Fotoa: sports up, Wiesbaden

Digitalisierung im Fitnessstudio

Teil 2: Datensicherheit

Überblick über die 5-teilige Serie

Teil 1: Netzwerksystem: Businessmodelle

Teil 3: EDV-basierte Mitgliederverwaltung

Teil 4: Softwaregestützte Anamnese und Zielkontrolle

Teil 5: Onlinemarketing

Datensicherheit und Datenschutz sind spätestens seit der NSA-Affäre Themen, die viele Menschen beschäftigen. Nicht nur der politisch interessierte Bürger, sondern auch unsere Mitglieder möchten wissen, wie mit ihren persönlichen Daten umgegangen wird und wie diese geschützt werden. Sie verlassen sich darauf, dass ihre Daten nicht unzulässig weitergegeben werden.

Die Annahme, dass ein Datenmissbrauch beim Verlust der eigenen Mitglieds- bzw. Transponderkarte entstehen kann, ist nicht gegeben

Foto: Lena Pary/shutterstock.com

Die Mitglieder schenken uns in erster Linie nicht nur das Vertrauen im Umgang mit ihrer Gesundheit, sondern vertrauen uns auch, was die sichere Aufbewahrung ihrer persönlichen Daten, wie zum Beispiel Anamnese, Trainingsergebnisse und auch Bankdaten, angeht. Diese persönlichen Datensätze sind für viele dritte Unternehmen bares Geld wert, sodass die Weitergabe dieser vertraulichen Informationen sehr lukrativ ist.

In der Vergangenheit hatte ein Ortstracking von Apple für negative Schlagzeilen gesorgt. Wie groß wäre erst der Skandal, wenn Gesundheitsanbieter nicht nur Standortdaten, sondern die persönlichen Daten eines Menschen, seine Gesundheitsdaten, verarbeiten und weitergeben würden? Dieser Skandal würde ein jahrelang aufgebautes Vertrauen zwischen dem Mitglied und dem Gesundheitsanbieter, also der Fitness- und Gesundheitsanlage, zerstören.

Datenschutz und Datensicherheit in Fitnessstudios

In erster Instanz sind Fitnessstudios Dienstleister, die zur Ausübung ihres Angebots Bestandsdaten erheben müssen, wie z.B. Name, Vorname, Geburtsdatum und Geschlecht. Die Verwaltungssoftwares benötigen diese Daten, um überhaupt ein Datensatz anlegen zu können. Sekundäre Daten wie Adresse, Telefonnummer und E-Mail-Adresse müssen nicht, können aber abgespeichert werden, sind aber für die weitere Kontaktaufnahme unerlässlich. Für die Trainingsplanerstellung benötigt der Trainer, der im Auftrag des Fitnessstudios handelt, Gesundheitsdaten, die im Anamnesebogen abgespeichert werden. Das sind meist hochsensible Daten zu Krankheiten, Gewicht, BMI, Blutdruck, Medikamenten, Bewegungs- und Konsumverhalten, Beruf, Hobbys, Freizeitgestaltung u.v.m. Bei weiteren Vernetzungsmöglichkeiten mit den Trainingsgeräten folgen die Trainingssteuerungs- und Dokumentationsdaten, z.B. pulsgesteuertes Training, Anwesenheit, Dauer der Trainingseinheit. Es werden also gerade im Fitness- und Gesundheitsbereich sehr viele biometrische und persönliche Daten von den Mitgliedern gesammelt – wahrscheinlich mehr Informationen, als selbst eine Krankenkassen gespeichert hat. An dieser Stelle die Erinnerung, wie lange die Krankenkassen für die Einführung der neuen Krankenversicherungskarte bzw. elektronischen Gesundheitskarte benötigt haben, da der Datenschutz der personenbezogenen Daten nicht gewährleistet gewesen ist. Die Angst war berechtigt, so hätte ein Verlust der elektronischen Gesundheitskarte ein Ausspähen der eigenen Daten bedeutet. Dank der neusten Verschlüsselungstechnologie SSL sind nun die persönlichen Daten auf der neuen Gesundheitskarte geschützt.

Datenmissbrauch durch Verlust der Mitgliedskarte?

Die Annahme, dass ein Datenmissbrauch beim Verlust der eigenen Mitglieds- beziehungsweise Transponderkarte entstehen kann, ist nicht gegeben. Eine RFID-Transponderkarte kann nur eine eindeutige Nummer speichern und keine personenbezogenen Daten. Im Klartext bedeutet das, dass ein Lesegerät, ob an einer Tür, an einem Trainingsgerät oder am Check-in, nur die Nummer ausliest, die in der Software mit einem Datensatz verknüpft ist, also zum Beispiel den Namen, der dann am Check-in angezeigt wird. Das Mitglied kann also selbst bei grob fahrlässigem Verhalten die eigenen Daten nicht an Dritte weitergeben oder verlieren.

In der Fitnessbranche ist das Thema „Datenschutz und -sicherheit“ noch nicht so präsent, wie es eigentlich sein müsste, wenn man bedenkt, wie viele persönliche Daten von den Mitgliedern gesammelt werden. Auch im Jahr 2015 bewahren noch viele Fitness- und Gesundheitsstudios oder kleinere Physiotherapien ganz offen Trainingspläne oder Anamnesebögen in Schubladen auf, sodass jede Person Zugang zu diesen Daten hat. Außerdem wird eher in den seltensten Fällen bei Unterzeichnung der Mitgliedschaftsvereinbarung eine Einwilligung zum Datenschutz vom Mitglied eingeholt. Dabei liegt es im Interesse des Studioinhabers, diese Einwilligung einzuholen, da in erster Instanz der Gesundheitsanbieter für den Datenschutz einstehen muss und bei Missbrauch oder Verlust haftet.

Liegt die Verfügungsgewalt allein bei den Studios?

Um dieser Frage nachzugehen, muss zunächst einmal das Cloud Computing erklärt werden. Vor knapp zehn Jahren entwickelten salesforce.com, Amazon, Google und Microsoft das Speichern von Daten auf entfernte Recheneinheiten, also auf Servern, die an einem entfernten Ort abgelegt werden, das sogenannte Filehosting. Diese Technologie verbreitete sich sehr schnell und heute ist für die meisten Menschen ein Arbeiten ohne Cloud wie iCloud, Google Drive, Dropbox oder OneDrive wohl kaum noch möglich. Diese neue Technologie hat Vor- und Nachteile. Ein Vorteil ist, dass die Netzwerkstruktur nicht mehr vor Ort gepflegt werden muss; dies übernehmen dann Drittanbieter. Die Daten können, müssen aber nicht mehr gesichert werden, da die Softwareunternehmen automatisch Backups erstellen.

Natürlich haben auch die Fitnessbranche und insbesondere einige Kraftgerätehersteller und Anbieter von Verwaltungssoftwares das Arbeiten in der Cloud für sich entdeckt. Die Vernetzung kennt keine Grenzen mehr und macht dank der entwickelten Fitness-Apps auch nicht mehr am Smartphone der

Mitglieder halt. Die Fitnesseinrichtung hat also die Möglichkeit, Softwares von Fitnessgeräteherstellern einzusetzen, die cloudbasiert Dienstleistungen bereitstellen. Auf den ersten Blick überwiegen die oben genannten Vorteile, die

Foto: Kzenon/shutterstock.com

Viele Kraftgerätehersteller und Anbieter von Verwaltungssoftwares haben das Arbeiten in der Cloud für sich entdeckt. Daraus resultieren einige wichtige Fragen: Wer hat in einem Softwareunternehmen Zugriff auf die Daten? Wo werden diese Daten exakt gespeichert und auf welches internationale Recht bezieht sich der Datenschutz?

sich bei einer Vollvernetzung bis in die kleinste Peripherie der Einrichtung erstreckt, also z.B. bis hin zu den vernetzten Kraft- und Ausdauergeräten. Fällt eine technische Einheit aus, übernimmt dies die Fernwartung des Softwareunternehmens der eigenen Wahl. Ein Netzwerkadministrator, der sich mit LAN, WLAN, Netzwerkstrukturen oder auch mit der Verwaltungs- und Trainingssoftware auskennt, wird nicht weiter benötigt.

Eine Cloud speichert also die Daten nicht auf einem Server physisch vor Ort. Die Nachteile, die sich dadurch ergeben, liegen auf der Hand.

Wer hat Zugriff und wo werden die Daten gespeichert?

Wer hat in einem Softwareunternehmen Zugriff auf die Daten? Wo werden diese Daten exakt gespeichert und auf welches internationale Recht bezieht sich der Datenschutz? Fragen, die wahrscheinlich auch der Key Account Manager nicht beantworten kann.

Jedes Unternehmen regelt dies in seinen eigenen Datenschutzrichtlinien. Die personenbezogenen Daten werden zwar nicht an dritte Unternehmen weitergegeben, aber trotzdem werden Cookies gesetzt, um den Mitgliedern Werbebotschaften dritter Unternehmen zu unterbreiten, die persönlich auf sie zugeschnitten sind. Auch werden anonymisiert Daten zur IP-Adresse, dem Betriebssystem, dem Browsertyp, die Adresse der Bezugswebsite, Informationen zu Mobilfunknummern und mobilen Gerätetypen gesammelt und ausgewertet. Des Weiteren wird auch der mobile Standort der Mitglieder erfasst, wenn diese die Dienstleitungen mobil nutzen. Also ein gesamtes Bewegungsprofil eines Menschen inklusive aller persönlichen Daten, die in einer Cloud gespeichert sind. Auch wenn eine Datenschutzrichtlinie der jeweiligen Unternehmen die Weitergabe dieser Daten verbietet und die Unternehmen bestrebt sind, die bestmögliche Sicherheit der Daten zu gewährleisten, so sind diese trotzdem online verfügbar.

Die Vorratsdatenspeicherung in öffentlichen, deutschen Einrichtungen beträgt sieben Tage, bei einigen cloudbasierten Softwares in der Fitnessbranche 24 Monate. Des Weiteren werden einfache räumliche und zeitlich unbeschränkte Nutzungsrechte der persönlichen Daten auch nach Beendigung des Nutzungsverhältnisses an das Unternehmen übertragen. Es besteht die Möglichkeit, dass die Mitglieder Einspruch dagegen einlegen können. Folglich führt dies zum Ausschluss der Nutzung der Software.

Die Fitnesseinrichtung – und somit der Clubbetreiber – sollte sich im Klaren sein, dass nach einem Anbieterwechsel der Fitnessgeräte und cloudbasierten Software alle Daten der Mitglieder wieder neu erhoben werden müssen, sodass dem Kraftgeräte- und Softwareanbieter die Möglichkeit eingeräumt wird, Werbemaßnahmen oder die Nutzung der Software für die Mitglieder in einer anderen Fitnesseinrichtung zu ermöglichen.

Vorsicht: Datenschutzbestimmungen checken

Die Datenschutzbestimmungen der Geräte- bzw. Softwareunternehmen sollten vor Unterzeichnung der Kaufverträge gründlich durchgelesen werden. Eine Unstimmigkeit führt zwar nicht zur Datenschutzveränderung in dem jeweiligen Unternehmen, kann aber die Entscheidung, welche Software für den eigenen Club geeignet ist oder nicht, durchaus beeinflussen. Auch sollten die Datenschutzbestimmungen für die Mitglieder beachtet werden. Wird mit einem cloudbasierten Unternehmen zusammengearbeitet, müssen die Mitglieder gleich zwei Datenschutzbestimmungen durchlesen und bestätigen: die eine des Gesundheitsanbieters und die andere des kooperierenden Softwareunternehmens.

Jedes Unternehmen muss sich die Frage stellen, wie es um den Datenschutz steht und wie mit den Daten der Mitglieder umgegangen werden soll. Sind diese Fragen hinreichend erörtert und diskutiert worden, kann der Clubbetreiber genau jene Software erwerben, die zu seiner Firmenphilosophie passt; entweder auf seinem eigenen Server in der Fitnesseinrichtung oder extern gehostet bei einem Drittanbieter. Im letzten Schritt entscheidet aber nur einer über seine Daten: das Mitglied!

Timo Rieder

Vormerken

Das Schwerpunktthema unserer nächsten Ausgabe (Erscheinungstermin 31. Oktober) lautet

IT im Fitnessstudio.

Den 3. Teil dieser Serie, „EDV-basierte Mitarbeiterverwaltung“, können Sie in der Dezember-Ausgabe lesen, die am 30. November erscheint.

Timo Rieder M.A. ist seit 15 Jahren in der Fitnessbranche tätig. Nach seinem Studium mit dem Abschluss Magister Artium (M.A.) hatte er die Möglichkeit, verschiedene Unternehmen in der Branche kennenzulernen. Einen großen Einblick gewährte ihm das Softwareunternehmen aktivKONZEPTE ebenso wie die monte mare Unternehmensgruppe als Global Player in den Bereichen Wellness, Sauna und Fitness. Diese Erfahrung nutzt er heute, um als Assistent der Geschäftsführung die sports up GmbH in Wiesbaden zu bereichern. Zudem schreibt er derzeit an seiner Dissertation im Bereich der Sportsoziologie.