

Bavarian Ministry of Justice

The Bavarian Ministry of Justice uses
Sanctuary Device Control to protect its data



Bavaria's Ministry of Justice knows a great deal about security. It goes without saying then that the authorities also impose very strict requirements on themselves in this area. This obviously includes IT security as well, and it is often not just the technology that causes problems. Nowadays, it is actually employees who pose a major risk in companies and local authorities. The external devices they use, which they connect to the network via USB ports, for instance, allow data to be stolen and malicious programs, such as viruses, to be introduced into the network. This is rarely done intentionally, but can often be attributed instead, to a large extent, to carelessness and ignorance.

As a result of this, many IT managers are facing the option of either allowing complete access to USB ports or banning them. But both options carry risks. If external devices are used without any controls peripheral devices may be possibly connected that contain viruses or other malicious applications. On the other hand, if employees do not have any chance at all to use USB ports, even connecting digital dictaphones can turn the working day into a daunting challenge.

A better solution required

"In order to keep the security risk to an absolute minimum, we deactivated all USB ports in the BIOS. This also meant that they were not basically available to end-users either. Many employees were not very happy about this situation," according to the view expressed by the Bavarian Ministry of Justice's IT managers. As a result, a solution needed to be found that would both meet IT security requirements and satisfy the users' interests. On the one hand, every effort had to be

made to avoid increasing the risk by unblocking the USB ports, while on the other, users had to be offered the opportunity to use USB ports in their day-to-day work.

One of the particular challenges presented by this project was considered to be the ever-growing security precaution requirements resulting from the use of USB devices. These are arising from the end-users' need for new devices, such as PDAs or flatbed scanners, and also from enhancements to existing technology, such as legacy-free cards for PCs and printers. However, USB ports should not be used indiscriminately, and specific permissions may be assigned without making it significantly more time-consuming to use.

Whitelist promotes greater flexibility

Consequently, as part of the "bajTECH2000" project, the Ministry was looking for a software application that could specifically facilitate the use of mobile devices. The authorities finally struck it lucky with SecureWave and its Sanctuary Device Control software. This operates based on the whitelist principle, which supports the controlled usage of portable storage media and devices. This ensures that external interfaces throughout the entire operating zone in the production environment are protected and can be managed centrally. This solution provides a very flexible method for satisfying user requirements. For instance, each employee can be assigned an individual portfolio of devices, along with the relevant unique signatures. This means that printers, scanners, PDAs and dictaphones are made available immediately, not in an indiscriminate manner, but only according to the specified permissions.

Using the whitelist approach, all users are banned automatically from accessing a device. To make hardware available, the administrator links the users or user groups to certain devices or complete classes of devices which access is required to. In this way, Sanctuary Device Control basically extends the standard Windows security model to control I/O devices. The software starts operating at kernel level, which means that users do not have any opportunity to get round it. New hardware is automatically assigned to one of the predefined classes as part of the plug&play identification phase. Sanctuary then uses the access rule applying to this device class. If a device is unknown and does not belong to one of the predefined classes, the software reverts to one of the restrictive Least Privilege Principle concept (only absolutely necessary permissions are granted), and access is refused until a different action is explicitly specified. Access permissions can also be assigned to a specific model on a particular computer.

Now even greater security at the Bavarian Ministry of Justice

The Bavarian Ministry of Justice launched the project in 2004, and it was already completed by early 2005. Through the internal rollout, the project initially involved only the newly rolled out devices. It was only in 2006, with the rollout of the last APC, that Sanctuary Device Control was rolled out to and installed on the entire stock of PCs and laptops. "The whole preliminary planning phase lasted around three months, and we were able to complete the project in just a few days," explains the Bavarian Ministry of Justice. The project was implemented extensively throughout the entire Ministry of Justice, in all the courts and in Bavaria's state prosecutor's offices. SecureWave's Sanctuary Device Control was installed in a total of around 250 offices. This software has since been used to protect around 14,400 clients in Bavaria's Ministry of Justice offices.

Planning is the key

The key aspect when using Sanctuary software is project planning. This establishes exactly which authorities, departments and employees can work with which devices in the future. An accurate internal analysis needs to be carried out for this in order to avoid numerous adaptations retrospectively. The whitelist includes the signatures of all the approved devices and is transferred in the rollout from the server to all the computers and laptops.

All in all, this software finally offers the Ministry of Justice the opportunity to facilitate access, though limited, to USB ports for employees in all its offices, without jeopardizing the security of sensitive data.



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.