Lumension SECURITY™

South London & Maudsley

Customer Statement – Chris Irving, Services Manager

The Risk

In October 2006, the ICT Department at South London & Maudsley (SLaM) NHS Trust began to look at ways of addressing the risks to patient and business critical data posed by the proliferation of USB flash drive devices.

The ICT department had already implemented a policy "Use of Memory Sticks and Flash Drives within SLaM" to comply with NHSIA security policies surrounding the Trust's NHSNet code of Connection. However, the ICT Department wanted to use software to reinforce this and ensure that the policies on the use of USB storage devices were being enforced throughout the Trust. The head of IT asked Chris Irving, Services Manager, to investigate suitable software that could identify and control the use of USB devices, to protect the data held on 4,000 PCs used within the Trust.

According to Chris Irving, "We wanted to be able to lock down USB device use on PCs and laptops in accordance with the Trust's stated security policy. It's all very well saying to staff that they should not be storing patient or business critical data onto USB flash drives, but we needed to be certain that this policy was being complied with and that we could prevent any unauthorised devices from accessing our corporate networked assets and data."

The Solution

After researching the main products on the market that can detect and manage the use of USB devices, Irving identified the following four solutions:
Sanctuary Device Control from SecureWave, now Lumension Security

- GFI's Languard Endpoint Security v3,
- Centennial's DeviceWall,
- DeviceLock

After a thorough review of each product, Irving recommended that South London and Maudsley NHS Trust install Sanctuary Device Control on all 4,000 PCs within the Trust.

"I recommended Sanctuary Device Control as the best product for the job of centrally managing USB use and enforcing policy, because it not only detected that USBs were being connected to the Trust's IT network, but it could also tell us which make and model of USB device that our staff members were attempting to use to store data onto," explains Irving.

Sanctuary Device Control uses a 'Positive Security Model', whereby only known and trusted devices are allowed to connect to the network. This enforces the Trust's policies, which state that only Disgo Pro USB devices that encrypt data can be used. Sanctuary blocks all other USB storage devices by default, whether they be MP3 players, cameras or PDAs. It also has the advantage of providing ICT with a record of every device that has ever tried to connect to the network, or has successfully connected and creates a back up of data downloaded to and from authorised devices. This record would greatly assist ICT in the event of a data leakage. Sanctuary's granular control, integrated with Active Directory user groups, can be used to grant USB privileges based on hospital shift patterns. For additional security, ICT can set size limits on files that can be downloaded to authorised devices.

As part of the ICT Department's IT security review, it was identified that the 250 laptops used within the Trust also posed a significant risk of data leakage. Irving explains the remedial steps taken: "During our product evaluation, we realised that Sanctuary also integrated really well with existing infrastructure to enable us to lock down laptops."

Marrying Policy to Technology

As stated, South London and Maudsley NHS Trust has a policy that only allows Disgo Pro memory sticks to be used on the Trust's PCs and laptops. Disgo Pro devices encrypt the data held on them, so that if the USB stick were to be lost or stolen, the data held on them could not be deciphered by any unauthorised person:

"Sanctuary also integrates with Active Directory so we can link it to the Trust's ICT policies, making the control much more granular, rather than imposing a blanket ban on all USB devices. For example, we can allow 'Trust Approved' memory sticks to be used by certain individuals, while blocking all other devices from connecting. So if a member of staff tries to connect a Disgo USB stick, it will be blocked. However, if they connect a Disgo Pro USB stick, which encrypts the data and if they have the necessary permission to download data in the first place, Sanctuary will enable ICT to allow this," reports Irving.

"We just want to tighten down and ensure that patient, or business critical data does not escape through this security hole created by high capacity USB storage devices such as PDAs, iPods, cameras or rogue USB memory sticks that people have been given for Christmas and brought into work," concludes Irving. "As well as preventing staff from storing sensitive information on unencrypted USB devices, it also reduces the risk of viruses infecting the network via USB

devices that had been plugged into home PCs."

Future Plans

At present Chris Irving and his team are in the process of identifying which members of staff belong within which groups in the Trust. This will enable them to create granular policies within Sanctuary that will allow specific staff members to store data on approved removable devices, so that their work is not impeded without compromising data security. "We're still working out which groups staff are sat in, so that we can use Active Directory and Sanctuary to allocate the correct permissions to the right people, while still blocking USB device use for the majority of our 4,250 PC and laptop users" concludes Irving.

Lumension SECURITY

Lumension Security - Luxembourg
Atrium Business Park
Z.A. Bourmicht
23, rue du Puits Romain
L-8070 Bertrange
Luxembourg
+352 265 364 11 / www.lumension.com