EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Single Sign-On – Einmal täglich

Fachartikel von Achim Stolz, Lead IAM Advisor, IPG AG

Im Krankenhaus- und Spitalumfeld ist das Abwägen von Sicherheit und Datenschutz gegenüber Umständlichkeit und Aufwand besonders wichtig und auch mit einer emotionalen Komponente verbunden. Schliesslich steht mit der Gesundheit des Patienten ein hohes Gut im Zentrum allen Handelns. In diesem Spannungsfeld zwischen unmittelbar benötigtem Zugriff auf Patienteninformationen und Datenschutz und Sicherheit sind Kompromisse zu Lasten der Sicherheit oft das Ergebnis.

Die entsprechenden Abkürzungen sind seit der Erfindung des Logins dieselben: Passwort aufschreiben, Logins gemeinsam nutzen, den einmal entsperrten Bildschirm für den nächsten Anwender entsperrt lassen, sind alltägliche Beispiele. Der mit Identity & Access Management erarbeitete Schutz der Daten vor unberechtigtem Zugriff und das ausgeklügelte Zugriffskonzept werden dabei komplett ausgehebelt.

Anwendungsbeispiele

Was sind die Anwendungsfälle aus Sicht von Gesundheitsfachpersonen wie Ärzteschaft und Pflege im Spitalumfeld?

- Mehrfache Anmeldevorgänge an unterschiedlichen Arbeitsstationen sowie auch Applikationen innert kurzer Zeit
- Wechsel der Arbeitsstation mit erneuten Anmeldevorgängen
- Wechselnde Nutzer derselben Arbeitsstation drücken sich gegenseitig weg

In eine Wunschsituation umgedeutet heisst dies:

- Die Gesundheitsfachperson beweist einmalig pro Tag ihre Identität (sie authentisiert sich mit Login, Secure Card o.ä.)
- Jede aufgerufene Applikation erkennt den Anwender anschliessend und gewährt ihm die zugewiesenen Rechte
- Aufgerufene Applikationen folgen dem Anwender auf andere Arbeitsstationen und stehen dort inklusive Arbeitsstand wieder zur Verfügung
- Eine belegte Arbeitsstation lässt sich durch einen Anwender kurzzeitig nutzen und steht anschliessend wieder anderen Anwendern zur Verfügung

Diese Anforderungen lassen sich mit den folgenden technischen Lösungen zu Gunsten der Sicherheit umsetzen:

Single Sign-On (SSO): Der Anwender meldet sich an einer Arbeitsstation einmalig an und erhält auf sämtliche danach aufgerufenen Applikationen Zugriff. Ergänzt werden kann das SSO mit Zwei-Faktor-Authentisierung wie z.B. mittels RFID-Karten, welche das Anmeldeprozedere nochmals deutlich einfacher machen.

Desktop Roaming: Hier wird die traditionell auf dem lokalen PC ausgeführte Arbeitsumgebung auf eine virtualisierende Server-Umgebung verlagert; der lokale PC ist entsprechend nur noch Anzeigegerät für die persönliche Arbeitsumgebung, was einen raschen Zugriff von jedem Endgerät aus erlaubt.

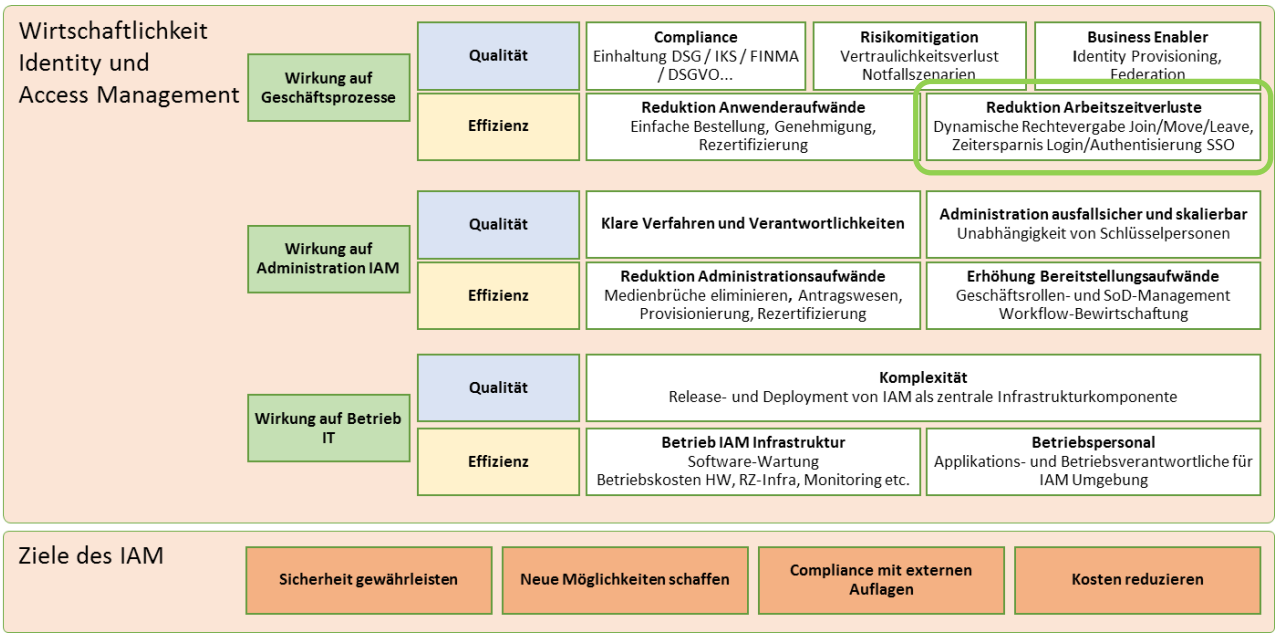
Fast User Switching: Ist speziell an «Kiosk-Arbeitsstationen» sinnvoll, damit diese geteilten Endgeräte jeweils mit dem persönlichen Login und nicht etwa mit – aus Compliance Sicht äusserst problematischen – Sammelaccounts verwendet werden können. Ebenso lässt sich damit vermeiden, dass eine Arbeitsstation permanent offengehalten werden muss, was prinzipiell jeder Person im Raum Einsicht in sensible Daten gäbe.

Welchen Nutzen bringen optimierten Authentisierungslösungen?

Optimierte Authentisierungslösungen sind eine wichtige Komponente für ein zuverlässiges Identity & Access Management, weil damit problematische Workarounds mit Sammelbenutzern etc. obsolet werden.

Gerade im Krankenhausumfeld tragen die Lösungen jedoch vor allem dazu bei, Arbeitszeitverluste bei den Gesundheitsfachpersonen zu reduzieren. Die eingesparten Login-Prozeduren ergeben ganz konkret mehr Zeit für Behandlung und Pflege. Darüber hinaus werden die technischen Erneuerungen durch das Personal akzeptiert, was eine Einführung stark vereinfacht. Konkrete Eindrücke dazu geben die Beispiele Kantonsspital Winterthur oder die Spitäler fmi AG.

Auch wenn entsprechende Business Cases sicherlich immer situationsbezogen und damit kritisch zu hinterfragen sind, lässt sich die Reduktion der Arbeitszeitverluste im Spitalumfeld im Einzelfall prognostizieren und auch messen; insgesamt ergibt sich eine Gesamtlösung, welche Compliance und Sicherheit erhöht und auch betriebswirtschaftlich innerhalb von ein bis drei Jahren einen Gewinn darstellt.



Gute Authentisierungslösungen zeigen eine direkte Wirkung auf die Effizienz der Geschäftsprozesse

EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Wie unterstützt IPG?

Als Experte für IAM unterstützen wir Sie gerne in der strategischen Planung, der Umsetzung und dem Betrieb von effektiven und effizienten Lösungen rund um die Verwaltung von Identitäten und Zugriffen zum Schutz Ihrer digitalen Infrastrukturen.

Kontaktieren Sie uns, wenn Sie mehr zu diesem Thema oder unseren IAM-Lösungen erfahren möchten.

Christian Rückert: Sales Manager Germany and Austria
christian.rueckert@ipg-group.com; Telefon +49 170 908 03 53

Arne Vodegel: Sales Manager Germany
arne.vodegel@ipg-group.com; Telefon +49 170 908 04 32

Marcel Weber: Sales Manager Switzerland
marcel.weber@ipg-group.com; Telefon +41 79 907 84 47