

E-Health, aber sicher!

Das Gesundheitswesen ist auf die Kommunikation und den Datenaustausch über das Internet angewiesen. Dies bedingt sichere Verbindungen, sichere Serverumgebungen und sichere Software. Das stellt IT-Organisationen vor neue Herausforderungen, insbesondere in den Bereichen der Sicherheit und des Betriebs. Kaspar Geiser

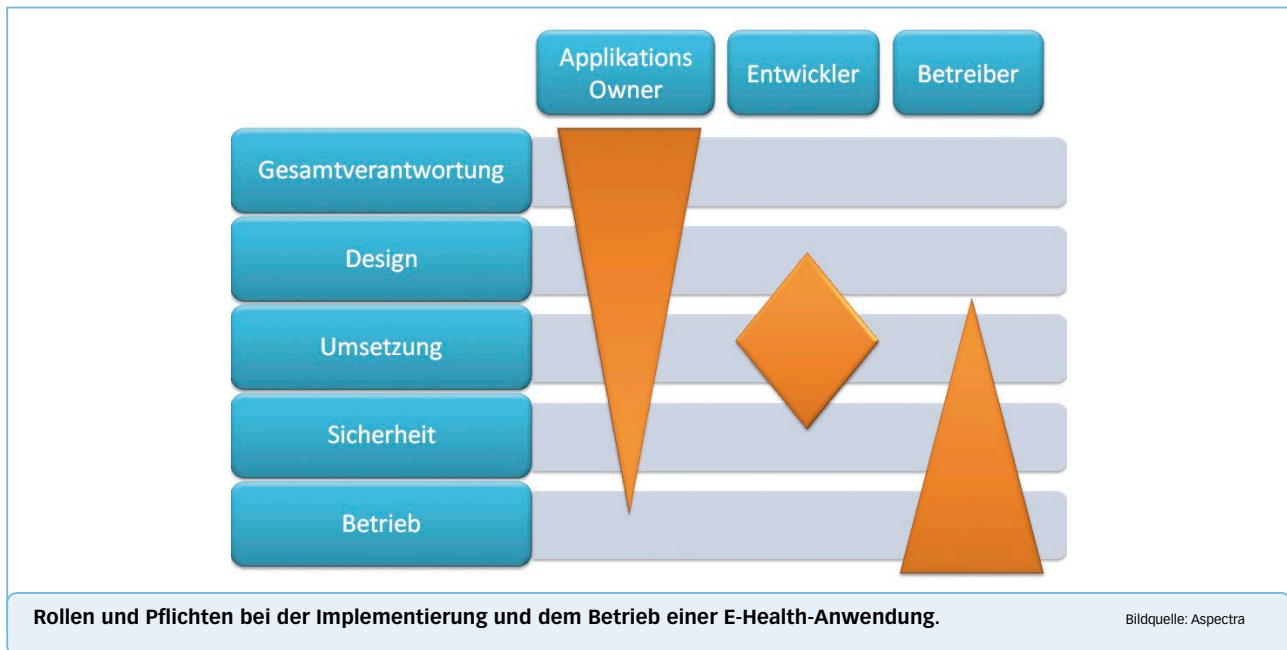


Kaspar Geiser
ist Geschäftsführer und
Mitinhaber der Aspectra AG.
kaspar.geiser@aspectra.ch

Vor den technischen Aspekten müssen die konzeptionellen geklärt werden: Im Zentrum steht dabei die Frage, welche Dienstleistungen und Daten überhaupt online angeboten beziehungsweise ausgetauscht werden sollen. Dann ist zu klären, wie der Austausch der Daten ablaufen soll. Beispielsweise können Daten bereits vor einer Übermittlung an eine andere Stelle anonymisiert werden. Oder aber die Daten werden zuerst zentralisiert und dann anonymisiert. Auch muss die Frage des Supports, also des Helpdesks für E-Health-Anwendungen, vor und nicht während oder sogar nach der Umsetzung eines solchen Projektes bestimmt werden. All diese Fragen sind konzeptioneller Natur und müssen vor der Umsetzung eines E-Health-Projektes geklärt und definiert werden.

Entwicklung und Betrieb sind zwei paar Schuhe

Ausgehend von den definierten Zielen müssen die nötigen Voraussetzungen für die «technische» Umsetzung geschaffen werden. Dies stellt bereits erste technische Anforderungen. Welche Core-Systeme des Unternehmens sind für die Erbringung der E-Health-Funktionen nötig? Was sind die Betriebszeiten dieser Systeme? Wie sicher sind diese Systeme? Wer betreut diese Systeme? Wie verläuft der Informationsfluss zwischen Leistungsnehmer, Leistungserbringer und den Core-Systemen? Welche zusätzlichen Systeme sind zum Betrieb einer E-Health-Anwendung nötig? Welche Risiken bestehen, wenn Teile einer Anwendung online zur Verfügung stehen? Die Entwicklung und der Betrieb von E-Health-Anwendungen sind zwei paar Schuhe. Stehen während der Entwicklung Themen wie Funktionen, Layout und Testing im Vordergrund, sind Fragen wie Verfügbarkeit, Sicherheit und Performance Sache des Operatings. Insbesondere die Frage nach möglichen Sicherheitsmechaniken sollte keinesfalls «nur» von der Entwicklung gestellt und be-



antwortet werden, sondern auch nach der Umsetzung – und dies permanent. Unter diesem Aspekt ergibt es Sinn, dass sicherheitsrelevante Elemente einer E-Health-Anwendung vom Betreiber realisiert und betreut werden.

Die Schulung ist nicht zu vernachlässigen

In der Verantwortung der Entwicklung steht somit die Umsetzung der gewünschten Funktionen. Die diesen Funktionen zugrundeliegenden Prozesse müssen von den Entwicklern verstanden und gemäß dem Geschäftsmodell umgesetzt werden. Diktiert die Technik dem Geschäft Prozesse und Vorgehensweisen, wird es schwierig, die nötige Akzeptanz für E-Health-Anwendungen innerhalb einer Organisation zu finden. Auch die Schulung aller involvierten Stellen muss innerhalb der Entwicklung stattfinden. So ist es der realisierenden Partei möglich, auf Wünsche und Fragen einzugehen und die Abläufe noch besser zu verstehen. Dies sollte mit jeder neuen Version einer E-Health-Anwendung wiederholt werden. Der Entwicklungsprozess verlangt somit nach sowohl technisch versierten wie auch beratenden und didaktisch fähigen Mitarbeitern. Eine optimale Usability erfordert zudem die Mitarbeit kreativer Köpfe in der Entwicklung, damit die gestellten Anforderungen sowohl ergonomisch sinnvoll, als auch in ansprechendem Design realisiert werden.

Hohe Anforderungen an den Betrieb

Wie bereits erwähnt, ist es sinnvoll, neben dem reinen Betrieb einer E-Health-Anwendung auch die sicherheitsrelevanten Aufgaben ein und derselben Partei zuzuordnen. An dieser Stelle daher eine kurze Umschreibung, was zu sicherheitsrelevanten Aufgaben und Komponenten gezählt wird. An erster Stelle stehen sicherlich die Firewalls und die Verbindungen zum Core-System. Diese müssen aktiv betreut werden und dies permanent, also auch ausserhalb der Öffnungs- und Betriebszeiten zum Beispiel eines Leistungserbringers. Als Nächstes müssen die Systeme und Stan-

dardapplikationen aktiv überwacht und im Bedarfsfall mit den nötigen Updates versehen werden. Dazu zählen das Betriebssystem, die Datenbank sowie die unter Umständen vom Entwickler eingesetzten Applikationsserver. E-Health-Anwendungen verfügen über sogenannte starke Authentifizierungsmechanismen. Dies sind neben Benutzername und Passwort Streichlisten, Zertifikate oder dynamische Einweg-Passwörter. Auch diese Komponenten muss der Betreiber zur Verfügung stellen. Diese Pflichten stellen hohe Anforderungen an das Betriebspersonal und an die eingesetzten technischen Systeme, die die Schutz- und Sicherheitsfunktionen übernehmen. Insbesondere kleinere, aber auch mittlere Unternehmen verfügen in der Regel nicht über das Personal für den sicheren Betrieb einer E-Health-Applikation. Aus dieser Überlegung heraus kann es somit sinnvoll sein, dass der Betrieb von E-Health-Anwendungen Dritten übergeben wird.

Gesamtverantwortung kann nicht ausgelagert werden

Unternehmen, die eine E-Health-Anwendung umsetzen, müssen sich bewusst sein, dass zwar Dritte eine Applikation entwickeln und betreiben können, dass aber die Gesamtverantwortung bei ihnen bleibt. Das bedeutet, dass sie auch nach der erfolgreichen Umsetzung mit geeigneten Massnahmen sicherstellen müssen, dass die Weiterentwicklung möglich und die betriebliche Sicherheit gewährleistet ist. Dazu zählen das Rapportieren von Fehlern, die akribische Dokumentation aller Änderungs- und Erweiterungswünsche sowie die periodische Überprüfung aller Funktionen und der Sicherheitsinfrastruktur. Management-Cockpits, die sowohl über den Systemzustand informieren als auch Dokumentation und Ticketingsystem beinhalten, können hier alle involvierten Parteien in ihrer täglichen Arbeit unterstützen. Was die Sicherheitsüberprüfung betrifft, ist es sinnvoll, dies wiederum Dritten, in die Umsetzung nicht involvierten Parteien zu übergeben. Diese Aufgabe soll auch von internen und externen Auditoren begleitet werden. ■