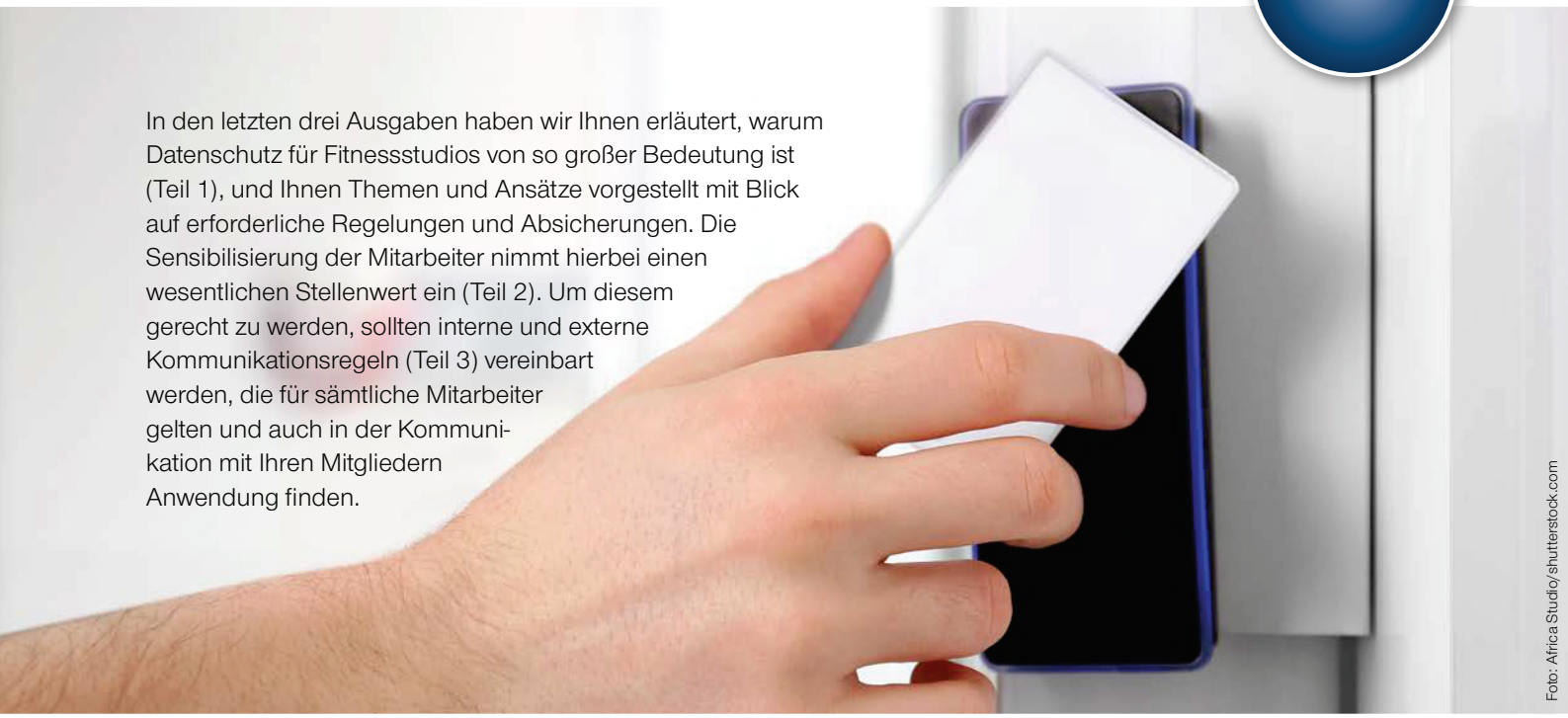
Datenschutz und -sicherheit

SERIE



In den letzten drei Ausgaben haben wir Ihnen erläutert, warum Datenschutz für Fitnessstudios von so großer Bedeutung ist (Teil 1), und Ihnen Themen und Ansätze vorgestellt mit Blick auf erforderliche Regelungen und Absicherungen. Die Sensibilisierung der Mitarbeiter nimmt hierbei einen wesentlichen Stellenwert ein (Teil 2). Um diesem gerecht zu werden, sollten interne und externe Kommunikationsregeln (Teil 3) vereinbart werden, die für sämtliche Mitarbeiter gelten und auch in der Kommunikation mit Ihren Mitgliedern Anwendung finden.

Foto: Africa Studio/shutterstock.com

Teil 4: IT-Systeme und Berechtigungen, bauliche Gegebenheiten

Überblick über die 4-teilige Serie

Teil 1: Warum Datenschutz auch für Fitness- studios zunehmend von Bedeutung ist

Teil 2: Sensibilisierung von Mitarbeitern und sensibler Umgang mit vertraulichen Daten

Teil 3: Interne und externe Kom-munikation sowie vertragliche Regelungen

Durch regelmäßige Schulungen können Sie das Bewusstsein Ihrer Mitarbeiter im Umgang mit personenbezogenen Daten schärfen. Zusätzlich sollten Sie sich vertraglich absichern und Ihre Mitarbeiter dahingehend in die Pflicht nehmen, dass sie vereinbarte Regeln und Leitlinien einhalten (Teil 2 und 3). Mit diesen Maßnahmen befinden Sie sich bereits auf einem guten Weg, um den Schutz der bei Ihnen erhobenen Daten zu gewährleisten. Dennoch sind Sie dadurch noch nicht komplett geschützt! Im heutigen digitalen Zeitalter gibt es Bedrohungen von „außen“, die Ihr Studio existenziell schädigen können.

Haben Sie sich schon einmal Gedanken darüber gemacht, ob Ihre IT-Systeme sicher sind? Wissen Sie, wie aktuell Ihre eingesetzten Softwareversionen sind, wo Ihre Systeme Schwachstellen haben könnten? Neben den digitalen Bedrohungen spielen auch die Gebäude- und Gerätesicherungen beim Schutz der eigenen Systeme eine Rolle.

Gebäude- und Gerätesicherung

Beginnen wir mit der Ansiedlung Ihres Studios: Liegt Ihr Club in einem stark frequentierten Zentrum/Gebäude oder am Stadtrand? Verfügen Sie über eine eigene Immobilie mit separatem Parkplatz oder befindet sich Ihr Studio mit weiteren Dienstleistern unter einem Dach? Findet eine Videoüberwachung des Außenbereichs statt, kann dies bereits eine Absicherung gegen Angreifer sein, die sich möglicherweise Zugang zu den IT-Systemen verschaffen wollen.

Im Anschluss stellt sich die Frage, wie Ihre Studionutzer Zutritt zu den Trainingsräumen erhalten. Die Außentüren

können verschlossen sein und nur per Chip oder Karte geöffnet werden oder sie sind nur während der Trainingszeiten geöffnet. Verfügen Sie über einen Empfang, der durchgängig besetzt ist und wo sich Ihre Mitglieder anmelden und legitimieren müssen oder können sich Personen unbemerkt Zutritt zu Ihrem Innenbereich verschaffen?

Sogar in den Umkleideräumen können digitale Komponenten Verwendung finden, beispielsweise in Form eines Chips oder einer Chipkarte, mit dem sich der Spind öffnen lässt. Moderne Trainingsgeräte, die sich durch Chip(-Karten) automatisch auf die Einstellungen des Nutzers anpassen, sind in heutigen Studios ebenfalls häufig anzutreffen.

Haben Sie sich damit beschäftigt, welche technischen Standards dem zugrunde liegen, wie die Komponenten funktionieren und miteinander vernetzt sind und inwieweit Manipulationsmöglichkeiten ausgeschlossen sind?

Schutz der IT-Systeme

Auch hier müssen Sie sich bewusst sein, wer in Ihrem Fitnessstudio Zugang zu den verschiedenen IT-Systemen und Computern benötigt und welche Vorgänge die Personen EDV-gestützt abwickeln. Auf dieser Basis sind Berechtigungen restriktiv nach Tätigkeitsfeldern zu vergeben. Hierzu gilt es einmalig ein Benutzer- und Berechtigungskonzept abzustimmen, welches unterschiedliche Freigaben einschließlich Lese- und Schreibberechtigungen für Daten bestimmt. Neben den Rollen und Berechtigungen sind Anforderungen an die IT-Systeme nach folgenden Grundsätzen umzusetzen:

Foto: SpeedKingz/shutterstock.com

Findet eine Videoüberwachung des Außenbereichs statt, kann dies bereits eine Absicherung gegen Angreifer sein, die sich möglicherweise Zugang zu den IT-Systemen verschaffen wollen

- Aktualisieren Sie Ihre eingesetzten Softwarelösungen regelmäßig!
- Prüfen Sie regelmäßig die Einstellungen Ihres Virenschutzes!
- Sorgen Sie für eine automatische Bildschirmsperre und ausreichende Passwortsicherung bei sämtlichen EDV-Zugängen!
- Seien Sie sorgsam mit der Verwendung von Wechseldatenträgern und mobilen Geräten!
- Erstellen Sie unbedingt regelmäßige Back-ups, um Ihre Daten zu sichern, und lagern Sie eine Sicherung an einem anderen Standort!
- Achten Sie bei der Nutzung von Clouddiensten auf den Anbieter und prüfen Sie dessen Leistungsangebot sorgfältig. Geben Sie Ihre Daten nur an ausgewählte Dienstleister.

Im Rahmen unseres Basischecks für Fitnessstudios haben wir die Erfahrung gemacht, dass vorkonfigurierte Grundeinstellungen der IT-Systeme häufig übernommen und nicht angepasst werden. Dadurch entstehen unnötige Sicherheitslücken, die potenzielle Angreifer nutzen können, um – neben den sensiblen Gesundheitsdaten – an die Bankdaten Ihrer Kunden zu gelangen. Schützen Sie daher Ihre Daten und IT-Systeme!

Fazit

Es wird ersichtlich, dass eine Abschottung Ihres Gebäudes, Ihrer Geräte und Ihrer Systeme mittels unterschiedlicher technischer und organisatorischer Maßnahmen zu erfolgen hat. Hierzu ist zunächst der Schutzbedarf individuell zu ermitteln und darauf aufbauend sind angemessene Maßnahmen zu ergreifen, um Ihr Gebäude, Ihre Innenbereiche und Ihre Systeme abzusichern. Entwickeln Sie ein ganzheitliches Sicherheitskonzept und legen Sie in diesem Zusammenhang Kontrollmechanismen fest.

Lassen Sie Ihr Studio anhand eines Mehrstufenmodells auf Herz und Nieren prüfen! Die Module bestehen aus Quick-Check, Beratung vor Ort und kontinuierlicher Begleitung einschließlich interner Schulung. Mit dieser Analyse wissen Sie, wie gut Sie bereits aufgestellt sind, und können im Bedarfsfall Ihr individuelles und ganzheitliches Sicherheitskonzept auflegen oder gegebenenfalls anpassen lassen. Alles im Sinne der Sicherheit Ihrer Kundendaten. Ralf Gorschlüter

Ralf Gorschlüter verantwortet als Gesundheitsökonom und Diplom-Kaufmann das Beratungsgeschäft der AuraSec GmbH und ist operativ in verschiedenen Projekten in den Bereichen Prozessmanagement, Strategie, IT-Systemintegration und als Initiator verschiedener Netzwerke, Prüfgemeinschaften und Individualprojekte im Kontext mit Datenschutz und Informationssicherheit aktiv.

Kontakt: +49 173 7253780; info@aurasec.de; www.aurasec.de