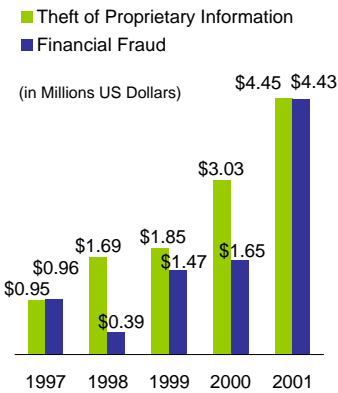




NETWORKS UNDER ATTACK

The Cost of Computer Crime



While 78% of the CSI survey respondents acknowledged financial losses, only 37% could actually quantify the losses.

Source: Computer Security Institute

Know Thy Enemy

The number one way to start defending yourself against security breaches is to know what are the biggest threats to your networks.

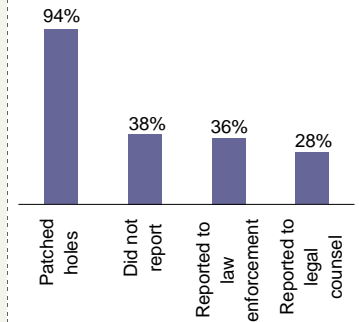
The enemy is real and is nearer than you think. In 1999, theft of proprietary information cost Fortune 1000 companies up to US\$45 billion in losses, according to the American Society for Industrial Security (ASIS) and PricewaterhouseCoopers.

A March 2001 survey by the Computer Security Institute (CSI) and the FBI found that 85% of U.S. corporations, government agencies and financial institutions experienced computer security attacks in the previous 12 months. In the same survey, 35% reported combined losses of more than \$377 million as a result of these attacks. In 2000 edition of the CSI/FBI survey, the losses from 249 respondents totaled \$265.5 million and the average total loss between 1997 and 1999 was \$120 million.

Whichever way you dice these figures, network security is an issue that managers and directors have to face head-on. But companies should act before security problems hit them: A recent IDC survey discovered that companies often only found the motivation to adopt security technology after they had suffered a security breach.

"If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tzu succinctly said in the Art of War. The best way to start defending yourself against security breaches is to discover who and what are the biggest threats to your networks.

What do you do in the event of a computer intrusion?



Reporting a security incident may subject the corporate victim to adverse publicity, regulatory scrutiny, and business losses. While the CSI recommends reporting incidents to law enforcement authorities, corporations are advised to alert management to the breach and to consult with legal counsel first.

Source: Computer Security Institute

WHAT ARE THE THREATS

Hackers

Hackers are persons that gain unauthorized access to computer resources to steal data or sabotage systems.

According to current research, in early 2001 as many as 210 hacker groups made attacks on around 1280 Websites + to learn a thing or two from organized crime: many of these incursions were accompanied by demands for protection money. With the international Mafia supporting these young hacker groups, hacking is turning from a malicious hobby to a new multi-billion dollar online extortion racket.

While we commonly associate hackers with the image of a professional cyber terrorist, usually former security experts from the former Eastern Bloc, using state-of-the-art tools, Marc Rogers, a Canadian forensic psychology expert at the University of Manitoba points out that there are also hacker newbies, the so-called script kiddies, who have little hacking skill, use other hackers' programs, and like to cause malicious damage such as defacing Web sites. Even though security professionals may often laugh at these technological neophytes, script kiddies pose a big threat to corporate security.

Security experts attribute the rise of this threat in part to the proliferation of simple, point-and-click programs that make it easy to exploit known holes in server software. The temporary shutdowns of Amazon.com, eBay and Yahoo! in 2000 were blamed on script kiddies armed with software they downloaded from the Internet.

Denial-of-Service attacks

In a DoS attacks, hackers flood Web servers and networks with sudden and overwhelming bursts of network data, slowing down server performance and eventually crashing the Web site. Unlike a virus or worm, which can cause severe damage to databases, a denial of service attack only interrupts network service for a limited period. But if your network is your business, even an hour of service outage can mean serious losses and angry customers.

In February 2000, DoS attacks took down five of the ten most popular Web sites in the world, including Amazon, Yahoo! And eBay. Yankee Group has estimated that these attacks caused at least US\$1.2 billion in lost revenues and subsequent drops in market capitalization.

Viruses and Worms

Virus and worm attacks are the most common form of security breach, costing businesses up US\$17.1 billion in 2000, according to Computer Economics.

In 1999, that amount was US\$12.1 billion. The costs incurred includes cleaning viruses from computer systems and networks, restoring lost or damaged files, and lost productivity of workers caused by system outages and downtime.

Computer Economics estimates that the Code Red worm and its variants - the latest Internet worm keeping network security professionals on edge - have infected 760,000 servers worldwide, to the tune of US\$2.05 billion in system repairs and lost productivity.

The Love Bug attacks that rampaged through systems worldwide in May 2000, caused the most damage financially, up to US\$8.7 billion in lost productivity and in system repairs.

Physical break-ins and theft

Security attacks don't only happen over the Internet. There's still the old-fashioned route: physical access to the hardware and software. All your firewalls, virus scanners, and encryption measures won't be able to protect you if a malicious individual gains unauthorized, physical access to your premises and destroys or steals computing equipment, including all the valuable data contained within.

Data thieves don't even have to break into the office. Portable computing and information devices like laptops and PDAs make it easy for your remote workers to touch base with the head office and exchange files and information. But this portability also makes it an easy target for data thieves, especially in conferences and airport lounges where a moment's inattention can give thieves and mischievous individuals the chance to walk away with your equipment and gain easy access to all the critical and confidential information stored away on the portable machines.

The situation gets a little more critical if your machines are set up to access corporate networks via a remote dial-up or virtual private network connection: The data thief is potentially only one-click away from all your company secrets, since any password mechanisms you have can be easily defeated by the plethora of password-cracking tools available on the Internet.

Insiders

Disgruntled company insiders like current employees and former workers are often represent the most dangerous security threats. They understand the business and how the computer systems work and more importantly, they have authorized access to network resources and critical company information.

In-house security breaches account for up to 70% to 90% of all security breaches, estimates The Hurwitz Group of Framingham, Mass. The percentage is probably even higher than that because most insider attacks go undetected: Dennis Szerszen, director of security strategies at The Hurwitz Group says for every in-house attack reported, there could be as many as 50 that go unreported or undetected.

In a recent study carried out by Digital Research, 57% of firms reported that their worst breaches of security occurred when their own users accessed unauthorized information. The next major problem happened when user accounts remained functioning after those users had left the company concerned. Only 21% of the corporate respondents said external cracking was their biggest security concern.

"The majority of high-value breaches - those costing US\$250,000 or more - are perpetrated from the inside," says Frank Prince, Senior Analyst at Forrester Research. "That's because insiders often know how to access the most valuable data."

NETstatistica Report is a free PDF newsletter that gives you a quick look at what's driving the global Internet, with a compilation of the latest key Internet stats, facts, and demographics from around the world.

More stats at MetricsWATCH

Browse through our online compilation of stats & facts organized by key countries & topics.

Visit MetricWatch at <http://www.netstatistica.com/netradar.cfm>

NETstatistica
Designing and creating quality online editorial content

NETstatistica helps technology companies ideate, create, and manage editorial content that will keep customers coming back for more. Contact info@netstatistica.com to find out more.



SECURING YOUR E-BUSINESS

Trends

Managed Security Services

Managed security services will become increasingly popular as SMEs seek security services without having to make massive investments in IT infrastructure. These managed services will provide constant monitoring of the security side of organizations' networks and systems.

Source: IDC Research, July 2001

Security remains the biggest business concern for US corporations

31% of US firms say security is their biggest Internet-related problem, according to a recent eMarketer report based on a recent study by N2H2. Personal or unauthorized use of the Internet by employees was identified as the biggest Internet-related problem by 21% of survey respondents.

Source: eMarketer, September 2001

Security issues not deterring users of online financial services

Lack of knowledge and the cost of going online appear to be bigger deterrents to new users of online financial services than security concerns. Security is however a major concern for those who are already using financial services online. Online financial services firms should consider security as crucial to customer retention strategy, rather than customer acquisition.

Source: Datamonitor, July 2001

"Always on" broadband will drive demand for consumer Internet security

The need for intrusion protection against unapproved PC and network access, as well as a greater need for virus and privacy protection, will drive demand for broadband Internet security products for the home over the next few years. Although 50% of consumers with a broadband connection today are without any form of intrusion protection such as a basic software or hardware firewall, the demand will grow once consumers become better educated about the need for Internet security. The US consumer broadband security market will grow from \$74 million in 2000 to over \$800 million by the end of 2005, driven, in large part, by strong sales in the firewall category.

Source: Cahners In-Stat Group

Information Security Action Plan

1. Keep it simple. "Complexity is the worst enemy of security," says Bruce Schneier. He argues that the more complex a system is, the more likely the people running it don't understand it. And their failure to understand a system makes it vulnerable to security threats. The bottom line: you should never use a system that's too complex for your team to manage.
2. Determine your security requirements. Create a security planning team with staff from IT and business functional areas. Creating a security policy needs to be a group effort, and representatives from different departments should be involved to keep everyone in the loop. Analyze your organization's security requirements. Understand your networks, and the business objectives they support. Some systems and information assets are more valuable than others, and not all of it needs to be protected equally.
3. Assess the threats, vulnerabilities and risks. Analyze the financial value of your assets, identify the threats and vulnerabilities, and assess the security to your information systems and assets. Determine the type and level of security measures you require. Define the priorities for implementing these measures. Assess your security budget against the business value of the information assets at risk, and against the potential losses due to security breaches.
4. Establish a security framework. Explicitly define and assign responsibilities for protecting information assets and implementing security measures. Create and implement a set of security standards that take into account the diverse requirements, problems, and priorities of your employees.
5. Plan for disaster. Develop and maintain appropriate recovery plans to protect and recover critical business processes from attacks and disasters.
6. Develop a clear security policy. Develop a thorough and achievable security policy, implement it and update it at regular intervals. A security policy stipulates who has the right to access what applications and what parts of the network. Security policies also provide ground rules for the use of a network (such as the documents and folders that may be accessed by an employee). Document your policy in clear and simple language and distribute it to all your staff.
7. Use appropriate security tools. An independent source of assessment products is much more likely to provide an unbiased evaluation of overall E-business security performance. Update security solutions like firewalls, authentication and encryption with adaptive technology to maximize their effectiveness and help prevent premature obsolescence.
8. Educate your staff. Provide your employee with adequate security education and train them to properly deploy and use security technologies. Teach them to report security incidents through the appropriate chain of command as quickly as possible.
9. Monitor your security plans. Hold regular reviews of IT systems and facilities for compliance with organizational security policies and standards.

Wireless LANs bypassing firewalls

By year-end 2002, 30% of enterprises will suffer serious security exposures from deploying wireless local area networks (WLANs), if they don't implement the proper security, says Gartner, Inc.

The primary risk associated with WLANs is that the over-the-air security built into today's 802.11b WLAN systems is too easy for hackers or cybercriminals with a laptop computer to intercept data, inject data or impersonate legitimate users. Most WLAN installations operate without even a minimal level of protection.

To implement secure WLANs, Gartner recommends that enterprises:

- Always activate the default level of product security for newly installed WLANs.
- Require IPSec virtual private networks to be run on all WLAN connections, at least until next-generation WLAN security standards are defined, tested and implemented in WLAN products.
- Take measures to detect unauthorized WLAN installations that may open holes in the enterprise's security perimeter.
- Define and distribute security policies on the use of WLANs in corporate and home offices. Educate employees on the risk.

Source: Gartner

E-commerce not secure

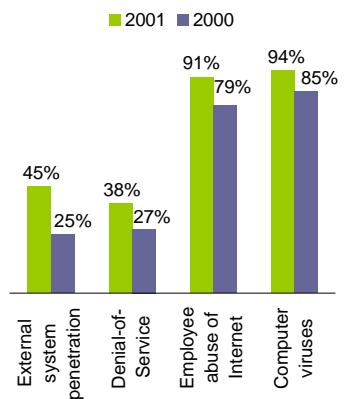
A recent eFraud survey by KPMG found that while the security of credit card numbers and personal information were the most important security concerns of customers, less than 35% of organizations performed security audits on e-commerce systems and only 12% had a seal on their website to show they had passed a security audit.

79% said they were most likely to suffer a security breach from an external attack and 50% said hackers were the greatest threat to their systems.

Half of the respondents had security incident response procedures but only 22% used computer forensic response guidelines.

Source: KPMG, August 2001

Attacks and Abuses Growth



Source: CSI Computer Crime and Security Survey 2001

Common Security Tools

Authentication

Protect networks against unauthorized access to sensitive information. Authentication mechanisms can range from the commonly-used usernames and passwords to advanced biometrics systems, which authenticate users through physical characteristics like fingerprints and eyes.

Anti-Virus Software

Anti-virus software protects computers from viruses by scanning computers for malicious code and repairing or removing infected programs and documents.

Firewalls

Firewalls protect networks against security breaches by examining data entering the network and blocking traffic that fails to meet specific criteria.

Intrusion Detection Systems (IDS)

IDS applications actively monitor operating systems and network traffic for security attacks and breaches, giving a near-real-time update on the status of the network. IDS can be host-based or network-based.

Host-based systems use software agents installed on servers to report network activity to a central control console. Network-based systems sniff the network and match live traffic to a list of known attack patterns.

Public Key Infrastructure (PKI)

PKI uses a system of digital certificates and certificate authorities to encrypt data and verify the identity of the sender. However there is still no clear standard for PKI yet.

e-Security Market

European Security Spending

Euro 2.48 billion (US\$2.1 billion) will be spent on security services in Western Europe in 2001, and should grow to Euro 4.73 billion (US\$4 billion) by 2004.

Source: IDC Research, July 2001

Biometrics Market Growing

Increasing concerns about security, and the decreasing cost of Biometrics technology will drive market sales to US\$520 million in five years time. Two thirds of biometrics revenues will come from services, with the rest coming from hardware.

Biometrics applications predicted to become widespread are scanning of eyes, faces, hands, and fingers. Facial scans will be the preferred technology for use at ATMs as they are less intrusive for users than eye scans.

Source: Cahners In-Stat, June 2001

Get More Insights From eComFocus

Visit the free B2B e-commerce information and resource site for the United Kingdom.

<http://www.ecomfocus.com>

NETstatistica Report is a free PDF newsletter that gives you a quick look at what's driving the global Internet, with a compilation of the latest key Internet stats, facts, and demographics from around the world.

More stats at MetricsWATCH

Browse through our online compilation of stats & facts organized by key countries & topics.

Visit MetricWatch at <http://www.netstatistica.com/netradar.cfm>

NETstatistica
Designing and creating quality online editorial content

NetStatistica helps technology companies ideate, create, and manage editorial content that will keep customers coming back for more. Contact info@netstatistica.com to find out more.