

Diako



IT security is a major priority for Bremen's church social welfare organization: SecureWave's Sanctuary Device Control protects external devices from data misuse

Germs and data have one thing in common: they are so small that they can get into other people's hands without being noticed. But they have something else in common - you can protect yourself against this happening. The DIAKO main public hospital in Bremen recognized this early on and took preventive measures. In February 2005 it completed the installation of Sanctuary Device Control from SecureWave to prevent data from being accessible from outside via USB sticks, diskettes or PDAs. Now, only devices and media that are approved can be used; approval is given for each individual worker and every device. This investment guarantees reliable protection, so that patients can feel cared for in every respect.

The DIAKO main public hospital, located in West Bremen, with a catchment area of more than 100,000 inhabitants. The University of Göttingen academic teaching hospital has 446 beds in seven specialist departments. There is also an oncology day clinic and a dialysis department providing partial in-patient services. Every year, an estimated total of 35,000 patients are treated at the DIAKO hospital - 16,000 of them on a full or partial in-patient basis and 19,000 as out-patients. The hospital has a staff of around 1,000 workers (including an average of 60 trainees). But it has not achieved this position

overnight; it has been continually evolving since 1867. The hospital in Gröpelingen, which is still being used today, was opened in 1961 and can offer 446 beds, following various extension programs. The hospital has been run as DIAKO Ev. Diakonie-Krankenhaus gemeinnützige GmbH since 1988. It also includes a state-of-the-art business management structure, run according to strict commercial criteria.

State-Of-The-Art And Secure

This also means that the hospital must be able to keep its own Website running, which has been operating as www.diako-bremen.de since 2001. In the same year, the Bremen health network was also set up, which takes in another five local hospitals, in addition to the DIAKO hospital. Its goal is to set up a security infrastructure and internal communications platform within the health network to handle electronic information, such as patient records. Along with this, 1,500 licenses of Sanctuary Device Control were installed within three weeks. The DIAKO hospital uses 100 of these for worker PCs and servers. This enables external I/O devices to be protected and controlled.

"By introducing Windows 2000 and Windows XP across the whole organization, virtually every user had administrator rights for the USB connection and could use data without any kind of restriction. This is no longer possible using the SecureWave solution," says Georg Reimann, head of DIAKO's IT department. "Using this solution gives us security and flexibility which is exactly what we need from a business-oriented IT structure."

Implementation on site was carried out by SecureWave's partner Safeconsult, a Braunschweig-based IT consultancy firm, specializing in security solutions for public sector bodies. The Bremen health network already had mail and Web filters from SurfControl installed, along with antivirus software from Symantec. SecureWave now completes this IT shield so that all ports connected to PCs are monitored, and sensitive personal data are completely protected from prying eyes.

"SecureWave technology offers exceptionally good functionality in terms of protecting the Company's network," says Jörg Kretzschmar, Safeconsult's CEO. "The hospitals were still able to continue providing treatment, as the rollout was implemented during normal operation and did not hamper day-to-day activities."

Clean Bill of Health Thanks to WhiteList

Sanctuary Device Control allows administrators to create and implement highly-detailed security rules at device, user, application and activity level. As of now, workers at the DIAKO hospital can only access an approved peripheral area of the network, and only then, according to the rights they have been assigned, for example, with time restrictions or allowing them only to read or write data. All authorized components are registered and uniquely identified in a whitelist. The administrator only needs to grant access rights and attributes to users, groups or a particular PC. The access control list contains all the information about devices and user rights. Every time the system is used, any request is blocked by Sanctuary Device Control at the kernel level and only released if both the device and

user are recognized and authorized. All activities such as administrator activities and data movements can be logged, meaning that extensive protection is provided not just on the network but also with devices operating standalone, like laptops.

“We have been won over by SecureWave’s solution when we’ve

run it live too, as it is ideal for our state-of-the-art IT environment. It’s not about rigorously screening things, just making careful selections. This allows us to manage dataflow proactively,” explains Reimann.

Cooperation between the two companies has not just stopped after installation. Service agreements mean

that administrators are always using the latest version of the software, so, the hospital’s doors will continue to be open in the future for serious cases.



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.