SecureWave
Safeguarding Tomorrow

by SecureWave
Sanctuary
Application and Device Control

Arkansas State Medical Board

Background

The Arkansas State Medical Board (ASMB) is a state government agency that was established to license and regulate the practice of medicine by, medical doctors, occupational therapy, respiratory therapy and physician assistants in the state of Arkansas. The Board's mission is to protect the public and act as its advocate by effectively regulating the practices of allopathic medicine, osteopathic medicine, physician assistants, medical corporations, respiratory therapists, occupational therapists and occupational therapy assistants.

Any healthcare professional applying for work in Arkansas must submit extensive background information to the ASMB for licensure purposes. The Board operates a separate program called the Centralized Credentials Verification Service (CCVS) that makes this information available to hospitals, insurance companies and other healthcare organizations. The breakdown of the current active licenses statistics, approximately are: 7,830 medical doctors, 353 osteopathic doctors, 1,666 respiratory therapists, 841 medical corporations, and 73 physician assistants.

The Challenge

The ASMB IT staff is charged with protecting the highly-sensitive information contained in the Board's databases. "Because of the nature of the information we have in our systems, we are continuously concerned with all types of security issues from outside threats as well as those from within," said Tim Bolton, network administrator. "We need to proactively address all malware, data leakage and other types of threats because if our systems are compromised, information involving more than 10,000 healthcare professionals becomes vulnerable."

Like most organizations, the ASMB's IT staff is especially concerned with viruses, worms, spyware and other forms of malicious code. To combat malware, the ASMB built a security infrastructure that consisted of firewalls, two factor authentication, restricted user groups, anti-virus solutions, and the use of Microsoft's Group Policy for Windows Server 2003. Although ASMB's network has never been compromised, the IT staff soon realized that this was an inefficient approach to thwarting the growing malware menace or for controlling unauthorized storage devices.

"On several occasions, the nightly updates from our current anti-virus solution were either corrupted, or had quarantined files that were needed," said Bolton. "This brought down our production machines. A recent update we received produced several frustrating issues with the management console, including machines shown as being offline when in fact, they were online, and scans on the production PCs would run intermittently throughout the day instead of the scheduled time, causing numerous calls and complaints to the IT help desk. Our current anti-virus solution is now as much of a nuisance as the malware that it is supposed to protect us from. We are a small organization with a tight budget, so we do not have the financial resources for someone to baby sit their product each day."

In addition to malware, data leakage was another serious security concern for the ASMB IT staff. One of the easiest ways information could be pilfered from the system was by handheld portable storage media. Employees could simply connect a device to a networked computer, download sensitive information and walk out the front door. The ASMB's data entry staff experiences frequent turnover, so controlling devices is an especially important component to a complete security infrastructure. However, Bolton's first attempts at resolution were unsuccessful.

"I physically unhooked all of the floppy disk and CD-ROM drives on all of our computers, as well as utilizing all of the BIOS options," said Bolton. "I had no idea how to deal with open USB ports. I considered completely stripping them out, but thought that might void the warranty. I needed something that would prevent a user with physical access to a PC, from becoming a threat. We also tested a product, but it was all or nothing. That is, you can only allow a device or completely ban it. There were no granular options."

The Solution and Benefits

In January 2006, Bolton was introduced to SecureWave, a maker of endpoint security solutions. SecureWave's Sanctuary product suite takes an entirely different approach to traditional anti-virus and other solutions that rely on a blacklist. Sanctuary allows administrators to create an automated whitelist of allowed applications and devices and all malware, unwanted software and unauthorized devices are denied by default. Any device or executable that is not on the approved whitelist simply will not work on a Sanctuary-protected corporate endpoint.

"All security solutions should be this seamless and easy to use. Choosing a product that uses a whitelist versus a blacklist was a no-brainer," said Bolton. "The granularity of SecureWave allows me to tailor settings per machine, user or both. I can allow a specific employee to use a specific USB device, and only on a specified machine. I can also document everything that was downloaded to that device."

Bolton and the IT staff compiled the initial whitelist of safe applications and allowed devices in about one day. Whenever updates need to be made, Bolton said it takes about five minutes to scan a computer and make the necessary edits to the whitelist. Since deploying Sanctuary, the ASMB has not experienced any security incidents and its computers have remained malware-free. Bolton recognizes that Sanctuary proactively protects his network.

"Before we deployed Sanctuary, we had a user who was trying to hack into and manipulate our databases by downloading various malicious programs," said Bolton. "She was unable to do any damage but someone with the right tools and technical know-how could have caused serious problems. I only found out she was doing this after she was fired for unrelated issues and I was cleaning out her computer. Now that we have Sanctuary, I am not worried about this type of thing because all unwanted or unauthorized applications will not work."

Conclusion

SecureWave's solutions have been so effective in proactively protecting the information housed in the ASMB's systems that Bolton is encouraging other state agencies to deploy Sanctuary. "Every state government agency is required to have anti-virus, anti-spyware or some other form of anti-malware on its PCs, but I'm trying to show officials that Sanctuary is a better solution," said Bolton. "When our current anti-virus solution subscription expires, we will select another AV solution to meet the state's requirement, but it will be used strictly as an additional layer of protection that compliments SecureWave's solution. In fact, we have seen immediate performance improvements after un-installing our current anti-virus solution from several of our PCs. It is a good feeling to know that Sanctuary will keep our systems completely malware-free. It also lets our IT staff sleep much better at night."

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