SecureWave
Safeguarding Tomorrow

by SecureWave
Sanctuary
Device Control

Diakoniekrankenhaus Rotenburg

The Diakoniekrankenhaus Rotenburg chooses software from SecureWave to protect its data

Service and security are two things which are sadly often mutually contradictory. For example, mobile storage devices such as USB sticks, iPods and PDAs have opened up huge opportunities both in private and in business life. Data can be easily transported, forming the basis for a mobile workplace. However, the negative aspect of this is the "open" network, where there are no security measures in place, enabling third parties and unauthorized people to access internal company data. If an organization is too trusting and does not provide any protection for its USB and Firewire ports, tiny storage devices, small enough to be hidden in a ballpoint pen or a watch, can be used to download several gigabytes of data in a matter of seconds. The fact is that it is very difficult to maintain control over every computer at all times. Someone can come into the building and simply sit down at a computer. There are huge potential risks, particularly in a hospital where so many people are constantly coming and going.

However, this should not mean that the use of external devices should be completely blocked, otherwise completing everyday tasks would be like running an obstacle course. More important is central management and a central concept for every department. A security approach using the whitelist principle involves setting up an access control list (ACL) for every individual computer which specifies and implements all the individual authorizations. It's no longer possible to simply plug-and-play using the device of your choice. The Diakoniekrankenhaus Rotenburg chose this proactive approach with the help of Sanctuary Device Control software from SecureWave. In the future, only devices that have been authorized in advance, such as USB sticks, digital dictation machines, CDs and digital cameras, can actually be used. All other devices are strictly blocked and cannot be used to read or to store data. It is also possible to identify a specific product and to authorize its use for only one user. The solution provides protection not only against the inadvertent introduction of viruses and other harmful software to the hospital network, but also against the theft of the hospital's highly sensitive data.

Digital care

The Diakoniekrankenhaus Rotenburg is a state-of-the-art hospital, both in medical and technological terms. Around 100,000 in-patients and out-patients are treated every year in its 19 clinics by 2000 employees and more than 15,000 operations are carried out each year. From an IT perspective, this involves managing more than 800 networked PCs, plus 70 notebooks, PDAs etc.

The planning process for the installation of Sanctuary is currently underway and the necessary products are being defined by the individual departments. "You can't buy a ready-made IT security solution. It's not just a question of the technology, but also of how it is implemented on site," explains Hans-Jürgen Krahmer, deputy IT manager at the Rotenburg Hospital. "This is why we're focusing heavily on project management at the moment. We estimate that installing the software will not take more than a day."

The ability to manage all the workplaces centrally from the server was a very important factor for the hospital. This allows individual rules, for example the authorization of a CD with X-rays of a patient for the doctor providing the treatment, to be put in place within minutes by the administrator. "We expect the Sanctuary software to reduce further the risk of virus infections, as private applications can no longer be installed. This guarantees the quality of our entire environment," continues Hans-Jürgen Krahmer. It is also possible to renew the authorization of devices or to block identifiers remotely. Depending on the setting, a push-update can be sent to the workplaces straightaway, or the next time a user logs in. If a specific device is needed only for a short period in a clinic, the administrator can immediately provide scheduled access for a predefined time, possibly only allowing data to be read.

At the heart of the system

The management console is used to configure Sanctuary Device Control and to carry out the daily administrative tasks. This is where the information about domains, users, user groups and computers is stored. However, in case of a problem it is important to identify the cause. Sanctuary allows the logging of device and user reports to find these potential

problems. This Shadow option makes it possible to store on the server a copy of data written to and read from a storage device. In addition, the volume of data which a user can copy every day to external media can also be restricted.

The management console consists of five modules. Using the Device Explorer administrators can regulate access to I/O devices for users and user groups. The Shadow Files Explorer allows administrators to display recordings of the process of copying data onto authorized devices and the content of the data copied. In the Logs Viewer, administrators can monitor changes to device access permissions. The CD Authorizer allows specific CDs to be authorized for user access. The User to CDs Explorer gives customized access to authorized CDs and/or DVDs. In order to spread the workload, the management console can be installed on several machines, which means that while there is still central responsibility for IT security, it is not restricted to one employee.

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

DR - Apr. 07 - V1.0