



Davidson Healthcare:

Health care organization relies on smart planning and smart tools to avert Blaster worm disaster.

Whether you visit a doctor for treatment of the common cold or for a serious medical condition, personal health records are some of the most private documents that exist. And patients trust that their records remain confidential – in other words, secure – within their doctor's care.

The healthcare industry's shift from paper to electronic documentation has been seen as a more secure method of storing patient health information. However, this only holds true if the information is stored in a secure network.

Davidson Healthcare, an organization in Lexington, NC is composed of Lexington Memorial Hospital, six physician offices, an urgent care clinic, a pharmacy and a home health agency. Davidson Healthcare's information network includes 500 workstations and 30 servers among all the sites. The hospital also has a wireless Local Area Network (LAN) for patient care and point-of-care documentation.

Due to the sensitive patient information accessible on workstations and servers across the organization, Davidson Healthcare recognized the importance of eliminating network vulnerabilities in order to secure patient information and maximize network availability and access.

The Challenge

Several years ago, in an effort to prevent network damage by viruses or worms, Davidson Healthcare implemented anti-virus software in their network.

After a scan of the operating systems and applications on 428 machines, HFNetChkPro found that Davidson Healthcare's network was missing 7,100 patches.

However, the "I love you" Melissa virus still infected 29 machines in the Davidson Healthcare network.

"We knew there were network vulnerability issues, but we simply didn't have the time or the budget to invest in solutions," said Kevin Buchanan, MIS director for Davidson Healthcare.

As Davidson Healthcare's HIPAA (Health Insurance Portability and Accountability Act) security compliance officer, Buchanan is responsible for developing a comprehensive security plan. As part of the plan's environmental security regulations, Buchanan's top priority was eliminating all network security vulnerabilities – whether related to worms, viruses, or any other type of security breach.

In addition to firewalls, anti-virus software, intrusion detection and vulnerability assessments, Buchanan knew that patch management played an important role in ensuring network security. But, according to records, patching at Davidson Healthcare occurred sporadically, typically every six months – if it occurred at all.

"In 2002, an outside company did a vulnerability scan for us and we found that we were missing about 4,000

Davidson Healthcare



cumulative patches on all servers and workstations," said Buchanan. "Our IT department consists of 10 people—of which only two are dedicated to desktop management. In an organization as big as Davidson Healthcare, two people just don't have the time to manually keep up with patching."

The Solution

Recognizing the vulnerabilities in their network due to the large number of missing patches, Buchanan turned to the Internet to search for an automated patch management product.

"I first looked at the Microsoft Web site, and I found a link to Shavlik Technologies. I clicked through and discovered that Shavlik had a comprehensive patch management product," said Buchanan. "And Shavlik's partnership with Microsoft gave it strong credibility."

In July 2003, Buchanan downloaded the free version of Shavlik's automated patch management solution, HFNetChkPro, from the Shavlik Web site. A scan of the operating systems and applications on 428 machines found that Davidson Healthcare's network was missing 7,100 patches. At an average of 4.5 minutes to patch each machine manually, this meant that Davidson's two IT specialists would need to spend 14 weeks doing nothing but patching systems.

Davidson Healthcare decided to opt for an automated approach which would help them roll out patches to desktops and servers. In August Buchanan purchased HFNetChkPro 4.0 and the company implemented it immediately

The Results

With the click of a button, Davidson Healthcare can now scan all its servers for patch status, and

One nearby hospital had over 2,000 machines infected by Blaster, and its network was down for three days. Several other neighboring healthcare facilities were also seriously hit. But Davidson Healthcare was not affected by Blaster.

HFNetChkPro will immediately send reports on server status and which ones need patch updates. The HFNetChkPro PatchPush™ capabilities also make automatic patch deployment on servers fast and easy. Through a drag-and-drop interface, patches can be deployed to individual servers, or to groups.

HFNetChkPro also includes a testing environment, so administrators can test patches in a virtual environment before deploying them to servers. This helps limit damage from patch interference with existing applications.

Just two weeks after implementing HFNetChkPro 4, 146 patches had been applied to the Davidson Healthcare network. A month later, the number of missing patches was less than 800 and the network was more secure than just weeks before.

At the time, Buchanan didn't realize how ideal the timing had been. Just over a week after implementing HFNetChkPro, Microsoft announced a critical patch for the RPC (Remote Procedure Call) vulnerability.

Buchanan installed the RPC patch the same week – just before the Blaster worm that exploited the RPC vulnerability was launched.

One nearby hospital had over 2,000 machines infected by Blaster, and its network was down for three days. Several other neighboring healthcare facilities were also seriously hit.

Davidson Healthcare



But Davidson Healthcare was not affected by Blaster. As of October 2003, Davidson Healthcare has been able to achieve a 99.98 percent overall network uptime on applications, servers and supporting network infrastructures.

"I wanted a patch management solution that would work reliably to secure our network, while saving both time and money," said Buchanan. "Thus far, Shavlik's HFNetChkPro has delivered on all accounts and we achieved an immediate return on our investment."

Due to its success, Shavlik Technologies HFNetChkPro 4.0 is now formally included in Davidson Healthcare's HIPAA security plan.

network. A month later, the number of missing patches was less than 800 and the network was more secure than just weeks before.

At the time, Buchanan didn't realize how ideal the timing had been. Just over a week after implementing HFNetChkPro, Microsoft announced a critical patch for the RPC (Remote Procedure Call) vulnerability.

Buchanan installed the RPC patch the same week – just before the Blaster worm that exploited the RPC vulnerability was launched.

One nearby hospital had over 2,000 machines infected by Blaster, and its network was down for three days. Several other neighboring healthcare facilities were also seriously hit.

But Davidson Healthcare was not affected by Blaster.

As of October 2003, Davidson Healthcare has been able to achieve a 99.98 percent overall network uptime on applications, servers and supporting network infrastructures.

"I wanted a patch management solution that would work reliably to secure our network, while saving both time and money," said Buchanan. "Thus far, Shavlik's HFNetChkPro has delivered on all accounts and we achieved an immediate return on our investment."

Due to its success, Shavlik Technologies HFNetChkPro 4.0 is now formally included in Davidson Healthcare's HIPAA security plan.

"We knew there were network vulnerability issues, but we simply didn't have the time or the budget to invest in solutions," said Kevin Buchanan, MIS director for Davidson Healthcare.