



Federal Computer Week

October 9, 2006

Circle the wagons Technologies to protect data from getting tapped, leaked or stolen

By Wade-Hahn Chan

Government officials need an arsenal of weapons to protect digital assets, including tools that fortify databases, prevent sensitive information from leaving an agency and give laptop computer users secure access to corporate networks.

The rise in data security breaches at federal agencies and in the private sector has made security managers aware of the need to do more than secure networks with firewalls and expose intruders with intrusion-detection systems. Experts say security managers must focus on protecting databases and stopping data leakages by tracking the flow of data.

In addition, the reports of stolen government laptop PCs indicate the need for agencies to install encryption tools to shield data from unauthorized users. Agencies also should add software that forces laptop users to adhere to their security requirements before they can access the network, experts say.

“Content protection and being able to encrypt it is important and so is strong authentication, so when people get on to [computers], they must provide a password or something stronger like a biometric,” said Wayne Jansen, a computer scientist at the National Institute of Standards and Technology.

Agencies need “some sort of controls for the flow of the data on the device — not only firewalling — and what type of connections can be made or received,” Jansen said. “You also certainly would like some antivirus software.”

Inside protection

User privacy legislation and reports of intruders accessing information at financial institutions are driving efforts to boost database security. Officials at Symantec Research Labs say financial institutions reported more than 130 data breaches last year. Those breaches affected more than 57 million records. This month Symantec will offer Symantec Database Security, an appliance that monitors database activity in real time.

Several companies such as Application Security, Guardium, Incache and Lumigent also offer database vulnerability assessment and intrusion-detection tools that can identify unauthorized transfers.

“Attackers have discovered three things,” said Alan Paller, director of research at the SANS Institute. First, “Oracle and other database management systems have significant security holes,” he said. Second, “database

programmers make mistakes, and [finally], government agencies are making database queries available over the [Internet]. This has led to an explosion in database attacks.”

Extrusion detection

Emerging tools known as extrusion-detection systems are helping government agencies and private companies detect whether sensitive information is leaving their organizations. For example, the Pension Benefit Guaranty Corp. uses Fidelis Security Systems’ DataSafe appliance to protect the personal and financial information of millions of workers and retirees, company officials said.

Another company in the extrusion-detection arena is Vericept.

“Our goal is to monitor traffic from the inside going out,” said Daniel Hedrick, product manager at Vericept and a former intelligence officer in the Air Force. “If I see content going out the door, with or without the approval or the knowledge of the user, I will automatically encrypt it.”

Hedrick said that to prevent data from leaking from an organization, the technology must understand employees’ behavioral trends. Using extrusion-detection technology, security managers would be able to tell if an employee cut and pasted insider secrets to a blog or message board. He added that such tracking is possible on mobile computers, too, based on logging information.

Using extrusion-detection technology, security managers could tell the difference between malicious behavior and accidents by analyzing the occurrences’ frequency, Hedrick said. The trend analysis finds repeat offenders rather than nipping leaks in the bud, he added.

“Looking at a Web page or going out to a blog or just sending out information like an attachment, we’re not necessarily going to be able to tell the intent of the person,” he said. “Over time, if we begin to see [that] a user consistently and repeatedly does this type of behavior, then we’ll consider it malicious.”

Tracking behavior is an issue that goes beyond technology, however, and many companies such as PortAuthority Technologies have extensive executive assessment programs to look at individual employees.

Other companies that offer behavioral analytics include Oakley Networks, whose SureView software suite can give a full replay of user behavior for investigations. It also offers analysis of important phrases and filters to passively analyze user behavior and create a document trail that an organization could use to terminate or prosecute an employee.

Fingerprinting technology is another way to track data leaks through file identification. This technology uses a hash of a file, or a string of hex numbers usually at least 128 bits long, to create a fingerprint of a file.

The file’s fingerprint changes when someone edits a file, so an organization can easily determine if a user altered or copied and pasted data from it.

PortAuthority Technologies goes further than hash technology with its PreciseID product, which tracks multiple aspects of a file, including keywords, and compares information in the file with external databases.

Securing the endpoint

Mobile data and remote connections have their own security challenges, experts say. C.J. Desai, director of product management for client and host security at Symantec, said security is dependent on where users connect their work laptops.

“[You’ve] bought all this security software like antivirus or firewall, but that particular [computer] endpoint connects to my corporate network through a [virtual private network] from home” or some other remote location, Desai said.

“The footprint of our mobile devices continues to change thanks to the personalization of the mobile computer,” said Ross Brown, chief executive officer of eEye Digital Security. He has seen federal workers with their Apple Computer iPods connected to their government laptops, sorting through music with iTunes. If a program such as iTunes needs a critical security update and the user doesn’t update it, the laptop could have a data leakage hole, he said.

Brown said there are three reasons to deploy technology for data protection: “keeping bad guys off the devices while you’re mobile, keeping your user from taking data off of the mobile devices [and] keeping the device within the user’s control.”

Secure network access

Identity management software is instrumental in providing secure remote access. Novell provides secure remote access through the company’s Identity Manager. The software manages remote connections, and network administrators can assign permissions to specific user groups.

“You need to have a policy, but the policy needs to know who you are,” said Jason Werner, product manager at Novell. “Where we really shine is we know who you are on the network, and we manage it based upon who you are and what you’re doing.”

When it becomes available, Microsoft Windows Vista Enterprise Edition will offer another take on identity management that will boost remote access. The latest Windows operating system will include BitLocker, an integrated data-protection feature that encrypts the entire operating system.

BitLocker will require users to provide an authentication key or password in addition to a detachable USB key before booting a computer. Those multiple security layers ensure that the mistakes of convenience don’t cause a data leak.

Security managers must also safeguard the connections from a user’s laptop to agencies’ databases. A big source of leakage is laptops that contain a keylogger program or malware and connect to internal databases.

“If you’ve got data on a laptop [and] you’re in a hot spot, someone who wants that data [has] a very good shot at getting that data,” said Richard Rushing, chief security officer of AirDefense. Security solutions that protect network access are the best way to remedy such vulnerabilities. They uphold a standard security configuration that users of remote devices must meet. If their device doesn’t have the proper security configuration or has security weaknesses, the network will deny access.

The two big proprietary players for network access protection, Cisco Systems and Microsoft, announced in early September that they would make Cisco’s Network Admission Control and Microsoft’s Network Access Protection interoperable. The joint architecture would add a dual layer of network protection.

After solving the connection issues, file encryption is the next step in protecting sensitive data. “You can try to protect every gigabyte” of that hard drive, said Benjamin Jun, vice president of Technology at Cryptograph Research, or you can encrypt it with something as short as a 256-bit encryption key.

The Blink software suite at eEye Digital Security protects mobile devices from data leakage via mobile storage devices, such as USB and Firewire devices. Blink includes a policy-based control system for such devices, which prevents unauthorized units from connecting.

Microsoft Windows' Rights Management Services feature also does that, and it can also prevent users from writing to or from detachable media.

Patch workaround

In addition to controlling who accesses devices, organizations must deal with many users who don't keep up with security patches.

"How can I ensure that all this software is properly configured and up to date?" Desai asked. You can't, he said.

But agencies can deploy products such as Symantec's host-based intrusion-prevention system, which stops intrusions by blocking malicious connections and operations, or at least quarantining them. Competing vendors include Mitre, Cisco and Sana Security.

Although Desai recommended host-based intrusion prevention as a way around unpatched security programs, he encouraged organizations to use other tools, such as virus scanners and spyware and malware blockers.

Those tools do the house cleaning, Desai said. Some suites, such as the open-source NOD32 antivirus and WatchGuard Technologies' Gateway AntiVirus/Intrusion Prevention Service, offer antivirus and intrusion-prevention systems in addition to real-time automatic updating, he said.