il possible un jour d'immuniser un hôpital contre les cyberattaques?
Dans le secteur hospitalier tout spécialement, il faudra toujours trouver un compromis entre les solutions techniques et les besoins opérationnels. Or cela n'est pas toujours facile de concilier un accès rapide aux données sensibles, indispensables pour les médecins, avec des normes de sécurité élevées. Mais en Suisse, nous sommes les spécialistes du compromis, et donc je suis sûr que nous y arriverons.

Crédits photo:
Portrait mis à disposition par P.-F. Regamey.
Photo exposé Chambre médicale: Tobias Schmid/FMH.

bkesseli[at]emh.ch