Migros

Zentrales SAP-Portal für Lieferanten

Für viele Schweizerinnen und Schweizer ist die Migros fester Bestandteil ihres Lebens: Täglich kaufen rund 1,4 Millionen Kunden in den Super- und Fachmärkten des 1925 gegründeten Traditionsunternehmens ein. Migros ist mit rund 84 000 Mitarbeitern gleichzeitig der größte Arbeitgeber des Landes. 2008 erwirtschaftete der Konzern einen Gewinn von 701 Millionen Franken und der Marktanteil lag erstmals über 20 Prozent.

Der Eintritt internationaler Handelsketten in den Schweizer Markt konfrontiert auch die Migros mit einem verschärften Wettbewerb. Die erhöhte Dynamik und der damit verbundene Preiskampf haben den Konzern bereits vor einigen Jahren veranlasst, eine prozessorientierte Strategie für die einheitliche Warenbewirtschaftung zu verfolgen und die IT-Systeme mit SAP for Retail zu vereinheitlichen. Um besonders die Prozesse für die Angebotserstellung effizienter zu gestalten, sollten 2008 die nationalen und internationalen Lieferanten die Möglichkeit erhalten, ihre Angebote direkt in SAP einzugeben und an Auktionen teilzunehmen.

Zentrales SAP-Portal mit vorgelagerter Authentisierung

«Die Ziele waren klar: Einfacher Zugang für unsere Lieferanten zum Supplier Replenishment von SAP», sagt Peter Rieder, Leiter IT-Infrastruktur Dienste bei den Migros IT-Services. «Aus IT-Perspektive ergaben sich folgende Herausforderungen: Sichere Authentifizierung und Zuweisung von Berechtigungen, Schutz der internen SAP-Server vor unberechtigten Zugriffen und Anwenderfreundlichkeit durch die Integration der Backend-Systeme in ein zentrales Portal.»

Die SAP-Server für Lieferanten direkt über das Internet bereitzustellen, war keine Option. Die Migros hätte dafür sorgen müssen, dass die Zulieferer die entsprechenden Kommunikationsports geöffnet haben. Bei den vielen weltweit verteilten Unternehmen wäre dies ein immenser Aufwand und ein grosses Sicherheitsrisiko, denn jeder Server müsste eine öffentliche IP-Adresse haben. Zudem sollten die Backend-Systeme unter einer einzigen prägnanten URL erreichbar sein, um die Handhabung zu erleichtern.

Obwohl die Migros über eine eigene Certificate Authority und Public Key Infrastructure (PKI) verfügt, wollte man den Unternehmen die Verwendung bestimmter Client-Certificates nicht vorschreiben und weitere Authentisierungsmethoden unterstützen. «Client-Certificates, wie sie bei der Migros intern im Einsatz sind, bieten ein hohes Mass an Sicherheit», sagt Peter Rieder. «Wenn man Lieferanten auf der ganzen Welt hat, braucht man eine sichere, aber auch einfache Lösung. Certificates sind ohne Zweifel sicher, aber nicht unbedingt einfach. Wir wollten vermeiden, einem chinesischen Lieferanten die Installation auf seinem PC erklären zu müssen. Deshalb gehörten alternative Authentisierungsmethoden mit abgestuften Berechtigungen zu den Grundanforderungen.»

Flexibler Single Sign-on für Lieferanten mit Airlock WAF

Das IT-Team der Migros stiess in der Evaluationsphase schnell auf die Web Application Firewall Airlock WAF, wie Peter Rieder bestätigt: «In anderen Bereichen hat die Migros Alternativprodukte im Einsatz. Daher kannten wir deren Limitierungen und wussten, dass sie nicht die geforderte Flexibilität bieten. Airlock WAF war uns bereits im Rahmen unserer Marktbeobachtung aufgefallen – mit dem SAP-Portal-Projekt war jetzt auch ein Einsatzszenario da.»

Im Vergleich mit dem Wettbewerb überzeugte die flexible Unterstützung verschiedener Authentisierungsmethoden für Single Sign-on auf dem SAP-Portal. Im Rahmen der vorgelagerten Authentisierung melden sich Anwender heute mit einem Client-Certifcate, mit Login/Passwort oder in Kürze auch mit einem One Time Passwort (OTP) bei Airlock WAF an. Die Berechtigungen werden entsprechend vergeben: In einem Meta-Directory sind alle internen und externen Anwender erfasst. Pro Applikation gibt es eine Gruppe, wobei Lieferanten einer oder mehrerer dieser Gruppen angehören können. Über LDAP-Server und Meta-Directory überprüft Airlock WAF das Certificate und die Gruppenzugehörigkeit

des Anwenders, um die Applikationen freizugeben. Bei Verwendung eines OTP kontrolliert Airlock zunächst Login/Passwort im Meta-Directory und zusätzlich die Challenge auf dem Token-Server. Insgesamt unterstützt Airlock WAF drei Authentisierungsmassnahmen, die voraussichtlich noch durch einen anonymen Zugriff mit stark reduzierter Berechtigung ergänzt werden.

Verschiedene Certificates und Login-Mapping

Certificates von Lieferanten, die nicht von Migros stammen, werden auf dem Meta-Directory installiert, sodass die Gültigkeit jederzeit geprüft werden kann. Besteht keine Lieferantenbeziehung mehr, wird das Zertifikat im Meta-Directory gelöscht. «Dieses Verfahren erfordert einige Flexibilität von Airlock WAF, da unser Tree im Meta-Directory nicht genau den Angaben auf dem Certificate entspricht. Die Lösung hat sich jedoch im Betrieb bewährt und funktioniert bestens.» Eine weitere gelöste Herausforderung: Die Migros schreibt als Login die Verwendung der Mail-Adresse vor, während SAP für Logins weder das @-Zeichen noch mehr als 8 Buchstaben unterstützt. Deshalb übernimmt Airlock im Meta-Directory das Mapping der Logins auf SAP-Anwendernamen.

Nach der erfolgreichen Authentisierung gelangen die Lieferanten auf das zentrale SAP-Portal, hinter dem sich die einzelnen Server verbergen. Die Anwender erhalten dabei nur Zugriff auf die für sie freigegebenen Funktionen.

Alle URLs führen auf Airlock WAF

Von aussen betrachtet führen alle Links immer auf Airlock WAF, was den direkten Zugriff auf die SAP-Server verhindert. Die Basis dazu ist das Umschreiben aller internen URLs durch Airlock WAF. Dies ist möglich, obwohl SAP absolute URLs verwendet und nicht von sich aus Reverse-Proxy-fähig ist.

Das Suchen und Umschreiben der URLs sowie die Anpassung der Filter stellt nach Einschätzung von Peter Rieder die grösste Aufgabe bei der Implementierung dar: «Natürlich ist das eine komplexe Aufgabe, die wir aber gemeinsam mit dem Airlock-Support gut bewältigt haben. Die grosse Kompetenz des Airlock-Teams war dabei sehr hilfreich.»

Trotz der reibungslosen Umsetzung blieb eine Frage offen: Was passiert bei einem grösseren SAP-Update? «Ich kann aus Erfahrung sprechen, weil wir kürzlich genau einen solchen SAP-Update durchgeführt haben. Lediglich zwei Regeln mussten auf Airlock WAF angepasst werden, alles andere lief problemlos weiter», sagt Peter Rieder.

Airlock bei Migros: Mehr als SAP

Das zentrale SAP-Portal und die vorgelagerte Authentisierung für die Lieferanten sind nicht die einzigen Einsatzbereiche: So werden zum Beispiel Rechnungen für Migros-Industrieunternehmen eingescannt und elektronisch auf einem Server abgelegt. Über einen Workflow werden dann jeweils von verschiedenen Personen die nötigen Kontroll- und Genehmigungsvisa erteilt. Um sicherzustellen, dass es sich dabei um die richtigen Anwender handelt, wird Airlock WAF zur Überprüfung der Certificates eingesetzt.

Darüber hinaus soll das Portal um zusätzliche SAP-Applikationen aus dem Marketing-Bereich und weitere Prozesse erweitert werden. Langfristig soll sich den Anwendern per Single Sign-on eine ganze Welt von Funktionalitäten erschliessen: «Konkret geht es um die Integration von SAP und Microsoft SharePoint in ein übergeordnetes Portal. Deshalb haben wir bereits in der Evaluierungsphase auf eine mögliche Unterstützung von Kerberos geachtet – was uns Ergon als einziger Hersteller verbindlich zusagen konnte», sagt Peter Rieder.

Die Machbarkeit bewies das Airlock-Team durch einen Proof-of-concept, der in einem Tag umgesetzt wurde. Anhand des Certificate identifiziert Airlock WAF den Benutzer und seine Berechtigungen und löst daraufhin ein Kerberos-Ticket vom Domain Controller. Mit diesem Ticket gelangt der Anwender auf Microsoft SharePoint. Gleichzeitig wird es für die Anmeldung beim SAP-Portal verwendet. Das Handling der Session-Zugriffe erfolgt über Cookies. Dazu Peter Rieder: «Auf diesem Weg können wir mit Single Sign-on und Certificates zwei Anwendungswelten zusammenbringen. Airlock WAF hat auch hier in kurzer Zeit überzeugt.»

Beste Zusammenarbeit

Im Verlauf komplexer Projekte treten unweigerlich Herausforderungen auf, die nicht nach «Schema F» gelöst werden können. Die Zusammenarbeit mit einem lokalen Hersteller bringt gemäss Peter Rieder eindeutige Vorteile: «Ein Hersteller in der Nähe ist Goldwert. Nicht nur die geografische Nähe wirkt sich positiv aus, sondern auch der selbe kulturelle Hintergrund, wie zum Beispiel die Ansprüche an Qualität. Das Engagement für die Umsetzung von Kundenwünschen ist nach meiner Erfahrung ebenfalls höher. Airlock ist der beste Beweis dafür.»

Über Ergon Informatik AG und Airlock Suite

Die 1984 gegründete Ergon Informatik AG ist führend in der Herstellung von individuellen Softwarelösungen und Softwareprodukten. Die Basis für unseren Erfolg: 235 hoch qualifizierte IT-Spezialisten, die dank herausragendem Know-how neue Technologietrends antizipieren und mit innovativen Lösungen Wettbewerbsvorteile sicherstellen. Ergon realisiert hauptsächlich Grossprojekte im B2B-Bereich.

Die Airlock Suite kombiniert die Themen Filterung und Authentisierung in einer abgestimmten Gesamtlösung, die punkto Usability und Services Massstäbe setzt. Das Security-Produkt Airlock ist seit dem Jahr 2002 am Markt und heute bei über 300 Kunden weltweit im Einsatz.

ergon

Ergon Informatik AG
Merkurstrasse 43
CH–8032 Zürich

+41 44 268 89 00
www.airlock.com
twitter.com/ErgonAirlock