



SPECIAL BRIEFING

Defending Against the Insider Threat

Attacks don't always come from the outside. Your own employees can carry them out—unless you take steps to stop them.

SPONSORED EXCLUSIVELY BY:



PRODUCED BY:



Figures vary on the prevalence of “insider” attacks on corporate IT systems, but there’s no debating that insiders have the ability to inflict tremendous damage, willfully or not. The question, then, is how best to detect insider attacks and defend against them.

As is almost always the case when it comes to security, the effectiveness of the solution depends on a combination of defenses. They include proper use of a variety of security products—including antivirus tools, firewalls, intrusion detection and prevention systems, and network access control systems. Ideally, you should also be able to correlate the information that each product provides such that you can more easily weed out the real threats from the noise. But tools alone won’t suffice. You must combine them with a heavy dose of process and procedure along with employee education before you’ll be on your way to protecting your organization from insider threats.

It won’t be easy, in part because the insider threat is both frequent and insidious. The Identity Theft Resource Center (ITRC), which tracks all types of breach reports in the United States, says in 2008, one in six breaches (15.7 percent) were attributed to insiders—more than twice as many as in 2007 (6 percent). In the 2008 CSI Computer Crime and Security Survey, insider attacks ranked second only to viruses as the most common type of security attack. And in its 2008 Data Breach Investigations Report, based on more than 500 forensic investigations of security breaches, Verizon Business found that half of all internal breaches were conducted by IT administrators.

Defining the insider threat

Explicitly illegal behavior by IT staff (or any other employee or contractor) is one form of insider threat. In some cases, the employee or contractor is deliberately trying to steal data for financial gain, or in the case of a disgruntled employee, to

get back at the company for a perceived wrong. Examples range from stealing credit card numbers to more elaborate schemes, such as the case of a billing clerk at a New York hospital who sold patient insurance information to a third party.

Probably more common are employees who make serious but unintentional errors, such as losing laptops and USB storage devices that contain sensitive data. In a survey conducted by EMC’s RSA unit at three of its security events—in the United States, Mexico and Brazil—one in 10 respondents reported losing a laptop, smart phone and/or USB flash drive that had corporate information on it.

The damage from such acts can be devastating. Consider the case of a U.S. Veterans Affairs employee who took home his laptop along with disks containing records on some 26 million U.S. veterans—and had them all stolen out of his home.

Some incidents are the result of simple carelessness, such as an employee who leaves his laptop in a car while he goes to a restaurant, perhaps not even bothering to put it out of sight. In other cases, it’s lack of knowledge. In its survey, for example, RSA found that 64 percent of employees frequently or sometimes send work documents to their personal email address so they can work on them from home.

Social engineering is another common form of attack, where insiders are duped into giving up sensitive information. In 2005, for example, thieves posing as legitimate customers managed to set up some 50 accounts with the data aggregation company ChoicePoint. That opened

the door enough for the thieves to steal at least 145,000 customer records—and resulted in ChoicePoint taking a charge of more than \$11 million in 2005 for costs related to the incident, along with a Federal Trade Commission settlement of \$15 million.

A call to arms

Defending against such attacks starts with properly deploying a series of security tools that provide a defense-in-depth strategy. Antivirus and anti-spam tools are must-haves, as are firewalls. And you should protect not only the perimeter of your network but the inside, to guard resources such as application servers and sensitive databases from nefarious and unauthorized insider activity.

Intrusion detection systems, which can alert you to attacks in progress, are likewise crucial. So are intrusion prevention systems, which can take actions to thwart the attacks. It's important to be able to detect not only signatures that identify known forms of attacks, but those based more on behavioral anomalies—an authorized user downloading massive amounts of data at 3 a.m., for example. To ensure that the anomaly is an attack,

feeds from multiple devices should be correlated to confirm or reject the alarm rather than generating false positives.

Many companies are also installing network access control (NAC) tools. While they can take various forms, most NAC products inspect a client before it connects to the corporate network to ensure its security state complies with company policy, such as

checking for up-to-date antivirus and antispam software. NAC systems can also complement identity management tools, which help verify the identity of employees or contractors before allowing them access. Identity management tools also provide fine-grained access control to corporate applications and data—meaning users can get at only those resources they are authorized to access.

Another crucial tool for your security arsenal is a security event information management (SEIM) system. Such tools can collect alerts from your various security tools and look at them as a whole to weed out the “noise” and false positives from the potentially serious threats—and do it in real time.

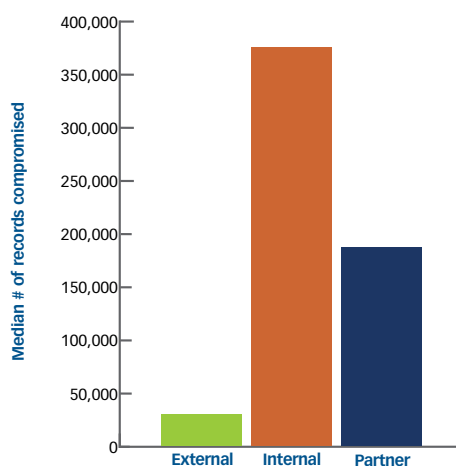
Perhaps just as important, SEIM tools can also help detect false negatives—an attack that goes undetected by any one security tool but is found by correlating data from many systems. Such attacks are difficult for humans to detect even if they are diligent about monitoring logs.

Open and scalable

For security tools to be most effective, it's best to employ an open security framework, where products from various vendors can communicate with one another. When an IDS detects an attack, it would utilize feeds from other devices to help confirm the attack. It may need to communicate with a firewall to shut down a certain port or interact with SSL to limit access for a specific user. While buying all of your security products from a single vendor will (theoretically) ensure that the tools play well together, an open architecture provides greater choice with respect to product capabilities and price.

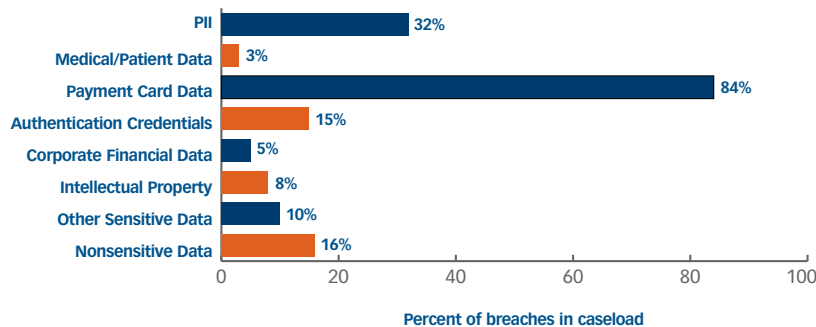
Scalability is another consideration when selecting security products. At least two key factors play into the scalability equation. First is the product's ability to support your specific

Breach Size and Source



Source: Verizon Business, 2008

Compromised Data Types



Source: Verizon Business, 2008

environment, whether it's the number of users, devices or amount of bandwidth. Second, the tools must be able to support that environment without sacrificing performance.

Process and procedure

While security products play an important role in protecting against insider threats, they should be combined with a well-defined set of policies and procedures for how to handle various IT tasks.

Guidelines for coming up with these policies are available through such resources as the IT Infrastructure Library (ITIL), Control Objectives for Information and related Technology (COBIT), as well as ISO 27001 and ISO 27002 (ISO 27001/2). The idea is to provide consistency in how IT services are managed and delivered.

While ITIL, COBIT and ISO 27001/2 cover many IT disciplines, configuration management has a profound effect on security. In their 2008 study on insider threats, the U.S. Secret Service and Carnegie Mellon University's CERT program found examples such as insiders using scripts or autonomous agents to delete or corrupt files and releasing obvious, potentially harmful changes to company Web sites. Such attacks can be prevented by requiring a dual sign-off in a configuration management system

before changes can be made, at least for sensitive, high-value systems.

Another preventive measure against unauthorized changes is to use your access control system to keep track of who can access what resources, and under what circumstances. If insiders know their actions are being tracked, they are far less likely to conduct attacks in the first place.

Ongoing education

Some security policies will extend beyond IT to the end user population at large, which means you'll need to educate users on those policies. At the same time, users require ongoing education on best practices to keep them from becoming unwitting accomplices in an attack.

Education can—and should—take various forms, and continuous reinforcement is critical. It's wise to offer various forms of education, including in-person discussions, and Web- and paper-based tutorials.

Conclusion

The security threat posed by company insiders is all too real. In these times of economic uncertainty and widespread layoffs, the potential to create disgruntled employees is all the greater.

But there are steps you can take to protect yourself, starting with a sound, defense-in-depth, collaborative security strategy that includes tools and an open platform to provide numerous and multifaceted defense mechanisms. Augment those tools with processes and procedures that can help detect both rogue employees as well as honest mistakes. Finally, be diligent about educating all employees on the various threats they face—and their role in preventing them. And by all means, don't wait till it's too late. Get started now.

Juniper Delivers on Security and Performance

With its line of products built with both security and performance in mind, Juniper Networks helps companies across the globe implement networks that combine top-notch security with superior performance, support and management.

Ajisen Ramen China, one of the largest chains of casual dining restaurants in mainland China, Hong Kong, and Macau, chose Juniper when it was looking to build a new network to support an ERP system for unified management, purchasing and distribution.

The company selected a solution comprising Juniper Networks firewall/IPsec VPN, SSL VPN, and enterprise-level routers and switches. A Juniper Networks ISG 1000 at headquarters supports VPN tunnels to more than 240 branches and restaurants, providing firewall performance of up to 2 Gbps and 3 DES IPsec VPN performance of up to 1 Gbps through up to 2,000 VPN tunnels. A Juniper Networks NetScreen-208 firewall separates Internet traffic from the IPsec VPN network traffic, making sure ERP traffic gets sufficient bandwidth while providing complete security. Ajisen Ramen also uses the SSL VPN-based Juniper Networks Secure Access 2000 (SA 2000) to give mobile users secure access to the servers at the headquarters.

"Each store can now securely transmit real-time business and inventory data to the headquarters, allowing us to manage our inventory and business issues more effectively," says Michael Wang, IT Director for Ajisen (China) Holdings Limited. At the same time, Juniper's Network and Security Manager (NSM) allows IT personnel to manage and

monitor the VPN from a single platform, greatly improving management efficiency and security while reducing operational costs.

Protecting intellectual property, as well as the inherently sensitive nature of human resources data, means that security is a top priority for workforce management provider Kronos. Because of a growing volume of business and applications, the company also needed to dial up the capacity on the Internet connection at its Chelmsford, Mass., headquarters.

When considering its options for a high-performance router to support the company's OC3 Internet connection, Kronos chose the Juniper Networks M-series multiservice edge router. "The reason we bought Juniper routers is superior hardware architecture, consistent upgrade release schedule, and reliability," says Doug Tamasanis, chief IT architect and director of networks and security at Kronos.

The results: IT productivity has improved because the network is easier to manage centrally. Field offices do not have IT staff, even though several of the larger locations have hundreds of employees. In particular, segmenting the network into zones simplifies troubleshooting. Tamasanis noted that the investment protection inherent in Juniper gear affords him long-term savings. Nearly two dozen field offices have relied on the same Juniper firewalls for more than seven years. "We don't have to buy a new box to get more performance in the future, because Juniper equipment lasts and the products scale at performance," he says.

Banking on Juniper: Handelsbanken

When the Swedish bank Handelsbanken was looking to upgrade the network that serves its 450 branch offices, it settled on an integrated solution from Juniper that provides not only the top-notch security that any bank requires, but superior performance, support and management.

Handelsbanken's business strategy is to focus on achieving high profitability by offering customers better service, while keeping its own operational costs relatively low, a feat it accomplishes in large part by investing in secure, reliable IT networks.

When the bank was looking to provide additional bandwidth to its network, which serves sites in Sweden, Norway, Denmark, Finland and the United Kingdom, it looked for a vendor that could combine security with performance. "Being a bank," says Lars Wibeck, Head of Data Communications at Handelsbanken, "our priority has always been for network security, so we would only install the very best network security products."

He selected a variety of Juniper products to provide VPN encryption and firewalls at each branch, along with denial of service protection [DoS], antivirus and Web filtering. Specifically, the bank installed two Juniper Networks Integrated Security Gateway (ISG) 2000 integrated firewall/VPN systems, 450 Juniper Networks Integrated Threat Management (ITM) devices at its branches, and a Juniper Networks Network and Security Manager (NSM) management platform for its central site.

The ISG 2000 system is a purpose-built, high-performance security system that integrates best-in-class deep inspection firewall, VPN and DoS solutions. It delivers linear performance for all packet sizes at gigabit levels that support applications requiring low latency and small packet throughput.

The ITM devices, meanwhile, integrate key security applications, routing protocols and resiliency features to provide a cost effective, easy-to-manage solution. Inbound and outbound traffic is controlled by policies that determine what traffic is allowed.

NSM is a centralized management solution that controls all aspects of the Juniper Networks firewall/ IPsec VPN devices—including device configuration, network settings and security policy.

In keeping with its corporate strategy, the Juniper security solution has proven to be cost effective, efficient and easy to deploy.

"The hallmark of a good security system is that it is invisible to its users even though it does its job," Wibeck says. "We have gained many benefits from our new MPLS network, but it is the Juniper devices that keep everything moving at line speed rate while keeping everything secure."