



KPMG ANALYSIS

Companies Aiming to Plug USB Data Leakage

February 23, 2007

By Dave Pelland, Managing Editor, Technology Insider

Corporate security professionals are trying to regulate the internal use of flash memory sticks, digital music players and other portable storage devices that can provide an unguarded route for documents to leave an enterprise.

The growing ability of workers to take and use data outside network boundaries is raising concerns about information being misappropriated or exposed if a portable storage device is lost.

For instance, a California university in November reported the theft of a portable disk drive containing personally identifiable information for 2,500 students and applicants. In September, health care providers in Tennessee and Michigan each reported the loss of flash drives containing more than 4,000 names and Social Security numbers.

"Data used to be locked in sealed file cabinets at night, but those days are well past us," says Dennis Szerszen, senior vice president of security provider SecureWave. "Now employees are demanding mobility and portability, and removable media scares the pants off a lot of companies."

In addition to the threat of losing sensitive information, enterprises are also afraid about a worker who joins a competitor will take data with him; they are also concerned that documents transferred to portable storage may be accessible beyond the dates specified in a company's retention policies.

While the amount of information that can fit on a flash drive varies, a typical 2-gigabyte flash drive, available in mass-market retailers for under \$50, can easily store thousands of word-processing documents and spreadsheets.

The problem is multiplied with hard-drive equipped music players, which can be used for document storage and offer capacities up to 80 gigabytes.

"These devices give someone the right to bypass your security and store and transmit data without being detected," said Richard LeVine, global leader, digital rights management and intellectual property rights management for Accenture, at the RSA Security Conference in San Francisco.

LeVine said most information security managers would probably like to ban portable storage devices outright. But the popularity of flash drives and music players make such bans tough to enforce in a corporate setting. (Military organizations often apply epoxy to USB ports to prevent unauthorized devices from being attached to PCs.)

According to John Geldman, senior level technologist on Lexar Media's emerging product team, flash-based storage devices are becoming extremely sophisticated. Along with memory, flash drives also have small processors and often come with backup, synchronization and antivirus software. They can contain operating systems that give

MORE...

Attachment Spam May Emerge as Malware Vector

AUGUST 8 PDF attachments are the latest effort to evade corporate spam filters, and may foreshadow the use of e-mail attachments as a way to deliver malware.

Selected Technology Company Earnings

JULY 31 Technology and media companies generally reported earnings growth in the second quarter.

Transfer Pricing Risk Hitting Boardroom Agendas

JULY 25 Technology companies face a major challenge in transfer pricing risk as national governments seek new sources of tax revenue.

Product Placement Takes Its Role on the Global Stage

JULY 18 The head of a television studio talks about how product placements are expanding across the globe.

Data Protection Gets Policy, Tech Backing

JULY 11 The focus of enterprise security is shifting to data protection and stronger policies for accessing and storing information.

IT Governance Is a Matter of Information Over Technology

JULY 5 A language barrier between audit committee members and technology officers can severely complicate IT risk oversight.

For Better Security, Web Browsers Go Green

JUNE 26 The latest generation of Web browser certificates could help reduce phishing attacks against banks, retailers and other companies.

drives the ability to run programs such as Internet telephony or virtual private network clients.

"The upside is that workers can be more productive, but the downside is that the devices can carry more risk," Goldman said. "Like a PC, USB flash drives can be hacked."

According to the Consumer Electronics Association, factory sales of flash media products to dealers are expected to reach \$4.7 billion in 2007, up from an estimated \$3.4 billion in 2006.

Producers of flash memory drives hope the inclusion of security software will help them avoid the commoditization of their products in the face of falling prices for memory. Nomura Securities the spot market prices for 4-gigabyte NAND modules fell nearly 25 percent between the second week of December 2006 and January 2007.

To help reduce the risk of data loss -- while still allowing removable media -- companies are installing encryption and management software on flash drives, PCs and network appliances to oversee the use of portable storage devices.

"Enterprises are paying a lot more attention to endpoint policy management, and extending [those concepts] to applications and devices," says SecureWave's Szerszen. "They're making administrative decisions about the devices with which end-users can access the network and trying to eliminate a lot of security risk."

For example, companies can create a "demilitarized zone" between the network and a portable storage device in which software monitors the flow of information being stored on flash drives. The software can prevent sensitive data from being copied to unapproved devices, according to Ron LaPedis, product marketing manager, security [while] enterprise products, for storage producer SanDisk.

When a flash drive is plugged into a laptop, the device checks with a security appliance to make sure it is assigned to an active employee with appropriate access. If not, the device can be prevented from accessing the PC or data stored on the device can be erased.

Software also tracks the documents being transferred to and from an authorized flash drive, and compares that activity with an organization's business rules. For instance, a chief financial officer may be allowed to download spreadsheets or presentations that other employees would be blocked from copying.

"If someone is downloading a lot of Excel files and you're not seeing those files being updated or brought back to their PC, that can trigger rules and raise some security flags," LaPedis says.

Similarly, the Trusted Computing Group, which develops open, vendor-neutral security standards, is working on mutual authentication protocols that would create a framework for specifying access control and encryption between flash drives and host devices (such as desktop or laptop PCs). For instance, this would allow companies to link flash drives to specific laptops.

Szerszen says the use of flash-drive encryption remains in the early stages, with adoption first emerging among financial services and health care firms, as well as government agencies.

"The demand is there, and companies are starting to provision end-users with removable media with embedded encryption and sometimes biometrics," he says.

To print this article or share it with a colleague, click an option below.

[Print this Article](#)

[E-Mail this Article](#)

PLEASE RATE THIS ANALYSIS

Quality of Analysis

1 2 3 4 5
POOR EXCELLENT

Comments or Questions

e-Mail Address (optional to enable Insiders to reply)

[Submit](#)