betasystems

AUTOMATISIERTES IDENTITY MANAGEMENT MIT SAM IN EINER VERZEICHNISBASIERTEN SICHERHEITSARCHITEKTUR

Referenzprojekt

EINE DER WELTGRÖSSTEN FLUGGESELLSCHAFTEN

AUTOMATISIERTES IDENTITY MANAGEMENT MIT SAM IN EINER VERZEICHNISBASIERTEN SICHERHEITSARCHITEKTUR

Einbeziehen aller sicherheitsrelevanten Systeme

Der internationale Luftfahrtkonzern verfügt über einen äußerst umfangreichen Mitarbeiterstamm, der auf mehrere Tochterunternehmen verteilt ist: Passagierbef örderung, Cargo, technischer Service, IT-Service und weitere. Aufgrund dieser weit verzweigten Struktur war es für das Unternehmen zunehmend schwierig geworden, die 160.000 Benutzer in den diversen Systemen und Anwendungen effizient zu verwalten.

Darüber hinaus benötigte das Unternehmen eine Provisioning-Lösung, um das Unternehmensverzeichnis stets aktuell zu halten und damit die Sicherheitsanforderungen des Unternehmens zu erfüllen und eine effektive Überprüfung zu ermöglichen.

Bei dem Luftfahrtunternehmen erkannte man, dass ein Identity Management-System benötigt wurde, um die Benutzerverwaltung zu zentralisieren und zu automatisieren. Die Aufgaben des neuen Systems bestanden darin, alle Benutzer- und Unternehmensdaten aus verschiedenen Quellen zu bündeln, zu verarbeiten und an die entsprechenden Zielsysteme weiterzuleiten.

Nach sorgfältiger Prüfung entschied sich das Unternehmen für SAM, da diese Lösung leistungsfähige Provisioning-Funktionalitäten bietet, höchst skalierbar ist und sich problemlos in eine verzeichnisbasierte Umgebung einbinden lässt. Mit SAM ist es zudem möglich, die vielfältigen im Unternehmen verwendeten Systeme zuverlässig zu integrieren.

Die Herausforderung

Der Konzern betreibt eines der weltweit größten Novell-Netzwerke. Daher musste eine IdM-Lösung gefunden werden, die hervorragend mit der Novell NetWare-Umgebung interagiert und zudem diverse unterschiedliche Systeme wie RACF, vier Windows NT-Domänen, ein SAP-System, das Unternehmensverzeichnis und andere LDAP-Verzeichnisse sowie drei unternehmensintern entwickelte Anwendungen (ein Unisys-basiertes Buchungssystem und zwei Mannschaftsverwaltungssysteme) einbinden kann.

Eine weitere Herausforderung bestand darin, dass alle 160.000 Benutzerprofile des Unternehmensverzeichnisses über 50 unterschiedliche Attributstypen pro Benutzer enthalten. Daher musste die Provisioning-Lösung in der Lage sein, eine Reihe von Eingangsquellen zu unterstützen und damit das Verzeichnis permanent aktuell zu halten, Sicherheitslücken zu vermeiden und eine präzise Überwachung der Abläufe zu ermöglichen. Diese Funktionen sollten ohne manuelle Eingriffe der Administratoren ausgeführt werden – daher war die vollständige Automatisierung der Abläufe erforderlich. Aus verwaltungstechnischen Gründen war es notwendig, die angebundenen Tochterfirmen innerhalb desselben IdM-Systems als eigenständige Unternehmen zu behandeln, da nur auf diese Weise die Vertraulichkeit des Datenverkehrs sowie eine saubere Administration sichergestellt werden konnte.

Das Unternehmen

Die Fluggesellschaft ist eines der weltweit größten und erfolgreichsten Unternehmen in der Luftfahrtbranche. Die Gruppe setzt sich aus sechs strategischen Geschäftsbereichen zusammen, die über 400 weltweit tätige Tochterfirmen und Partner umfassen. Passagierbeförderung und Cargo im In- und Ausland bilden die Kernbereiche.

Darüber hinaus bietet das Luftfahrtunternehmen ein breites Spektrum angegliederter Dienstleistungen wie Flugzeugwartung, Reparatur und Überholung (MRO, Maintenance, Repair and Overhaul), Catering, IT-Services sowie Schulung von Cockpit- und Kabinenpersonal. Die Bereiche Finanzen und Dienstleistungen sind ebenfalls in Tochterunternehmen ausgelagert. Dieses Dienstleistungsangebot richtet sich an Partner sowie andere Mitglieder der Allianz, der auch die Fluggesellschaft selbst angehört. In den letzten Jahren hat das Unternehmen im Zuge der zunehmenden Globalisierung der Luftfahrtindustrie verstärkt internationale Märkte erschlossen.

Die Umsetzung

Der erste Schritt

Um den ROI in möglichst kurzer Zeit zu erreichen, setzte der Konzern zunächst auf die Optimierung und Automatisierung der Benutzerverwaltung. Als erste Maßnahme wurden das Novell NetWare-Netzwerk, RACF sowie die Windows- und Unisys-Systeme an SAM angebunden und die Benutzerverwaltung der Konzerngesellschaft für Passagierbeförderung automatisiert.

Dabei wurden fünf Datenquellen mit SAM verbunden: zwei HR-Systeme, eine Datenbank externer Partner und zwei Datenquellen für unternehmensbezogene Informationen. Änderungen in diesen Systemen wurden an SAM übermittelt und anhand eines regelbasierenden Vorgangs in Benutzerkonten, Gruppenverbindungen sowie Autorisierungen der diversen angebundenen Sicherheitssysteme umgewandelt.

Implementierung des neuen Verwaltungskonzepts für weitere Tochtergesellschaften

Der erfolgreiche Produktivbetrieb des Systems für die erste Tochtergesellschaft ermutigte das Projektteam dazu, die umfangreiche Konzerngesellschaft Cargo in die Lösung mit einzubeziehen. Da sich mit SAM sehr einfach mehrere Organisationen innerhalb einer einzelnen IdM-Lösung verwalten lassen, konnte die hinzugefügte Tochtergesellschaft mühelos in die Verwaltung eingebunden werden. Gleichzeitig wurde SAP als weiteres Zielsystem integriert, um auch hier von der automatisierten Benutzerverwaltung zu profitieren.

Kontinuierliche Weiterentwicklung und Erweiterung der Lösung

Bereits im Jahr 2000 hatte sich die Gesellschaft für die Einführung von SAM Jupiter als IdM-Lösung entschieden. Im Laufe der Jahre kamen wesentliche neue Funktionen hinzu, darunter das Biometrische Passwort Reset über Voice Recognition, Self-Service-Funktionen, eine SPML-Schnittstelle für User-Daten sowie Integrationsmöglichkeit über Webservices.

Die permanente Weiterentwicklung mündete im Jahr 2011 in die Migration von SAM Jupiter auf SAM Enterprise, welches seit September 2011 produktiv läuft. Mit der neuen Version kann die Gesellschaft nun alle aktuellen Anforderungen im Bereich IdM optimal erfüllen. Man hatte auch Alternativlösungen evaluiert, sich aufgrund der langjährigen guten Zusammenarbeit mit Beta Systems aber dann dafür entschieden, beim bisherigen Technologielieferanten zu bleiben.

Im Laufe der Jahre wurde SAM zudem auf weitere Konzerngesellschaften ausgedehnt – inzwischen werden rd. 200.000 Beschäftigte der Gesellschaft und ihrer Konzerntöchter mit der Beta Systems Lösung administriert. Auch weitere Anwendungssysteme wurden nach und nach integriert, darunter als eines der letzten Peregrine Asset Center.

Die Lösung

Direkte Integration in Novell eDirectory über SAM eConnect

Das Unternehmen betreibt sein Unternehmensverzeichnis, das 160.000 Benutzer umfasst, auf Basis von Novell eDirectory. Die interne PKI (Public Key Infrastructure) und zahlreiche Anwendungen sind darauf angewiesen, dass die Benutzerdaten zuverlässig und zeitnah zur Verfügung stehen. Die Vorteile einer nahtlosen Integration der Provisioning-Lösung in das Unternehmensverzeichnis über den Standardkonnektor SAM eConnect lagen von Anfang an auf der Hand: Durch die Bündelung der Datenquellen und dank der leistungsfähigen Funktionen von SAM eConnect konnte eine häufige Aktualisierung der Benutzer, Benutzerattribute und Sicherheitsdefinitionen des Unternehmensverzeichnisses erzielt werden, die regelmäßig automatisiert durchgeführt wurde . Das Ergebnis: Die geschäftsprozessbezogene Sicherheitsverwaltung konnte zu 80% automatisiert werden.

SAM ermöglicht höhere Service-Level

Zusätzlich zu den oben beschriebenen Provisioning-Funktionen bietet bzw. unterst ützt SAM zahlreiche weitere Funktionalit äten zur Benutzerverwaltung. Zentrale Administratoren können beispielsweise SAM nutzen, um komplexe Verwaltungsaufgaben manuell durchzuführen. Supportmitarbeitern hingegen dient die Helpdesk-Funktionalität von SAM als bequeme Schnittstelle zum Einrichten und Löschen von Benutzern oder zum Ändern von Kennwörtern.

SAM Jupiter ist mit dem kundenspezifischen Intranetportal verbunden. Dadurch können Mitarbeiter und externe Partner, Konten und Benutzerrechte über einen abgestimmten Genehmigungsworkflow beantragen. Die bewilligten Konten- und Rechteanfragen werden an SAM übermittelt. SAM wiederum führt diese in den verbundenen Systemen und Verzeichnissen aus. Dieser Prozess gestattet es der IT-Abteilung, ihren Kunden eine sehr hohe Servicequalität anzubieten: Dank der technischen Einbettung eines Workflowsystems in SAM können alle Sicherheitssysteme bereits wenige Minuten nach der der Erteilung der Genehmigung aktualisiert werden.

Zuverlässige Überprüfung mit SAM

Unter Einsatz der plattformübergreifenden Berichterstellungs- und Überwachungsfunktionen von SAM kann der konzerneigene ITDienstleister vollautomatisch monatliche Prüfberichte erstellen, die alle relevanten Benutzer- und Sicherheitseinstellungen enthalten, und diese per E-Mail an die jeweils verantwortlichen Unternehmensmanager schicken. Pro Konzerngesellschaft wird zudem für die Sicherheitsadministratoren der unterschiedlichen Zielsysteme ein wöchentlicher Bericht über geänderte Benutzerattribute und deaktivierte bzw. gelöschte Konten generiert.

Aufgrund der zentralisierten und automatisierten Benutzerverwaltung ließen sich in der Administration erhebliche Kosteneinsparungen erzielen. Mit SAM verfügt die Fluggesellschaft über eine homogene Provisioning-Lösung für das Unternehmensverzeichnis und die strategischen Sicherheitssysteme. SAM versorgt alle angebundenen Systeme zuverlässig und zeitnah mit den benötigten Benutzerdaten.

Dank SAM ist es der Fluggesellschaft möglich, die umfassende Benutzerverwaltung effizient durchzuführen und den übrigen Konzerngesellschaften einen hohen Service-Level zu garantieren. Die hohe Skalierbarkeit von SAM macht es außerdem möglich, die aktuelle Lösung beliebig um weitere Konzerngesellschaften oder externe Kunden zu erweitern, was die TCO sehr positiv beeinflusst.

Migration auf SAM Enterprise

Von der Migration auf das neueste Release der IdM-Lösung von Beta Systems profitiert die Luftfahrtgesellschaft in zweierlei Hinsicht: Zum Einen fügt sich die SAM Enterprise Architektur optimal in die neue Zielarchitektur des Konzerns ein. Dieser hatte unlängst einen Plattformwechsel hin zu Microsoft vollzogen. Während SAM Jupiter auf einer Mainframe-Plattform basierte, läuft SAM Enterprise auf dezentralen Servern und nutzt dabei auch Microsoft-Datenbanken. Weil der Betrieb von SAM in einer dezentralen Microsoft-Architektur wesentlich günstiger ist als auf Mainframe-Basis, spart die Gesellschaft durch den Wegfall der Mainframe DB2 und die Einführung von SAM Enterprise nun auch deutlich Kosten.

BERLIN | KÖLN | NEUSTADT | CALGARY | WASHINGTON D.C. | PARIS
MADRID | LONDON | STOCKHOLM | MAILAND | BRÜSSEL | WIEN | ZÜRICH

BETA SYSTEMS SOFTWARE AG | ALT-MOABIT 90D, 10559 BERLIN | WWW.BETASYSTEMS-IAM.DE