Global Information Assurance Certification Paper

Terry Boston
10/24/00

THE INSIDER THREAT

Introduction:

When considering your defense in depth configuration, you must give great consideration to the insider threat. The insider can be a treat against all three computer security bedrock principles: confidentiality, integrity, and availability. It is estimated that 80% of attacks are from within the organization. The most serious security breaches resulting in financial losses occurred through unauthorized access by insiders. Insiders represent the greatest threat to computer security because they understand their organization's business and how the computer systems work. Therefore, an insider attack would be more successful at attacking the systems and extracting critical information. The insider also represents the greatest challenge in securing your network because they are authorized a level of access to your network and are granted a degree of trust.

Who is the Insider Threat

Insiders are those individuals who work for the target organization or have a relationship with the organization that grants the individual some level of access. This includes employees, contractors, business partners, customers, subcontractors, etc. The insider may have various motives, financial, social, political, or personal. However, the greatest threat to computer security in regards to the insider is lack of knowledge and social engineering. A threat is defined as that which if unchecked will cause a loss to the organization. Therefore the insider threat is defined as those who have authorized access to your organization that could possibly cause a loss to the organization if computer security goes unchecked.

Insider Threat and the Lack of Knowledge

Many network security intrusions are the result of employees' lack of knowledge. Educating your users is essential to computer security. Ensure that your users are

warned about the dangers of allowing other users access to their accounts. Caution users against opening insecure access on their personal computers (such as setting up a FTP server on their own computer with full anonymous access or running a small Web server that may not be secure as the official servers). Emphasis should be placed on not sharing information with unauthorized personnel (such as giving their password to others and mentioning the products and versions of products used on your network). Users should be warned against writing their passwords on post-its and putting it on their computer, selecting easily guessed passwords, and opening email attachments from unknown people.

Users also must be knowledgeable of the organization's security policy. If your organization does not have a security policy, develop one quickly. It is essential to good security practices and defending your network. The requirements for a good security policy are addressed later in this document.

Insider Threat and Social Engineering

Social engineering is a low-tech method of cracking network security by manipulating people inside the network into providing the necessary information to gain access.[1](It is also defined as the ability to achieve a goal through the use of effective persuasion.[2](Some of the methods used in social engineering include: Cunningly soliciting the help of an unsuspecting and sympathetic user, the intruder admiring the way a user performs a certain function and getting the user to instruct them on how to perform the function, and intimidation (the intruder convincing the user that there would be repercussions if the user did not assist him). Another tactic is requesting information from a user just before quitting time. The user will more than likely fulfil the request to expedite his departure. Social engineering can be a very effective means of intrusion. It plays on the human desire to be helpful and do the "right thing", relying on the helpfulness and politeness of the

[1] Network Security Fundamental, Peter Norton and Mike Stockman, Copyright SAMS publishing company 2000

[2] Information Security, Donald L. Pipkin, Copyright Prentince Hall PTR 2000

user. The defense against such attacks is an awareness and training program that informs employees of the nature of such attacks.

Protecting Your Network Against the Inside Threat

There are steps that you can take to protect your network against the inside threat. Educating your users is a very important element to securing your network. Train users on the use of strong passwords. Ensure that users understand how viruses and other programmed threats spread and what they can do to help prevent such spreading. Train users to be alert to the possibility of infected email attachments. Users should be able to recognize and report virus symptoms and be apprised of new threats and related intrusion events. Make users aware of social engineering and how to handle such situations when confronted.

There are also policy considerations that must be addressed to minimize the possibility of an inside attack. Your organization must develop a sound security policy that is approved by management and understood and practiced by all employees. Your organization's security policy should address password requirements, define user and system administrator authority, an anti-virus policy, address the handling of proprietary information, incident handling, and physical security.

Additional Protective Measures

There are additional measures that can be taken to mitigate the risks of insider threat.
Run backups and secure in a safe place.
Install and execute appropriate anti-virus tools.
Regularly check for viruses.
Ensure that your computers have the most recent versions of anti-virus software.
Update your anti-virus tools using vendor updates as they become available.
Store copies of anti-virus tools offline, in a secure manner.
Install software updates and patches.
Routinely check for and update threat detection tools as needed, especially when new threats are discovered.
Prevent unauthorized outgoing access at the firewall.
Ensure that permissions are properly set.

Computer Crime Statutes

Computer crime is any illegal act which involves a computer system, whether the computer is an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime[3]. Rarely are criminal charges pursued against insider attacks. If the attacker is an employee, the prevalent course of action is disciplinary in nature. If the attacker is a business partner with the victim then a financial retribution is usually preferred. However, there are a number of statues which make computer crime punishable. The following are six main U.S. Statues used in the prosecution of computer crimes.

Computer Fraud and Abuse Act, 18 U.S.C. 2030

Economic Espionage Act, 18 U.S.C. 1831, to 1839

Trafficking in Fraudulent Access Devices, 18 U.S.C. 1029

Wire Fraud, 18 U.S.C. 1343

Wiretap Act, 18 U.S.C. 2511

Access to Stored Electronic Communications, 18 U.S.C. 2701

References:

Computer Security Institute March 4, 1998 Release

Peter Norton and Mike Stockman, *Network Security Fundamentals*, Copyright SAMS publishing Company 2000

Donald L. Pipkin, *Information Security*, Copyright Prentice Hall PTR 2000

Randall K. Nichols, Daniel J. Ryan, and Julie J.C.H. Ryan, *Digital Assets,* Copyright McGraw-Hill 2000

http://www.securityfocus.com

[3] Network Security Fundamen6als, Perter Norton, Copyright 2000 SAMS publishing

http://www.securityportal.com

http://www.cert.org

http://www.cerias.purdue.edu/coast/intrusion-detection/introduction.html