SecureWave
Safeguarding Tomorrow

by SecureWave
Sanctuary
Device Control

City of Lake Forest

City of Lake Forest safely enables use of removable storage media

Background

Lake Forest, Ill., a suburb of Chicago, is a municipality of about 21,600 people. The city employs about 250 people and has 300 PCs and laptops spread throughout its various offices. Joe Gabanski, network administrator, is part of a four-person IT team that is responsible for all aspects of Lake Forest's technology initiatives, including ensuring that the city's proprietary information and systems are protected.

Challenge

While the introduction of USB memory sticks and other removable storage media into the enterprise was intended to enhance productivity, this proliferation creates new security risks, including data leakage and introduction of malware. The storage capacity of some of these devices is enormous, enabling someone to pilfer a tremendous amount of sensitive information. What's more, malware is now being transferred from personal gadgets onto corporate networks. This created a dilemma for the Lake Forest IT department.

"At first, we loved the idea that our employees could easily and quickly store and transfer information via USB drives. We even issued devices to a few departments," said Gabanski. "For example, our police officers have computers in their squad cars. We provided them with memory sticks so they could easily bring information collected in the field back to the police station."

Despite the business value that these devices added, Gabanski and the IT staff soon began to realize the security issues associated with their use. After reading a slew of news articles—and wanting to remain proactive about IT security measures—Gabanski realized that the uncontrolled use of removable storage media could potentially create a nightmare scenario.

"Generally speaking, all devices had to be approved by our IT department if someone wanted to use them at work," said Gabanski. "However, we didn't have a formal written policy or anything concrete. And we certainly didn't have any technology in place to control the use of these devices and protect ourselves against the incidents of data leakage and introduction of malware that are constantly making headlines."

However, because Lake Forest does not have an unlimited IT budget, there needed to be a more compelling rationale to purchase a solution beyond simply taking a precautionary measure. "A few people lost the devices we gave them but it was not a valid cause for concern. The 'what if' factor was in place, but that doesn't justify IT spending," said Gabanski.

Solution and Benefits

In May 2006, while evaluating various device control solutions, SecureWave provided Gabanski and the IT staff all the evidence they needed to justify a purchase. During an on-site visit, the SecureWave engineer used the company's Device Scanner utility on Lake Forest's systems. Device Scanner is a free utility that reveals every device currently connected to a network as well as every device that has ever been connected. Gabanski was shocked at the results of the scan.

"We were surprised at how many unapproved devices had been connected. There were several digital music players connected to computers with secure access and a handful of modems that we didn't realize where there," said Gabanski. "We thought we had the use of removable storage media under control but the Device Scanner showed us that the use of devices was much more prevalent that we thought."

Shortly after witnessing the results produced by Device Scanner, Lake Forest's IT department purchased SecureWave's Sanctuary endpoint security software for all of its 300 workstations. Sanctuary enables Lake Forest's IT department to create a whitelist of allowed media, denying all other devices by default. Sanctuary also allows administrators to assign granular permissions. For example, policies can be enforced by device class, specific device/media to user(s)/user group(s) or to a specific computer, time constraints, encryption, volume of data transferred and much more.

"Sanctuary prohibits employees from simply plugging any device they want into one of our PCs, laptops or servers," said Gabanski. "Everything must be approved by the IT department and added to the whitelist or it simply won't work. Sanctuary provides us with the management and enforcement capabilities we need to control the use of removable storage media without banning them completely."

As an added layer of security, Sanctuary's shadowing and logging features provide Lake Forest's IT staff with a complete copy of all data transferred to and from allowed devices.

"If we do allow a device, we can see exactly how employees are using it," said Gabanski. "With Sanctuary, we can be sure that the use of removable storage media is limited to appropriate city business only."

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

Lake Forest - May. 07 - V1.0