Nutzung von Cloud-Diensten nicht auf die leichte Schulter nehmen

Vertrauliche Patientendaten richtig schützen

Für vertrauliche Patientendaten ist ein hohes Schutzniveau unerlässlich, besonders wenn ein Krankenhaus Cloud-Dienste nutzt. Die Sicherheit muss dabei an erster Stelle stehen, die Realität sieht allerdings vielfach anders aus. Oft werden schon grundlegende Aspekte wie starke Authentifizierung oder Verschlüsselung nicht adäquat berücksichtigt.

Die Cloud liegt im Trend und auch öffentliche Institutionen können sich diesem mittel- und langfristig nicht entziehen. Gleiches gilt für Krankenhäuser. Sie nutzen überdies oft schon Cloud-Dienste – offiziell oder inoffiziell. Verbreitet ist etwa der Einsatz von CRM-Systemen, Microsoft Office 365 oder Dropbox. Teilweise haben Krankenhäuser sogar ihre interne IT-Infrastruktur in die Cloud verlagert – Stichwort Infrastructure-as-a-Service.

Sicherheit oder Trugschluss?

Aber auch wenn ein Spital offiziell auf eine strikte «No-Cloud-Policy» setzt, ist das oft nur die halbe Wahrheit. In der Tat verfolgen etliche Krankenhäuser aus Sicherheitsbedenken eine solche Strategie. Dass sie damit auf der «sicheren» Seite sind, ist allerdings meistens ein Trugschluss, denn was nützt ein organisatorisches Verbot, wenn es keine Möglichkeit zur Überwachung, Durchsetzung und Kontrolle dieser Richtlinie gibt und die Nutzer daher unbemerkt auf nicht autorisierte Cloud-Dienste zugreifen können? So baut sich in der Regel eine Schatten-IT durch Nutzung unautorisierter Cloud-Dienste im Unternehmen auf. Diese lässt sich mittels eines Shadow-IT-Assessments belegen. Deshalb sollten Organisationen auf jeden Fall eine Strategie zur Kontrolle der Cloud-Nutzung verfolgen.

Für vertrauliche Patientendaten ist ein hohes Schutzniveau unerlässlich, besonders wenn ein Krankenhaus Cloud-Dienste nutzt.

Dass die unkontrollierte Cloud-Nutzung in Kliniken ein enormes Sicherheitsrisiko darstellt, dürfte ausser Frage stehen. Hinsichtlich der Mittel und Möglichkeiten, die Sicherheitsrisiken in den Griff zu bekommen, bestehen allerdings häufig noch Unklarheiten beziehungsweise falsche Einschätzungen.

Klare Vorgaben für den Cloud-Service-Provider

Wenn vertrauliche Daten in der Cloud gespeichert werden, muss das auslagernde Krankenhaus dem Cloud-Service-Provider klare Vorgaben machen und auf die Einhaltung elementarer Sicherheitsmassnahmen achten. Dazu gehören Regelungen hinsichtlich Datenhoheit und Speicherort der Daten sowie Massnahmen wie Datenverschlüsselung, Multifaktor-Authentifizierung oder Schutz privilegierter Konten. Bei der Nutzung von Cloud-Services ist die Überwachung von Datenzugriffen gerade auch im Hinblick auf privilegierte Benutzerkonten mit erweiterten Rechten, wie sie etwa Administratoren besitzen, von hoher Bedeutung. Der Grund: Auch bei der Auslagerung von Daten an einen externen Provider bleiben die Anforderungen an das Risikomanagement für den Outsourcer bestehen.

Vor allem aber die Themen Authentifizierung und Verschlüsselung sind von essenzieller Bedeutung und sollten genau auf den Prüfstand gestellt werden. Zugriffsrechte müssen klar geregelt sein und adäquate Authentifizierungsverfahren genutzt werden. Angesichts der sensiblen Daten ist dabei eine einfache Authentifizierung beispielsweise mit einem Passwort nicht ausreichend. Es empfiehlt sich auf jeden Fall zumindest eine Zweifaktor-Authentifizierung, etwa mittels eines Passwortes und eines Hardware- oder Software-Tokens.

Eindeutige Authentifizierung

Ebenso wichtig wie die sichere Authentifizierung ist die Datenverschlüsselung. Mit Datenverschlüsselung argumentiert nahezu jeder Anbieter von Cloud-Diensten. Das jeweils genutzte «Verschlüsselungsverfahren» ist allerdings kritisch zu hinterfragen. In der Regel handelt es sich dabei um eine reine «Offline»-Verschlüsselung, die letztendlich nur einen Diebstahlschutz bietet, das heisst, wenn gespeicherte Daten abhandenkommen, bleiben sie verschlüsselt geschützt. Bei der Bearbeitung sind die Daten allerdings entschlüsselt und damit ungesichert. Lösungen für die Verschlüsselung von Daten auch bei der Bearbeitung sind aber heute verfügbar und ihr Einsatz sollte durchaus in Betracht gezogen werden.

Eine zusätzliche Sicherheitsstufe bietet noch die Pseudonymisierung der in der Cloud abgelegten Daten. Sie ist allerdings mit einem erheblichen technischen Aufwand und hohen Kosten verbunden und bringt auch Funktionseinschränkungen mit sich: etwa hinsichtlich der Suchfunktion. Deshalb ist die Nutzung solcher Sicherheitslösungen heute noch eher die Ausnahme.

Den Datenabfluss nicht unterschätzen

Ein weiterer Punkt, der bei einer Cloud-Nutzung in aller Regel zu kurz kommt, ist der potenzielle Datenabfluss. Hacker verfolgen beim Angriff mit Malware häufig das Ziel, Patientendaten zu stehlen. Mögliche Schäden sind die Verletzung von Persönlichkeitsrechten, Imageschäden und Schadenersatzforderungen. Ein unerwünschter Datenabfluss muss deshalb zuverlässig verhindert werden. Das wird gewährleistet durch beispielsweise das Management der Zugriffsrechte nach dem Need-to-Know-Prinzip, die Überwachung der Datenübertragung von und zur Cloud mittels DLP (Data Loss Prevention) sowie den Schutz der Daten selbst durch DRM-Technologien (Digital Rights Management). Ganz allgemein gilt: Bei der Nutzung von Cloud-Services muss ein Krankenhaus auf jeden Fall die Sicherheitsrichtlinien des Service-Providers überprüfen. Ist dies aus Ressourcen- oder inhaltlichen Gründen nicht möglich, sollte ein externer Dienstleister mit ausgewiesener Cloud-Kompetenz hinzugezogen werden.

Führungsrolle wahrnehmen

Nicht zuletzt darf eines auf keinen Fall übersehen werden: Wenn die Krankenhaus-IT versäumt, die Führungsrolle bei Cloud-Initiativen zu übernehmen, findet die Migration in die Cloud trotzdem statt – aber ungeplant und unsystematisch. Dadurch entsteht eine Schatten-IT innerhalb der Organisation, die erhebliche Sicherheitsgefahren nach sich zieht. Besser heute als morgen sollte folglich auch das Thema Cloud auf der IT-Agenda von Krankenhäusern stehen.

Autor: Sven Gerlach, Senior Manager ESA & Infrastructure NTT Security