isResearch

a product of linmun research, llc

Best Practices in IT Security

Summer 2004

Analyst: M. Villano

Introduction

In today's ever-changing business environment, nothing is more important than securing the corporate network. In addition to the constant threat of a hacker assault from both inside and outside the corporate network, the number of security attacks increases virtually every day, presenting still other concerns for Chief Information Officers and network security administrators. The recent outbreaks of viruses such as MyDoom and NetSky, coupled with the recent network worm known as Sasser that terrorized the world, underscore the importance of building an enterprise security architecture that preserves the sanctity of corporate data and resources against any threat. With networks, as with life, it's clear that one can never be too safe.

To wit: According to the Computer Emergency Response Team, enterprises reported roughly 4,000 security incidents in 2003, up slightly from the number of incidents reported in 2002. Of these, a majority of attacks are exploiting known operating system and application vulnerabilities; In *InformationWeek*'s 2003 U.S. Information Security Survey, only 21 percent of the 815 companies surveyed said their systems were attacked through "unknown" operating system weaknesses. This year alone, more hundreds of flaws also were identified in the very products that users buy to safeguard their systems, including products from vendors such as Internet Security Systems, Zone Labs, Check Point Software Technologies, and Symantec. IT research firm Gartner reports that these flaws cost enterprises an average of hundreds of thousands of dollars at best, and millions at worst.

This white paper outlines the best ways of establishing a strategy to tackle security issues as they arise now, and explores some of the most critical components of security today. It identifies ten key areas of perimeter and internal security, and suggests best practices in each. Finally, the paper looks to the future, suggesting security strategies in emerging technology areas such as multi-factor authentication, identity management, and biometrics. After all, it's never too early for an organization to begin securing its network for the threats of tomorrow.

Security Planning

For organizations of every size, a network security strategy must start with a plan. There are many ways to devise this plan, but perhaps the best way is through a planning team comprised of people involved in different aspects of IT from different areas of the enterprise. Creating the policy should be a group effort, and responsible representatives from different departments should be involved to keep communication flowing. The team should not only include IT staff members; knowledgeable people from elsewhere in the organization can offer valuable input, too, and should be encouraged to participate.

Once the team is created, their first job is to analyze business requirements. What services are required for business? How might these requirements be met securely? How much do employees depend on Internet access, e-mail, and the availability of Intranet services? How important is remote access? The hardest part of answering these questions is distinguishing wants from needs. It takes discipline to ask repeatedly, "Is this a business requirement?" Still, this is the most important question, and the best way to navigate the planning process quickly, in a manner that always keeps the organization's interests in mind.

Next, this phase must involve the development of a vulnerability analysis (sometimes it also is referred to as a "risk analysis" or a "threat assessment"). The analysis encompasses identifying assets, evaluating potential threats, appraising existing countermeasures, and determining a cost/benefit analysis for each. Numerous factors should be considered in this process, including how information is used and managed, and how effective and relevant existing security measures really are. Key questions here include:

- What are we trying to protect?
- Which attacks are possible? Which are probable?
- Where are we most vulnerable?
- What security measures are in place?
- How much would it cost to counter an attack?

Root Security Policy

Once a security organization has answered questions like these, the next step is to develop a root security policy. This policy is where the vulnerability analysis and business requirements come together, where security managers address how their organization handles information, whom may access that information, and how they would go about doing so. The policy also specifies allowed and denied behaviors, and lists controls that are to be put in place. It is, put simply, an organization's security Bible, and provides the framework upon which all required information and sub-policies hang.

Specifically, the root policy tackles issues such as security architecture guidelines, incident response procedures, acceptable use policies, and system administration rules. Security architecture guidelines specify countermeasures to the threats detailed in the vulnerability analysis, and dictate how to establish perimeter and desktop security. Incident response procedures outline what to do in the event of an attack. Acceptable use policies describe which end-user actions are permitted and prohibited on the network. Finally, system administration rules offer lock-down guides that address organization-specific steps for hardening vendor-supplied systems.

While every aspect of root policy differs by company, it is most important for contributing security team members to familiarize themselves with modern-day realities in the area of security architecture. The two major components of this discipline are perimeter security and desktop security, and in order to understand best practices on each level, IT professionals first must be comfortable with specific security considerations across the entire network.

Perimeter Security

The process of securing an enterprise network begins at the network edge, otherwise known as the perimeter. Not surprisingly, security at this level consists of monitoring the types of traffic that come in and out of the router and over the transom to the corporate network itself. There are a variety of ways to do this, from firewalls to VPNs, intrusion detection to intrusion prevention. In the last 12 months, the perimeter security marketplace also has seen an entirely new niche develop – a niche devoted to the notion of managing patches for all of the other devices that are used to guard the network edge.

Firewalls

The best way to do monitor basic perimeter-level traffic is with the help of a firewall. A 2003 Evans Data survey of more than 500 North American enterprises found that firewall devices are the most likely method to secure data, with point anti-virus and VPN tools a distant second and third, respectively. Firewalls burst onto the scene before the e-commerce revolution of the 1990s, and were designed to stop threats cold. These original devices were built as plug-and-play hardware appliances with the sole purpose of stopping attacks from the outside; since then, the network security landscape has evolved dramatically. Today many vendors boast hardware-software combinations that integrate a number of security-oriented functions into one plug-and-play device.

Naturally, the integrated devices work best. Security issues change multiple times a day, and in order to protect against all of the latest threats, point solutions require constant updates that frequently come too late to do any good. What's more, because many of these solutions are hardware-based, they have short shelf-lives, and require that enterprises make frequent purchases simply to stay ahead of the game. With integrated devices, organizations can sign up for automatic updates from the vendors themselves. These update programs also include version upgrades as well, meaning that once an enterprise makes the initial investment, they don't need to purchase any more hardware unless they expand capacity significantly.

There are quite a number of integrated firewall appliances on the market today, but some of the more cost-effective ones include:

- FortiGate from Fortinet
- Sleuth9 from DeepNines
- NetScreen 5GT series from Juniper
- Proventia from Internet Security Systems
- 5400 Series from Symantec
- InterSpect from Check Point
- IntruShield from McAfee

Virtual Private Networks (VPNs)

VPNs are private networks that are configured within a public network in order to take advantage of the economies of scale and management facilities of large networks. They are widely used by enterprises to create wide area networks (WANs) that span large geographic areas, to provide site-to-site connections to branch offices and to allow mobile users to dial up their company Local Area Networks (LANs). There are literally dozens of VPN clients on the market today, but few of them have any security precautions beyond the basics. With this in mind, the best VPNs to choose are those that are totally encrypted, otherwise known as VPNs that feature a Secure Sockets Layer (SSL).

SSL VPNs are the most secure VPN an organization can buy. SSL is the leading security protocol on the Internet. When an SSL session is started, the server sends its public key to the end user, which the end user then uses to send a randomly generated secret key back to the server in order to have a secret key exchange for that session. The SSL VPN ensures security by randomly generating a new key every single time a user logs on. Developed by Netscape, SSL technology has been incorporated into some of the leading VPN products from vendors such as Cisco, Check Point, Aventail, Nokia, and Secure Computing.

Taken by themselves, however, even SSL VPNs are not foolproof. In a recent report, analysts from IT research firm Yankee Group suggested that organizations require that security software is running before they allow a VPN connection of any kind. The report encouraged organizations to tear down the VPN session if an end user's security software is turned off while the network link is established. It also said that organizations should terminate sessions if a user turns off his or her security software after the VPN connection has been successfully enabled. In both cases, there is no way to know if the system is compromised, or if the user is actually a hacker in disguise.

Intrusion Detection Systems (IDS)

An IDS is a software-based solution designed to detect an attack on a network or computer system. Technically, there are two types of IDS – the Network IDS (NIDS), which is designed to support multiple hosts, and the Host IDS (HIDS), which is set up to detect illegal actions within the same host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

In theory, this approach was a revolutionary spin on real-time network monitoring; in practice, however, experts say that it suffers from a variety of shortcomings. First, without extensive, continual tuning, a network-based IDS triggers too many false alarms, generating thousands of alerts for every actual attack detected. Secondly, the system generally can't handle the high speeds of internal networks, failing to detect attacks at "wire speed," or in real-time. Citing management and performance drawbacks, a 2003 Gartner Information Security Hype Circle report declared the IDS category a "market failure," and recommended that organizations shift resources to vulnerability scanning, server hardening, and newer, deep-packet inspection firewalls.

For organizations looking to perform best practices, it's a good idea to steer clear of IDS.

Intrusion Prevention Systems (IPS)

IPS, however, is another story all together. An IPS is a software-based solution that sits close to the network perimeter and actively prevents an attack on a network or computer system. The technology is a significant step beyond IDS, because while the latter only detects threats, the former stops attacks from damaging or retrieving data. Put differently, while IDS technology passively monitors traffic by sniffing packets off a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets.

The biggest benefit to IPS, of course, is that the technology blocks attacks in real-time. With integrated firewall appliances flooding the market over the last 6 months, analysts note that the best way for organizations to incorporate IPS is to purchase an integrated device that has the technology built-in. For those enterprises seeking a standalone IPS solution, some of the highest-rated products include the Entercept and IntruShield tools from McAfee (formerly Network Associates), and the Security Tandem tool from Symantec.

Patch Management

As threats continue to mount, an organization's need to make sure its defenses are secure increases as well. Inevitably, hackers will find new vulnerabilities in existing software and hardware products, necessitating an aggressive and consistent strategy on the part of an enterprise to patch these holes. Most organizations call this strategy patch management. How an enterprise administers the strategy, however, can make or break the entire effort.

The golden rule: patching is not simply updating software. Many analysts suggest that enterprises engage in the practice of patching secure remote systems configurations. Others add that the act of patch management should also include the distribution of new software updates and changes to the configurations of the remote system. It's a safe bet for enterprises to conduct new security assessments of remote endpoints after new configurations have been installed. The service provider Fiberlink has announced a partnership with patching vendor BigFix and currently leads in this market. Other vendors to consider for this process include:

- Shavlik
- PatchLink
- BindView
- Ecora
- St. Bernard Software
- LANDesk

Desktop Security

Securing the perimeter is one thing; securing the desktops inside an enterprise's LAN and/or WAN is a completely different ballgame. While the former strategy revolves around scanning the entire spectrum of network traffic for general threats and attacks, the latter focuses on scanning traditionally weak spots on the network for specific problems. Almost every vendor in the security space offers products designed to secure the desktop. Some products are better than others; while this paper attempts to recommend the best of the best for specific solutions, enterprise managers should try products and consult industry test center reviews for a more complete rundown.

Anti-Virus

Anti-virus programs, or virus scanners, are pieces of software that search for binary signatures (patterns) of known viruses that have attached themselves to executable programs. As new viruses are discovered, the signature database has to be updated in order for the anti-virus program to be effective. Many anti-virus vendors generally offer downloads via the Web in order to keep current; some even offer these updates automatically, saving network managers the trouble of manually staying on top of the process every day.

There are two ways in which these scanning devices work. One type scans every file each time you boot the computer and each time a file is opened. The other takes a blueprint of all existing executables one time and scans the file only when it has changed. This latter method saves time when starting or rebooting the computer since there is no processing performed. In addition, opening files is quicker, because the anti-virus software does not scan the file unless it has been changed, and it can determine if the file has been changed much faster than it can scan it for thousands of viruses.

Some of the best anti-virus products on the market today include:

- Norton Anti-Virus from Symantec
- VirusWall and House Call from Trend Micro
- ZoneAlarm with Antivirus from Zone Labs
- VirusScan from McAfee

Anti-Spam

Much like viruses, spam has become a scourge on the Internet as hundreds of millions of unwanted messages are transmitted daily to almost every e-mail recipient, as well as to newsgroups. To prevent this, enterprises can install spam filters on user machines or in the mail server, in which case, the user never receives spam in the first place. Spam filtering can be configured to trap messages based on a variety of criteria, including sender's e-mail address, specific words in the subject or message body or by the type of attachment that accompanies the message. Enterprises also can choose to block messages if the messages come from habitual spammers, illegitimate senders frequently found on industry address lists known as blacklists.

Not all spam filters are created equal. Basic filters block messages based upon the simplest criteria. More sophisticated spam filters use artificial intelligence techniques known as heuristics that look for key words and attempt to decipher their meaning in sentences in order to more effectively analyze the content and not trash a real message. These top-level spam filters also divert mail that comes to users as "Undisclosed Recipients," instead of having a user's e-mail address spelled out in the "to" or "cc" field. Spam products to consider in this top category include:

- PGPUniversal from PGP
- Brightmail Anti-Spam from Symantec
- MailFrontier Desktop from MailFrontier
- Antigen 7.5 from Sybari

Anti-Spyware

The latest security threat, spyware, software designed to collect user data without their knowledge, began, like many other threats, as a consumer problem but has quickly moved into the corporate world. Secretly piggybacking on downloaded Internet software, spyware passes through a corporate firewall and either slows traffic with pop-up advertisements or transmits information about computer usage back to its creator. The threat is as common as it is complex. An April 15 report from ISP EarthLink and WebRoot Software indicated that the average computer is crammed with 28 pieces of spyware.

With such widespread implications, government officials are taking the threat seriously. In the U.S. Congress, at least three bills have been introduced in the past six months to address the problem, and in late May, Utah will enact the Spyware Control Act, which calls for a $10,000 fine for violators. Vendors are also taking steps to combat spyware. Last month, Zone Labs unveiled a new version of its Integrity software designed to detect and disable spyware. Products from vendors such as Symantec, McAfee and Cisco Systems include some of the same capabilities. Even Bluecoat has gotten in on the act by adding spyware capabilities to its ProxySG device. Another good option for snuffing out spyware: UnityOne, from TippingPoint.

Compliance Management

Another issue that network security experts find themselves facing lately is the need to comply with reporting regulations that govern companies today. As such, many security vendors now specialize in solutions that facilitate regulatory compliance without hindering the alacrity or financial resources of a business. In the wake of recent corporate accounting scandals, as well as the Health Insurance Portability and Accountability Act of 1996, now there are a bevy of regulations with which corporations must comply. Understandably, then, there are literally dozens of compliance management programs tailored to help enterprises comply with regulations in a variety of different industries.

Because some of the regulations facing enterprises today are so complex, the process of managing compliance across an IT network can become incredibly expensive. With this in mind, organizations are encouraged to enter the compliance management space slowly, focusing on one regulation at a time.

Endpoint Management

Finally, the endpoint. It's no secret that remote users are among the most common sources of enterprise attacks. Mobile employees pick up viruses and worms on the road, and infect the corporate network when they access remotely through a VPN or plug in at the office. With threats changing every day, network administrators struggle constantly to establish policies to make sure that these vulnerable portions of their networks are safe. Perhaps the best way to do this is to establish a policy of endpoint management.

Endpoint management is a growing trend. In May 2004, at the Network Interop conference in Las Vegas, members of the newly founded Trusted Computing Group (TCG) gained a roster of new members determined to write a spec for security policy enforcement for anti-virus, patch levels and intrusion-prevention systems. This move followed similar announcements from industry-leading vendors such as Cisco Systems and Microsoft, which both say they're working on applications that would force users' computers to be submitted for automated inspections, every time they log on.

In particular, industry insiders suggest that after this initial scan, enterprises should quarantine users that cannot be certified as secure, and keep them quarantined until they install or apply the appropriate patches and/or extraction processes. These experts say that in today’s day and age, it’s not enough to ensure that security software is running on an endpoint computer. Instead, they note, systems should be running the latest anti-virus signatures, the latest firewall or IDS/IPS software, and the latest anti-spyware technology to keep hackers out. Forcing all users to take these precautions before granting them access to the network will reduce exposure to worms propagating throughout a network after the network has been cleaned, and will prevent attacks before the dirty systems can connect in the first place.

Other Considerations

The previous perimeter and desktop security concerns are undeniably the top ten issues facing network security managers today. Even still, other security considerations are emerging as critical for enterprises to take into account to ensure security down the road.

The first is identity management, the management of a user's identity in an organization and what resources that person has access to. The backbone of this technology is a system of directories and directory-enabled applications. Because the solution controls access, though, it is considered a part of security, and is one of the fastest-growing segments of the security marketplace. Market leaders in this space include vendors such as IBM, Singlestep, Oblix, and MaXware. Each of these vendors offers identity management packages for networks of any size.

Another emerging security niche is authentication, the process by which users actually sign on to their individual computers. In the past, users accomplished this task by typing in passwords or simply turning their machines on. Today, however, an increasing number of companies are implementing USB authentication tokens that users must insert before they log on, providing multi-factor proof that the user is who he or she says. One alternative for hard authentication is a Smartcard, a plastic card with a microchip that contains valuable information about its user. Companies that employ this method require users to insert their Smartcards into readers before logging on. Users must then keep their Smartcards in the readers for the duration of the time they are using the machine; if a card comes out, that user must go through the entire authentication process again.

Finally, the most sophisticated enterprises today are securing their physical facilities with a technology called biometrics. Biometrics is the biological identification of a person, and includes characteristics of structure or action such as hand geometry, voice responses to challenges and the dynamics of hand-written signatures. Biometric technology represents a more secure form of authentication than typing passwords or using Smartcards because biometric identifiers cannot be stolen – they are part of each individual user, and are unique to each one. Some forms of biometric authentication, however, such as iris scans and fingerprints, have relatively high failure rates.

Conclusion

Whichever methods an enterprise uses to enhance security, the bottom line is that when it comes to securing corporate information, an enterprise never can be too safe. Perhaps nothing is more important than building an enterprise security architecture that preserves the sanctity of corporate data and resources against any threat. Enterprises can attempt to construct this security strategy quickly and thoughtlessly, or they can invest the time and energy to think out vulnerabilities, plan a response, set a policy, and prepare by establishing the best architecture money can buy. In the end, an organization truly will receive what it pays for. But only the smartest enterprises will survive.

Resources:

The following books and Web sites can provide insight into the development of sound security policies and procedures:

- Firewalls and Internet Security: Repelling the Wily Hacker. Bill Cheswick and Steve Bellovin. Addison-Wesley, June 1994.
- Designing Systems for Internet Commerce. Win Treese and Larry Stewart. Addison-Wesley, 1998.
- Web Security Sourcebook. Aviel Rubin, Daniel Geer, and Marcus Ranum. Wiley Computer Publishing, 1997.
- Information Warfare and Security. Dorothy Denning. Addison-Wesley, 1999.
- Information Security: Policies and Procedures. Thomas R. Peltier. CRC Press, Auerbach Publications, December 1998.
- The Information Systems Security Officer's Guide: Establishing and Managing and Information Protection Program. Gerald Kovacich. Butterworth-Heinemann, May 1998.
- The Sans Institute, www.sans.org.
- The Computer Security Institute, www.gosci.com.
- Project Coast, www.cerias.purdue.edu/coast.