

Allgemeine Bausparkasse



Building security

The Allgemeine Bausparkasse reg. Gen. m. b. H uses SecureWave software for comprehensive data security

Investments are confidential. This applies both to financial securities and building society savings accounts. For banks this means in concrete terms that, because almost all information is in electronic form, their systems must be as secure as the Mona Lisa in the Louvre. For the building society the Allgemeine Bausparkasse, which has its headquarters in Vienna, the "NT2XP" project – the upgrade of its IT system to Windows XP – came at just the right time to allow it to tighten its IT security. "Extremely satisfied" is project team member Thomas Aumüller's reaction to the implementation of Sanctuary Application Control and Sanctuary Device Control software from SecureWave. The IT department has full control over system security, with the close cooperation of the individual departments. The white list principle means that only approved applications and devices are authorised on an individual basis for users. This also applies to the mobile computers used by salespeople in the field. Security breaches resulting from unauthorised applications being installed by employees without the consent of the building society or data downloads via USB ports have become a thing of the past.

The Allgemeine Bausparkasse (ABV) was founded in 1929, which makes it

the oldest building society in Austria. As a result of collaborations with banks and insurance companies its current clientele is far more varied than you might suspect from the original purpose for which the building society was set up. The society's 600,000 or so building savings contracts are managed by around 230 permanent employees, including the field sales force, and numerous partners. The ABV itself admits that it has "a soft spot for younger savers" and therefore offers special youth accounts with staggered savings amounts and significantly reduced charges. Some young people may find that the dream of owning their own home will become a reality sooner than they had imagined. The employees of the ABV are ready to provide advice and support for customers all over Austria, from Vorarlberg to Vienna and from Upper Austria to Carinthia.

Thomas Aumüller, system manager for the Windows environment at the Allgemeine Bausparkasse, explains the building society's requirements, "What we needed was a comprehensive and yet unobtrusive security solution for hardware and applications. We also had to ensure that notebooks did not present a security risk when they were reconnected to the corporate network." Following an internal selection process the decision was made to implement Sanctuary Application Control and Sanctuary Device Control from the Luxembourg software supplier SecureWave. SecureWave's implementation partner IBV Informatik from the Swiss town of Urdorf bought 250 licences. According to Aumüller: "The competition's products didn't make the grade, not only because of the price, but also because of technological and operational shortcomings." The building society came across SecureWave by (a lucky!)

chance on the web. In the meantime the NT2XP project was successfully completed in April 2005. The Sanctuary products have been running for a few months longer.

Working from 8.00 until 18.00

The principle behind the Sanctuary product range is as simple as it is effective. The software does not distinguish between good and bad applications and devices, but works only on the basis of an existing authorisation from the IT department. This principle is called the white list procedure. For employees who provide consultancy services to customers this means that, as part of their everyday work, they can access customer data, spreadsheets and e-mail applications, but cannot download data to USB sticks. These are generally used only by the field sales force, whose laptops are only intended for business use, which does not include private computer games. It's even possible to set up restrictions for specific brands or times of day. For example, iPacs can only be synchronised during specific periods of time and the use of scanners is also restricted. It's possible to read, but not write DVDs. There are many more similar examples, but the approach is already clear: not a fundamental block, but targeted availability for devices and applications.

Two members of the IT team at the ABV spent just a single day installing Sanctuary on the system and ensuring that it ran smoothly. Before the installation took place, a large amount of advance planning work was carried out, in order to identify the parameters to be defined. Which applications does each department need? How

will exceptions be handled? Where are external devices, such as PDAs, USB sticks, digital cameras etc., being used? Numerous meetings were held with each department in order to be able to answer questions of this kind.

In the best society

Sanctuary software simply needs to be installed on Windows SQL Server. The administrator creates a white list and manages it. This access control list includes all the files that can be executed. If an employee logs onto his workstation and wants to use a device (for example, a USB stick) or an application (for example, the

customer database), the Sanctuary client automatically sends a query to the server. If the server has an identifier for the product in question, the employee is allowed to use it. The procedure is the same if there is no identifier, but the outcome is different. Even laptops are protected, because computers not connected to the network have a local copy of the most recent list of HASH codes (permitted applications and devices). The list is updated when the computer is connected to the network again.

The option of setting up user groups considerably reduces the administrative workload. Updates

and new rules are deployed centrally using Enteo software. When the white list principle was first implemented, the support hotline telephones were, of course, busy for a while. Despite the fact that employees had been introduced to the new system, it took a little time before everyone understood the consequences. But in the end it was the system's success throughout the organisation that counted: "It is very difficult to express this in figures, but we are convinced that our IT system is more secure than it was before," says Thomas Aumüller in conclusion. And the people who will benefit the most from this are the building society's customers.



SecureWave
Safeguarding Tomorrow

www.securewave.com
info@securewave.com

North America

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America
+1 (703) 713 - 3960 Phone
+1 (703) 793 - 7007 Fax

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom
+44 (0) 1908 357 897 Phone
+44 (0) 1908 357 600 Fax

Continental Europe and Rest of World

Atrium Business Park
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364-11 Phone
+352 265 364-12 Fax

© 2007 SecureWave SA. SecureWave and Sanctuary are registered trademarks of SecureWave SA. All third party trademarks are the property of their respective owners.