Informationssicherheit beim Cloud Computing

eHealth Aktuell

Thomas Kessler

Thomas Kessler studierte Physik an der ETH Zürich und ist seit mehr als 25 Jahren in der Informationssicherheit tätig. Er ist Geschäftsführer der TEMET AG in Zürich.

Cloud Computing in der (Arzt-)Praxis

Beim *Cloud Computing* (oder «Rechnen in der Wolke») befinden sich Informatikanwendungen oder Daten nicht mehr lokal beim Anwender, sondern zentral bei einem Cloud-Service-Anbieter. Diese Verschiebung der IT in die Cloud hat auch in der Arztpraxis längst begonnen und lässt sich nicht aufhalten. Das Tempo ist aber für die verschiedenen Anwendungsfälle unterschiedlich:

- Am weitesten verbreitet ist der *Datenaustausch über die Cloud*. Streng genommen handelt es sich bei einem externen E-Mail-Postfach (z.B. HIN Mail, bluewin oder gmail) bereits um eine Cloud-Lösung mit mehr (oder eben weniger) Sicherheit. Leider werden auch Cloud-Speicher wie Dropbox oder WeTransfer für den Austausch von grossen Datenmengen verwendet, indem der Absender die Daten zwischenspeichert und dem Empfänger die Adresse für den Zugriff (Hyperlink) zustellt.
- Die zeitlich unbefristete *Datenablage in der Cloud* ist heute in der Konsumelektronik gang und gäbe, wobei gerade das Gesundheitswesen (z.B. Fitness-Tracker) hierbei eine Vorreiterrolle spielt. Auch Hersteller von Laborgeräten und anderen Medizinalgeräten (z.B. für Radiologie) haben diesen Trend aufgenommen und transferieren erfasste Daten auf eigene zentrale Speicher.
- Die *Datenverarbeitung in der Cloud* über sogenannte Software as a Service (SaaS) Lösungen erlebt derzeit in verschiedenen Branchen einen rasanten Aufschwung, der auch Arztpraxen erfasst hat. Die meisten Hersteller führen heute eine *Praxissoftware as a Service* im Angebot und forcieren Cloud-basierte Archivierungssysteme. Diese Lösungen dürften sich flächendeckend durchsetzen, sobald noch bestehende Vorbehalte bezüglich Datensicherheit und Netzwerkzuverlässigkeit ausgeräumt sind.
- Der *Cloud Desktop*, bei dem das Endgerät des Anwenders nur noch als Bildschirm für den beim Cloud- Anbieter betriebenen Arbeitsplatz dient, wäre die wohl konsequenteste Form des Cloud Computing. Ob und wann dies auch für eine Arztpraxis praktikabel wird, lässt sich derzeit allerdings kaum abschätzen.

Tabelle 1: Zehn Fragen an Ihre potentiellen Cloud Service Provider

1	Werden meine Daten ausschliesslich innerhalb der Schweiz gespeichert und verarbeitet?
2	Genügt die Vertragsgestaltung den rechtlichen Anforderungen aus dem Arztgeheimnis?
3	Wie kann ich sämtliche Daten eines einzelnen Patienten konform zum Datenschutzgesetz löschen?
4	Unterstehen alle Personen mit Zugriff auf meine Daten der ärztlichen Schweigepflicht?
5	Kann ich jederzeit eine Liste aller Personen einfordern, die Zugriff auf meine Daten haben?
6	Wie wird die Datensicherheit überprüft und kann ich die Prüfberichte jederzeit einsehen?
7	Wer ist mein Ansprechpartner für Sicherheitsfragen und wie werde ich über Vorfälle informiert?
8	Wie sind meine Daten von den Daten und Anwendungen anderer Kunden isoliert?
9	Wie erhalte ich ein tägliches Backup meiner Daten, das ich auch andernorts einspielen kann?
10	Sind alle Verbindungen verschlüsselt und wie aktiviere ich eine 2-Faktor-Authentifizierung?

Sicherheitsrisiken beim Cloud Computing

Grundsätzlich lassen sich drei Risikobereiche unterscheiden:

- *Sicherheitsrisiken beim Cloud-Service-Anbieter:* In den allermeisten Anwendungsfällen werden die Daten nicht vor dem Transfer in die Cloud verschlüsselt. Vertraulichkeit und Integrität der Daten müssen deshalb vom Cloud-Service-Anbieter sichergestellt werden, und zwar auf drei Ebenen: Erstens muss der Cloud-Service-Anbieter sicherstellen, dass seine Mitarbeitenden nur die für ihre Tätigkeit notwendigen Zugriffsrechte erhalten (*need-to-know* oder *least-privilege* Prinzip). Zweitens muss er die Anwendungen und Datenbestände seiner Kunden so voneinander isolieren, dass sich Schwachstellen oder Fehler beim einen Kunden nicht auf andere Kunden auswirken können. Und drittens muss er dafür sorgen, dass seine Infrastruktur nicht von anonymen Angreifern aus dem Internet korrumpiert wird. Hinzu kommen gewisse Risiken in Bezug auf die Verfügbarkeit der Daten beispielsweise bei ei-

nem Ausfall des Rechenzentrums oder einem Konkurs des Cloud-Service-Anbieters.
- *Sicherheitsrisiken bei der Netzwerkverbindung:* Beim Cloud Computing kommuniziert der Anwender über ein öffentliches Netzwerk mit dem Cloud Service. Wenn sich die Endpunkte der Kommunikation nicht gegenseitig zuverlässig authentifizieren, dann kann sich ein Dritter den Zugang auf die Daten und Anwendungen in der Cloud verschaffen. Bei einer unverschlüsselten Kommunikationsverbindung besteht zusätzlich das Risiko, dass die transferierten Daten auf einem dazwischenliegenden Netzwerkknoten unbemerkt mitgelesen werden.
- *Sicherheitsrisiken beim Anwender:* Mangelhaft geschützte Endgeräte oder fehlendes Sicherheitsbewusstsein beim Anwender können auch die Sicherheit des Cloud Computing beeinträchtigen: Eine schädliche Verschlüsselungssoftware (Ransomware) auf dem Arbeitsplatz verschlüsselt die Daten auch dann, wenn sie auf einem Cloud-Speicher abgelegt sind. Und auch gegen ein trojanisches Pferd, das Passwörter mitliest und für den späteren Missbrauch abspeichert, sind die Betreiber von Cloud Services weitgehend machtlos.

Cloud Computing ist nicht *per se* sicherer oder weniger sicher als die herkömmliche lokal betriebene Informatik. Grundsätzlich hat der Betreiber eines Cloud Service eher bessere Voraussetzungen dafür, seine zentralen Systeme laufend zu aktualisieren und nach einem hohen Sicherheitsstandard zu betreiben. Die Vernetzung schafft aber zusätzliche potentielle Sicherheitsschwachstellen, die kontrolliert werden müssen.

Das Management der Informationssicherheit wird aber auf jeden Fall anspruchsvoller, weil mehrere Parteien involviert sind und zusätzliche Schnittstellen bestehen. Dies trifft insbesondere auf das Risiko eines Kollateralschadens zu, wenn entweder der Betreiber des Cloud Service oder ein mangelhaft isolierter anderer Kunde Opfer eines Angriffs wird.

Handlungsempfehlungen

Vermeiden Sie die unbewusste Nutzung von Cloud Services

Klären Sie bei der Kommunikation mit Patientinnen, Spitälern oder anderen Leistungserbringern, auf welchen IT-Systemen Ihre Daten zwischengespeichert werden, und meiden Sie öffentliche Cloud- Speicher wie Dropbox oder WeTransfer für den Austausch von Patientendaten. Informieren Sie sich darüber, ob Ihre Praxissoftware oder Laborgeräte Daten ungefragt in einen Cloud-Speicher kopieren.

Stellen Sie sicher, dass die Daten in der Schweiz verbleiben

Das Schweizer Strafrecht und insbesondere das ärztliche Berufsgeheimnis nach Art. 321 StGB kann nur durchgesetzt werden, wenn sich die Daten und alle auf die Daten zugreifenden Personen in der Schweiz befinden. Dies kann bei ausländischen Anbietern von Cloud Services kaum sichergestellt werden.

Wählen Sie Ihre Cloud-Service-Provider sorgfältig aus

Als Anwender eines Cloud Service bleiben Sie für die Sicherheit Ihrer Daten verantwortlich, auch wenn Sie keinen direkten Einfluss auf die vom Anbieter getroffenen Sicherheitsmassnahmen haben. Dies ist beim Vertragswerk angemessen zu berücksichtigen und erfordert ein hohes Mass an Vertrauen. Stellen Sie jedem potentiellen Anbieter die in der Tabelle 1 aufgelisteten 10 Fragen, bevor Sie sich für sein Angebot entscheiden.

Halten Sie eine Kopie Ihrer Daten als Backup

Wird die Cloud nur für den Datenaustausch verwendet, dann können Sie im Fehlerfall wieder auf das Original zurückgreifen. Bei allen anderen Anwendungsfällen kann ein Fehler beim Cloud-Service-Anbieter dazu führen, dass Ihr Praxisbetrieb nachhaltig beeinträchtigt wird. Es ist deshalb essentiell wichtig, dass Sie lokal bei sich oder bei einem zweiten Cloud Service eine Kopie Ihrer Daten aufbewahren, auf die Sie nötigenfalls zurückgreifen können.

Aktivieren Sie die starke Authentifizierung beim Zugriff auf Cloud Services

Passwörter bieten keinen ausreichenden Schutz gegen Angriffe aus dem Internet, wenn es um den Zugriff auf Patientendaten geht. Verlangen Sie deshalb von Ihrem Cloud-Service- Anbieter, dass er Ihnen eine sichere und benutzerfreundliche 2-Faktor-Authentisierungslösung zur Verfügung stellt.

Nutzen Sie nur verschlüsselte Kommunikationsverbindungen

Achten Sie darauf, dass alle Kommunikationsverbindungen zwischen Ihren Endgeräten und dem Cloud Service verschlüsselt sind. Dies betrifft auch die Maschine-zu-Maschine-Kommunikation von Laborgeräten und anderen medizinischen Einrichtungen.

Sichern Sie Ihre Arbeitsplätze

Auch die sicherste Cloud-Lösung kann wenig gegen eine auf dem Arbeitsplatz des Benutzers installierte Schadsoftware ausrichten. Es ist und bleibt deshalb wichtig, dass Sie Ihre lokalen Geräte sicher konfigurieren und stets auf dem aktuellen Stand halten.

Korrespodenz:
Thomas Kessler
Partner und Geschäftsführer
TEMET AG
Basteiplatz 5
CH-8001 Zürich
Tel: +41 79 508 25 43
thomas.kessler[at]temet.ch