Sichere und schnelle Authentisierung in Spitälern

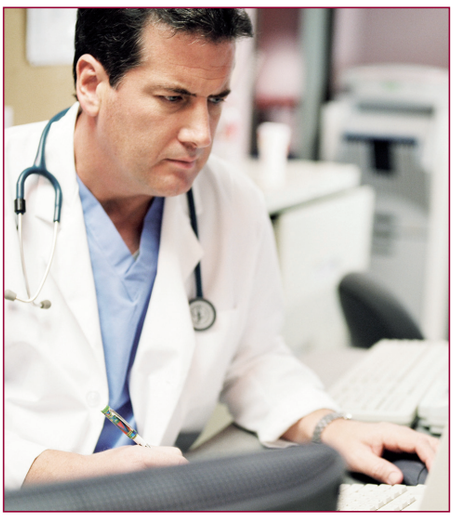
Den Zugriff auf (Patienten-)Daten und Applikationen wirksam zu schützen und die zugriffsberechtigten Personen bei deren Anmeldung sicher zu identifizieren: Dieses Bedürfnis ist im Gesundheitswesen besonders ausgeprägt – und eine anspruchsvolle Herausforderung. Thomas Boll

Der Website «e-health-suisse.ch» kann folgende Aussage entnommen werden: «Ziel (von E-Health) ist es, mehr Sicherheit und Qualität im Gesundheitswesen zu schaffen und langfristig zur Stabilisierung der Kosten beizutragen.» In diesem Bestreben von Bedeutung sind sowohl der gesicherte Zugang zu Anwendungen und Daten als auch die sichere Authentisierung der jeweiligen Person(en) – ein Themenbereich mit ausgeprägtem Optimierungspotenzial. So machen komplizierte, mehrstufige Anmeldeverfahren mit unterschiedlichsten Kombinationen von Benutzernamen und Passwörtern das Leben der User schwer. Kein Wunder, dass sie häufig einfache Identifikationscodes verwenden, ein und dasselbe Passwort für unterschiedlichste Anwendungen nutzen und es vermeiden, Zugangsdaten in regelmässigen Abständen zu ändern. Dass die so verwendeten Passwörter in der Regel nicht den Bedürfnissen einer sicheren Authentisierung entsprechen, erstaunt nicht. Fehlen ergänzende Identifikationskomponenten wie OTP-Token (One Time Password) oder biometrische Authentisierungslösungen, ist eine «starke Authentisierung» undenkbar. Um dieser Problematik zu begegnen, sind Lösungen gefragt, die folgende Funktionen integral unterstützen:

- Starke Authentisierung/Authentication Management
- SSO (Single Sign-on)
- Session Roaming/Fast User Switching

Starke Authentisierung

Basieren Log-in-Prozeduren lediglich auf User-Name und Passwort, handelt es sich um eine sogenannte «schwache Authentisierung», die den Sicherheitsbedürfnissen zahlreicher Branchen nicht entspricht. Werden hingegen zusätzliche Hardwarekomponenten für den Nachweis der eigenen Identität eingesetzt, ist von einer «Strong Authentication» beziehungsweise von einer «Multi Factor»-Authentifizierung die Rede. Zum Einsatz gelangen dabei sowohl Smartcards und aktive/passive RFIDs als auch Fingerprint-Sensoren und OTP-Token. Letztgenannte generieren Zahlenkombinationen, die jeweils nur für eine begrenzte Zeit Gültigkeit haben. RFID-Cards ihrerseits ermöglichen ein schnelles und komfortables beziehungsweise berührungsloses Log-in am Desktop. Denkbar ist die kombinierte Anwendung unterschiedlicher Hardwarekomponenten. Dabei lässt sich mittels Policies definieren, welche Form der Multi-Faktor-Authentifikation pro User, Anwendung und Arbeitsplatz unterstützt wird.



Zahlreiche Spitäler machen sich die Vorzüge der integralen SSO- und Authentication-Appliance «OneSign» von Imprivata zunutze. Bildquelle: photos.com

Von grosser Bedeutung ist die «Strong Authentication» auch bei der Einbindung dezentraler Anwenderinnen und Anwender. Sie ermöglicht eine sichere Authentisierung von Remote-Usern (zum Beispiel Ärzte und externe Leistungserbringer) und bildet so die nötige Voraussetzung für einen gesicherten Zugang zu Anwendungen und Daten – unabhängig davon, wo sich der Anwender befindet.

Einer für alle

Unternehmen, die für den geschützten Zugriff auf Daten, Applikationen oder Netzwerke auf eine starke Authentisierung setzen, schaffen beste Voraussetzungen für die Implementation einer «Single Sign-on»-Lösung (SSO) – und somit zur Verbesserung der Produktivität bei gleichzeitiger Steigerung der Sicherheit. SSO-Lösungen gewähren den Nutzern über ein starkes Passwort einen konsolidierten Zugang zu allen individuell freigegebenen Applikationen und Ressourcen. Hat sich der Benutzer authentisiert, ist er automatisch bei allen ihm freigegebenen Anwendungen angemeldet – ohne Eingabe von zusätzlichen Log-in-Daten.

SSO-Lösungen steigern die Passwortsicherheit nachhaltig. Sie ermöglichen beispielsweise eine automatisierte Implementierung von Passwortrichtlinien. Dazu werden im Hintergrund eindeutige und sichere Passwörter erstellt, die die Einhaltung von Richtlinien garantieren. Ferner lassen sich komplexe Passwörter mittels Zufallsgenerator erstellen. Diese sind dem jeweiligen Benutzer nicht bekannt und können folglich nicht an Drittpersonen weitergegeben werden. Zudem lassen sich regelmässige Passwortänderungen automatisieren.

Moderne SSO-Appliances lassen sich einfach in bestehende IT-Infrastrukturen implementieren, ohne dass dazu in den Code bestehender Systeme eingegriffen werden muss oder spezifische Konnektoren notwendig wären. Dazu erlernen sie die Authentisierungsmechanismen der jeweiligen Applikationen, synchronisieren mit den vorhandenen Domains und anderen LDAP User Directories und erstellen auf Basis der vorhandenen Passworteigenschaften für alle Anwendungen XML-Profile. Diese werden mit den entsprechenden Regeln in der Appliance gespeichert und bei jeder neuen Benutzerauthentisierung überprüft.

Der Hektik ein Schnippchen schlagen

In Umgebungen, in denen sich User mehrmals täglich an verschiedenen Arbeitsplätzen einloggen und abmelden müssen – ein

Thomas Boll ist Geschäftsführer von Boll Engineering.

Für den Nachweis der eigenen Identität lassen sich unterschiedliche Hardwarekomponenten wie Smartcards und aktive/passive RFIDs oder Fingerprint-Sensoren und OTP-Token einsetzen. Bildquelle: Imprivata

Fakt, der im Healthcare-Bereich besonders ausgeprägt ist –, erhält das Thema «Session Roaming» besondere Bedeutung. So müssen Arbeiten an einem Desktop (ohne Abmeldung) unterbrochen und an einem beliebigen anderen Arbeitsplatz fortgesetzt werden können. Wichtig ist dabei, dass Applikationen am neuen Arbeitsplatz automatisch an derselben Stelle geöffnet werden, wo sie der User unterbrochen hat. «Session Roaming» verleiht den Anwendern ein hohes Mass an Komfort und Mobilität. Voraussetzung dazu sind eine virtualisierte Umgebung oder Lösungen wie Citrix/Terminal Server Roaming.

Die im Spitalbereich ausgeprägte Mobilität der User rückt mit der Funktion «Fast User Switching» ein weiteres Leistungsmerkmal in den Fokus der Aufmerksamkeit. Dabei sollen mehrere User an einem gemeinsam genutzten Arbeitsplatz auf ihren persönlichen Windows-Desktop beziehungsweise auf die individuell freigegebenen Daten und Applikationen zugreifen können («Hot Application»), ohne dass sie sich beim Benutzerwechsel an- oder abmelden müssen. Ziel entsprechender Lösungen ist es, den Benutzerwechsel an den einzelnen Arbeitsstationen möglichst schnell (innert weniger Sekunden) zu ermöglichen.

In diesen Themenkreis gehört ferner eine mit «Secure Walk Away» bezeichnete Sicherheitsfunktion. Dabei werden in Ergänzung zu «klassischen» Prozeduren ergänzende Komponenten und Mechanismen zum Verriegeln beziehungsweise Abmelden an einer gemeinsam genutzten Workstation verwendet. So besteht etwa die Möglichkeit, Karten (Badges) wie Proximity- und RFID-Cards zur Verriegelung einzusetzen, Inaktivitätszeiten einzustellen oder auf Hot-Key basierende Abmeldemechanismen zu nutzen. Ferner stehen biometrische beziehungsweise visuelle Verfahren zur Verfügung, die das Entfernen des Users erkennen und die Workstation automatisch verriegeln.

Werden Funktionen wie SSO, Multi-Faktor-Authentifizierung, «Secure Walk Away» und «Fast User Switching» in einem System vereint, lassen sich hochsichere Zugriffs-Lösungen etablieren und die Komplexität gleichzeitig reduzieren. Entsprechende Systeme wie beispielsweise «OneSign» von Imprivata leisten folglich einen wichtigen Beitrag zur der von «e-health-suisse.ch» gestellten Forderung nach «Sicherheit und Qualität im Gesundheitswesen». <

DER DYNAMIK IM HEALTHCARE-BEREICH BEGEGNEN

Zahlreiche Applikationen und Datenbanken sowie mannigfaltige Log-in-Prozeduren machen das Leben der in Spitälern tätigen Personen nicht eben einfach. Erschwerend kommt hinzu, dass etwa Ärzte und Therapeuten, Pflege- und administratives Personal an unterschiedlichsten, oft gemeinsam genutzten Arbeitsstationen wirken. Dabei muss jedem User an jedem Desktop sein individuelles Profil – wie beispielsweise Sprache und freigegebene Ressourcen – zur Verfügung stehen. Gleichzeitig ist dafür zu sorgen, dass etwa Patientendaten nicht durch Drittpersonen eingesehen werden können – beispielsweise dann, wenn der behandelnde Arzt ohne sich abzumelden den Desktop verlässt.
Um den im Gesundheitswesen anspruchsvollen Sicherheitsanforderungen zu entsprechen, ist folglich eine hochsichere und trotzdem komfortable Authentisierung der User notwendig. Diesem Aspekt wird durch den Einsatz intelligenter «Single Sign-on»-Lösungen (SSO) mit integrierter «Multi Factor»-Authentifizierung entsprochen. Diese vereinfachen den Zugang zu den individuell freigegebenen Ressourcen markant. Idealerweise werden dazu Hardwarekomponenten wie beispielsweise Smartcards und Fingerprint-Readers eingesetzt, mittels derer sich die Anwenderinnen und Anwender einfach und komfortabel an jedem beliebigen Arbeitsplatz einloggen können. Noch komfortabler erweisen sich kontaktlose Systeme beziehungsweise RFID-Karten. Befindet sich der User in unmittelbarer Nähe zum Desktop, erfolgt die Anmeldung automatisch via Funk. Als ebenso wertvoll erweist sich der Einsatz der RFID-Technologie bei der Abmeldung am Arbeitsplatz. Verlässt der User die Workstation, wird diese automatisch gesperrt. Auch Gesichtserkennungstechnologien kommen in diesem Bereich zum Einsatz. Imprivata zum Beispiel ermöglicht mit der Funktion «Secure Walk Away» die automatische Sperrung eines Desktops, sobald der berechtigte Benutzer nicht mehr anwesend beziehungsweise sichtbar ist.
Ergänzend zu den Kernfunktionen einer integralen IAM-Lösung leisten ganzheitliche Systeme einen wichtigen Beitrag zu den im Spital- und Gesundheitswesen wichtigen Compliance-Anforderungen (z.B. HIPAA). So werden unter anderem sämtliche Anwendungs- und Datenzugriffe automatisch geloggt und stehen anschliessend für entsprechende Audits zur Verfügung.

STARKE AUTHENTISIERUNG

Werden für das Log-in beziehungsweise für den geschützten Zugriff auf Daten, Applikationen oder Netzwerke lediglich User-Name und Passwort benötigt, handelt es sich um eine sogenannte «schwache Authentisierung». Von einer starken Authentisierung («Strong Authentication»/«Multi Factor Authentication») hingegen ist dann die Rede, wenn ergänzende Authentisierungskomponenten eingesetzt werden. Die Kombination folgender Elemente bildet die Basis für eine «Strong Authentication»:

- Etwas, das ich weiss (z.B. Passwort, Pin-Code, User ID …)
- Etwas, das ich besitze (z.B. Smartcard, Proximity Card …)
- Etwas, das zu mir gehört (z.B. Fingerprint, Sprache, Iris-Scan …)