

# Mehr Sicherheit bei den Patientendaten

Im Gesundheitswesen stellen die Patienten, die Mitarbeiter und der Datenschutz heute sehr hohe Anforderungen an die Vertraulichkeit, Verfügbarkeit und Integrität von Patientendaten. Damit wird das Identity Management immer mehr zur Herausforderung. Marco Bolliger



**Marco Bolliger**  
ist Head Client & Server  
Security bei der  
InfoTrust AG.  
marco.bolliger@infotrust.ch

Unternehmen des Gesundheitssektors müssen die Sicherheit und Verfügbarkeit ihrer Patientendaten zu jeder Zeit nachvollziehbar gewährleisten. Die einzelnen Anforderungen daran werden aber längst nicht mehr nur vom Staat und den Behörden vorgegeben. Kliniken und Spitäler müssen sich im hart umkämpften Gesundheitsmarkt mittlerweile viel mehr nach den Sicherheitsbedürfnissen ihrer Kunden, also ihrer Patienten ausrichten sowie die Forderungen ihrer Mitarbeiter im Bereich Verfügbarkeit und Komfort berücksichtigen. Eine grosse Herausforderung für die IT-Security-Beauftragten und eine besondere Verantwortung für das Management eines solchen Unternehmens.

## **Mehr Arbeit mit dem Computer als mit dem Patienten**

Ein beachtliches Sicherheitsrisiko geht von der Komplexität der Passwortverwaltung bei Mitarbeitern im Gesundheitswesen aus. Für fast jedes System innerhalb der meist sehr heterogenen IT-Infrastruktur gibt es eine eigene Benutzerverwaltung mit unterschiedlichen Benutzernamen, Passwörtern und Policies. Ein Anwender muss sich typischerweise mehr als fünf verschiedene Kombinationen aus Benutzernamen und Passwort merken. Hinzu kommt, dass im Gesundheitswesen viele Mitarbeiter für ihre tägliche Arbeit nicht ihre persönliche Arbeitsstation einsetzen. Das Personal ist im Gebäude sehr mobil und an verschiedenen Stationen im Einsatz. Häufig stehen gemeinsam genutzte Rechner zur Verfügung, was ein weiteres Sicherheitsproblem darstellt. Entweder findet gar keine Authentisierung statt oder alle Nutzer verwenden ein gemeinsames Log-in, was wiederum eine ungenügende Nachvollziehbarkeit zur Folge hat. Wie aber kann man die Herausforderungen mit den zahlreichen Zugängen meistern? Wie kann man verhindern, dass Patientendaten in falsche Hände gelangen?

Wenn es um den Schutz von Patientendaten geht, stehen Themen wie die Verwaltung von Identitäten und Zugriffsrechten, das sichere Authentisieren eines Anwenders, Single Sign-On, aber auch Auditierungsmöglichkeiten sowie die Nachvollziehbarkeit im Zentrum. Was aber macht eine professionelle Physical-&-Logical-Access-Lösung aus und welche Vorteile ergeben sich daraus?

### Zentrales Identity Management

Eine der wichtigsten Komponenten ist das zentrale Management der Identitäten. Dieses ermöglicht eine durchgängige Verwaltung der Benutzer mit ihren entsprechenden Passwörtern, Tokens und Zertifikaten. Die Lösung muss aber verschiedene Schnittstellen für die Authentisierung der Benutzer und gegenüber den Applikationen anbieten. Der zentrale Ansatz vereinfacht auch die Administration und erhöht die Sicherheit, da weniger Eingriffe notwendig sind.

### Strong Authentication – sicherer und einfacher

Im Gesundheitswesen, wo mit hochsensiblen Patientendaten gearbeitet wird, hat eine sichere und effiziente Authentisierung oberste Priorität. Die Lösung heisst Strong Authentication. Darunter versteht man Zugangssysteme, die mehrere Faktoren (zum Beispiel One-Time Password Token und PIN) zur Identitätsprüfung heranziehen. Diese können nicht weitergegeben oder gemeinsam genutzt werden.

Der Markt bietet mittlerweile eine Vielzahl verschiedener Lösungen an. Eine umfassende Physical-&-Logical-Access-Lösung muss daher zwingend eine grosse Produktpalette unterstützen. Damit wird eine Integration in die bestehenden Systeme erst möglich. Es haben sich diverse ID Token (One-Time Password), Smartcards (Zertifikate) sowie RFID Token am Markt etabliert. Immer stärker nachgefragt werden auch biometrische Leser, wie beispielsweise der Fingerabdruckleser. Die Sicherheit wird damit massiv verbessert und für den Benutzer bringt es eine zusätzliche Erleichterung.

### Single Sign-On – Log-ins zentral verwaltet

Die Idee dahinter ist einfach: Der Mitarbeiter authentifiziert sich einmal, zum Beispiel beim Betreten des Firmengeländes, und soll dann automatisch, ohne Eingabe weiterer Passwörter, bei allen weiteren Anwendungen, Websites oder Kommunikationssystemen automatisch

angemeldet sein. Es sind verschiedene Ansätze denkbar, wie das erreicht werden kann. In der Vergangenheit waren aufwendige Anpassungen an die jeweiligen Applikationen (Scripting) notwendig, da es oft keine gemeinsamen Schnittstellen gab. Einfacher ist der Einsatz sogenannter Agents, die auf den Arbeitsplatzrechnern installiert werden. Diese speichern Anmelde-Credentials wie Benutzername und Passwort zentral in einem sicheren System ab. Die Log-in-Masken der jeweiligen Anwendungen werden vom Agenten für den entsprechenden Benutzer «ausgefüllt». Der Administrationsaufwand für die Integration von Applikationen wird durch den Einsatz lernfähiger Systeme spürbar reduziert.

### Die Integration von physischer Zugangskontrolle

Werden die physische und die logische Sicherheit zentral verwaltet, können Informationen aus beiden Welten genutzt werden. So kann ein Zugriff auf ein speziell schützenswertes System beispielsweise nur gewährt werden, wenn sich der Mitarbeiter auch im entsprechenden Raum befindet. Ein Log-in im Namen eines anderen Benutzers kann so verhindert werden. Ziel ist es, alle benötigten Funktionen mit einem Gerät abdecken zu können – beispielsweise eine Smartcard mit integrierter RFID-Komponente. Der RFID-Teil der Karte wird für den sicheren Zugang zum Gebäude verwendet und kann gleichzeitig für die Anmeldung an den IT-Systemen eingesetzt werden. Als Alternative zur Authentisierung mittels RFID können auch auf der Smartcard gespeicherte Zertifikate verwendet werden. Bereits die Umsetzung von Teilgebieten führt zu einer Verbesserung der Sicherheit und Optimierung der Arbeitsabläufe.

Eine konzeptionelle Analyse der Anforderungen zeigt, welche Massnahmen im konkreten Fall sinnvoll umgesetzt werden können. Da die Patientendaten in mehreren Applikationen bereitgestellt werden und die Zahl der Anwendungen

täglich zunimmt, wird das Identity Management immer mehr zur Herausforderung. Abhilfe schafft eine zentrale Lösung, die die physische und logische Zugriffskontrolle vereint und dabei den Zugang zu Workstations, Applikationen und Patientendaten einfacher und sicherer gestaltet. Ein für die Mitarbeiter komfortables Identity Management verbessert neben der Sicherheit ausserdem die gesamten Arbeitsprozesse, die Produktivität und nicht zuletzt auch die Zufriedenheit. ■

