

The right security strategy will save your company money while bringing you peace of mind.

Background

The Internet and recent world events have fundamentally changed the way organizations approach security. Only a decade ago, network protection centered mostly on the concept of keeping people out at all costs. Anytime an outsider gained access to an organization's system, it was considered a serious problem. Today, the Web and networked e-business applications, telecommuting, branch connectivity, partner connectivity, and wireless mobility have emerged as increasingly important tools. As a result, protecting data is paramount.

Today's companies face myriad network security risks: Web site vandalism, viruses and Trojan horses, denial-of-service attacks, data destruction and theft, and a variety of other problems. These threats can come from outsiders or from employees, who may compromise security either intentionally or unintentionally. According to Computer Security Institute's 2002 Computer Crime and Security Survey, (<http://www.gocsi.com/press/20020407.html>) 90 percent of respondents—mostly large corporations and government institutions—had detected computer security breaches within the previous 12 months. Not surprisingly, 74 percent cited their Internet connection as a frequent point of attack.

Attacks are getting more sophisticated, and at the same time, much easier to deploy. In addition, companies face potential hazards from accidents and natural disasters. These security breaches can compromise application availability, data confidentiality, and data integrity while presenting legal ramifications. Perhaps most important, they interrupt business, which can lead to enormous costs to the organization.

Challenge

Today's e-business environment is particularly challenging because of the great number of threats that exist, and the large number of sites to protect. As more companies extend networked applications to their remote offices and to teleworking employees, they need to extend the same level of services to these employees that are available to their colleagues back at the corporate office. And that means that IT managers are faced with the challenge of protecting all these environments and locations.

To guess passwords, hackers use sophisticated random number generators. To gain unauthorized access to systems, they use port scanners. To gain remote access, they rely on keystroke capture software that's planted on a system, sometimes through a worm or Trojan horse disguised as a game or screen saver. To gain access, some use Internet protocol (IP) spoofing, which falsifies a legitimate host. And they rely on an array of other techniques that can cripple systems and destroy data.



Securing Your Business

“Every network is vulnerable, and security is a prime concern,” says Laura Koetzle, an analyst for Forrester Research. (<http://www.forrester.com>) “An organization that doesn’t take network security seriously can find itself crippled by attacks and other threats.” She divides potential assaults into two categories: internal and external. Employees, consultants, and visitors make up the former category, while hackers and unwitting accomplices—whose e-mail programs infect PCs with viruses or Trojan horses—are included in the latter category.

One of the biggest challenges for organizations, is covering the bases for all the different types of assaults that are possible. Network security is only as good as each individual component, it requires a number of different technologies that must be tightly woven into the entire enterprise security structure. A business must understand its unique points of vulnerability and how to minimize risk. Only then is it in a position to protect its network.

“An organization that doesn’t take network security seriously can find itself crippled by attacks and other threats.”

—*Laura Koetzle, Analyst for Forrester Research*

Solution

Many companies aren’t as secure as they’d like to believe, and the problem is growing worse. For example, Computer Security Institute found that 70 percent of those attacked reported vandalism in 2002, up from 64 percent in 2000. In addition, 55 percent reported denial of service, and a remarkable 40 percent detected system penetration from the outside.

Every device on a network is a potential point of attack. A company must have a comprehensive blueprint in place for how to plug numerous technologies together, and it must develop a solid security policy. This two-pronged approach, combining technology and business practices, offers the best chance at keeping a network secure.

Among the tools and methods that can protect a company:

- *Firewalls*—Corporate firewalls are a necessity. Yet it’s also wise to install personal firewalls on individual PCs that workers use to access the network remotely. This strategy protects these PCs from being hacked. Some personal firewalls also monitor outgoing traffic and alert users when an unauthorized program tries to send data across the Internet.
- *Network infrastructure*—Switches and routers have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and security management.
- *Network monitoring*—Routers can mitigate denial-of-service attacks by limiting the bandwidth available to each type of application, thus making bandwidth unavailable to attackers.
- *Access control*—Perimeter and physical security are essential. In addition, easy-to-use authentication, authorization, and accounting services ensure that only authorized users gain access to the network.
- *Virtual private networks*—These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.



- *Antivirus software*—The onslaught of viruses, worms, and Trojan horses has reached epidemic proportions. “It’s not good enough to use antivirus software,” Koetzle points out. “It’s essential to update definitions across all the PCs on a network on a regular basis.” In addition, a growing number of companies and Internet service providers are using antivirus software at gateways.
- *Intrusion detection and protection*—Port scans and denial-of-service attacks are an ongoing reality on the Internet—and a firewall can’t protect against them. However, intrusion detection and protection tools can identify potential threats and allow a company to take immediate action to block a hacker or a particular IP address that’s being used to launch an assault. Packet analysis tools allow even more sophisticated detection. In addition, host-based intrusion detection can protect servers from attack, particularly when a Trojan horse or worm such as Nimda or Code Red gets inside the firewall and infects PCs across a network.
- *Encryption*—Unsecured e-mail and documents can represent a threat for organizations sending sensitive data across the Internet. Likewise, wireless local-area networks lacking encryption create an easy way for data thieves to steal information. In a retail environment, for example, unsecured communications (wired or wireless) can translate into stolen credit card numbers.
- *Secure wireless local-area network access*—The use of wireless local-area networks (WLANs) within corporate intranets is soaring. Employees like the freedom and mobility that WLANs provide, and companies like the increased employee productivity they bring, which enhances the bottom line. But IT managers see the risks of illegitimate network access from rogue access points and unauthorized client devices. To mitigate attacks and keep the network secure, corporate WLANs need to be installed with robust authentication and encryption capabilities.

Benefits

Organizations that adopt strong security solutions and back them up with appropriate policies and physical security greatly reduce the risk of theft, vandalism, or interruption of services. While there’s no way to sidestep all risk, it is possible to make it difficult for hackers and thieves to exploit a network. In the end, it’s all about playing the odds.



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 International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. 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 PRC • Colombia • Costa Rica • Croatia • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • 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

Copyright © 2003 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, and PIX are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.