

# Secure Identity Management

*In grösseren Unternehmen und Institutionen werden Benutzerdaten heute meist dezentral und redundant über eine Vielzahl applikations- und systemspezifischer Benutzerverwaltungen gepflegt. Dies verursacht beträchtliche Aufwände und kann bei ungenügend definierten Prozessen zu Sicherheitslücken führen. Aktuell werden auf dem Markt eine ganze Palette von Software-Produkten angeboten, welche über die Einführung von «Secure Identity Management» (SIM) rasche Abhilfe versprechen. Doch mit dem Kauf einer SIM-Software allein ist es nicht getan. Die Umstellung auf SIM bedingt die Definition entsprechender technischer und betriebsorganisatorischer Prozesse und verursacht damit einen erheblichen Initialaufwand. Aber die Investition zahlt sich aus – sofern die globale Benutzeridentität dann effektiv unternehmensweit genutzt werden kann.*

## Was versteht man unter Secure Identity Management?

Unter Secure Identity Management (SIM) versteht man die unternehmensweite Verwaltung von Benutzeridentitäten. Eine Benutzeridentität besteht aus den so genannten Stammdaten wie Vorname, Name und einer eindeutigen

### CHRISTIAN GROB\*

Benutzer-ID ergänzt durch kontextspezifische Daten wie Benutzerrollen und Profildaten. Zusätzlich zu den Funktionen zur Verwaltung der Benutzeridentität bietet die aktuelle Generation der SIM-Systeme Sicherheits- und Auditingfunktionen sowie eine koordinierte Verteilung der Daten an.

## Was bringt die Einführung einer SIM-Lösung?

Im Vordergrund steht das Vermeiden redundanter Aufwände beim Erfassen und Verwalten von Benutzeridentitäten sowohl bei firmeninternen Prozessen wie auch bei Prozessen, in welche Kunden involviert sind. Pflege und Abgleich redundanter Daten generieren hohe Aufwände und bergen Sicherheitsrisiken.

Ein globales Identitätsmanagement schafft zudem ideale Voraussetzungen für die Realisierung einer Single-Sign-on-Lösung (SSO), welche dem Benutzer den Zugriff auf eine Vielzahl integrierter Anwendungen über ein einziges Log-in ermöglicht. Die Einführung einer SSO-Lösung mit SIM bringt doppelten Gewinn. Sie wirkt sich sowohl auf den Benutzerkomfort wie auch auf die Sicherheit positiv aus. Das ist selten. Ein Mehr an Sicherheit wird in der Regel mit einem Verlust an Benutzerkomfort bezahlt.

## Wirkt sich die Zentralisierung der Verantwortung sicherheitstechnisch ausschliesslich positiv aus, oder gene-

## riert sie auch neue Bedrohungsszenarien?

Die Zentralisierung der Benutzerdatenverwaltung vereinfacht die Datenverwaltungsprozesse, erhöht dadurch die Transparenz und Nachvollziehbarkeit (Audit) und ermöglicht eine bessere Kontrolle und Überwachung. Das wirkt sich auf die Sicherheit auf jeden Fall positiv aus. In den meisten Fällen werden schlankere Prozesse zudem besser verstanden und dadurch auch konsequenter eingehalten.

Allerdings verlangt die Zentralisierung der Verantwortung für die Benutzeridentität unter Umständen die Definition neuer Prozesse im betriebsorganisatorischen Bereich, die je nach Organisation auch aus rechtlichen Gründen beliebig kompliziert und schwerfällig ausfallen können. Hier leidet dann wiederum die Benutzerakzeptanz. Und Prozesse, die nicht eingehalten werden, sind immer ein Sicherheitsrisiko. Wichtig ist deshalb auch eine entsprechende Auswahl und Schulung des Personals.

Ein weiterer Punkt ist, dass man mit der Verwaltung immer auch das Risiko zentralisiert. Gelingt es jemandem, in das System einzudringen, so kann er grossen Schaden anrichten. Umso wichtiger ist deshalb bei zentralisierten Lösungen ein optimaler Schutz der Kernkomponenten und -prozesse.

## Wie erzielt man mit einer neuen SIM-Lösung möglichst rasch einen Return on Investment?

Die Einführung eines zentralen Identitätsmanagementsystems macht nur dann Sinn, wenn die Benutzeridentitäten auch wirklich von der Mehrheit der Anwendungen genutzt werden. Bleibt das System selbst eine Insellösung, sind die Kosten unter Umständen höher als der Nutzen. Trotzdem sollen bestehende Applikationen nicht einfach wahllos, sondern nach dem Pareto-Prinzip (80/20-Regel) integriert werden. Mit anderen Worten, es empfiehlt sich, mit etwa 20% des Aufwands 80% der Applikationen zu integrieren und sich den Aufwand von 80% für die letzten 20% zu sparen und diese Applikationen bei

Gelegenheit abzulösen. Erfahrungsgemäss haben Applikationen, die nur mit hohem Aufwand zu integrieren sind, mittelfristig sowieso kaum Überlebenschancen.

## Worauf muss bei der Einführung einer SIM-Lösung geachtet werden?

Bei der Einführung einer SIM-Lösung gilt es in erster Linie zu bedenken, dass Secure Identity Management nicht ein Produkt ist, sondern ein Prozess. In einem ersten Schritt muss deshalb ein firmenadäquater Prozess für die Verwaltung von Benutzeridentitäten definiert werden. In einem zweiten Schritt erst kann dann nach einer SIM-Software gesucht werden, mit der sich der definierte Prozess abbilden lässt. Das ist unter Umständen mit beträchtlichem Aufwand verbunden. Sorgfalt zahlt sich hier aber mittelfristig auf jeden Fall aus.

Ein weiterer wichtiger Faktor ist die Integration der SIM-Software ins Gesamtsystem. Denn nur wenn die neue Benutzeridentität effektiv unternehmensweit genutzt werden kann, lohnt sich die Investition. Hier empfiehlt sich die Einbindung neuer und bestehender Applikations- und Servicekomponenten über eine erprobte Integrationsplattform, welche eine sichere Propagation der generierten Benutzeridentitäten unterstützt. Längerfristig ebenso wichtig ist wie bei allen Infrastrukturkomponenten der modulare Aufbau und der Einsatz offener Standards. Sie erlauben eine investitionsschonende Integration neuer Technologien und standardkonformer Produkte anderer Anbieter und sorgen damit dafür, dass die neue Lösung nicht morgen schon von gestern ist.

ADNOVUM

AdNovum Informatik AG  
Röntgenstrasse 22  
8005 Zürich  
<http://www.adnovum.ch>

\* Christian Grob, Dipl. Informatik-Ing. ETH, ist Software Architect & Engineer bei AdNovum und befasst sich zurzeit mit der Integration einer SIM-Lösung in einem Schweizer Grossunternehmen.