Data: Intrusion Tools Meet Trade Secrets

By
Robert H. Turner
GSEC v1.4
5/14/2002

Data: Intrusion Tools Meet Trade Secrets

Abstract

Companies today face significant challenges when protecting not only their Internet exposure but also their financial viability. While the destructive power of e-mail worms, virues, and denial-of-service attacks is well known, few consider the significant "hacking" risk to their data and what that data may represent. The growing world economy, increasing competition, and expanding Internet membership has resulted in the rise of cyber criminals. Combining the same corporate spying techniques from the past with the hacking tools and techniques widely available today on the Internet, cyber criminals have found they may have more discrete methods for pilfering your data. Understanding your data's financial value with regard to your competition or product delivery will allow you to understand how and why a cyber criminal may target your company. In light of this growing threat and the costs it represents not only to individual companies but also to the United States economy, economic infrastructure, and copyright protections, measures such as the United States Department of Justice's CyberCrime website to the very same tools used by cyber criminals can be employed to protect your data. This paper will attempt to establish a connection between your company's financial vulnerabilities and the wide use and knowledge of hacking tools and corporate espionage techniques. When one considers the risks to their data and the large target those data represent to other companies or countries, one can then take significant steps to appropriately secure that data.

Introduction

The network security realm has come full circle in recent years. After the now famous Mitnick attack occurred, many companies and novice computer users became aware that their computer systems were indeed vulnerable to attack. Despite the ubiquity of network security tools, antivius software, and security white papers, most computer users understand network security issues that relate merely to either nuisance or data loss. Corporations have been slow to adopt network security measures despite a growing desire to develop their Internet profile. Since 2000, companies have formalized roles such as "Chief Technical Officer" in response to the growing technological costs and to address new security concerns. While technological advancements have provided technology officers with the tools and information they need to secure their company's data, a combination of naivety, costs constraints, and the available tools for cyber criminals has made difficult their ability to adequately secure their company's financial posture. For every new tool developed for network administrators, that same tool is also available to a hacker. With the growing understanding that real threats come from those gaining access across the Internet, a newly coined category, "Cyber Crime" has emerged. The United States government has tasked the Department of Justice to address not only the threat to America's network infrastructure but to also protect the financial solvency of America's capital structure. The FBI has elucidated the ever-growing costs associated with these nuisances. The "2001 Computer Security Institute/FBI Computer Crime and Security Survey" (Symantec, 2001) indicated that financial costs associated with computer crime exceeded $370 million for the only 186 companies that responded to this survey. This survey certainly raises the prospect that any company is at risk of financial loss. Mindful of this, the following analysis will attempt to clarify the precise nature of network and systems security and the potential costs of these threats to a company.

Methods

The threats apparent to a network environment are borne from purchased and currently installed and configured equipment, employees, interfaces, and storage media. This significantly porous environment nurtures several considerable vectors.

Vectors

Internet: The Internet provides a doorway through which others may access your company's data. The method by which an intrusion occurs is not always readily apparent. While a direct user name/password attempt can trigger suspicion, other valid tools exist that may be employed to either derive information and/or gain entry into a company's resources. These include:

1. Downloading: taking advantage of a user's naivety, a cyber criminal can maintain a web page on which he can provide any number of downloadable programs or files in which he has embedded virus code, worms, or Trojan programs such as Back Orifice. To maintain some distance between himself and an actual web address, the astute cyber criminal would attempt to compromise a host web server

through known vulnerabilities, revealed accounts, or buffer overflow and then upload viral code or Trojans and allow nature to take its course.

2. Foot printing: Much as would a burglar or mugger, a cyber criminal will case a corporation well in advance of an actual attack. Casing methods include:

    a. WhoIs lookup: this allows the cyber criminal to find the DNS server address from which the target company's website is maintained. The cyber criminal can glean several important pieces of information from this lookup such as the company's range of network addresses, network administrator's name and telephone number, potential modem numbers, and company's mailing address. In fact one of the better tools for gathering DNS information is Sam Spade (http://www.samspade.org) or GeekTools WhoIs CGI lookup (www.geektools.com) with which you can collect vital network information such as DNS IP Addresses and Network Administrator name and telephone number.

    b. Web Search: A simple Internet search can yield information on company size, distribution of business centers, number of employees, clients, contractors, and other logistic data. Furthermore, the cyber criminal can uncover news articles or marketing ads about your equipment, clients, projects, phone numbers, and hours of operation. Using the "Link:" command in your web search can help elucidate client or news-related information that links back to your company's website.

    c. NMAP: Once recognized, a company's Internet profile will be put to the test with any number of port scans. NMAP is a port scanning utility that will not only list open and listening ports on remote machines but it may also reveal the operating system running on that machine. While not exclusively powerful in revealing information about a corporation's Internet presence, it can be used along with PING sweeps and TRACERT to view operating machines and open paths to them. Knowing what ports are open can help the attacker know what machines are most vulnerable to launch his next steps at gaining entry to your network.

3. Null Sessions: Knowing what machines are running and on which ports they are listening may allow a cyber criminal means to logging onto one of your machines without accessing of your user's accounts. Null Session logon takes advantage of an open NetBIOS port, TCP port 139. A remote attacker can logon to a machine while not having the capacity to utilize remote shares the attacker can use NBTSTAT or other network enumeration tools to find user lists, network shares and groups. The most notable damage a remote attacker can employ to gain access or information on your network while in a null session with one of your computers is by Legion. This utility will attempt logons to detected network shares. The implications here are obvious: once connected to your accounting share, the cyber criminal is free to manipulate sensitive data.

4. E-Mail: By far the most efficient vector for a cyber criminal is E-Mail. Simply using a virus tool kit or by embedding his remote tools in a worm, the attacker can spread his influence into your network and wait until a compromised system begins beaconing its status. Some of the better tools to deploy through Trojan techniques include Sub7 and Back Orifice. These two are known as "backdoor" tools, a category of which allows a remote attacker access and control of an infected machine. Another commonly deployed tool is a keystroke logger. This tool helps the cyber criminal gain user name and passwords, allowing the attacker to gain privileged access to your network and its resources.

5. Social Engineering: Users become dependent upon their technical support staff but in large organizations, users may not have a by-name relationship with members of their technical support staff. As such social engineering techniques such as those utilized by telemarketers (i.e. Sense of urgency, assertiveness, building rapport, etc.) may be employed to glean information from your users. When the attacker researches your company's registration information, such as through WhoIs or by using Register.com, the cyber criminal can dupe unsuspecting users into believing that he is or works for the network administrator.

Remote Access, Dial-In: Remote access is a broad range of access to your network through mediums other than direct Internet access. This includes dial-in through public switched networks, ISDN dial-up, and virtual private networking (VPN). The reason VPN is considered herein as remote access will be described shortly.

1. Modem Dial-In: Prior to broadband's rapid deployment, modem dial-in was the most prevalent remote access method. Dial-in's vulnerability lies both with the operating system and with the prevalence of war dialers. War dialers are software that automate dialing within a given range of phone number prefixes. Because POTS dial-up is still the primary means of remote access, war dialing will continue to be a threat to your network's data. Freely available software such as ToneLoc and THC-Scan along with a modem or modems provides the cyber criminal the means by which your remote access lines may be located. Simple foot-printing such as reading your registry information can provide the attacker with all the prefixes he will need.

2. Virtual Private Networking: VPN takes advantage of a networking protocol such as Point-to-Point Tunneling Protocol (PPTN) to gain an IPSec encrypted connection to a remote network. Instead of authenticating at one of your servers, a remote user must now connect at the firewall or VPN router. VPN can be considered dial-up for two important reasons: the VPN router's address, like the ISP number, is stored on the target machine and; VPN connections allow a secure connection to a remote network, seemingly bypassing the firewall. By compromising a machine on which VPN has been configured, an attacker can be one step closer to gaining unfettered access to your network. Where in the case of Internet-based attacks your firewall may detect and/or deny remote scans or attacks, an authenticated VPN connection leaves a hole in your network. The

problem becomes more apparent when one considers that most remote users will save their user name and password in the VPN connection dialog box in Windows. Moreover, many remote users do not use intrusion detection software and may not maintain their virus scanning software.

Physical Access: Physical access to your network is obviously the single most significant and potentially damaging threat to your data. Several resources make this type of access even more powerful.

1. Windows 95: Windows 95/98/ME machines have little built in security. In fact, their security stops at screensaver or BIOS passwords, both of which are easy to defeat. It is not necessary to log onto a Windows 95 type machine to gain access to its networking devices. It is however necessary to log onto the network domain to access your resources but since group security policies can not be set on these machines, there is nothing stopping an unauthorized user from downloading and installing tools such as L0phtCrack, Getadmin, Legion, and userdump onto a compromised machine. Moreover, a physically located attacker could merely load a keystroke logger onto the machine, configure that machine with Back Orifice, and connect to it later to reel in user names and passwords for later remote access.

2. Passwords: Once a list of usernames has been collected, passwords are the weakest link in your security chain. Poor password administration allows users to create and maintain simple passwords. Many companies do not audit their users passwords and even more do not incorporate password time limits. Even when password lengths and timeouts are enforced, users often resort to simple passwords or writing passwords on highly visible sticky pads. There are several methods by which your password policies may cause trouble:

    a. Length: zero password policies result in zero password lengths. Nothing makes hacking easier.

    b. Common names: the next easiest passwords to guess are those with common words or names. L0phtcrack, now known as @Stake has a password-auditing tool called LC3, which also makes a cyber criminal's job simple. With access to a network or simply to a workstation, an attacker can crack through common names using dictionary guesses with LC3. In most cases, LC3 will guess all dictionary-based passwords within three seconds.

    c. Password Expiration: easily created passwords for user accounts that stay active for years are similar to a baited mousetrap. Sooner or later, that trap is tripped. Once an attacker gains access through that password, he will continue to gain access to your resources as long as that user does not change his or her password.

   d. Documentation: new users often write their passwords on paper and keep that paper immediately adjacent to their computer. Some companies even go so far as to have new employees write a chosen password on their employee information card. Who's watching these cards? Imagine the threat to your company's financial data if the head of your accounting department keeps his password conveniently taped to the glare screen.

3. Logon restrictions: All users do not need access to all your data all the time. Unfortunately, most companies do not consider where their employees go on the network when they're bored. By extension, an attacker with a compromised user name can access this very same data. Using group policies, the network administrator can assign users to well-defined groups with well-defined privileges on the network. Now only accounting department personnel will have access to critical financial data. Restricting the time during which certain groups can access the network simplifies network audits helping administrators catch unauthorized network activity.

4. Logon: Most users despise log off/log on activities. Log on takes time and log off causes the user to lose track of work. Novice users are not familiar with workstation locking and users on Windows 95-type machines have only the screensaver password on which to rely. Therefore, many users simply walk away from machines while they are logged on. Personnel such as neighbors, facilities, or passers by will instantly gain the same privileges of that of your user.

5. Social Engineering: As with networking exploits, social engineering is equally effective when conducted in person but the modus operandi is different. The cyber criminal will use rapport building. The attacker may, however, employ psychological methods to gain sufficient trust with an employee to uncover personal information (i.e. children's names, spouse's name, birth date, favorite color, etc.). The end result being that the attacker at some point attempts to gain remote access using this user's account or gains entry into that employee's business and attempts logon there.

6. Users: Your employees are the most dangerous vectors to your network. Employees introduce threats in four distinct manners:

   a. Infected disks: employees often do not protect their personal computers and thus do not detect that they have a virus. They may copy infected files to floppy, Zip, or CD-ROM disks then open those files on their workplace machine.

   b. Downloads: your employees often browse the Internet and find interesting files or programs, then download these onto their workplace computer the unwittingly run a virus.

   c. E-Mail: most viruses and Trojans propagate through e-mail. Unless properly trained to recognize this risk, employees will continue to open file attachments without first saving them. This problem is compounded when your e-mail gateway is not configured with a virus shield, thus allowing many easily filtered virus attachments to find their way into your network. Viruses such as “I Love You”, Klez, and SirCam were effective for nothing more than just creating provocative or familiar subject lines.

d. File Modification: through accidental mousing or by deliberate intent, employees will move, modify, or delete your files. Oftentimes, most file modifications occur by mistake during the normal course of work but the time lost searching for these files can soon lead to production shortages. For the cyber criminal, copying your trade secretes, client lists, or production materials is the ultimate goal.

Financial Impact

Estimating your company’s data value is tricky. The true economic value of invariables such as trade secrets and client lists primarily depends on the size and scope of your business combined with the number and collective size of your competition. While there are many companies such as Applied Economics and InfoScreen, Inc. it is still difficult to both find a company to estimate your data value and agree on that value.

The 2001 Computer Security Institute/FBI Computer Crime and Security Survey demonstrates why you need to gain an understanding of the various data that reside on your network and the value they represent. From the one hundred eighty-six companies that responded to the survey, the total value of damages due to corporate espionage was over $370 million. To place this in proper context, that would average two million dollars per company in financial loss. Could your company survive beyond such loss?

As Internet Espionage becomes more familiar, now known as “Netspionage” these types of financial losses could become small by comparison. Pricewaterhouse Coopers reported that more than 59% of companies with an Internet profile have had intrusions (MSNBC, 2000). For many cases, this percentile may be optimistic. Many companies who have significant financial profiles in combination with an Internet connection, hard copy data, and exclusive trade secrets or processes will have undetected intrusions. In addition to deliberate damage or theft, companies have general Internet threats such as hacking, viruses, and workplace catastrophes with which to be concerned. Although a serious threat, Internet based denial-of-service attacks, surface intrusions, and viruses pose little risk but garner the media’s attention best. In a September 2000 article, “The Untold Tally of ‘Netspionage’,” MSNBC appropriately coined these types of attacks as “toilet-clogging techniques” (MSNBC, 2000) in that they are primarily, except in rare cases, a nuisance. The true crime begins at the moment data is collected.

Notably, large corporations, those within Fortune’s elite, lost more than $45 billion worth of proprietary information in one year. Fueling the trend is the collapse of the Soviet Union, globalization, and increased competition for intellectual property each of which has provided computer scientists, former secret government agents, and young hackers with unique opportunities. More and more companies are turning to alternative means to collect information on or outright infiltration of their competitors. One such method is to use teen-aged children, hacking adept to reveal holes in their competitor's network, and then employ a combination of private investigators and professional hackers to gain significant entry into their competitor's data warehouse and begin infiltration and/or modification. Keep in mind, the chief goal here is to trump your competition, slow their processes, or cause them large financial damage.

Consider a military contractor with national security interests having its clients and projects embedded through steganography and posted on the Internet; formatted hard drives leave a top-secret nuclear testing facility to later have their original data extracted; an engineer develops a design for his mobile phone employer by using a design stolen from a chief competitor. These stories may seem interesting material for fiction novels but they have happened. They happen because companies do not assume value in their data, the hardware on which it is stored, or the paper on which it is printed. Consider the number of documents in your employees' trash bins and the data therein, the computers left logged onto the domain unattended, and the information stored on lost laptops. Further consider what recovery actions your company could take if your accounting database had been modified and these changes had not been noticed until a month later.

Prevention

The large number of vectors available combined with your data's logical value and your competitor's need for that data create a deadly triangle for netspionage. First recognizing that this triangle exists is a critical first step to defending your company's financial solvency. Next, you must formulate a plan for defending your company's goods.

Pricewaterhouse Coopers, Symantec, the Better Business Bureau, the FBI's National Infrastructure Protection Center, the SANS Institute and others have developed general guidelines for helping your company categorize and protect its data. Categorizing your data allows your administrators to figure out by whom and at what times certain data should be accessed. This will also help your security analysts provide reasonable cost solutions for protecting the most data with the lowest overhead possible. Some of the notable solutions follow:

1. Install antivirus software
2. Install and configure a firewall
3. Use Encryption for both e-mail and stored, sensitive data
4. Evaluate your data
    a. Consider what data represent your most critical financial profile. These may include:
        i. Strategic plans
        ii. Business Operations
        iii. Finances (Symantec, 2001)

   b. Develop in-house asset evaluation or contract this a recognized authority, such as The Advisory Group.

5. Utilize a tripwire using products such as Tripwire that will tip-off any changes in your critical data.
6. Install host-based and Internet-based intrusion detection solutions. To keep your expenses low, install host-based intrusion detection, such as BlackIce, on systems from which your most critical data is accessed.
7. Use the same tools hackers employ such as NMAP, Legion, LC3, Null Sessions, DNS lookup, and others to test your network security compliance. Gain written approval from your legal staff, chief operating officers, or each division's executive director prior to conducting such tests or audits.
8. Set controls for access to your tape backup, CD ROM, Zip disk, floppy disk, and other data media. This control should extend to hard drives, compact flash cards, and any media on which data can be stored and retrieved.
9. Develop controls procedures for handling hardcopy data. Identify types of printed data that represent critical operational or financial information or that may be pieced together with other printed data to represent that information and be transported outside your company.
10. Construct written policies that detail explicit expectations of your employees. Include each of the above items as well as other best practices as a template for explaining how your network is secured and how employees are expected to handle your data. Include an educational schedule to cover new employees as well as reinforcing policies with all employees.
11. Create a disaster recovery plan. Include backup tape locations and latest dates. Also, regularly create backup or system recovery disks as well as making registry back ups on critical systems.
12. Review security best practices. These can be downloaded from SANS.ORG or from companies that create security software or hardware such as Cisco. As technology changes, so must the steps with which you take to secure your network and data.

Details

Incorporating good preventative measures can be a good first step but they are certainly not going to prevent an incident from occurring. You must consider the responsibilities that underlie each measure such as having established guidelines for your technology staff that include:

1. Perform regular firewall log review.
2. Block all unnecessary ports with your firewall. Use the concept of "deny all except that which is explicitly allowed."

3. Update antivirus software every week or as conditions warrant. Set your virus scanner to check all files as well as perform heuristic scanning.
4. Maintain your operating systems with the latest patches and hotfixes.
5. Revaluate your critical data at regular intervals to rule out previous bad assumptions or to determine if certain forms of data have had an elevation of their financial impact.
6. Review tripwire and/or audit logs daily. In cooperation with firewall and intrusion detection logs this will allow you to develop an eye for intrusion signatures.
7. Develop and review logs for how your removable data is stored, checked out, installed, modified, or destroyed. This should extend to the handling of any hard drives that have been moved or removed.
8. Perform garbage and recycle bin spot checks. This refers to physical garbage bins where hardcopy data is placed. Much of a cyber criminal's footprinting or theft activities involve digging through a company's trash.
9. Review company security policies regularly. As needs arise or as issues develop, update and promulgate your written security polices to assure compliance. Old or out-of-date security policies or policies that are rarely enforced are as good as having no policies altogether. In particular, develop and enforce best practices with regards to your company's password policy. Do not allow lax password security to negate the hard work and costs that you have put into place. Enable Windows password filter (passfilt) to help you enforce minimum password length, character inclusion, and password expiration.
10. Educate your employees. While you wouldn't want to reveal your trade secrets to every employee, it is necessary to educate each employee as to his or her role in the company's profitability and financial stability with respect to access to your data. Employees should be reminded to not give their password to anyone, to regularly lock or log off their workstations when they are leaving even for short breaks, to review the company's security policies, to watch what they throw away, and to not reveal the specifics of what they do to anyone outside the company.

These steps will certainly allow your company a good foothold on maintaining your company's secrets and to its operational stability.

Conclusion

In a competitive and ever-expanding economy, there is an equally competitive and ever-expanding need to succeed. A small slice of strategic information leaked to one of your competitors, while possibly negligible in your employees' estimates, may bring your competition more market share and lead your company to bankruptcy court. Even though the precise nature of Internet-based corporate espionage may be difficult to determine, most experts agree that it is occurring and will definitely increase in scope as access to the Internet proliferates. While the threat of toilet-clogging techniques like syn-flooding, DOS attacks, and e-mail worms may be real, the often hidden cyber criminal attacks that reveal trade secrets, financial data, or client lists are far more damaging. Understanding that with competition comes risk is the first step to understanding how to defend your company's financial goods.

References

CenterGate Research Group Geektools.com (2002). WhoIs Lookup
http://www.geektools.com/cgi-bin/proxy.cgi

NMAP
http://www.insecure.org/nmap/index.html

Komarnitsky, A. (2002). NMAP-Web: Quick-n-Dirty Web Interface to NMAP.
http://www.komar.org/pres/nmap-web/

Mnemonic (1999). NT4 Intrusion and Security.
http://secinf.net/info/nt/nt4sec.txt

Näf, M. (2001). Ubiquitous Insecurity? How to “Hack” IT Systems.
http://www.isn.ethz.ch/onlinepubli/publihouse/infosecurity/volume_7/b3/B3_index.htm

MSNBC (2000). The Untold Tally of ‘Netspionage’.
http://www.zdnet.com/zdnn/stories/news/0,4586,2626931,00.html

Chaturvedi, A., Gupta, M., Mehta, S., and Valeri, L. (2002). Fighting the Wily Hacker: Modeling Information Security Issues for Online Financial Institutions Using the SEAS Environment.
http://www.isoc.org/isoc/conferences/inet/00/cdproceedings/7a/7a_4.htm

Verton, D. (2002). Insider Threat to Security May Be Harder to Detect, Experts Say.
http://www.computerworld.com/securitytopics/security/story/0,10801,70112,00.html

Boni, W. & Kovacich, G., (2001). Netspionage Coming of Age.
http://www.blonnet.com/businessline/2001/08/13/stories/211339bc.htm

Sandstorm Phonesweep
http://www.sandstorm.net/products/phonesweep/

Tang, C. & Gossels, J. (1999). Wardialing: Practical Advice to Understand Your Exposure.
http://www.systemexperts.com/tutors/wardial0299.pdf

Arizona State University (1993). Data Access Policy.
http://www.asu.edu/data_admin/data_administration-Data%20Access%20Policy.html

Indiana University (2000). Data Access Policy.
http://dataadmin.iu.edu/da_access_institutdata.html

Applied Economics Partners (2002). High Technology.
http://www.aep-econ.com/high_technology.htm

Safeco (2002). Small Business Loss Control.
http://www.safeco.com/safeco/insurance/smallbusiness/sblosscontrol/

Symantec (2002). Small Business e-Business Plan.
http://www.symantec.com/region/sg/smallbiz/esecurity.html

United States Department of Justice, Cybercrime.gov (2002). The Electronic Espionage Act of 1996.
http://www.cybercrime.gov/usamay2001_6.htm

Seki, S. & Toren, P., Pricewaterhouse Coopers (2002). Electronic Espionage Act Penalties.
http://www.pwcglobal.com/extweb/newcojou.nsf/DocIDManagement/30E1D7D383EA32BC8525662100642918

National Conference of Commissioners on Uniform State Laws (1985). Uniform Trade Secrets Act.
http://nsi.org/Library/Espionage/usta.htm

Konrad, R., CNet News (2000). Leaks and Geeks: International Espionage Goes Hi-Tech.
http://news.com.com/2100-1001-242620.html?legacy=cnet

United States Department of Justice, Cybercrime.gov (2002). Eitelberg Arrest, US Department of Justice Cybercrime CCIPS Section.
http://www.cybercrime.gov/eitelbergArrest.htm

Better Business Bureau (2002). Protecting Your Business Against Hacker Attacks.
http://www.bbb.org/library/hackerattacks.asp

Symantec (2001). Information Protection – Why Bother?.
http://enterprisesecurity.symantec.com/article.cfm?articleid=855

Cisco Systems, Inc. (2002). Network Security Policy: Best Practices White Paper.
http://www.cisco.com/warp/public/126/secpol.html