Plugging the hole in Windows USB security

July 10 2005

As new ways of transferring and sharing data become commonplace in the workplace, software developers are marketing products to corporations to fill the void left by Microsoft Windows in portable-media-device security.

"The reality today is that organizations need a quick and reliable way to stop the unauthorized transfer of information to and from removable media devices," Brant Hubbard, general manager of Centennial Americas in Portland, Ore.,, told United Press International in an e-mail.

Centennial Software, headquartered in the United Kingdom, is the maker of DeviceWall, which gives companies the ability to manage and restrict access to USB ports on employee computers.

The development of USB or universal serial bus as a convenient way to connect peripheral devices to computers also has generated certain security risks."When people introduce new technology, they choose functionality and don't look at risk factors," Winn Schwartau, founder of Interpact Inc.in Seminole, Fla, an information-security services company, told UPI.Microsoft Windows does not include built-in USB security protection.Although its Service Pack 2 offers a lock-down feature, it does not include USB ports in its security protocols.

"Microsoft's failure to address USB security is one of the top five mistakes of 2005," Hubbard said."This focus on application convenience, not security, provides a great opportunity for Centennial Software to offer that more robust functionality."

Vladimir Chernavsky, chief executive officer of AdvancedForce InfoSecurity Solutions in San Ramon, Calif.,, said his company's DeviceLock allows administrators to control the input and output devices on corporate workstations.

"Maybe Microsoft should have implemented security measures in Windows and, sooner or later, I am sure they will, but we are constantly adding new functionality and features and should be one step ahead," Chernavsky told UPI.

The "Information Security Breaches Survey 2004," sponsored by the United Kingdom's Department of Trade and Industry, found two-thirds of companies surveyed had experienced some form of malicious incident involving their databases in the previous year.Such incidents were defined as viruses, unauthorized access, theft or fraud on a company's network.This was up from just over one-half when the survey was conducted in 2002.

Large companies that responded said 44 percent of their security incidents were known to have originated internally, while 38 percent were known to have an external origin.According to Centennial Software's "DeviceWall security attitudes survey 2005," which included 259 IT managers, 70 percent of security incidents at Fortune 1000 companies are internal and 70 percent of employees have stolen corporate information.

Products such as DeviceWall and DeviceLock enable several layers of protection.For instance, administrators can choose to block USB ports completely, allow only human-interface devices such as mice and keyboards, or create a white list of USB devices based on registered serial numbers.DeviceWall also includes a feature that warns when an improper action has occurred.

Companies must deal with security threats by deciding how to balance functionality and security, Hubbard said."Complete lockdown is actually counter-productive, as it blocks the USB port not only to storage devices, but also to keyboards, mice and printers," he noted.Both Hubbard and Chernavsky said they think although USB security awareness is growing and their list of clients is expanding, many companies still do not take proper precautions.Centennial Software's survey found 50 percent of all companies have placed no controls on portable media devices.

The U.K.security-breaches survey found that, on average, companies spent only 3 percent of their IT budgets on security measures.Less than half of those surveyed had conducted any type of cost-benefit analysis for security measures.Companies tend to view such measures as expenses rather than investments, the survey said.

"(Chief security officers) have seen viruses and spyware as more pressing security issues," Chernavsky said, "but with the price of portable media devices dropping and their capabilities increasing, it is becoming more of a problem and receiving more attention."

Hubbard said recent high-profile incidents involving removable media devices have caused the security issue to climb rapidly "to the top of the (chief information officer's) to-do list.When organizations compare the cost of purchasing DeviceWall against their risk exposure, many will simply 'find' the budget."

Both executives said encryption of portable media devices is the next step in securing data downloaded from company computers.