Developing a Sense of Security

Government agencies turn to endpoint security to ensure system safety.

It's almost impossible to make it through a day without encountering news about hackers, computer viruses and increasingly ingenious methods of identity theft. Today, government agencies face a world fraught with risks and growing concerns about security. It is estimated that viruses cost organizations approximately $55 billion in damages in 2003. Overall, The Computer Security Institute (CSI) reports that the average cost of a security breach is now $204,000.

Government is particularly at risk because many agencies operate data warehouses and databases containing large volumes of information. "In many cases, attackers are motivated by the fact that a great deal of personal information resides in government systems," says Larry Dietz, senior director of Government Solutions at security software provider Symantec. In addition, "There's the threat of activists and terrorists attacking government systems to cause damage or destruction."

Today, no agency can afford to lose valuable data or see its systems damaged. Viruses, spyware, rootkits, phishing and pharming techniques, malicious code, and outright theft are all growing dangers. Without a multifaceted and layered approach to security — using the right tools and techniques — disaster can ensue. "Hackers have become more targeted and sophisticated. It's up to organizations to respond appropriately," says Joseph Feiman, a research vice president at Gartner Inc., in Stamford, Conn.

Better protection isn't only about reducing the costs associated with a security breach, both in staff time and actual losses. Agencies that find themselves in the crosshairs of hackers or thieves may face legal liabilities, diminished employee productivity, damage to their reputation, and reduced system and network performance levels. And, in today's digital economy, the most basic solutions are no longer enough. Viruses and worms evolve and change forms, and social engineering schemes such as pharming and phishing can trick even the most sophisticated users.

Coping With Threats

Hackers and thieves are constantly on the lookout for weak points within organizations. Although IT security risks have been around since the first mainframes appeared decades ago, the advent of the Internet and open architectures has spawned bigger and more insidious attacks. "As new technologies take hold and there are more ways to connect, a greater number of vulnerabilities occur," says Sam Curry, vice president of Security Management at software provider CA.

In many cases, the result is a cat-and-mouse game that has each side making countermoves to respond to increasingly complex tactics. For example, some malware writers now have achieved "Zero Day" status, meaning they exploit a security vulnerability the day it becomes known. Meanwhile, a few individuals have introduced polymorphic viruses, which have the ability to modify their own code each time they replicate. This makes it easier to slip malicious code past antivirus software and ratchets up the challenges for an organization looking to defend data and assets.

The Human Element

Social engineering has become an increasingly popular method used by thieves to steal identity data. Over the last few years, phishing (fraudulently acquiring sensitive information, such as passwords and credit card numbers, by masquerading as a trustworthy person or business) and pharming (the exploitation of a vulnerability in DNS server software that allows a hacker to acquire the domain name for a Web site, and to redirect the site's traffic to another site) have emerged as major problems for government agencies.

"Phishing has become a serious threat, and it continues to thrive," Symantec's Dietz says. While most phishing techniques target individuals through spam and many appear to come from banks and other financial services firms, a few have attempted to glean data from the IRS and other official organizations. Increasingly, government agencies find themselves the target of phishers, who hope that a few individuals will respond and hand over private data. Yet the Government Accounting Office has also identified some messages that may appear to come from other government agencies and request information about specific employees.

In fact, the emergence of a new type of phishing technique has emerged: spear phishing. "In some instances, it is targeted to a specific person or group," points out Kevin Haley, Group Product Manager for Symantec's Endpoint Security Product Line. "If a person is clever enough to gain entry into the organization, a great deal of damage can result." These tactics usually focus on a password, verification of a password, an internal passkey or some other valuable data or authentication element.

> "As security threats evolve, government agencies must evolve. Sound practices and the right tools can build a foundation for success."
>
> — Sam Curry, Vice President of Security Management, CA

Spyware and adware also have become major problems. As the Internet has evolved into a mainstream tool, it has redefined the notion of privacy and security. Some hackers and data thieves send e-mail attachments that contain hidden applications that install themselves on a PC and use stealth methods to control systems, glean data or log keystrokes. Less malevolent adware infests a PC with code that generates pop-up ads. These can waste staff time and drain overall productivity.

A few applications also install rootkits. These programs, which install surreptitiously on Windows, Linux, Solaris and other platforms, conceal running processes, files or system data, thus making it easier for an intruder to gain and maintain access to a system without detection. By modifying parts of the operating system or installing themselves as drivers or kernel modules, it's next to impossible to detect these applications. Unfortunately, they often allow viruses, worms, Trojans and other malware to enter a system without detection.

Application security also is emerging as a key component in an overall defense strategy. Although it isn't as mature as other forms of security and, until recently, has been largely overlooked, it's now attracting a good deal of attention.

Simply put, it uses software, hardware and specialized procedures — including code analysis — to identify and protect applications from a wide variety of threats. It bolsters tools such as intrusion detection and firewalls.

Risky Business

Maintaining a high level of security is no simple proposition. Over the last few years, attacks have grown in sophistication and malware has become far more dangerous, unpredictable and widespread. Not only have hackers stepped up their assaults on government agencies, they've become smarter and more creative, using buffer overruns, spoofing, stolen IDs, SQL Injection techniques and an array of other approaches.

Because so many pieces to the security puzzle exist, many organizations find themselves allocating growing money and resources to a variety of security flash points, including infrastructure, virtual private networking (VPN), intrusion detection, monitoring tools and actual code. While these security solutions are sometimes expensive, organizations increasingly view them as a basic cost. In fact, many understand that they're no longer an option but a necessity.

Some organizations are turning to a sophisticated hardware approach to protect networked and non-networked endpoints by providing users with access to a fully secured virtual private network. A Secure Sockets Layer (SSL) VPN enables universal access to protect mobile and office endpoints from worms, viruses, spyware, keyloggers, Trojan horses or hacking.

The Cisco ASA 5500 Series VPN Edition offers flexible VPN technologies for any connectivity scenario with scalability for up to 5,000 concurrent users. Providing easy-to-manage full-tunnel network access through both SSL VPN and IPSec VPN, this security appliance enables IT administrators to create secure connections across public networks to mobile users, remote sites and approved system partners.

For application-embedded attacks, such as spyware or adware spread through file-sharing peer-to-peer networks, the Cisco ASA 5500 Series deeply examines application traffic to identify dangerous payload and drops its contents before threats reach their target and cause damage. Whether users are accessing the network from a networked-managed PC, personal machine or public terminal, the Cisco Secure Desktop helps ensure complete data protection before, during and after the SSL session.

Symantec's Client Security software provides comprehensive protection against blended threats, spyware, unauthorized network access and mass-mailer attacks, with virus and vulnerability-based detection. Meanwhile, CA's Integrated Threat Management combines a number of functions within a single software package. The list includes antivirus, spyware, keyloggers and other malicious code. "It's no longer possible to view security threats in isolation. It's essential to develop an overall strategy using more sophisticated tools," Curry explains.

Authentication is also a key to preventing security breaches. Establishing strong log-on passwords and short time-out periods to restrict access to sensitive data is an important start. In addition, a growing number of agencies are using IP address restrictions to limit exposure to inappropriate or restricted materials. According to Gartner's Feiman, it's important to establish access policies and procedures up front by defining clear roles and responsibilities. It's also crucial to educate and train workers to use systems correctly.

Finally, IT must oversee increasingly complex patching requirements. It's essential to apply current security patches and updates on a regular basis — and in a consistent manner

— in order to address security flaws, bugs and usability problems. Larger patches, also know as "service packs," address a number of issues simultaneously and play a key role in reducing the vulnerabilities of a system.

Although each organization must discover its unique route to security and build a framework that suits its needs, best-practice organizations place an emphasis on standards, conduct a thorough and ongoing analysis of systems, invest in tools and processes that provide maximum protection, and provide employees with the training and skills to use systems effectively and safely.

"As security threats evolve, government agencies must evolve," CA's Curry explains. "Sound practices and the right tools can build a foundation for success."

Seeking IM Protection

In the early days of computing, virus attacks usually arrived via disks and e-mail, but now, attacks have become more sophisticated and varied. One of the most vulnerable areas is instant messaging (IM), which has exploded in popularity over the last few years. Today, many employees expect instant messaging as a basic service offering but are unaware how effective it is at carrying and spreading malicious code, including viruses, worms and Trojans.

The biggest problem with instant messaging is that there's no way to verify or authenticate the person on the other end. This makes it easier to spread malware. Consider that in March 2005, a worm named Kelvir began appearing in chat tools, enticing recipients to click a link to a Web page that spreads a virus. Ultimately, those with infected PCs wind up sending copies to other IM users. One thing that makes Kelvir so effective is that appears in mid-conversation with another IM participant — making it seem like the message and link are coming from that person.

According to a 2005 study by technology market research firm Radicati Group, 88 percent of workplace users will rely on instant messaging by 2008. While IM brings enormous benefits and boosts productivity, it also raises alarms on the security front. That's because even interoffice messages travel across the Internet and are thus outside the control of network administrators. On the other hand, interoffice e-mail can stay completely within the control of IT.

E-mail viruses continue to evolve as well. Some messages spoof known users, while others use the HTML scripting ability in a mail client, such as Outlook or Eudora, to download malicious code. Still others use stealth techniques that intercept an antivirus software's requests to scan a file. A few also combine malware with social engineering to trick users into visiting a Web page, where they download a virus or fill out information that looks real but is in reality a scam.

For instance, in December 2005, e-mails began to circulate that appeared to come from the CIA and FBI. Although the originating address appeared to be legitimate, listing mail@cia.gov or mail@fbi.gov on the "from" line, it requested information about illegal Web sites that a person may have visited. When an unwitting recipient clicked on the attachment in the e-mail message, the W32.Sober.X@mm or WORM_SOBER AG viruses invaded the user's system. It attempts to lower security settings while spreading to other PCs.

The Barracuda Instant Messaging Firewall is an integrated IM server and management solution that can address this security issue for agencies. The firewall provides such benefits as IM traffic identification and logging, a private and secure IM server and network, keyword identification and reporting, and secure file transfer.

Steps to Keep Systems Safe

Use top-notch security tools and keep them up to date. The list includes antivirus software, a spyware scanner, rootkit detector, firewall, intrusion detection, VPN and authentication, and logon tools.

- Whenever possible, use software suites or devices that provide a more integrated level of protection.
- Install patches and security updates quickly and consistently across the organization.
- Put protections in place to ensure that DNS servers (which translate names into IP addresses on the Web) aren't hijacked and used for a pharming scheme.
- Focus on security at the application level, using testing tools to identify vulnerable code.
- Make sure that staff receive adequate education and training on how to choose passwords, avoid suspicious attachments and links, and spot phishing scams.
- Stay informed by reading articles about evolving threats, including RSS feeds from major security vendors.