GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Corporate Responsibility to Network Security -The Buck Starts Here
Anita Erno
Version 1.2f

Introduction

Corporations today must take responsibility in securing their networks. It is all too easy to offer up a network administrator in the wake of a securitybreach. Management is obligated to employees, customers and shareholders to provide a secure network in which to work and retain corporate value. Why management is responsible for IT security and several basic security steps will be discussed herein.

It is no longer possible to ignorantly connect a computer to a network without taking responsibility for it's security. Long gone are the days when companies would set up elaborate networks with little or no thought of it's vulnerabilities. Today, CIOs and IT professionals are constantly challenged with the responsibility of securing their networks. IT security is an area CIOs constantly cite among their most important concerns, yet it is also one issue in which their corporate non-IT peers often do not share or understand. With the rise of computing in the workplace came the rise of the IT departments. For decades, universities world wide have taught business as it relates to Finance, Marketing, Management and so on. These subjects are not only taught in the formal class environments but also at the dinner table. It is no wonder that our management counterparts are not only at a loss, but just don't understand their role in IT security. Believe it or not, educating management is considered among security professionals as a moderate challenge. The most difficult challenge is getting management to admit that network security is an area where vulnerabilities exist.

Although some may think that educating an executive in IT security basics is a daunting task, consider this: in a June 2001 survey by CIO Insight, more than half of the 556 CIOs and senior IT executives polled said their IT departments had not performed a formal risk assessment to check their organization's security risk level. "The Internet is the most complex machine mankind has ever built. Every year it will get more and more complex and less and less secure." says Steve Bellovin, a security expert at AT&T Labs. He continues, "The fact that viruses and bugs are showing up inside firewalls, which so many CIOs still believe will protect them-is a real warning sign." Bruce Schneier, a cryptographer and author of *Secrets and Lies: Digital Security in a Networked World* shares his concern, "Most CIOs still have their heads in the sand." What we are dealing with is a simple case of denial, perhaps the most difficult barrier CIOs face to embracing their responsibility of IT security.

Risk Management and Who Owns It

As our networks are constantly under attack on multiple fronts, we are painfully aware we are at risk. We can no longer plead ignorance in the wake of a security breach. Those with less than honorable intent are scanning our networks daily for vulnerabilities that they may exploit. Their one and only goal is to compromise the networks

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

confidentiality, integrity and availability. Known as the Three Bedrock Principles of security, according to Stephen Northcutt of The SANS Institute, these are the three key dimensions of protection and attack. Without thoroughly understanding these elements of security, one can not mitigate risk.

So who is responsible for understanding and managing network security and the risk associated with it? Ultimately, we all are. When we are the last to leave our place of work, do we lock the door? When we take the last cup of coffee, do we turn off the pot? We know that if we leave the door unlocked, an unauthorized intruder may come in. Or if we leave the empty coffee pot on the burner, it may cause a fire. Let's take it a step further. We know it is not acceptable to give out a personal phone number of a co-worker. One would not give out proprietary company information either.

How did we learn that these things were not appropriate? Some comes from common sense while much we have learned the hard way. For example, we did not know that port 12345 (or 12346) would be used maliciously until the Netbus Trojan hit our networks. The Code Red worm is another good example of being blissfully unaware of a network vulnerability. Unless you had checked Bugtraq or Microsoft's web site and installed the patch to secure your IIS server you probably succumbed to the Code Red worm.

If the information is available, don't we have responsibility to it? IT organizations and their management worldwide have a responsibility for obtaining this information and safeguarding against it. They have a responsibility to educate their peers throughout the organizations in which they operate. CIOs and IT executives have a duty to themselves to fully understand the role they have and the speed at which it changes. Is it really very different if you hand a competitor proprietary information or leave the door open so they can come in and take it? By turning away from the ongoing changes in network security we are leaving ourselves wide open to compromised network confidentiality, integrity and availability.

Security Policy

An information security policy is at the foundation of the IT security with an organization. With the information available today on the Internet CIOs and IT Managers have access to all the tools necessary to aid them in writing a security policy. If you don't have a security policy, now is the time to get one. Develop a policy if it doesn't exist, but make sure it works for your organization. Following management's approval, implement your policy properly. That means that you should communicate the policy to everyone it governs. Finally, manage compliance to the policy. It must be clear and enforceable to be useful. Know your responsibility and limitations and the policy will work for you. A security policy should be used as a roadmap for IT management to fulfill their responsibilities to employees, customers, and shareholders.

Obligation to Employees

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Companies have an obligation to the safety and wellbeing of their employees as much as the employees are obligated to their employer. Most employees are not given free access to an entire network. That access is managed by a password which they are expected to keep confidential. The employee has a responsibility to the network to use it only for company business and attempt access to only those areas allowed. The use of passwords should be clearly understood in the security policy from the user perspective. Likewise, it is the IT departments' responsibility to clearly communicate what access is granted to the user and the rules which govern that use.

To be employed today, a large amount of personal information is required by the employer. Information such as social security numbers are considered a hot commodity on the electronic black market. We have heard story after story of people who have had their social security number stolen only to find their credit ruined, or worse, their identity. Do companies who store employee information take security seriously? Human Resources alone can not be held responsible. After all, we would not give out an employee phone number. Why would we let someone into our network and take it?

We have heard much regarding the abuse of Internet access by employees. In fact, in the "2001 Computer Crime and Security Survey" Ninety-one percent of the organizations surveyed detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems). Only seventy-nine percent detected net abuse in 2000. This is a clear message to IT executives that security policy has not been created, it is not clear, or it is not enforced. In any case, the buck starts here. It is obviously management's responsibility to the employee to take steps to ensure this behavior stops.

Obligation to Customers

CIOs and IT executives also have a responsibility to the organization's business partners and customers. They have an obligation of protecting partner data as well as business longevity and viability. People do business with those companies they expect to be in business for the long term. Should a network be compromised and specific information stolen organizations run the risk of losing the trust of their customers and ultimately that business. There is a long standing business practice of trust going with a handshake. Those days are long gone. So much of that trust is at risk due to this electronic age. It is impossible to ever be one hundred percent secure, but it is expected by all that IT management is staying current and doing the best they can with the information available.

Obligation to Shareholders

Network security managers are relied on heavily to secure the company's confidential data. A organization's value relies on the security of that data. It never occurs to shareholders to assure data confidentiality, integrity and availability when they assess the organization's value. It is assumed that their investment is sound and safely

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

guarded by a qualified IT staff. However there have been many cases where we have learned this is not true. And many cases of financial loses we will never hear of.

Sixty-four percent of the respondents in the "2001 Computer Crime and Security Survey" acknowledged financial losses due to computer breaches. Thirty-five percent (186 respondents) were willing and/or able to quantify their financial losses. These 186 respondents reported $377,828,700 in financial losses. It is important to note that these loses can be attributed to stolen proprietary information, network downtime and many other reasons. What is alarming is that this number is 11 million dollars more than reported in the same 2000 survey. We need to ask ourselves; Is this number growing because more organizations are reporting? Are the number of hackers growing? Are we turning a deaf ear to the security experts? Regardless of the reason for this growth in financial losses we are losing shareholder trust, something which lost over time will cause the financial ruin of an organization.

A Practical Guide to Securing the Workplace

The following basic security recommendations should be addressed in a security policy and adhered to by all it governs. Often the most simple policies are the one's we are the most vulnerable to. They are the very things that those who seek to breach our networks often target:

- Password Policy: A reasonably secure password should be used by all users. This may include upper and lower case letters, special characters and numbers. Avoiding dictionary words should be a requirement. Passwords should expire periodically such as every 90 days. More frequent expiration requirements drive users to write them down.

- Backup Policy: In the event of a security breach, internal or external, critical data may be maliciously corrupted or deleted. A company which performs backups and backup verifications on a regular schedule can easily and quickly restore any compromised data.

- Virus Protection Policy: Not only should virus protection be installed on each networked computer but it must be current and running at all times. In addition to this software it also must be stated in a policy what procedure will take place in the event that a virus does reach it's target.

- Firewall Policy: Firewalls are a relatively inexpensive solution to a potentially costly problem. Properly configured firewalls are required to protect a network from the outside world where hackers are lurking.

- Computer use Policy: When not is use computers should be turned off or disconnected from the network. When users step away logging off their computers or using a password protected screen saver should be considered.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- E-mail Policy: While e-mail policies can be quite lengthy a few things to include should be scanning e-mail directories for viruses. Users should not open e-mail from individuals they do not know or from those they know but with a very odd subject line such as “I Love You” like the infamous I Love You virus.

- Version (or Patch) Policy: All security software such as firewall, IDS, Virus, etc., should always be kept current with the latest patches available. Many security breaches are attacks at known vulnerabilities.

In addition to those listed above the following are some basic guidelines to include in a security policy. It is important to implement each of these as they relate to your organizations needs.

- Personnel. Those who secure your networks carry an enormous amount of responsibility. You may consider conducting background checks on individuals filling these positions to screen out possibly untrustworthy individuals.

- Incident Handling. Don’t wait for something to happen to figure out your incident handling process. In the midst of chaos humans make mistakes. Follow this six-step model: prepare, detect, contain, eradicate, recover and lessons learned.

- Contingency Planning. Always have a contingency plan which carries out the activities of making backups, updating documentation, and practicing responding to contingencies.

- Security Awareness, Training, and Education. It is the most important job a CIO and his or her staff will ever do. Everyone responsible for the confidentiality, integrity and availability of a network should be trained in security procedures and should be aware of the importance of security. In addition, they provide technical expertise needed to teach users how to secure their systems.

- Physical. The immediate physical area around the computer system must be secured.

- Technical Controls. The technical controls must be securely installed, maintained, and used by knowledgeable IT staff. They create the user accounts, add users to access control lists, review audit logs for unusual activity and perform the countless operational tasks needed to use technical controls effectively.

- Configuration Management. IT staff ensure that changes to a system do not introduce security vulnerabilities by first establishing a baseline condition and then managing to that condition. This allows the IT staff to test the changes and their effect on the system.

Summary

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

With the help of organizations such as The SANS Institute and the Computer Security Institute we are getting smarter. Whether an organization's IT executives are willing to embrace and respond to this assistance is entirely up to them. Patrice Rapalus, CSI Director, remarks that the "Computer Crime and Security Survey," now in its sixth year, has served as a reality check for industry and government:

> "...The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with enterprise-wide information security."

Time as shown us there is strength in numbers. Now is the time to rally and rise to the issue of IT security. It is not just a nice thing to do, but also a responsibility that starts with the CIO or IT executives and will continue as long as computers are a part of our lives.

List of References

1. Dekker, Marcel, Published in "The Froehlich/Kent Encyclopedia of Telecommunications vol. 15.", New York, 1997, pp. 231-255.
URL: http://www.cert.org/encyc_article/tocencyc.html

2. Merkow, Mark, CCP, CISSP, "Reinforcing Your Network Security: Taking Personal Responsibility" March 10, 2000.
URL:http://ecommerce.internet.com/news/insights/outlook/print/0,,7761_319231,00.html

3. "2001 Computer Crime and Security Survey," March 12,2001
URL: http://www.gocsi.com/prelea/000321.html

4. Briney, Andrew, L., "Exposing Infosecurity Hype", January 2001
URL: http://www.infosecuritymag.com/articles/january01/columns_note.shtml

5. Epstein, Keith, CIO Insight "Internet Chernobyl?" September 2001
URL:http://www.cioinsight.com/sections/feature/index.asp?Issue=05&Section=&Article=infrastructure&Page=01

6. Perkowski, Mike and Kirkpatrick, Terry A., CIO Insight "Research: Security" August 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

URL:http://www.cioinsight.com/sections/executivebriefs/index.asp?Issue=04&Article=security&Page=01

7. Information Security Magazine "Viewpoints" March 2001
URL: http://www.infosecuritymag.com/articles/march01/departments_viewpoint.shtml

8. National Infrastructure Protection Center
http://www.nipc.gov/warnings/computertips.htm

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: March 30th, 2017

Upcoming Training

Click Here to {Get CERTIFIED!}

Mentor Session AW - SEC401	Grand Rapids, MI	Apr 07, 2017 - May 19, 2017	Mentor
Mentor Session - SEC401	Hollywood, CA	Apr 07, 2017 - May 05, 2017	Mentor
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201704,	Apr 11, 2017 - May 18, 2017	vLive
Community SANS Cleveland SEC401	Cleveland, OH	Apr 17, 2017 - Apr 22, 2017	Community SANS
Community SANS Virginia Beach SEC401*	Virginia Beach, VA	Apr 24, 2017 - Apr 29, 2017	Community SANS
SANS Baltimore Spring 2017	Baltimore, MD	Apr 24, 2017 - Apr 29, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Apr 26, 2017 - Jun 07, 2017	Mentor
SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
Community SANS Las Vegas SEC401	Las Vegas, NV	May 08, 2017 - May 13, 2017	Community SANS
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
Community SANS Columbia SEC401	Columbia, MD	May 15, 2017 - May 20, 2017	Community SANS
Community SANS Baton Rouge SEC401	Baton Rouge, LA	May 15, 2017 - May 20, 2017	Community SANS
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event