

# Anmeldung mit dem digitalen Ich

**IMPRIVATA: Moderne Single-Sign-on-Systeme und Authentifizierungsmanagement-Lösungen schließen die Lücke zwischen Datenschutzanspruch und -wirklichkeit.**

Bis zu 400 verschiedene IT-Systeme kommen in großen Krankenhäusern zum Einsatz, ein Klinikmitarbeiter nutzt im Durchschnitt bis zu sieben davon – und das bis zu zehn Mal täglich. Insgesamt kommen so in etwa 70 An- und Abmeldeprozesse zustande. Betrachtet man diese Nutzung durch die Datenschutzbrille, muss sich der Anwender an jedem dieser sieben Systeme mit einer eigenen Nutzererkennung und einem Passwort anmelden, das aus einer Kombination aus Buchstaben, Sonderzeichen und Zahlen besteht und das mindestens alle 12 Wochen verändert wird. „Die bisherigen Sicherheitsmechanismen sind einfach zu umständlich und die Einhaltung extrem zeitintensiv. Darum bilden sich im Alltag Umgehungsmechanismen heraus: Das Passwort klebt in Form eines Post-its am Monitor, eine ganze Station nutzt den Zugang des Oberarztes für ein System oder stationsübergreifende Prozesse werden der Einfachheit halber papierbasiert erledigt“, erklärt Dr. Anna Niemeyer, Medizinerin und



**Dr. Anna Niemeyer, Medizinerin und Expertin für klinische Prozesse und strategische IT-Beratung in Krankenhäusern**

Expertin für klinische Prozesse und strategische IT-Beratung in Krankenhäusern.

## „Intuitive Authentifizierung“ in die digitale Welt übertragen

In der analogen Welt waren und sind die Authentifizierungsprobleme überschaubar, wie Anna Niemeyer weiß: „Die Berechtigung wird über das simple Sehen und Erkennen einer Person vergeben. Jeder im Team weiß, welcher Mitarbeiter welchen Status hat und dementsprechend auch, wer was einsehen, anweisen oder abzeichnen darf.“ Diese intuitiven Unterscheidungsmerkmale gehen im Zuge der Digitalisierung systembedingt erst einmal verloren und werden durch komplizierte Identifizierungsprozesse ersetzt.

Spezifische Lösungen wie die Single-Sign-on- und Authentifizierungsmanagement-Systeme (AM) von Imprivata sind allerdings in der Lage, die individuelle und schnelle Identifikation am Arbeitsplatz zu simulieren – sei es durch die Freigabe mittels eines Mitarbeiter-Ausweises oder das Einlesen biometrischer Daten. Eine solche Authentifizierung umfasst die Anmeldung am Desktop sowie die an verschiedenen Anwendungssystemen und -modulen – unabhängig davon, ob diese an physischen oder virtuellen Desktops stattfindet oder ob über einen VPN-Tunnel auf die Infrastruktur zugegriffen wird. Im gleichen Zuge wird die Komplexität des Anmeldeverfahrens reduziert, weil Passwörter und Benutzernamen nicht mehr zwingend eingegeben werden müssen. Das spart Zeit und erleichtert die Nutzung der IT-Systeme.

„Eine solche Authentifizierung hat noch einen weiteren Vorteil, der den

Workflow im klinischen Alltag optimiert: Der Anwender kann von jedem Arbeitsplatz aus direkt auf sein individuelles Setting zugreifen. Und das unverzüglich, also ohne die Wartezeit, die mit einer An- und Abmeldung normalerweise verbunden ist. Im hektischen Klinikalltag ist dies ein wertvoller Pluspunkt. Bei virtualisierten Desktops profitieren Anwender außerdem davon, dass Aufgaben unabhängig vom Arbeitsplatz jederzeit an exakt der gleichen Stelle wieder aufgegriffen werden können, wenn – was häufig der Fall ist – beispielsweise eine laufende Dokumentation unterbrochen werden musste“, ergänzt Anna Niemeyer.

## Mehr Anwenderzufriedenheit, weniger Arbeit für die IT-Abteilung

Der Einsatz des Imprivata Authentifizierungsmanagements führt zu einer signifikant höheren Zufriedenheit der Mitarbeiter mit den IT-Systemen, weil der Benutzerwechsel schnell und einfach möglich ist. Gleichzeitig entlasten sie die IT-Abteilungen, weil weniger Passwort-Zurücksetzungen, Neueinrichtungen oder Änderungen vorgenommen werden müssen.



- ▶ **Imprivata Inc.**
- ▶ **Hagen Reiche**
- ▶ **Zeltnerstr. 1-3**
- ▶ **Büro: +49 -(0)911 8819 7330**
- ▶ **Mobil: +49 -(0)172 893 09 06**
- ▶ **90443 Nürnberg**
- ▶ **hreiche@imprivata.com**
- ▶ **www.imprivata.de**