Cloudlösungen: Freund oder Feind?

Digitalisierung

Cloud-Speicherlösungen können Aufwand und Kosten für die IT verringern. Doch wie schneiden sie ab in puncto Datenschutz und -sicherheit? Worauf müssen Gesundheitsfachpersonen achten, damit sensible Daten auch in der Cloud genügend geschützt sind?

Lucas Schult

Speichern auch Sie Ihre persönlichen Dokumente bei Google Drive, OneDrive, Dropbox, iCloud oder einer ähnlichen Cloud-Speicherlösung? Ja, diese Möglichkeit der Datenablage hat einige Vorteile. So ist beispielsweise der
Zugriff auf die Informationen standort- und geräteunabhängig möglich, es wird keine zusätzliche Hardware benötigt und das manuelle Erstellen von Backups entfällt. Dass sich Cloudlösungen auch im beruflichen Umfeld immer mehr durchsetzen, erstaunt also wenig.

Gesundheitsdaten in der Cloud?

Gemäss Datenschutzgesetz gelten Gesundheitsdaten als besonders schützenswert, das brauche ich Ihnen als Gesundheitsfachperson nicht zu erklären. Entsprechend müssen diese Daten sorgfältig vor Missbrauch und vor Zugriffen Dritter geschützt werden – das gilt auch, wenn sie in einer Cloud gespeichert oder mittels einer solchen ausgetauscht werden. Dies ist keinesfalls schlecht oder verboten. Es ist jedoch unabdingbar, dass Sie mögliche Cloudlösungen vor deren Nutzung sorgfältig prüfen und sich mit den Risiken auseinandersetzen. Denn: Wer wenig Verantwortung hat – ein Vorteil der Cloud – hat leider oft auch wenig Kontrolle. Laden Sie Daten in eine Cloud, können Sie schwer kontrollieren, was danach damit passiert: Wo werden sie gespeichert? Wer kann sie einsehen und allenfalls gar bearbeiten?

Datenschutz und -sicherheit gewährleisten

Grundsätzlich müssen Sie bei der Speicherung sensibler Daten drei Punkte einhalten: Die Daten müssen sicher sein vor Diebstahl, unbefugter Bearbeitung und Datenlecks; sie müssen geschützt sein vor unberechtigten Zugriffen und Cyberattacken; und die Einhaltung gesetzlicher und regulatorischer Vorgaben muss gewährleistet sein. Dies müssen Cloudlösungen im Gesundheitswesen also garantieren können. Entsprechend gibt es eine Vielzahl an Kriterien, die Sie bei der Evaluation eines geeigneten Cloudanbieters überprüfen sollten. Einige Beispiele: Der Anbieter sollte eine gute Web Application Firewall einsetzen, regelmässig Backups durchführen und über ein durchdachtes und mit entsprechenden Restriktionen versehenes Accessmanagement verfügen.

Auf Zertifizierungen achten

Einen ganzen Katalog an Kriterien für verschiedene Anbieter zu prüfen und zu vergleichen, gestaltet sich komplex und aufwendig. Um sich einen Überblick über die Qualität und Seriosität eines Anbieters zu verschaffen, sind meiner Meinung nach dessen Zertifizierungen aufschlussreich. Informieren Sie sich, ob die Sicherheitsrichtlinien und -verfahren des Anbieters auf allgemein anerkannten Sicherheitsstandards wie dem ISO 27001 oder dem NIST (National Institute of Standards and Technology) basieren. Ist dies der Fall, ist bereits ein guter Sicherheitsstandard garantiert. Des Weiteren empfehle ich, beim Anbieter nachzufragen, ob er die Anforderungen des Datenschutzgesetzes (DSG), die Ausführungsbestimmungen in der Datenschutzverordnung (DSV) und die Schweizerische Datenschutz-Grundverordnung (DSGVO beziehungsweise GDPR) berücksichtigt.

Andere Länder, andere Sitten

Nicht in allen Ländern wird Datenschutz und -sicherheit ein so hoher Stellenwert beigemessen wie in der Schweiz. In den USA beispielsweise ist es durch den Patriot Act und das Gesetz FISA (Foreign Intelligence Survaillance Act) schwierig, einen Datenschutz nach europäischen Vorgaben sicherzustellen. Firmen – und somit auch Anbieter von Cloudlösungen – unterliegen jeweils der Rechtslage des Landes, in der sie ihren Firmensitz haben. Möchten Sie sich also nicht im Detail mit den Datenschutzvorgaben anderer Länder auseinandersetzen, empfehle ich Ihnen eine Cloudlösung eines Schweizer Anbieters zu nutzen, bei der Ihre Daten zudem jederzeit in der Schweiz bleiben.

Sorgfalt walten lassen

Wie oft bei den Themen Datenschutz und -sicherheit gilt also auch bei Cloudlösungen: Sorgfalt ist das A und O. Gratislösungen nutzen und vorher nicht prüfen, was mit den hochgeladenen Daten passiert, ist definitiv keine gute Idee. Seien Sie sich der Sensibilität von Gesundheitsdaten jederzeit bewusst und wählen Sie Ihre Cloudlösung entsprechend sorgfältig. Fühlen Sie sich unsicher, kann eine IT-Fachperson unterstützen.

Lucas Schult
Lucas Schult ist Geschäftsführer (CEO) von HIN. Er schreibt an dieser Stelle regelmässig über digitale Sicherheit.

Literatur