CISCO SYSTEMS

Network Security:
An Executive Overview

Over the past few years, Internet-enabled business, or e-business, has drastically improved companies' efficiency and revenue growth. E-business applications such as e-commerce, supply-chain management, and remote access allow companies to streamline processes, lower operating costs, and increase customer satisfaction. Such applications require mission-critical networks that accommodate voice, video, and data traffic, and these networks must be scalable to support increasing numbers of users and the need for greater capacity and performance. However, as networks enable more and more applications and are available to more and more users, they become ever more vulnerable to a wider range of security threats. To combat those threats and ensure that e-business transactions are not compromised, security technology must play a major role in today's networks.

Why Networks Must Be Secured

Attacks

Without proper protection, any part of any network can be susceptible to attacks or unauthorized activity. Routers, switches, and hosts can all be violated by professional hackers, company competitors, or even internal employees. In fact, according to several studies, more than half of all network attacks are waged internally. The Computer Security Institute (CSI) in San Francisco estimates that between 60 and 80 percent of network misuse comes from inside the enterprises where the misuse has taken place. To determine the best ways to protect against attacks, IT managers should understand the many types of attacks that can be instigated and the damage that these attacks can cause to e-business infrastructures. The most common types of attacks include Denial of Service (DoS), password, and root access attacks.

DoS attacks are particularly malicious because although they do not provide intruders with access to specific data, they "tie up" IS resources, preventing legitimate users from accessing applications. They are usually achieved by hackers sending large amounts of jumbled or otherwise unmanageable data to machines that are connected to corporate networks or the Internet. Even more malicious are Distributed Denial of Service (DDoS) attacks in which an attacker compromises multiple machines or hosts. According to the 2001 Computer Security Institute (CSI) and FBI "Computer Crime and Security Survey," 38 percent of respondents detected DoS attacks, compared with 11 percent in 2000.

Historically, *password attacks*, attacks in which a perpetrator gains unauthorized access to network passwords in order pernetrate confidential information, have been the most common type of attacks. When a hacker "cracks" the password of a legitimate user, he has access to that user's network resources and typically a very strong platform for getting access to the rest of the network. For example, in December of 2000, a hacker stole user passwords from the University of Washington Medical Center in Seattle and gained access to files containing confidential information regarding approximately 5000 patients. Hackers can often easily obtain passwords because users typically choose common words or numbers as their passwords, enabling the hacker's use of software programs to methodically determine those passwords. Hackers also deploy social engineering techniques to gain access to passwords. Social engineering is the increasingly prevalent act of obtaining confidential network security information through nontechnical means, such as posing as a technical support representative and making direct phone calls to employees to gather password information.

From the early days of the Internet, when only e-mail servers were on the network, a hacker's ultimate goal was to gain *root access* to the UNIX host that ran these applications. With root access, the hacker had full control of the system and could often collect enough information to gain access to the rest of the network and other partner networks. E-business application hosts have increased the number of targets for hackers. Hackers often exploit security vulnerabilities, or security holes, in the operating systems or applications of these hosts that system administrators have not safeguarded. Using buffer overflows, trojan horses, and other common techniques, hackers gain control of hosts that can be used as platforms for launching other attacks. These practices often result in a full compromise of an organization's IS infrastructure and can lead to serious financial losses or legal liabilities.

Cost of Intrusions

Network attacks cause organizations several hours or days of downtime and serious breaches in data confidentiality and integrity. Depending on the level of the attack and the type of information that has been compromised, the consequences of network attacks vary in degree from mildly annoying to completely debilitating, and the cost of recovery from attacks can range from hundreds to millions of dollars.

When *application availability* is compromised by attacks, companies can easily lose millions of dollars per hour. For example, companies that run e-commerce Web sites lose revenue as customers "shop" elsewhere for their products and services; informational Web sites can lose precious advertising time; and manufacturing organizations that use supply-chain management applications can be forced to shut down their lines because they cannot access information regarding their raw materials.

When data *confidentiality* is compromised, the consequence to an enterprise is not always immediate but it can be costly. For example, if a hacker gains access to an organization's e-mail system, proprietary information that provides competitive advantage might be stolen resulting in a loss of research and development dollars spent in gaining that advantage.

When *data integrity* is compromised, an organization must often incur prohibitive costs to correct the consequences of attacks. For instance, a malicious hacker might modify a Web site, replacing relevant information with nonsensical or offensive content. This compels the proprietor of the site to spend money not only to fix the site, but also to counter the resulting bad public relations.

The legal ramifications of breaches in data confidentiality and integrity can also be extremely costly for organizations. The US Government has enacted and is currently developing regulations to control the privacy of electronic information. In fact, there are currently approximately 50 bills before the US Congress related to the regulation of online privacy and security. The existing and pending regulations generally stipulate that organizations in violation could face a range of penalties. For example, organizations in violation of the Gramm-Leach Bliley Act, which includes several privacy regulations for US financial institutions, might face a range of penalties from termination of their FDIC insurance to up to US$1 million in monetary penalties.

Even if an external hacker is the perpetrator of an attack, the company storing that information can potentially be found negligent by the courts if the information was not adequately safeguarded. Furthermore, companies that suffer breaches in data integrity might be required to defend against lawsuits initiated by customers who are negatively affected by the incorrect or offensive data and seek monetary or punitive damages.

Designing the Security Infrastructure

The objective of network security is to protect networks and their applications against attacks, ensuring information availability, confidentiality and integrity. When organizations design their network security architectures to meet this objective, they must consider a number of factors. Not all networks and their associated applications have the same risks of attacks or possible costs of repairing attack damages. Therefore, companies must perform cost-benefit analyses to evaluate the potential returns on investment for various network security technologies and components versus the opportunity costs of not implementing those items. In the process, enterprises should make sure to consider their network security implementations as competitive advantages that can attract customers, employees, and partners.

Security Policy

Usually, the primary prerequisite for implementing network security, and the driver for the security design process, is the security policy. A security policy is a formal statement, supported by a company's highest levels of management, regarding the rules by which employees who have access to any corporate resource abide. The security policy should address two main issues: the security requirements as driven by the business needs of the organization, and the implementation guidelines regarding the available technology. In addressing these issues, the security policy typically includes several elements. For example, the security policy usually includes an authentication policy that defines the levels of passwords and rights required for each type of user (corporate, remote, dial-in, VPN, administrators, and so forth). Because business requirements and security technologies are always evolving, the security policy should be a living document that is updated regularly (at least once per year).

Security Architecture

The security architecture should be developed by both the network design and the IT security teams. It is typically integrated into the existing enterprise network and is dependent on the IT services that are offered through the network infrastructure. The access and security requirements of each IT service should be defined before the network is divided into modules with clearly identified trust levels. Each module can be treated separately and assigned a different security model. The goal is to have layers of security so that a "successful" intruder's access is constrained to a limited part of the network. Just as the bulkhead design in a ship can contain a leak so that the entire ship does not sink, the layered security design limits the damage a security breach has on the health of the entire network. In addition, the architecture should define common security services to be implemented across the network. Typical services include:

- Password authentication, authorization, and accounting (AAA)
- Confidentiality provided by virtual private networks (VPNs)
- Access (trust model)
- Security monitoring by intrusion detection systems (IDSs)

After the key decisions have been made, the security architecture should be deployed in a phased format, addressing the most critical areas first.

Security Technologies

As noted earlier, network security design requires that corporations determine the level of implementation investment and the total cost of intrusion they can withstand. Then corporations must decide how to allocate their available network security budgets to adequately secure their networks. To ensure the most comprehensive level of protection possible, every network should include security components that address the following five aspects of network security.

Identity

Identity is the accurate and positive identification of network users, hosts, applications, services and resources. Identity mechanisms are important because they ensure that authorized users gain access to the enterprise computing resources they need, while unauthorized users are denied access. Cisco Systems networks use the AAA capabilities of the Cisco Secure Access Control Server (ACS) to provide a foundation that authenticates users, determines access levels, and archives all necessary audit and accounting data.

Perimeter Security

Perimeter security solutions control access to critical network applications, data, and services so that only legitimate users and information can pass through the network. This access control is handled by routers and switches with access control lists (ACLs) and by dedicated firewall appliances. A firewall provides a barrier to traffic crossing a network's "perimeter" and permits only authorized traffic to pass, according to a predefined security policy. Complementary tools, including virus scanners and content filters, also help control network perimeters. Firewalls are generally the first security products that organizations deploy to improve their security postures. Cisco provides organizations considerable flexibility in firewall choices. The Cisco PIX® Firewall is the world's leading firewall, providing network customers of all sizes unmatched reliability, scalability, and functionality. The Cisco IOS® Firewall provides embedded firewall capabilities in the routing and switched infrastructures.

Secure Connectivity

Companies must protect confidential information from eavesdropping or tampering during transmission. By implementing Virtual Private Networks (VPNs) enterprises can establish private, secure communications across a public network—usually the Internet—and extend their corporate networks to remote offices, mobile users, telecommuters, and extranet partners. Encryption technology ensures that messages traveling across a VPN cannot be intercepted or read by anyone other than the authorized recipient by using advanced mathematical algorithms to "scramble" messages and their attachments. The Cisco VPN 3000 Concentrator Series is a best-of-breed, remote-access VPN solution. Incorporating the most advanced, high-availability capabilities with a unique purpose-built architecture, the Cisco VPN 3000 concentrators allow corporations to build high-performance, scalable, and robust VPN infrastructures to support their mission-critical, remote-access applications. An ideal way to build site-to-site VPNs is with Cisco VPN-optimized routers, which include the Cisco 800, 1700, 2600, 3600, 7100, and 7200 routers.

Security Monitoring

To ensure that their networks remain secure, companies should continuously monitor for attacks and regularly test the state of their security infrastructures. Network vulnerability scanners can proactively identify areas of weakness, and intrusion detection systems can monitor and reactively respond to security events as they occur.

Intrusion detection systems and vulnerability scanners provide an additional layer of network security. While firewalls permit or deny traffic based on source, destination, port, or other criteria, they do not actually analyze traffic for attacks or search the network for existing vulnerabilities. In addition, firewalls typically do not address the internal threat presented by "insiders." The Cisco Intrusion Detection System (IDS) is the industry's first real-time, network intrusion detection system that can protect the network perimeter, extranets, and increasingly vulnerable internal networks. The system uses sensors, which are high-speed network appliances, to analyze individual packets to detect suspicious activity. If the data stream in a network exhibits unauthorized activity or a network attack, the sensors can detect the misuse in real time, forward alarms to an administrator, and remove the offender from the network. The Cisco Secure Scanner is an enterprise-class software scanner application that allows an administrator to identify and fix network security holes before hackers find them.

Security Policy Management

As networks grow in size and complexity, the requirement for centralized security policy management tools that can administer security elements is paramount. Sophisticated tools that can specify, manage, and audit the state of security policy through browser-based user interfaces enhance the usability and effectiveness of network security solutions. Cisco provides a centralized, policy-based, security management approach for the enterprise. Cisco Secure Policy Manager (CSPM) supports Cisco security elements in enterprise networks, ensuring a comprehensive, consistent implementation of security policy. Using CSPM, customers can define, distribute, enforce, and audit security policies for hundreds of Cisco Secure PIX firewalls, IDS sensors, and Cisco IOS firewalls from a central location. CSPM also supports Cisco IP security (IPsec) VPN and intrusion detection technologies. In addition, the CSPM solution is also being integrated with CiscoWorks2000, Cisco's enterprise network management system, so it can leverage the full capabilities of this widely adopted management solution.

SAFE Blueprint for Secure E-Business

SAFE is a comprehensive, robust security blueprint based on Cisco AVVID (Architecture for Voice, Video and Integrated Data). The SAFE blueprint consists of modules that address the distinct requirements of each network area. By adopting a SAFE blueprint, security managers do not need to redesign the entire security architecture each time a new service is added to the network. With modular templates, securing each new service as it is needed and integrating it with the overall security architecture is easier and more cost effective.

SAFE is the first industry blueprint that recommends exactly which security solutions should be included in which sections of the network and why they should be deployed. Each module in the SAFE blueprint specifically provides maximum performance for e-business while allowing enterprises to maintain security and integrity.

SAFE programs include:

- Cisco security services partners that are experienced at translating business requirements into working security policies
- Cisco certification programs for security technology and products, ensuring that Cisco partners can plan, design, and deploy customers' security architectures
- A spectrum of security operation options that range from comprehensive outsourced services to consulting services for developing an operation plan and running regular security posture assessments (SPAs)

For more details on SAFE, visit http://www.cisco.com/go/safe/

For further information on network security, visit www.cisco.com/go/security/

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe