Zentrale User-Verwaltung mit XENTIS Lightweight Directory Access Protocol

XENTIS unterstützt zwei verschiedene Single-Sign-on-Verfahren, so dass nach der erstmaligen Anmeldung durch den Benutzer im Firmennetzwerk eine weitere Anmeldung in XENTIS unnötig ist. Die Variante Silent-Sign-on wird durch das Lightweight Directory Access Protocol (LDAP) in Verbindung mit einer zentralen Benutzerverwaltung ergänzt.

AUSGANGSLAGE

Die Themen Benutzerverwaltung, Autorisierung (Vergabe von Benutzerrechten), Authentisierung (Nachweis eines Anwenders genau der Anwender zu sein, den er vorgibt zu sein in einem IT-System) und Authentifizierung (Prüfung der Authentisierung bzw. Identifikation des Benutzers durch ein IT-System) stehen im direkten Kontext zu IT-Sicherheit und sind somit auch für jede Unternehmensrevision relevant. Die jeweiligen Prozesse zur IT-Sicherheit sind im Detail zu definieren und wenn möglich, für sämtliche Applikationen einer IT-Landschaft anzuwenden. Beispielsweise ist aus Revisionssicht unbedingt sicherzustellen, dass unter dem Benutzerkonto eines Mitarbeiters, der ein Unternehmen verlassen hat, nicht nur keine weiteren Geschäfte abgewickelt, sondern mit dem Austritt auch sämtliche Berechtigungen gelöscht werden.

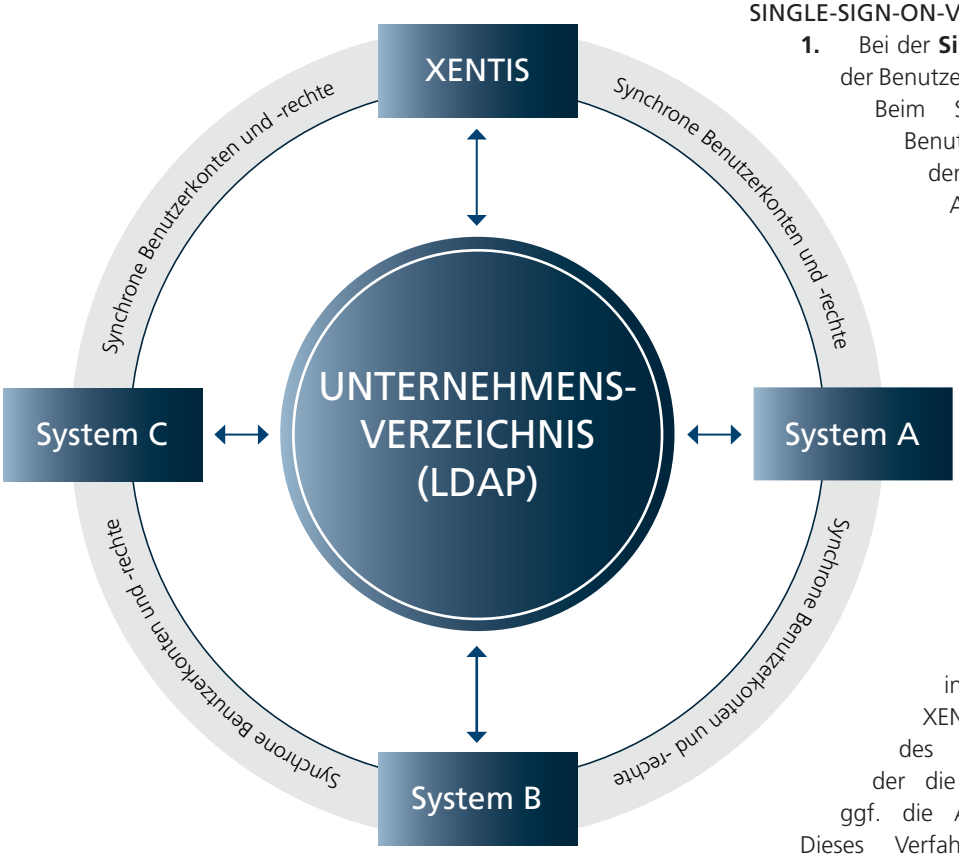

Abb. 1: Authentifizierung des Benutzers und Synchronisation der Benutzerkonten sowie der Benutzerrechte

SINGLE-SIGN-ON-VARIANTEN IN XENTIS

1. Bei der **Silent-Sign-on-Variante** authentisiert sich der Benutzer zunächst an seinem Arbeitsplatzrechner. Beim Start erhält der XENTIS-Client die Benutzerangaben, um die Verbindung mit dem XENTIS-Server aufzubauen. Ist die Authentifizierung des Benutzers durch den XENTIS-Server erfolgreich, kann der Benutzer sich in XENTIS ohne Eingabe des Passwords anmelden. Die Vorteile dieser Variante liegen in den geringen Kosten für die Einrichtung und der einfachen Inbetriebnahme. Sicherheitsaspekte werden jedoch nur in begrenztem Masse berücksichtigt. Aus diesem Grund kann die Silent-Sign-on-Variante um den Austausch von X.509-Zertifikaten erweitert werden. Für die Authentifizierung wird ein speziell eingerichteter Server in den Anmeldeprozess integriert. XENTIS reicht die Anmeldeinformationen des Benutzers an diesen Server weiter, der die Echtheit der Anmeldung prüft und ggf. die Authentizität des Benutzers bestätigt. Dieses Verfahren gilt zwar als fortschrittliches Authentifizierungsverfahren, erfordert jedoch eine speziell eingerichtete Infrastruktur. Diese Variante bietet

hohe Sicherheit und ist typischerweise revisionstauglich. Die automatische Entfernung des Benutzerkontos eines Mitarbeiters beim Austritt wird jedoch nicht vorgenommen.

2. Mit der **LDAP-Variante** kann die Authentifizierung und die Autorisierung in ein LDAP-Verzeichnis, z.B. das sehr verbreitete Microsoft Active Directory, verlegt werden. Die Benutzer- und Berechtigungsverwaltung erfolgt somit in einer zentralisierten Berechtigungsumgebung des anwendenden Unternehmens, d.h. Rollen werden Benutzern im LDAP-Server durch das für die Berechtigungsvergabe verantwortliche Personal zugewiesen. Die Definition der jeweiligen Rollen und deren Rechte erfolgt jedoch in XENTIS. Bei einem Login in XENTIS wird dann die Authentifizierung nicht von XENTIS vorgenommen, sondern als Anfrage an die zentrale Benutzerverwaltung gesendet. Diese Anfrage dauert kaum länger als eine direkt von XENTIS durchgeführte Authentifizierung. Neben der Authentifizierung werden gleichzeitig auch die in XENTIS definierten Rollen und deren Rechte mit den in der zentralen Benutzerverwaltung vergebenen Rollen synchronisiert (**Abb. 1**) bzw. vorgenommene Änderungen bei der Rechtevergabe unmittelbar in die Benutzerverwaltung übernommen. In Bezug auf das erwähnte Szenario eines Mitarbeiteraustritts wird hiermit die Löschung des Benutzerkontos gewährleistet. Diese Variante erfüllt höchste Sicherheitsstandards und gilt als vollumfänglich revisionstauglich.

FAZIT

Mit der Integration von LDAP in XENTIS eröffnet sich die Nutzung einer zentralen Benutzerverwaltung, der eine automatische Synchronisation mit den in XENTIS geführten Benutzern zugrunde liegt. So werden eine konsistente Berechtigungsvergabe und Benutzerkonten gewährleistet. Sofern Kunden ein alternatives Single-Sign-on-Verfahren bevorzugen, bietet XENTIS mit Silent-Sign-on eine weitere Variante an.

Für weitere Informationen
kontaktieren Sie bitte

Dr. Frank Jenner
Geschäftsleitung
+41 44 736 47 47
frank.jenner@profidata.com

SWITZERLAND
Bändliweg 30
8048 Zurich

GERMANY
Stephanstrasse 3
60313 Frankfurt am Main

LUXEMBOURG
5 Rue Gabriel Lippmann
5365 Munsbach

UNITED KINGDOM
New Derwent House
69-73 Theobalds Road
London, WC1X 8TA

SINGAPORE
75 High Street
Singapore 1794351

info@profidata.com
www.profidata.com