

Visana Services AG

Visana Services AG uses SecureWave
to protect its IT network



There is insurance available to provide protection for numerous diseases, but every company must look after the security of its IT network itself. Visana, one of the leading insurance companies in Switzerland, takes this responsibility very seriously and uses Sanctuary Device Control software from SecureWave to protect against external computer access. Only mobile devices and storage media owned by the company, such as USB sticks, PDAs and digital cameras, which have been explicitly approved beforehand, can be used at the company's headquarters and other branches in Switzerland. This prevents, for instance, unknown applications being downloaded or data being saved without permission. IBV Informatik AG was Visana's implementation partner on site. The project was successfully completed in 2005 after a total planning and implementation period of six months.

Visana is one of the biggest health and accident insurance companies in Switzerland. It has just under 1,500 employees. In addition to its headquarters in Bern, it also has 21 full-time offices and 200 part-time offices, as well as 10 processing centers. Visana provides private insurance (for individuals and families) and corporate insurance (for companies, public institutions and associations). It has a premium volume in excess of SFR 2 billion and covers around 870,000 persons. The company therefore has good reason for taking IT security just as seriously as looking after its customers.

Exclusion allowed

Technical expertise alone is no longer sufficient nowadays to ensure protection for a company's network. In order to obtain a comprehensive over-

view, numerous legal aspects such as confidentiality, authentication and availability need to be taken into account. In the worst case scenario, legal regulations may have financial repercussions, such as Basel II with individual credit guidelines, and therefore directly affect the calculation basis. But the other areas matter just as much. If internal information were to fall into the wrong hands this could risk damaging a company's image. This is why trust alone is not sufficient. It is important therefore to organize the IT system so that every employee has access only to the areas they each require, and external access is not available for everything.

“We opted for Sanctuary as this software not only protects our USB ports, but also all our other connections such as FireWire, WLAN and Bluetooth,” remarks Martin Burri, IT Security Manager for the Visana Group. This solution facilitates proactive monitoring of all mobile devices through using the whitelist principle. In other words, all external hardware devices such as USB memory sticks, external FireWire disks, WLAN adapters, audio players, digital cameras, PDAs and CD/DVD burners have a unique ID for the device signature. During the project planning phase, every device that will and can be used in the future is registered. The relevant signatures are then entered in the Access Control List (ACL) and stored locally. From now on, only devices that are registered in the ACL can be connected and used. Any other devices are blocked immediately. There are also other parameters available that can determine device usage. Optional criteria include, for example, a time limit, encryption, data volume or data transfer.

Changes to the list cannot obviously be made by users of their own accord. This can only be done centrally by the administrator directly on the server. If, for instance, a device is required urgently for a short period of time, permission to use it can be transferred “on the fly” to the machine for a specific period of time. New permissions are usually granted, for example, the next time the user comes online.

End to proliferation

Visana deploys a total of 1,350 licenses from Sanctuary. The project started off with an inventory to find out which devices were currently being used and which should also be used in the future. One particularly crucial aspect of this was the inclusion of the PDAs, which are an important tool for the numerous local agents. Another important aspect of this process was to actively include employees and make them aware of this issue. Ultimately, the aim was for them not to feel patronized, but more secure. For example, if the company network is infiltrated by a Trojan horse via a USB stick the entire network is affected. At the same time, information cannot be transmitted externally via unauthorized storage media, thus increasing data protection overall.

The existing software distribution solution was used to distribute Sanctuary to the clients. The installation routine is not visible on the computers. “Since we have been using Sanctuary Device Control, it is exclusively our decision as to which devices can be used across the company. The introduction of these controls has put a definite stop to the proliferation of viruses, which is something prevalent in many companies,” continues Martin Burri. IBV Informatik carried out further maintenance and updates to the system.

Keeping an eye on things

If companies do not “just” want to rely on the Access Control List, Sanctuary can offer, using shadowing technology, the facility to record the information that is read from and written to diskettes, CDs/DVDs and mobile devices. There is also an extensive audit protocol for recording every event, whether it is an approved action or an unauthorized, failed attempt, including access attempts using unauthorized code. As an extra option, a complete copy of the data written to and read from a device can even be recorded and saved.

This information is not only important in terms of verifying the permissions that have been set up, but also for proving compliance with legal regulations. This means that concepts like Sarbanes-Oxley Act, Basel II or KonTraG are no longer threat scenarios, but are part and parcel of everyday activities.



Lumension Security
15880 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260
480.970.1025 / www.lumension.com

©2007 Lumension Security. All rights reserved. Lumension Security, the Lumension Security logo, and the PatchLink and Sanctuary product names and logos are either registered trademarks or trademarks of Lumension Security. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.