A Case-Based Approach for Designing a Security System: A Seven Step Process for Managers

Hossein Bidgoli, California State University-Bakersfield, hbidgoli@csub.edu

ABSTRACT

This paper examines six recent real life cases related to computer and network security breaches, vulnerabilities, and successful security enforcements and then propose a seven step process for managers to consider when designing a security system. The steps include (1) understanding the landscape of computer and network security, (2) putting together the basic safeguards, (3) identifying security threats, (4) identifying security measures and enforcement, (5) understanding the services of computer emergency response team, (6) preparing a comprehensive security system, and (7) the business continuity planning. If these steps are followed they should increase the chances of success in designing and implementing a security system and keeping the hackers and computer criminals at bay.

INTRODUCTION AND BACKGROUND

Recently, several major private-sector and public-sector organizations have been hacked, including, the Home Depot, Target , Neiman Marcus, Adobe, RSA, Lockheed Martin, Oak Ridge National Laboratories, and the International Monetary Fund. Ponemon Research conducted a survey of 583 U.S companies, ranging from small organizations with less than 500 employees to enterprises with workforces of more than 75,000. Ninety percent of the respondents indicated their organizations' computers and network systems had been compromised by hackers at least once in the previous 12 months; nearly 60 percent reported two or more breaches in the past year. Over half the respondents indicated they had little confidence in their organization's ability to avoid further attacks. Roughly half blamed a lack of resources for their security problems, and about the same number said network complexity was their main challenge to implementing security protections [2].

UNDERSTANDING THE LANDSCAPE OF COMPUTER AND NETWORK SECURITY

Hackers, computer criminals, and cyber criminals, both domestic and international, could cost the U.S. economy over $100 billion and 500,000 jobs per year, according to a 2013 report by the Center for Strategic and International Studies (CSIS), a Washington D.C. think tank. The costs will include stolen identities, intellectual property, and trade secrets as well as the damage done to companies' and individuals' reputations. The total cost will also include the expense of enhancing and upgrading a company's network security after an attack. The CSIS report went further and included the opportunity costs associated with downtime and lost trust as well as the loss of sensitive business information. Job losses would include manufacturing jobs as well as jobs where stolen trade secrets and other intellectual properties resulted in jobs being moved overseas. Actually, the total cost may even be higher than the CSIS report projects, given that businesses often do not reveal or admit certain cybercrimes or do not even realize the amount of damage that has been caused by computer criminals and cyber criminals [6]. Table 1 lists basic security risks.

Table 1
Basic Security Risks

Spyware and Adware
Phishing and Pharming
Keystroke Loggers
Sniffing and Spoofing
Computer Crime and Fraud (ID theft, industrial espionage, sabotage)

Spyware is software that secretly gathers information about users while they browse the Web. This information could be used for malicious purposes. Spyware can also interfere with users' control of their computers, through such methods as installing additional software and redirecting Web browsers. Some spyware changes computer settings, resulting in slow Internet connections, changes to users' default home pages, and loss of functions in other programs. To protect against spyware, you should install antivirus software that also checks for spyware or you should install antispyware software, such as Spy Sweeper, CounterSpy, STOPzilla, and Spyware Doctor.

Adware is a form of spyware that collects information about the user (without the user's consent) to determine which advertisements to display in the user's Web browser. In addition to antivirus software, an ad-blocking feature should be installed in your Web browser to protect against adware.

Phishing is sending fraudulent e-mails that seem to come from legitimate sources, such as a bank or university. The e-mails usually direct recipients to false Web sites that look like the real thing for the purpose of capturing personal information, such as Social Security numbers, passwords, bank account numbers, and credit card numbers.

Pharming is similar to phishing in that Internet users are directed to fraudulent Web sites with the intention of stealing their personal information, such as Social Security numbers, passwords, bank account numbers, and credit card numbers. The difference is that pharmers usually hijack an official Web site address by hacking a Domain Name System server, then alter the legitimate Web site IP address so that users who enter the correct Web address are directed to the pharmers's fraudulent Web site.

Keystroke loggers monitor and record keystrokes and can be software or hardware devices. Sometimes, companies use these devices to track employees' use of e-mail and the Internet, and this use is legal. However, keystroke loggers can be used for malicious purposes, too, such as collecting the credit card numbers that users enter while shopping online. Some antivirus and antispyware programs guard against software keystroke loggers, and utilities are available to install as additional protection.

Sniffing is capturing and recording network traffic. Although it can be done for legitimate reasons, such as monitoring network performance, hackers often use it to intercept information.

Spoofing is an attempt to gain access to a network by posing as an authorized user in order to find sensitive information, such as passwords and credit card information. Spoofing is also when an illegitimate program poses as a legitimate one.

Computer fraud is the unauthorized use of computer data for personal gain, such as transferring money from another's account or charging purchases to someone else's account. Many of the technologies discussed previously can be used for committing computer crimes. In addition, social networking sites, such as Facebook and MySpace, have been used for committing computer crimes.

Another computer crime is sabotage, which involves destroying or disrupting computer services. Computer criminals change, delete, hide, or use computer files for personal gain. Usually called hackers, many of them break into computer systems for personal satisfaction, but others seek financial gain. Surprisingly, most computer crimes are committed by company insiders, which makes protecting information resources even more difficult.

CONCLUSION

This paper examined six recent real life cases related to computer and network security breaches, vulnerabilities, and successful security enforcements. The experiences and insight gained from these cases provided a background for the proposed seven step process for managers to consider when designing a security system. The steps include (1) understanding the landscape of computer and network security, (2) putting together the basic safeguards, (3) identifying security threats, (4) identifying security measures and enforcement, (5) understanding the services of computer emergency response team, (6) preparing a comprehensive security system, and (7) the business continuity planning. If these steps are followed they should increase the chances of success in designing and implementing a security system and keeping the hackers and computer criminals at bay.

REFERENCES

[1] Anderson, H. "Case Study: The Motivation for Biometrics." *HealthCareInfoSecurity.com*. 24 June 2010. Accessed 13 July 2010 @ *www.healthcareinfosecurity.com/articles.php?art_id=2686*.

[2] Bidgoli, H. (2015), MIS5, Course Technology/Cengage Learning, Mason, OH.

[3] Bidgoli, H, ed. *Global Perspectives in Information Security: Legal, Social and International Issues*. Hoboken, NJ: John Wiley & Sons, 2008.

[4] Bueb, F., and P. Fife. "Line of Defense: Simple, Complex Security Measures Help Prevent Lost and Stolen Laptops." *California Society of Certified Public Accountant and Gale Group* (2006). Accessed 10 August 2010 @ *www.thefreelibrary.com/Line+of+defense:+simple,+complex+security+measures+help+prevent+lost...-a0155477162*.

[5] Cooney, M. "U.S. Needs to Be On Guard for a Big Cyberattack." *Computerworld*. 14 September 2011. Accessed 12 November 2011 @ *www.computerworld.com/s/article/9220018/U.S._needs_to_be_on_guard_for_a_big_cyberattack*.

[6] Corbin, K. "Cyber Crime Costs U.S. Economy $100 billion and 500,000 Jobs." *InfoWorld*. 24 July 2013. Accessed 2 January 2014 @ *www.infoworld.com/d/security/cyber-crime-costs-us-economy-100-billion-and-500000-jobs-223352?source=IFWNLE_nlt_sec_2013-07-25*.

[7] Kitten, T. "DDoS Attacks on Banks: No Break in Sight." *BankInfoSecurity.com*. 24 April 2013. Accessed 2 January 2014 @ *www.bankinfosecurity.com/ddos-attacks-on-banks-no-break-in-sight-a-5708/op-1*.

[8] Kuchera, B. “Sony Admits Utter PSN Failure: Your Personal Data Has Been Stolen.” *ars technica*. Accessed 11 August 2011 @ *http:// arstechnica.com/gaming/news/2011/04/sony-admits-utter-psn-failure-your-personal-data-has-been-stolen.ars*.

[9] Lederman, J. “IRS Missing Billions in ID Theft.” *Associated Press*. 2 August 2012. Accessed 14 December 2012 @ *http://news.yahoo.com/irs-missing-billions-id-theft-164707999.html*.

[10] McCumber, J. *Assessing and Managing Security Risk in IT Systems*. Boca Raton, FL: Auerbach, 2004.

[11] Perlroth, N., and Q. Hardy. “Bank Hacking Was the Work of Iranians, Officials Say.” *New York Times*. 8 January 2013. Accessed 2 January 2014 @ *www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0*.

[12] “Prevent Data Theft Using Removable Devices.” *Get Safe Online*. 2009. Accessed 10 August 2010 @ *www.getsafeonline.org/nqcontent.cfm?a_id=1103*.

[13] Samson, T. “Cyber Criminals Tying Up Emergency Phone Lines Through TDoS Attacks.” *InfoWorld*. 1 April 2013. Accessed 2 January 2014 @ *www.infoworld.com/t/cyber-crime/cyber-criminals-tying-emergency-phone-lines-through-tdos-attacks-215585?source=IFWNLE_nlt_sec_2013-04-02*.

[14] Saunders, S. “Putting a Lock on Corporate Data.” *Data Communications*. January 1996: 78–80.

[15] Schiesel, S. “PlayStation Security Breach a Test of Consumers’ Trust.” *New York Times*. 27 April 2011. Accessed 11 August 2011 @ *www.nytimes.com/2011/04/28/arts/video-games/sony-playstation-security-flaw-tests-consumer-trust.html*.

[16] Stuart, K. “PlayStation 3 Hack—How It Happened and What It Means.” *Theguardian.com*. 7 January 2011. Accessed 11 August 2011 @ *www.guardian.co.uk/technology/gamesblog/2011/jan/07/playstation-3-hack-ps3*.

[17] Talbot, D. “Computer Viruses Are ‘Rampant’ on Medical Devices in Hospitals.” *MIT Technology Review*. 17 October 2012. Accessed 2 January 2014 @ *www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals*.

[18] “The Sarbanes-Oxley Act of 2002.” Accessed 10 August 2010 @ *www.soxlaw.com*.

[19] Weaver, C. “Patients Put at Risk by Computer Viruses.” *Wall Street Journal*. 13 June 2013. Accessed 2 January 2014 @ *http://online.wsj.com/news/articles/SB10001424127887324188604578543162744943762?mod=djem_jiewr_IT_domainid*.

[20] Vijayan, J. “90 Percent of Companies Say They’ve Been Hacked.” *Computerworld*. 23 June 2011. Accessed 11 August 2011 @ *www.infoworld.com/d/security/90-percent-companies-say-theyve-been-hacked-118*.