MANAGING THE MOST CRITICAL INTERNET SECURITY VULNERABILITIES: ONE EFFECTIVE APPROACH

TOMMIE SINGLETON

Security continues to be the most significant risk (in terms of costs) associated with businesses, their information systems (IS), and information assets — especially those on the Internet. A new vulnerability or exposure seems to appear every week. A strong argument can be made that vendors ought to be held more responsible for their faulty systems. Although absolute security is impossible, and although a secure system today will have new risks next week, there are some developing tools of interest to assist auditors and security professionals in the management of the most critical Internet security vulnerabilities. Some expert assistance is being provided, not only in the publishing of alerts as new vulnerabilities occur, but also in assembling various broad analyses of Internet attacks and providing the results to the public. For example, a list from the SANS Institute and the FBI, called “Twenty Most Critical Internet Security Vulnerabilities,” serves as an excellent check-sheet for those responsible for security. This article attempts to provide tools and techniques that can mitigate these types of security risks.

INTRODUCTION

Be afraid. Be VERY afraid.

This quote from the entertainment world is quite applicable to security on the Internet. Security threats have become a ubiquitous problem and an ever-evolving challenge for those responsible for information systems (IS). There is a seemingly endless barrage of attacks from computer criminals with the intent to destroy systems, data, and information assets. Mailing lists such as those from BugTraq, CERT, and the SANS Institute put out a continuous stream of warnings about emerging risks, from new viruses to vulnerabilities in operating systems.
systems and browsers. The costs of these security problems appear to outweigh even those of Internet fraud. The Computer Security Institute and the FBI conducted a study of organizations that experienced security breaches. The respondents who could put a dollar amount on the cost of a security breach averaged more than $2 million in financial losses.

These risks are associated with the exponential growth of the Internet and electronic commerce (E-commerce). Between 2002 and 2005, the number of consumers using online account management will more than double, reaching 45 percent of the U.S. adult population. On the retail sales side (B2C), E-commerce sales grew 92 percent from 1999 to 2000, with a total of $29 billion (see Exhibit 1). On the wholesale side (B2B), E-commerce transactions increased 17 percent from 1999 to 2000, with a total of $813 billion. In the service sector, sales increased 48 percent from 1999 to 2000, with a total of $37 billion. Retail sales for 4Q 2001 were up 13 percent over 2000, at $10 billion. It is estimated that sales for the year 2001 were $32.6 billion, an increase of 19 percent from 2000.
The rate of the growth of the Internet and IT budgets declined in 2001, but the scope of this exposure is approaching 100 percent because it affects both suppliers (hosts/servers) and users (clients). Whether it is Web servers (hosts), E-commerce systems, extranets, or just access to the Internet (clients/browsers), firms are exposed to a plethora of possible attacks if they are connected in any way to the Internet. Obviously, those firms with servers (hosts) have a much greater risk. Theoretically, data can be accessed by anyone. Attacks range from hackers who are on a cyber-space joy ride, to crackers who are out to kill, steal, and destroy. The risks also include viruses and intelligent agents (e.g., distributed denial-of-service (DDoS) agents). To a lesser extent, it includes those objects whose intent is to clog bandwidth: urban legends, hoax viruses, and chain letters. Those responsible for information security (InfoSec), operational audits, and internal controls have a very difficult task managing the risks associated with the Internet.

SEVERITY OF PROBLEMS WITH SECURITY

In eWeek Lab’s wrap-up of the year, a number of its analysts made best and worst picks of 2001. Security issues figured heavily on just about every analyst’s list — whether named as the top tech story of the year or bemoaned as the latest vendor marketing tool. Microsoft products — namely, IIS and Outlook — have the dubious distinction of appearing on several analysts’ lists for their continual problems of gaping holes that allow Internet viruses and worms to infect and harm systems. No wonder. Experts estimate that U.S. corporations spent about $12.3 billion to clean up the damage resulting from computer viruses in 2001. Some predict viruses and worms could cause even more damage in 2002.

A survey was conducted by the Computer Security Institute and the FBI’s San Francisco computer crime squad. The seventh annual survey polled 503 American corporations, government agencies, financial and medical institutions, and universities. It reported that about 90 percent of respondents detected computer security breaches in the past year. Survey respondents said they lost at least $455 million as a result of computer crime, compared with $377 million the previous year. In both surveys, only about half chose to quantify their losses. Thirty-eight percent of the respondents said their Web sites have been broken into over the past year, and 21 percent said they were not sure. Eighteen percent reported some sort of theft of transaction information, such as credit card numbers or customer data, or financial fraud.

While the news is bad in many ways, the news is also good in one respect. “From an operational standpoint, cybersecurity today is far worse than what ... best practices can provide,” said the Computer Science and Telecommunications Board, part of the National Research Council. “Even without
any new security technologies, much better security would be possible today if technology producers, operators of critical systems, and users took appropriate steps.\textsuperscript{11}

In the past, many IS administrators complained that they had not corrected many of the known flaws because they simply did not know which vulnerabilities were the most dangerous, and they were too busy to correct them all. However, U.S. computer systems are increasingly vulnerable to cyber-attacks, partly because companies are not implementing security measures already available, according to both the Computer Science and Telecommunications Board (CSTB)\textsuperscript{12} and National Academy of Sciences (NAS).\textsuperscript{13}

**WHAT IS THE RESPONSIBILITY OF THE VENDORS?**

Why is security vulnerability not a vendor problem? The problem with viruses results from the way computer systems operate. For example, to protect against boot sector viruses, why do vendors not simply have the operating system rewrite the boot track during shutdown, thereby foiling any boot sector virus that might invade the system? For application viruses, such as Word macros, why not admit that arbitrarily executing foreign code is a bad idea, and at least give the user the option to run it or turn it off. That option would stop malicious macros dead in their tracks\textsuperscript{14}

The same could be said about system availability. There is a high cost when systems are unavailable. It costs in productivity, people time, and wasted materials. That downtime includes rebooting multiple times a day to restart a failed computer system, or to get a clean copy of the operating system loaded. Should vendors not be held responsible for these failures? Perhaps you have heard the old joke:

If Bill Gates had a nickel for every time we’ve had to reboot Windows … wait a minute! Bill Gates DOES have a nickel for every time we’ve rebooted Windows!

Two groups, the CSTB and NAS, suggest that one possible remedy to security breaches would be to make software vendors liable for them. Regarding vendor responsibility, the CSTB states:

…one possible remedy would be to make software companies, system vendors and system operators liable for system breaches and to mandate reporting of security breaches that could threaten critical social functions.\textsuperscript{18}

The NAS makes its suggestion about vendor responsibility as well:

In addition to shouldering some of the blame for security breaches, the authors recommend that vendors develop better security interfaces for their products to simplify...
administration and conduct better testing of their products for security vulnerabilities.¹⁶

Microsoft and other vendors could learn a valuable lesson from the past. In the late 1960s, IBM was faced with similar growing complaints about the security of its computers. IBM created a liaison with the accounting profession (mostly auditors and the Big Eight), who would serve as advisors in developing security tools for their computers. Sam Albert held that position and helped IBM build a strong reputation for furnishing tools to assist auditors, and for incorporating security features into their systems based on the recommendations obtained by the liaison. For example, logs were improved to record computer activities and resource manuals related to security were furnished to auditors for each IBM computer during that time frame.

Hopefully, competition from Linux, Sun, and other sources will eventually lead to more secure systems with high availability. But for now it is not likely that Microsoft and others are ready to assume any liability. For example, on April 10, 2002, Microsoft released a bulletin warning of ten new security vulnerabilities in several versions of its IIS Web server, several of which could give an attacker total control over a vulnerable system.¹⁷ “The beat goes on.”

Yet there are some resources that can make the job easier to help secure systems connected to the Internet.

RESOURCES AVAILABLE

Hackers and crackers¹⁸ are opportunistic, taking the easiest and most convenient route in conducting their abhorrent deeds. That is, they count on organizations not fixing known vulnerabilities and regularly scan the Internet for any vulnerable system. They are right more often than not. The bad news is: there are a lot of vulnerabilities, and more are developing every week. The good news is: if those responsible for security will plug the known vulnerabilities, they will likely deter most attacks. Hackers and crackers will go somewhere else because so many sites remain vulnerable.

Enterprises should establish processes to make sure they promptly apply all security patches to all Internet-exposed systems. A good basic plan to secure Internet systems is:

1. Find a reputable source that can provide a list of known, popularly used vulnerabilities that can be used as a check-sheet.
2. Plug the applicable leaks from the list as quickly as possible.
3. Become a subscriber to at least a couple of the mailing lists that specialize in providing security alerts.
4. Regularly plug the applicable leaks from the alerts.
5. Test all changes offline before allowing the system to be active online (see Exhibit 2).

Microsoft has been known to issue bad patches. In addition, one basic tenet of the system development life cycle (SDLC)
approach to network maintenance is to test changes offline before those changes are applied to production systems. This approach brings some reasonable management to the highly volatile boiling pot of security risks, threats, and vulnerabilities on the Internet.

One encouraging sign is the number of resources that have a broad scope — Internet-wide. One worth mentioning is The Internet Storm Center (TISC), sponsored by the SANS Institute. Some of the Internet-wide information provided includes: top ten ports (most probed ports, graphed), top ten attackers (IP addresses and host names), and early warning systems for attacks. Such information can be extremely valuable for settings of firewalls. The Internet Storm Center also provides a mailing list.

An example illustrates the value of TISC. On March 22, 2001, intrusion detection sensors around the globe logged an increase in the number of probes to port 53 — the port that supports the domain name service. Attacks on port 53 are significant only because a software program called Berkley Internet Name Domain (BIND) uses that port, and versions of BIND that had not been recently updated had a vulnerability that attackers could use to take over the systems. Thousands of organizations that had not updated their version of BIND were being infected with a worm called Lion. Lion stole password files from infected machines and sent them to a site in China, and it installed a distributed denial-of-service (DDoS) tool so that the infected machines could be used in denial-of-service attacks. But hundreds of intrusion detection sensors that were logging attacks had become part of regional and industry-specific security monitoring networks. They sent their logs to analysis sites. There, the data was aggregated and charted automatically and posted for analysis at SANS. Analysts immediately saw a spike in the number of attacks on DNS port 53. Some kind of man-made “electronic storm” (actually an electronic packet storm) was sweeping through the Internet. The analysts determined what damage the worm did and how it was able to do it, and then they developed a computer program to determine which computers had been infected. They tested the program in multiple sites and they also let the FBI know of the attack. Just 14 hours after the spike in port 53 traffic was first noticed, the analysts were able to send an alert to 200,000 people warning them of the

Exhibit 2. Basic Vulnerability Plan

1. Make a list of probable vulnerabilities (broad scope of input).
2. Use list as checklist to plug applicable vulnerabilities.
3. Subscribe to security-related mailing list (security alerts).
4. Regularly use the alerts to plug emerging leaks.
5. **ALWAYS** test all changes, fixes, plugs **OFFLINE** before putting the system back online.
attack in progress, telling them where to get the program to check their machines, and advising what to do to avoid the worm. This episode demonstrated the value of sharing intrusion detection logs in real-time. Only in the regional and global aggregates was the attack obvious, and allowed the expeditious response to slow and then stop the attacks. The technology, people, and networks that found the Lion Worm were all part of the SANS Institute’s Consensus Incident Database (CID) project that had been monitoring global Internet traffic since November 2000. CID’s contribution the night of March 22 was sufficient to earn it a new title: Internet Storm Center™. Today, the Internet Storm Center gathers more than three million intrusion detection log entries every day. It is rapidly expanding in a quest to do a better job of finding new storms faster, isolating the sites that are used for attacks, and providing authoritative data on the types of attacks that are being mounted against computers in various industries and regions around the globe. The Internet Storm Center (TISC) is a free service to the Internet community. The work is supported by the SANS Institute from tuition paid by students attending SANS security education programs. On February 15, 2000, 30 Internet experts met to identify actions needed to defeat the wave of distributed denial-of-service (DDoS) attacks and to keep the Internet safe for commerce and growth. One of the resulting initiatives was a project to develop a communitywide consensus list of the most often exploited vulnerabilities. Their findings, along with detailed instructions on how to eliminate the vulnerabilities, were released in October of that year.

THE SANS INSTITUTE AND FBI’S “TOP TWENTY” REPORT

The above initial effort led to the release of “Top Ten Most Critical Internet Security Vulnerabilities.” This document was developed jointly with the National Infrastructure Protection Center (NIPC) and SANS. SANS says that thousands of organizations used that list to prioritize their efforts by focusing on the most dangerous and popular holes first. Then on October 1, 2001, SANS and the FBI jointly updated and expanded that list to the “Top Twenty Most Critical Internet Security Vulnerabilities” (see Exhibit 3). Like TISC, it is valuable because it was developed from a very broad perspective — literally from Internet-wide data. The list is categorized into three areas: general vulnerabilities, Windows vulnerabilities, and UNIX vulnerabilities. It is also dynamic, being updated every few weeks.

This list is a valuable resource because the majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws contained on the list. For example, the spread of most deadly viruses (e.g., Code Red, NIMDA) can be traced to exploitation of unpatched vulnerabilities on this list. Hackers and crackers continue to
exploit the best-known flaws with the most effective and widely available attack tools. But this information is now readily available to all IS auditors and security professionals. The most recent version can be accessed from the SANS Web site.\

MITIGATING MOST OF THE “TOP TWENTY”

Manual methods for checking a system to see whether it has each of the listed vulnerabilities are presented in the “Top Twenty” document. But a more practical approach to finding the UNIX and Windows vulnerabilities is to use an automated scanner. Bob Todd, the author of the free Internet scanner SARA, has created a special version of SARA designed specifically to find and report on the status of vulnerabilities on the SANS/FBI “Top Twenty” list.\

It is interesting to review the “Top Twenty” list, especially the general vulnerabilities, and think about how to mitigate those risks. They are all solvable, and it is relatively easy and inexpensive to do so. For example, careful installation plans and check-sheets for operating systems (G1) and firewalls (G4, G5); effective password policies, procedures, and systems (G2); effective backup policies, procedures, and systems (G3) are all feasible and fairly inexpensive in terms of monetary costs. Yet careful implementation of these solutions will mitigate five of the “Top Twenty” risks! Many others require
only a patch (e.g., U3). Therefore, this list is reasonably manageable from a security standpoint.

For example, one report notes that passwords are the most common method used today to authenticate computer users, despite the fact that simple password systems are known to be insecure. A hardware token, or smart card, used together with a personal identification number or biometrics, would provide much better security for the computer system.27

CONCLUSION

The responsibility for the security of assets connected to the Internet falls on security professionals and IS auditors. The security professionals have to find ways to continuously plug continually emerging vulnerabilities. IS and internal auditors have to find ways to audit these systems for operation audits and evaluation of internal controls. The “Vulnerability Plan” provides InfoSec professionals with a manageable means to plug security leaks on an ongoing basis. It also provides internal and IS auditors with a tool to develop questionnaires and inquiries regarding internal controls (see Exhibit 4 for an example).

Some individual security professionals are developing monitoring systems of their own, using various applications to develop them. These graphical systems are extremely effective in monitoring possible attacks and security problems. But there are even better tools and techniques being developed; better because they are being developed from a broad perspective and are proving to be proactive, beneficial, and effective (e.g., The Internet Storm Center). The SANS Institute and the FBI have provided another such tool with their “Top Twenty Most Critical Internet Security Vulnerabilities” list and associated resources.

Yet all of these developing tools and resources will not cause the problem of security to go away. Nor will it in any way guarantee a secure system. Rather, the tools and resources discussed in this article are intended to provide some means to maximize security benefits from efforts to protect the organiza-
Security products alone do not solve the security problems. Security products alone do not solve the security problems, nor will using the “Top Twenty” from SANS/FBI. One possible remedy would be to make software companies, system vendors, and system operators liable for system breaches and to mandate reporting of security breaches that could threaten critical social functions. At least two groups have proposed such liability (CSTB and NAS). But it is not likely to happen in the foreseeable future.

There are other essentials to a good security environment. For example, the Gartner Group suggests security professionals use (1) security goals (policy), (2) benchmarks (standards), and (3) a framework in which to operate (architecture). And then there is the need for an incident response plan in case something does (inevitably) go wrong. But the SANS/FBI list and the “Basic Vulnerability Plan” provide some reasonable, basic, and fundamental protection against Internet security threats. Moreover, proactive approaches to security not only make for more effective protection of assets, but also lead naturally to a proactive approach to risk management. It pays to be proactive.

Notes

4. One estimate of Internet fraud for 2001 is $17.8 million (see URL http://www.computerworld.com/storyba/0,4125,NAV47_STO70007,00.html). The cost of viruses alone for 2001 was an estimated $12.5 billion! (see Note 9) ... Therefore, it appears security costs are actually greater than even fraud.
12. Ibid.
14. Special thanks to Michael Hines, Purdue University, for his input on this section of the article.
17. “Microsoft Warns of 10 IIS Flaws,” eWeek, April 10, 20002. See URL http://www.eweek.com/print_article/0,3668,a=25302,00.asp.
19. The Internet Storm Center is located at http://www.incidents.org.
20. BIND is one of the name services on the Internet — typically on UNIX, Linux, etc. based systems, although Windows XP does support BIND now.
21. See Internet Vulnerability U3 on the Top Twenty list.
22. The information for this paragraph came from a Web page at The Internet Storm Center’s Web site. The page is located at http://www.incidents.org/isw/iswp.php.
24. The information in this paragraph, and some of the rest of this section, comes from the Top Twenty list (Web page) at http://www.sans.org/top20.htm.
25. See URL http://www.sans.org/top20.htm for the latest list. As of this writing, version 2.502 from January 30, 2002, was the latest list.
26. The Top 20 Scanner can be downloaded from the Center for Internet Security’s Web site at www.cisecurity.org. Several commercial vulnerability scanners may also be used to scan for these vulnerabilities, and the SANS Institute will maintain a list of all scanners that provide a focused Top Twenty scanning function at www.sans.org.

Tommie Singleton is professor of accounting and computer information systems (CIS) at the University of North Alabama (UNA), and chair of the Department of Accounting and Business Law. Prior to obtaining his doctorate, Singleton was president for 11 years of a small value-added dealer of accounting information systems using microcomputers. His education and experience are a mix of information systems and accounting. Singleton has earned CISA, CMA, CPA, and CITP certifications, and he is a member of several professional organizations related to IT/IS and accounting. In 1999, the Alabama Society of CPAs awarded Singleton the “1998-1999 Innovative User of Technology Award.” He has published numerous articles and made many presentations on subjects related to IT/IS and accounting. Singleton teaches IS auditing, advanced auditing, and other classes related to security, auditability, and controls.