BUSINESS **SOLUTIONS**

Computer Crime: Network Attacks and Defense

Ingenious, profit-driven attacks offer new threats to business.

It seems security breaches are making new headlines every day. Today's attacks are more targeted against specific industries and enterprises rather than general attacks aimed at any computer on the network.

The attackers are looking for vulnerabilities that get them access to sensitive information or sensitive capabilities. Unlike the past when hackers were looking to have fun or claim fame, today they are looking to sell vulnerabilities or spyware applications for profit.

In the past two to three years, "We've seen a major shift in security attack targets," says Rohit Dhamankar, director of DVLabs at TippingPoint Technologies, an Austin, Texas, provider of network-based security systems.

"No longer are hackers seeking to exploit vulnerabilities in operating systems," he says. "Instead we are seeing more attacks on client-side and web applications."

Organizations need to guard against threats such as Trojans that can plant stealthy keylogger software to search a network for identity information; botnets that can hijack computers to launch outbound attacks on other networks; hackers looking for trade secrets; a host of spyware, viruses and other malware; and blended threats that combine several types of attacks.

Application Usage

Many organizations are writing customized web applications that help employees and businesses work more efficiently. "Unfortunately, these custom web applications are often full of security vulnerabilities," Dhamankar says.

"As more and more software and e-mail applications move to the web, these vulnerable applications are becoming gateways that facilitate data theft and corporate espionage," he adds.

Network and application usage is dramatically changing the way networks are designed, managed and protected, adds Jon Kuhn, director of product management at SonicWALL, a Sunnyvale, CA. security technology provider. Trends such as Web 2.0, that use web-based applications, have radically increased total traffic across networks.

"The new paradigm of network communications threatens to undermine control and policy across network boundaries," Kuhn says. "These could become the new conduit for evolving threats."

Creating a completely failsafe security environment is extremely difficult, given the changing nature of networks, security threats and other factors. But organizations can take steps to deploy technologies that can help bolster defenses and reduce the risk of attacks.

Here's a look at some key areas of defense.

Firewalls

The firewall is the first line of defense against outside intrusions against the network. Properly configured firewalls can defend against many types of attacks before they're able to penetrate various parts of the network.

Firewalls vary in terms of capabilities and ease of use. Some firewalls, particularly older or low-end products, came preconfigured with rules for blocking common attacks. These were likely not designed for the latest and most sophisticated attacks. Consequently, they should be replaced with products built to defend against newer threats.

The newer firewalls begin with a basic set of rules and allow managers to configure them so that they can provide the needed level of security. Today's firewalls are available in two main types: network-layer firewalls and application-layer products. These firewalls differ mainly in how deeply they inspect network traffic and in the complexity of their rules.

Network-layer firewalls are basic products that analyze Transmission Control Protocol/Internet Protocol (TCP/IP) packets at the protocol level. They use rules based on information found at that level, such as source or destination address, port numbers, Media Access Control (MAC) addresses and domain names.

Information in the TCP/IP header of each packet is scanned by the firewall and information is passed through or blocked based on rules. Oftentimes network-layer firewalls are able to block most undesired network traffic while allowing permitted traffic to flow.

Most application-layer firewalls provide the functionality of a network-layer firewall but go a step further by examining data within the packets. This allows organizations to deploy firewall rules based on content, such as allowing web browsing while blocking multimedia content.

Firewalls have come down in price and are generally easier to manage. Therefore, it might make sense to use multiple firewalls to protect a network configuration.

Antivirus and Antispyware

Antivirus and antispyware software products analyze files to protect against viruses, worms, Trojan horses and other malware, as well as to block spyware such as keyloggers. For this managers have a huge number of products from which to choose.

Signature-based scanning is the most common type of malware detection, and is particularly effective against known threats. On the negative side, there's always a lag between the time when threats are identified and the deployment of the signature for updating antivirus applications. Because of this, signature-based systems can't keep up with fast-changing malware threats.

Another type of scanning, called heuristic, is designed to detect viruses that were previously unknown. Rather than looking for pre-identified strings, the software searches for instructions or commands that aren't typically found in commonly used applications.

This type of scanning can detect viruses and worms whose signature has not yet been published. Heuristic scanning is used in conjunction with signature-based scanning but does not replace it.

Yet another approach to defending against viruses is Network Behavior Anomaly Detection (NBAD). These products, used in addition to conventional antivirus defenses, track critical network characteristics and sound alarms if they detect unusual events or trends that might indicate an attack.

Finally, reputation-based antivirus technology, like heuristic scanning, offers protection against so-called zero-day attacks. To be effective, these products rely on a frequently updated database of information about spam and viruses.

Because of the constantly changing nature of attacks, it's critical to keep antivirus and antispyware software up to date. "Antivirus/malware protection on the client machine is essential for overall security, whether or not there is a gateway device protecting the network," Kuhn says.

Intrusion Prevention and Detection

Because firewalls are somewhat limited by the way they're designed, many organizations need additional network defenses to protect against certain types of intrusions. A more advanced level of gateway protection, that involves more sophisticated decision-making, is intrusion prevention/intrusion detection.

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are similar to firewalls in that they examine network traffic and allow or block traffic based on set rules. However, an IPS/IDS is more complex, examining the data portion of network traffic to look for common elements in otherwise normal-appearing network traffic.

Because of this added capability, they can detect and stop attacks that might otherwise get past firewalls and other types of perimeter defenses. The detection method IPS/IDS technologies use, called pattern analysis, is similar to the technology used in virus scanners.

"An effective IPS should be able to stop a wide range of security attacks," TippingPoint's Dhamankar says. "These include worms, viruses, Trojans, Denial of Service (DoS) attacks, peer-to-peer bandwidth floods, spyware, phishing, cross-site scripting, Structured Query Language (SQL) injections, PHP file includes, Voice over Internet Protocol (VoIP) attacks and whatever other threats are emerging against operating systems, client-side applications and web applications."

Intrusion prevention systems provide not only a tighter lockdown of the environment to ensure against outside attacks, but also to guard against employee misuse or abuse of networks, adds Brian Grayek, vice president, product management at software vendor CA Inc. in Islandia, N.Y.

One key benefit of pattern-based IPS/IDS is that it protects organizations against zero-day attacks. If such an attack follows an identified pattern, the IPS/IDS will block the attack, even if the specific vulnerability hasn't yet been identified.

While offering many capabilities, IPS/IDS is not designed for widespread use. The systems are slower than comparable firewalls, and they're more difficult to maintain and configure due to their complexity. As a result, IPS/IDS technology is not likely to replace firewalls.

Internet Filtering

The filtering of web content is an effective way to block e-mail spam, data leakage, threats from websites that are known to contain malicious code and access to inappropriate websites. Internet filtering systems can also be applied to instant messaging systems and File Transport Protocol (FTP) file transfers.

In order to provide maximum protection, organizations should filter both incoming and outgoing web traffic. By filtering incoming e-mail traffic, for example, they can detect and block spam and malicious attachments. By screening outgoing e-mail, they can prevent the intentional or accidental disclosure of sensitive information such as customer data.

Filtering outbound web requests also allows managers to prevent user access to risky web addresses. Inbound filtering monitors file content, allowing managers to control the type and size of file downloads. These systems come with configuration controls that let managers control what is allowed or denied.

As with other security products, there are many different types of content filtering systems to choose from. A filter can be installed on a firewall, or be provided as a dedicated hardware appliance that runs in parallel with a firewall.

Internet filters typically use a combination of filtering methods based on file type, word or phrase detection, URL, header analysis, HyperText Markup Language (HTML) anomalies and blacklists.

Network Access Control

NAC technology is similar to firewalls and IPS/IDS in that it permits or forbids network access. But NAC products differ from those other systems because they provide user-focused access control, allowing or denying access based on the identity of the user and his or her role.

NAC systems provide network access control through authentication, endpoint-security assessment and network environmental information. Each of these factors is used in setting up access-control policies.

Authentication is the process through which a user asserts his or her identity, which is then validated by a server. Endpoint-security assessment is the foundation of NAC deployment and is the most complex element of NAC.

These products look at the security postures of all connecting systems, such as servers, desktops and notebook PCs, to be part of the access-control policy. So if a PC connected to the network is not equipped with the necessary antivirus software, for example, a different access control policy is applied to that user than that applied to a PC running updated software.

Network environmental information grants access to a network based on a user's location. If the user is connecting to a wireless network, for example, access might be more limited than it would if the user were connecting from within a building.

"NAC products go beyond traditional firewalls and VPNs [Virtual Private Networks] to authenticate and authorize users trying to enter a network, perform integrity checks on their devices and grant conditional access to specific locations or resources based on an integrated network-access policy," Dhamankar says.

Unified Threat Management

UTM systems are integrated suites of security products that provide the enterprise with multiple security functions. They combine firewalls with intrusion detection or prevention, antivirus, and e-mail and web-content filtering.

These emerging multifunction gateway appliances offer potential benefits such as ease of installation, management and maintenance. Experts say unified threat management is a promising approach to integrated gateway security.

With UTM, instead of having a management console for each security tool, managers can have a single console for configuring, monitoring, logging and managing all gateway security functions.

"UTM brings stateful firewall and application awareness together with antivirus, antispyware, intrusion prevention, content filtering and other forms of inspection," Kuhn says. "This is brought to the gateway on a single appliance that acts as the first and most comprehensive layer of network defense in an organization."

Building a Case for Additional Security Spending

IT budgets are tight, especially in a difficult economy. Technology managers need to build a strong case in order to glean extra budget dollars for network security measures.

"It is important for organizations to keep security spending on the forefront during a tough economy," says Rohit Dhamankar, director of DVLabs at TippingPoint Technologies, Austin, Texas.

"Although IT and security managers will face the tedious task of reducing security spending, they need to consider the potential price they'll ultimately pay for sacrificing security."

IT security managers need to make it clear to senior business executives that threats don't go away during an economic slowdown. In fact, they might even increase. Research also shows that the security technologists need to look for an influential executive to champion the cause.

"It's always a question of risk versus return. Security managers must first measure or quantify the risk," says Brian Grayek, vice president, product management at software vendor CA Inc. in Islandia, N.Y.

Then they need to provide a comparison to the costs of exposure to show management how the security spending will contribute to a better protection of the business and its continued operations, Grayek says.

"Security's ultimate goal is not to be an obstacle," Grayek adds. "It is to be an enabler to allow the business to continue to function at its optimum level."

Security spending "needs to be tied back to the business that the enterprise is engaged in," says Eric Maiwald, vice president and research director, Security and Risk Management Strategies, at Burton Group, a Midvale, Utah, research and advisory firm.

"Regulations will not go away just because the economy is bad, so some security activities will need to continue," he adds. "In a bad economy, the security team will need to meet the regulations efficiently. I'm not suggesting that there is an ROI here. However, there may be a cost savings available by performing the necessary activities more efficiently."