

Berliner Verkehrsbetriebe



Secure Network

Windows XP only with SecureWave: Berliner Verkehrsbetriebe (BVG) uses Sanctuary Device Control to manage mobile storage devices

Daily transport in Berlin is a major undertaking. In a city which is constantly on the move, managing journeys that equate to 18 circumnavigations of the earth every day and transporting around one billion passengers every year is by no means a straightforward matter for the public transport company BVG. The company's IT systems must also function perfectly to ensure that no errors occur in timetabling and resource planning and also in ticket sales.

When BVG migrated to Windows XP, it was therefore essential to close any security loopholes in advance. After testing a range of software products, the IT department chose Sanctuary Device Control by SecureWave. "It was the right route to take. Without SecureWave, Windows XP would have represented far too great a risk. Now we have full control over the access points for mobile storage devices. In practice this means that we know who is using specific devices and can authorise usage in individual cases," says Ingo Walther, project manager at BVG.

Mobility is taken for granted in Berlin. No one is more aware of that than the largest local public transport company in Germany, which transports tens of thousands of tourists across the city every year, including during major

events such as the Football World Cup.

But in the IT environment, mobility is a double-edged sword. USB sticks, MP3 players and digital cameras are brought onto company premises every day by employees and by business partners. The company is responsible for deciding to what extent they can be used in the workplace. The downside is that undesirable executables, such as malware, can find their way onto the system and open access to the network can put the entire system at risk. It is therefore important to take the preventive measure of protecting all the ports. However, this is exactly the problem that is frequently encountered when migrating to Windows XP. Berliner Verkehrsbetriebe therefore began looking for a solution and chose Sanctuary Device Control.

Following new routes

Sanctuary Device Control is based on the whitelist principle, where an access control list (ACL) is used to define which employees or user groups can work with specific peripherals, regardless of whether they are stationary or mobile. All other devices are blocked by default. If an employee attempts to connect a USB stick to a PC in order to copy data to it, he or she will find that this is not possible as the USB stick can only be used when it has been authorised centrally by the IT department. The unmonitored use of external devices such as mobile storage media, can have rapid and unpredictable consequences. On the one hand it is possible for viruses and other harmful programs to make their way onto the company's network from USB sticks or MP3 players without the user being aware of their presence. On the other hand internal data can be downloaded in a matter

of seconds and passed on to third parties. Managing the system centrally allows the unwanted exchange of data to be prevented and, in addition, helps to meet legal data protection requirements.

Sanctuary has been installed by BVG's internal IT team on all of the company's 3300 computers as part of the "New client operating system" project, which involves a migration from Windows NT 4.0 to Windows XP. "We decided on Sanctuary Device Control because of its excellent central management features, the easy integration into Active Directory and the available settings for interfaces and peripherals. For us the product was the best solution in terms of both technology and cost," says Ingo Walther, the BVG project manager. In January 2006 the migration was completed.

Ease of use

"Choosing Sanctuary also proved to be the right decision when it came to live operation," explains Ingo Walther. "Of course we had to set up authorisations for individual employees, but this is generally a one-off process and is easy to manage centrally because of the interface to Active Directory."



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.