Sécurité de l'information avec le *cloud computing*

eHealth actuel

Thomas Kessler

Thomas Kessler a fait des études de physique à l'EPFZ et travaille depuis plus de 25 ans dans le domaine de la sécurité de l'information. Il dirige la société TEMET AG à Zurich.

Le *cloud computing* au cabinet (médical)

Dans le *cloud computing* (ou l'«informatique en nuage»), les applications informatiques ou les données ne sont plus stockées localement chez l'utilisateur, mais de manière centralisée auprès d'un fournisseur *cloud*. Ce déplacement de la technologie de l'information vers le *cloud* a fait depuis longtemps son apparition au cabinet médical et rien ne pourra en arrêter l'évolution. Les différents types d'application se développent toutefois à des rythmes différents:

- *l'échange de données via le cloud* est l'application la plus répandue. A proprement parler, une boîte de courrier électronique externe (p. ex. HIN Mail, bluewin ou gmail) est déjà une solution *cloud* avec davantage (ou moins justement) de sécurité. Malheureusement, des supports de stockage dématérialisés comme Dropbox ou WeTransfer sont également utilisés pour échanger de grandes quantités de données; l'expéditeur enregistre temporairement les données et transmet l'adresse d'accès (lien hypertexte) au destinataire;
- le *stockage illimité de données dans le cloud* est aujourd'hui pratique courante dans l'électronique de consommation, et le système de santé y joue un rôle précurseur (p. ex. *fitness tracker*). Les fabricants d'appareils de laboratoire et d'autres équipements médicaux (p. ex. pour la radiologie) ont également suivi cette tendance et transfèrent les données saisies vers leurs propres mémoires centrales;
- le *traitement des données dans le cloud* via ce qu'on appelle un logiciel service (SaaS) connaît actuellement un essor fulgurant dans différentes branches, dont les cabinets médicaux. La plupart des fabricants proposent aujourd'hui un *logiciel service SaaS* et favorisent les systèmes d'archivage dématérialisés. Ces solutions devraient se généraliser dès que les réserves que suscitent actuellement la sécurité des données et la fiabilité des réseaux auront été dissipées;
- le *cloud desktop,* dans lequel le terminal de l'utilisateur ne sert plus que de moniteur pour le poste de travail mis à disposition par le prestataire *cloud*, serait la forme la plus conséquente du *cloud computing*. Il est cependant encore très difficile d'estimer avec précision si, et quand, cette tendance sera applicable au cabinet médical.

Tableau 1: Dix questions à poser à votre fournisseur de services *cloud* potentiel

1	Mes données sont-elles stockées et traitées exclusivement en Suisse?
2	Le contrat respecte-t-il les exigences légales découlant du secret médical?
3	Comment puis-je supprimer toutes les données d'un patient en conformité avec la loi sur la protection des données?
4	Toutes les personnes ayant accès à mes données sont-elles soumises au devoir de discrétion?
5	Puis-je demander à tout moment une liste de toutes les personnes ayant accès à mes données?
6	Comment la sécurité des données est-elle contrôlée et puis-je consulter à tout moment les rapports de contrôle?
7	Quel est mon interlocuteur pour les questions de sécurité et comment suis-je tenu informé des incidents?
8	Comment mes données sont-elles isolées des données et applications d'autres clients?
9	Comment puis-je recevoir une sauvegarde quotidienne de mes données afin de la reprendre ailleurs?
10	Toutes les liaisons sont-elles cryptées et comment puis-je activer une authentification à deux facteurs?

Risques sécuritaires du *cloud computing*

On distingue trois domaines de risques:

- *Risques sécuritaires liés au fournisseur cloud*: dans la grande majorité des cas d'application, les données ne sont pas codifiées avant leur transfert vers le *cloud*. La confidentialité et l'intégrité des données doivent donc être garanties par le fournisseur *cloud*, et ce à trois niveaux: premièrement, le prestataire *cloud* doit garantir qu'il ne fournit à son personnel que les droits d'accès nécessaires pour leur activité (*need-to-know* ou principe du droit d'accès minimal *least privilege*). Deuxièmement, il doit isoler les applications et les données de ses clients de sorte que les points faibles ou erreurs survenant chez un client n'aient pas de répercussions sur d'autres clients. Et troisièmement, il doit veiller à ce que son infrastructure ne soit pas corrompue par des pirates anonymes sur internet. A cela s'ajoutent certains risques liés à la disponibilité des données, par exemple en cas de

panne du centre de données ou de faillite du fournisseur *cloud*;
- *Risques sécuritaires liés à la connexion réseau:* dans le *cloud computing*, l'utilisateur communique via un réseau public avec le service *cloud*. Si l'authentification des points d'extrémité de la communication n'est pas réciproquement fiable, un tiers peut avoir accès aux données et applications dans le *cloud*. Une liaison de communication non cryptée présente le risque que les données transférées soient lues de façon non perceptible au niveau d'un nœud de réseau intermédiaire;
- *Risques sécuritaires liés à l'utilisateur:* une mauvaise protection des terminaux ou un manque de sensibilisation à la sécurité de la part de l'utilisateur peut également compromettre la sécurité du *cloud computing*. Un logiciel de cryptage malveillant (*ransomware*) au lieu de travail chiffre les données même si elles sont stockées hors site. Et face à un cheval de Troie qui récupère les mots de passe et les enregistre pour un abus ultérieur, les fournisseurs de services *cloud* sont pratiquement impuissants.

Le *cloud computing* n'est pas en soi plus sûr ou moins sûr que l'informatique locale habituelle. En principe, le fournisseur d'un service dématérialisé dispose plutôt de meilleures conditions pour une actualisation permanente de ses serveurs centraux et leur exploitation avec un haut standard en matière de sécurité. La mise en réseau crée cependant des vulnérabilités potentielles supplémentaires qu'il convient de contrôler.

Mais il ne fait aucun doute que la gestion de la sécurité de l'information gagne en complexité compte tenu de l'implication de plusieurs partenaires et de la présence d'interfaces supplémentaires. C'est notamment le cas du risque d'un dommage collatéral lorsque soit le fournisseur du service *cloud* soit tout autre client mal isolé est victime d'une cyberattaque.

Recommandations

Evitez l'utilisation non consciente de services cloud

Renseignez-vous auprès des patients, des hôpitaux ou des autres prestataires avec lesquels vous communiquez sur les systèmes informatiques où vos données sont provisoirement stockées et évitez les mémoires dématérialisées comme Dropbox ou WeTransfer pour échanger des données patients. Clarifiez si vos logiciels de cabinet ou appareils de laboratoire copient des données dans un support *cloud* de manière non sollicitée.

Assurez-vous que les données demeurent en Suisse

Le droit pénal suisse, et notamment le secret professionnel médical selon l'art. 321 CP, ne peut s'appliquer que si les données et toutes les personnes y accédant se trouvent en Suisse. Cette condition ne peut guère être garantie par les fournisseurs de services *cloud* étrangers.

Choisissez votre fournisseur de services cloud avec soin

En tant qu'utilisateur d'un service dématérialisé, vous restez responsable de la sécurité de vos données même si vous n'avez aucune influence directe sur les mesures de sécurité prises par le fournisseur. Ceci est à prendre en compte de manière appropriée dans le cadre contractuel et requiert un degré élevé de confiance. Posez à tout fournisseur potentiel les 10 questions énumérées dans le tableau 1 avant d'opter pour son offre.

Conservez une copie de vos données comme sauvegarde (backup)

Si le *cloud* n'est utilisé que pour l'échange de données, vous pouvez ainsi en cas de problème récupérer les données originales. Dans tous les autres cas d'application, une erreur du fournisseur de services *cloud* peut entraîner un dysfonctionnement durable de votre cabinet. C'est pourquoi il est essentiel que vous conserviez une copie de vos données localement ou auprès d'un second fournisseur *cloud*, ce qui vous permettra d'y accéder en cas de problèmes.

Activez l'authentification forte pour accéder aux services cloud

Les mots de passe n'offrent pas de protection suffisante contre les cyberattaques lorsqu'il s'agit d'accéder à des données patients. Pour cette raison, exigez de votre fournisseur de services *cloud* qu'il mette à votre disposition une authentification à deux facteurs facile à utiliser.

N'utilisez que des liaisons de communication cryptées

Veillez à ce que toutes les liaisons de communication entre vos terminaux et le service *cloud* soient cryptées. Cela concerne également la communication poste à poste des appareils de laboratoire et d'autres équipements médicaux.

Sécurisez vos postes de travail

Même la solution *cloud* la plus sûre est impuissante face à un logiciel malveillant installé sur le poste de travail de l'utilisateur. Il est et reste primordial que vous configuriez et actualisiez vous-mêmes vos appareils locaux.

Correspondance:
Thomas Kessler
Associé et directeur
TEMET AG
Basteiplatz 5
CH-8001 Zurich
Tél. +41 79 508 25 43
thomas.kessler[at]temet.ch