



Basel-Stadt

zid

phion in use at Basel's central computing centre: Web Applications Enjoy Special Protection

The central computing centre for Basel, the "ZID" - provides important services for all of the canton's offices and departments. The primary focus here is upon maintaining centralised databases and cross-section applications, running the central computing administration as well as upholding and managing the canton's communications network. Besides this the ZID also provides its customers with diverse web-based applications for daily work. With such high security and availability requirements the ZID uses airlock to protect its web-applications

The ZID has, as an across-the-board service provider, diverse responsibilities and tasks: For example they run the canton-wide data network for Basel (DANEBS), the canton, the town and two municipalities, a telephone combine, in which the university is also financially involved, mail systems and web services and even a security skills centre. ZID mainly offers its services to over 100 offices in the seven departments as well as diverse administrative institutions. The 280 buildings are all networked with approximately 8 000 end devices, the number of supported telephones add up to over 10 000 - with the exception of hospitals. The ZID, which also includes the fiscal authorities, has a total of some 100 employees. Decisive success factors for the ZID are not only the high deliverability, but also the high reliability and above-average quality. Because no compromises of any kind can be entered into when it comes to IT security.

Security for e-Government

DANEBS, the data communications infrastructure for the administration, is based on fibre optic cables and TCP/IP-technology. The network is protected by firewalls. The network operation, along with the respective firewall infrastructure and the security zones all form the basic network services together with the mail backbone and the network-related directory services which are run by the Infrastructure department and managed

by Hans-Peter Bieger. A special architecture model was defined for the e-Government applications in 2002. In order to meet the required security standards, the ZID planned not only to use firewalls in the outermost periphery, but also reverse proxy. The proxy server preceding the web servers process all incoming connections from the Internet and respond to the corresponding requests either completely autonomously or forward them on to the next level web servers.

airlock replaces Open Source

"The existing firewall infrastructure was pretty out of date, so we had to completely revise and restructure it as part of the e-Government project", explains Hans-Peter Bieger. "Once we had developed extensive specifications, we found the partner to realise this project, by means of an invitation to tender, at Siemens AG. When it came to the issue of Reverse-Proxy our technology partner recommended airlock as the ideal solution for us." Following thorough reviews of the various different tenders, ZID opted initially for an open source package - mainly for financial reasons "After about one year, it was apparent that we could not run the Open-Source solution as we had envisaged and that important functions were just not available", recalls Hans-Peter Bieger. This was when the decision fell in favour of airlock.

phion



One of the ZID office buildings in Basel, Source: ZID

However, the cost factor still represented a certain hurdle, so ZID and phion agreed upon an innovative rental model which cost roughly the same as an Open-Source solution.

A major role in many sub-projects

Replacing the Open Source solution with airlock was a smooth and unproblematic procedure. A good year later a major new project was started in which airlock once again assumed a very central role. The first sub-project "Intranet for Extranet" involved setting up an authentication platform for extranet networks that corresponded to the canton administration's strict Security Policies. Administration-related organisations - such as for example hospitals or the BVB - were thus granted access to the administration's intranet. The objective of the second sub-project was the introduction of remote access for the administration. Now users can access diverse applications quite simply via the official and publically accessible homepage using their personal login and protected by airlock. Both subprojects were realised by the phion partner ISPIN.

"The next two subprojects are currently both in the deployment or planning phase. One of these involves broadening access to the intranet to include additional user groups outside of the administrative network. The other plans to implement alternative authentication procedures, which we are examining at present." The applications protected by airlock at the ZID have been monitored continually since their introduction. In order to be authorised users must be successfully authenticated via authorised connections. Multilevel filters automatically identify and block unauthorised access or manipulation attempts. Or in other words: With airlock the canton administration for Basel has the most advanced and most effective mechanisms for guaranteeing the security and availability of their web applications.



Hans-Peter Bieger
Infrastructure Manager at the ZID in Basel