Migros

Centralised SAP portal for suppliers

Migros is an integral part of daily life for many residents of Switzerland. Eachday around 1.4 million customers shop in the supermarkets and stores run by this long-standing business founded in 1925. At the same, Migros is also the largest employer in the alpine country employing some 84,000 people. In 2008 the group posted profits of 701 million Swiss francs and for the first time in their history achieved more than a 20 percent market share.

However, following the entry of international commercial chains into the Swiss market, Migros was confronted with increasing competition. The increased dynamics and the ensuing price war forced the group to adopt a uniform merchandise management system and to standardise its IT systems using SAP for Retail. In order to make the process for bid proposal management more efficient, both national and international suppliers were given the opportunity (from 2008) to submit their offers directly into the SAP system and take part in auctions.

Centralised SAP portal with preceding authentication

"The specifications were clear: simple access for our suppliers to SAP's Supplier Replenishment system," says Peter Rieder, manager of IT infrastructure services at Migros IT Services. "The following challenges resulted from an IT perspective: secured authentication for users and allocation of access authorisation; protection of the internal SAP server against unauthorised access attempts, and user-friendliness by integrating the diverse back-end systems into one centralised portal."

It was not a viable option to make the SAP server directly available to suppliers via the Internet, particularly as Migros would then have had to ensure that the suppliers opened the corresponding communication ports. In view of the high number of companies spread across the globe this would have been a tremendous expense as well as a security risk, as each server would have a public IP address. Furthermore in order to simplify the operations, the back-end systems needed to be accessible under a single succinct URL.

Although Migros has its own Certificate Authority and Public Key Infrastructure (PKI), one did not wish to dictate the use of specific client certificates to the companies or to support additional authentication methods. "Client certificates – as they are used by Migros internally – guarantee a high level of security," commented Peter Rieder. "If a company has suppliers across the globe, then it needs a safe yet straightforward solution. Certificates, whilst no doubt secure, are by no means simple. We wanted to avoid having to explain the installation on a Chinese PC to a Chinese supplier, so we specified the requirement for alternative authentication methods with staged authorisation specificat."

Airlock WAF supports flexible Single sign-on for suppliers

The Migros IT team keeps abreast of new technology, and came across the Web application firewall Airlock WAF during the course of its investigations, explained Peter Rieder: "Migros already uses alternative products in other areas so we were already aware of their limitations and that they could not offer us the required flexibility. Our attention had previously been drawn to Airlock WAF. As part of our ongoing market observations – and once the SAP portal project got underway."

While making competitive comparisons, we were convinced by Airlock's flexible support for different authentication methods for single sign-ons into the SAP portal. Currently, under the preceding authentication, users login to Airlock WAF with a client certificate and login/password – in the near future they will also be able to login with one time passwords (OTP). Authorisations are assigned accordingly: All internal and external users are captured in a meta-directory. There is one group per application and suppliers can be in one or several of these groups depending on their authorisation levels. Airlock WAF checks the certificate and the user's group affiliation via the LDAP server and meta directory before releasing the application. If an OTP is being used, then

Airlock WAF checks the login/password in the meta directory first as well as the challenge on the token server. Airlock currently supports three authentication methods, most likely these will be complemented by an anonymous access with significantly reduced authorisation.

Different certificates and login-mapping

Certificates from suppliers, that do not originate from Migros, are installed on the meta directory, so that Migros can check their validity at any time. If a supplier is no longer current, then the certificate is deleted from the meta-directory. "This procedure demands a lot of flexibility from Airlock WAF because our tree in the meta-directory does not correspond exactly to the respective specifications on the certificate. However the solution has proven itself in practice and works perfectly." Another obstacle that has been successfully negotiated is that Migros stipulates the use of the mail address is used to login, but SAP supports neither the @-sign nor more than eight letters for logins. Airlock WAF thus maps the logins in the meta directory to SAP user names.

Following the successful authentication, suppliers access the central SAP portal behind which the individual servers are installed. Users are only given access to those functions for which they are authorised.

All URLs lead to Airlock WAF

Viewed from the outside, all links always lead to Airlock WAF so direct access to the SAP server is prevented. This is possible as Airlock WAF rewrites all internal URLs and works even though SAP uses absolute URLs and is therefore not capable of reverse-proxy in itself.

According to Peter Rieder the biggest challenge facing the implementation is, the searching and rewriting of the URLs as well as the filter adaptations: "This is, of course, a complex issue that we have managed to resolve together with the Airlock WAF support team."

Despite the smooth implementation one question remained unanswered: What would happens when SAP releases a major update? "We recently implemented just such a SAP update at Migros and I can therefore speak from experience." said Peter Rieder. "The result was that only two rules had to be adapted on Airlock WAF, everything else continued to run smoothly."

Airlock at Migros: more than SAP

A centralised SAP portal and preceding supplier authentication are important areas of use for Airlock at Migros, but by far not the only ones. For example, invoices (for Migros industrial companies) are scanned and saved in electronic format on the server. Different people are then assigned the necessary controll and approvals via a workflow. In order to ensure that it is the correct user, Airlock checks the certificates here.

There are also plans to expand the portal with additional SAP applications within the marketing area and other processes. In the long-term users should be able to access a whole "world" of functions using single sign-on: "In specific terms, the first issue is the integration between SAP and Microsoft Sharepoint on one presiding portal. Therefore, during the evaluation phase, we made sure that Kerberos can also be supported – and Ergon is the only manufacturer that could guarantee this for us," said Peter Rieder.

The Airlock team has already proven that this can be achieved with a proof-of-concept that was, according to Migros, implemented in just one day. Airlock uses the certificate to identify the user and the user's authorisations and then releases a Kerberos ticket from the domain controller. The user requires this ticket to access Microsoft Sharepoint and in this specific instance it can also be used to register on the SAP portal. The session access is run via cookies. "We have managed to merge two application worlds using single sign-on and certificates. It did not take Airlock very long to convince us of its capability in this area," commented Peter Rieder.

Exemplary teamwork

During the course of complex projects challenges inevitably arise which cannot be resolved by consulting the manual – and at times like this the hour strikes for support. Working with a Swiss manufacturer is, according to Peter Rieder, advantageous in several different ways: "Looking back, I have to say that having a manufacturer close by is extremely beneficial. It is not just the geographical proximity that is a plus, but also the same cultural background, which includes for example, the same quality expectations. My experience has also shown that the commitment to implement the customer's wishes is also higher. Airlock is living proof of this."

About Ergon Informatik AG and Airlock Suite

Founded in 1984, Ergon Informatik AG is a leading developer of bespoke software solutions and products. The cornerstone of our success: 235 highly qualified IT specialists who are committed to creating value for the client, anticipating technological trends and designing solutions that generate competitive advantage. Ergon focuses on implementing major B2B projects.

Airlock Suite deals with the issues of filtering and authentication in one complete and coordinated solution – setting standards for usability and services. Airlock, our security product, was launched on the market in 2002 and is now used by 300 customers around the globe.

ergon

Ergon Informatik AG
Merkurstrasse 43
CH–8032 Zürich

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