



Indiana University:

Automated Patch Management Helps Indiana University Secure Student Data.

In December 2003, U.S. Secretary of Education Rod Paige urged college students to be aware of the growing problem of identity theft. According to Paige, college students are particularly vulnerable to having their social security numbers stolen. In 2003, nearly 100 University of Tennessee students were victims of identity theft when a hacker accessed student names and social security numbers through the university's database.

Unfortunately, the Tennessee incident is only one of many similar issues at other institutions around the country. Colleges and universities should be held responsible for protecting student data, especially information as sensitive as social security numbers. However, in order to securely store this data today, administrators must ensure the entire campus network and IT infrastructure is secure.

Indiana University has eight campuses and more than 98,000 students. The original campus is located in Bloomington, an urban campus is in Indianapolis, and six regional campuses are located in the Indiana cities of Gary, South Bend, Fort Wayne, Kokomo, Richmond and New Albany. More than 15,000 faculty and staff members across the campuses use 20,000 computer workstations — all interconnected on one Indiana University network.

Due to the private student information stored on the Indiana University network, including student social security numbers, officials recognized the importance of securing and protecting the data. This meant

"Patch management can be a time-consuming task, and with busy schedules, it was especially burdensome," said Jim Kippenbrock, manager of local support provider services, Indiana University

identifying and eliminating network vulnerabilities and patching any possible network access points or weak spots. And to maintain the security, University system administrators also needed a way to simplify the ongoing patch management process.

The Challenge

For each of the 700 departments within Indiana University, a local system administrator is responsible for providing technical assistance, troubleshooting computer/network problems and keeping each workstation up to date, including security patching.

"Our system administrators constantly have faculty and staff 'banging' on their doors for technical support," said Jim Kippenbrock, manager of local support provider services, Indiana University. "Patch management can be a time-consuming task, and with the administrators' busy schedules, it was especially burdensome for them."

Not only was patch management time-consuming for department system administrators, the deployment of patches needed to occur during off-hours. This meant system administrators needed to work extra nights and weekends, which was highly inconvenient.



However, securing the Indiana University network is a top priority for all system administrators. Antivirus software and firewalls were already being used to protect some aspects of the network, but they didn't secure vulnerabilities in operating systems or applications. Kippenbrock knew that adding a tool to ease patch management would decrease the time needed and prove valuable to IU's system administrators.

"If Indiana University could find a tool to ease patch deployment, system administrators would more easily be able to address the important task of patching," says Kippenbrock. "And keeping up with patches was vital to eliminating vulnerabilities in our system."

The Solution

As with any purchase at Indiana University, a committee was formed to research a variety of automated patch management tools. The committee consisted of Kippenbrock's local support provider services group and members of the Indiana University's IT Security Office.

"We considered several different products as we looked for a patch management solution that was easy to use, offered remote scanning and deployment capabilities, and fit within our budget," Kippenbrock explained. "With tight budgets across the university, total cost of ownership was a key factor in our decision."

After receiving bids from three different patch management software providers, the committee selected Shavlik Technologies' automated patch management solution, HFNetChkPro, as the best tool to meet the needs of Indiana University. In May 2002, Indiana University purchased HFNetChkPro.

"System administrators have to react quickly to ensure vulnerabilities are addressed... and HFNetChkPro provides an efficient method for them to do just that," said Tom Davis, IT security officer at Indiana University

The Indiana University computing environment is highly distributed across departments and campuses, and no one central server exists on which to implement HFNetChkPro. Instead, Kippenbrock made HFNetChkPro available to the network administrators in each department. From each department host computer, administrators could then use HFNetChkPro to scan the network and deploy patches to department servers and workstations.

"We told the system administrators that we had this patch management tool they could use at no further cost to their department," says Kippenbrock. "It was not hard to sell —HFNetChkPro pretty much speaks for itself."

The Results

Because HFNetChkPro is agent-less software, Indiana University system administrators were able to install it on host computers as needed, without requiring agents to be installed on the 20,000 workstations. This significantly decreased the amount of setup required.

With the click of a button, system administrators can now scan all servers and workstations within their departments to check patch status. HFNetChkPro will then immediately send status reports and indicate where patch updates are needed. The HFNetChkPro



PatchPush™ capabilities make automatic patch deployment fast and easy. Through a drag-and-drop interface, patches can be then deployed to individual machines or to groups.

HFNetChkPro also includes a testing environment, so administrators can test patches in a virtual environment before deployment. This helps eliminate problems from patch interference with existing applications and decreases the time administrators have to spend on their own patch research.

Tom Davis, IT security officer at Indiana University, believes that HFNetChkPro has significantly improved the security of the university's systems and data.

"With HFNetChkPro, critical security patches can be distributed and applied to machines from a central location," said Davis. "System administrators responsible for applying security patches have to react quickly to ensure that the vulnerabilities addressed by the patches are corrected before they can be exploited — and HFNetChkPro provides an efficient method for them to do just that."

In addition to the security improvements, HFNetChkPro has also provided more time for system administrators to keep up with other projects and proactively invest in the goals of their department — rather than struggling to keep up with network maintenance.

In 2003, the rash of vulnerabilities and influx of computer worms prompted an increase in requests from Indiana University system administrators wishing to implement HFNetChkPro in their department. Many system administrators who hadn't already implemented HFNetChkPro were starting to recognize the benefit of patch management and the increased responsibility for network security.

With tools like HFNetChkPro we are striving to ensure a secure computing environment capable of effectively safeguarding sensitive student data," said Jim Kippenbrock, manager of local support provider services, Indiana University.

Because of this, vulnerabilities were patched and possible security issues were successfully averted by the Indiana University network.

"Securing the computing environment at Indiana University is a top priority," says Kippenbrock. "With tools such as HFNetChkPro we are striving to ensure a secure computing environment capable of effectively safeguarding sensitive student data."