Global Information Assurance Certification Paper

Securing the Help Desk: What You Need to Know

Kathy Hunt
August 4, 2003

GSEC Practical Assignment
Version 1.4b, Option 1

Table of Contents

Abstract

The world of Help Desks has rapidly changed in recent years. No longer is it a back office function that the best personnel shy away from. It is becoming the core of many businesses, the front-line to the customer, and a way for organizations to measure trends and take proactive approaches to customer service.

Critical success factors of the Help Desk include keeping problems under control and measuring performance. Achieving success means establishing policies and procedures for Help Desk personnel to follow. These procedures must emphasize security to ensure the confidentiality, integrity, and availability of corporate assets. This paper focuses on the security aspects of the Help Desk including Help Desk tools, authorization and authentication, password policies, social engineering, and physical security.

What is a Help Desk?

Running a Help Desk means more that just answering phones and entering job tickets. It is a front line interface for an organization.

The Help Desk can be a low-level function to strictly route calls to the appropriate IT group, or it can be responsible for solving complex requests such as responding to inquiries about sophisticated, customized enterprise applications.

Regardless of its specific duties, the Help Desk basically serves the following functions:

- An accessible service point which provides on-demand advice, information, or action to aid a user
- A front line service for customers
- The public face of an organization

Help Desk Systems

There are many different types of Help Desk systems and support tools on the market. There are a multitude of vendors selling Help Desk solutions and companies that make their livelihood by running Help Desks for other organizations that have outsourced that function. However, it is important for Help Desk managers to avoid purchasing the latest software tool strictly for its “bells and whistles”. Help Desk managers must carefully analyze their particular environment in relation to what tools will work and the level of security they require.

As part of their evaluation, managers should ask questions such as:

- Will this solution work in my organization?
- Will this solution provide the level of security demanded for our needs?
- Does this solution meet our requirements?

For example, a company with high call volumes requires a system that will interface with the phones, while a company with an emphasis of doing business via email requires a

system that integrates seamlessly with their existing email system. Banks and financial institutions are very concerned with both security and speed. Therefore, banks and financial institutions must ensure that any Help Desk system takes into account both of these factors and must weigh these factors heavily during the software review stage.

Call Tracking

It is vital that any system implemented for use by the Help Desk personnel be able to track call types and provide trends to management. For example, studies show that calls regarding password resets are fairly consistent. If the percent of security and password reset inquiries is much higher than 38%, it might indicate that a utility tool could decrease the number of these requests. However, if the percentage of those calls is much lower, it could indicate a security problem in that users may be bypassing password resets or someone else is handling those calls (Cuff, pages 1-2).

To analyze and understand these trends, the Help Desk system must be able to track call types and provide management reporting on these incident types. Such tracking also helps determine where additional communication is warranted such as the need to update the website FAQs or to provide additional end user training. It also points out areas of security concerns that should be addressed such as integrity concerns if it is easy to bypass the Help Desk when password resets are required.

Authentication

There are five elements of authentication (Smith, p. 3). Any Help Desk system with security concerns should include these elements as follows:

- Person or group of people being authenticated
- Distinguishing characteristic that differentiates that particular person or group from others
- Proprietor who is responsible for the system being used and relies on mechanized authentication to distinguish authorized users from others
- Authentication mechanism to verify the presence of the distinguishing characteristic
- Access control mechanism to grant some privilege when authentication succeeds and deny the privilege if authentication fails

User Authentication

The Help Desk system can grant control access by comparing the user name with the access rules tied to a particular file or other resource. Of course this is a simplistic view, and the real world is not so simple. In the perfect world, we would want to grant people only access to those exact resources they need. While not a perfect solution, this is accomplished using the philosophy of “least privilege”. This concept means that users get just as many permissions and privileges that they need, but no more.

For example, a Help Desk employee might have the ability to view a ticket opened by a colleague, but be unable to change the historical ticket information. Meaning, this person cannot edit/change information about who opened the ticket, when it was

opened, and any historical notes tied to the ticket. This functionality can be accomplished by Role-based Access Control where the Help Desk personnel are assigned roles based on their function. Groups are assigned authorization to perform functions on certain data. Managers and Administrators would be placed in a different role with Managers having more access to executive reporting and over-ride functions than the typical Help Desk employee.

Authenticating Computer Systems

People are not the only entities that need to be authenticated. For example, unattended computer systems such as web servers need to be authenticated. When a user accesses the Help Desk server to make an update to their data, they want to be sure that it is managed and controlled by that organization. This can be accomplished by the use of digital certificates.

A digital certificate allows users to confirm a web server's identity. Secure Socket Layer (SSL) enabled client software, such as a web browser, can automatically check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA). SSL server authentication is vital for secure transactions in which users are sending credit card numbers or confidential information over the Web and first want to verify the receiving server's identity

Authentication Factors

User authentication can be classified in terms of three factors, each of which relies on a different method to authenticate. These factors are as follows:

- Something you know: password
- Something you have: a token
- Something you are: biometric

This paper previously discussed the fact that the percentage of call types for passwords indicates improvement opportunities or areas of potential security concern for the Help Desk Manager. We also discussed the importance of authentication in the Help Desk System. While not the strongest authentication method, the password is a main authentication factor in many Help Desk Systems and is the focus of authentication in this paper.

Passwords

The benefits to using passwords are that they are cheap to implement and they are ideal for users who connect from remote systems. Unlike the token, the password travels with the user. However, passwords are weak since they depend on secrecy. Unless they are encrypted, hackers can use sniffers to detect passwords. Also, people either choose passwords that are too easy to remember or hard to remember, and thus end up writing down the password. This of course compromises security as it makes an attacker with access to the Help Desk's physical location able to read the password on the sticky note pasted to Help Desks' computer.

Strong Password Policy

It is important that no matter what system is put into place for tracking and resetting passwords, that the passwords be both strong and secure. Strong passwords include a mix of alphanumeric, numeric, and special characters. Strong passwords are important to thwart attackers from guessing which passwords a person is using. Attackers might social engineer a password by preying on the keen customer service inclinations of the Help Desk personnel (more on this topic to follow).

For maximum protection, users should be forced to change their password upon first login and should be required to rotate their passwords every x days depending on the environment. Additionally, passwords should not be reused within y number of times, for example five times. These guidelines help limit successful brute force attacks and password crackers to gain unauthorized access by obtaining active passwords.

Help Desk personnel should be taught to never leave their systems passwords on a sticky note under their keyboard and to never share their password with others. Help Desk personnel should each have their own unique passwords for auditing purposes. The system should maintain multi-level security based on userid so that only certain individuals can obtain access rights to more secure parts of the system. For example, only the Help Desk manager should be allowed to combine or delete trouble-tickets and a strict audit trail should be maintained of this activity.

As with all policies and procedures, the guidelines for passwords changes should be comprised of formal, written practices. Corporations should establish a policy of never sharing passwords with anyone, including administrators. All Help desk personnel should be familiar with the procedures, which should be posted in a central location, accessible to personnel at all times. Ideally, these procedures can be posted on the Corporate Intranet, accessible only to Help Desk personnel.

Password Storage

Passwords stored on the system should not be readable by someone who gains unauthorized access. One way of achieving this is to store the passwords via a hash. While not foolproof, the one-way hash mitigates the risk of a hacker compromising the password from the system or a tape back-up since the password cannot be retrieved by just viewing the stolen password file.

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value (Security.com).

The key to the hash is that there must be no practical way to convert the hash result back into the original data. When a user tries to logon, the computer applies the hash algorithm to the password supplied by the user. If the hash of the password matches the hash stored in the Help Desk system, the user is successfully authenticated.

It is important to take a moment here to stress that passwords have inherent weaknesses. The compromise of a password on a machine can allow the entire network to be comprised by an attacker. Therefore, care must be taken to follow the policies and procedures outlined by the organization in regards to safe password practices.

Social Engineering

While technology and processes are critical to ensuring a secure environment, the best technologies and the most well-written policies and procedures do not mean that a company is not vulnerable. Hackers often exploit personnel as the weakest link in the security chain.

Hackers looking to break into a corporate network frequently use social engineering techniques to achieve their objective. One of the preferred methods is to exploit the cooperative nature of the Help Desk personnel to gain access to sensitive information.

Social engineering goals can take various forms. Four of the most popular goals can be categorized as follows (Gaudin):

- Fraud
- Network Intrusion
- Industrial Espionage
- Identify Theft

Social Engineering Indicators

While companies often train Help Desk personnel on being customer service oriented and effective, they rarely teach them about being an integral part of the security process. Help Desk personnel should be trained to recognize potential social engineering attacks and be prepared to raise the flag to management in case of such attacks.

Indicators to be aware of include the following (Anonymous, Computer Security Institute):

- Refusal to give contact information
- Rushing
- Name-dropping
- Intimidation
- Small mistakes, for example: misspellings, misnomers, odd questions, etc.
- Requesting forbidden information

When Help Desk personnel encounter these indicators, a red flag should go up so the entire team can be alert to a possible attack.

Protection Against Social Engineering

Security experts offer the following advice for company protection against such attacks (Gaudin; "How to Thwart the Social Engineers"):

- Shred phone lists, company rosters, and other important company materials instead of simply throwing them in the trash
- Give extra security training to those on the company's perimeter such as Help Desk personnel
- Pay Help Desk workers well and try to minimize turn-over
- Implement procedures for handling calls for password resets, user ids, or other forms of authentication
- Let Help Desk employees know they should not be pushed around; If someone calls acting hostile, it should raise a red flag
- Set policies for what can be written in email, discussed over the phone, sent via fax, and verbalized outside of the office
- Ensure that Help Desk personnel follow basic security practices such as not writing down passwords
- Encrypt information on desktops, laptop, and PDAs
- Don't allow Help Desk employees to set up automatic email notifications or voice mails that they are out of the office as these actions can position the replacement as a target

Policies and Procedures

A security policy defines in writing how a company plans to protect its physical and information technology assets. The human element is often the weakest link in the security process and therefore should receive more scrutiny. The security policy should be a living document, changing as the environment changes (Security.Com, Glossary: Security Policy).

The security policy should indicate what is expected of people in a clear and concise manner. According to the SANs GIAC reading materials, a security policy should include the following items (Cole, p.341):

- Purpose—The reason for the policy
- Related documents—References to other documents that affect the policy
- Cancellation—Identifies any existing policy that is cancelled when the new policy takes effect
- Background —Provides information on the need for the policy
- Scope—States the range of coverage for the policy (to whom or what does the policy apply)
- Policy Statement—Identifies the actual guiding principles
- Action—Specifies what actions are necessary and when they are to be accomplished
- Responsibility—States who is responsible for what activities
- Ownership—Identifies who sponsored the policy and from whom it derives its authority, as well as defines who may change the policy

Types of Policies

Different types of policies include acceptable use, remote access, user account/password, firewall, and network policies. Acceptable use includes what is deemed acceptable use on a corporate-owned system. This includes sending potentially offensive emails, downloading streaming video, and installing unlicensed software.

The user account/password policy discusses password policies, such as how long passwords must be, what characters they should contain and how often they must be changed. This policy can also include comments on user accounts, such as new account requests must be approved by the user's manager and reviewed by the Help Desk manager (Andress).

Help Desk policies should take into account the individual business situation and manage a balance between good customer service and security. While designing a password policy so tight that it is virtually impossible for a user to receive a password reset will certainly help with data integrity and confidentiality, it does nothing for data availability and is therefore not a good security policy. In this case, Help Desk personnel will likely circumvent the policy in order to get their job done. This in turn will cause more security problems, not less.

If management is unaware of the security policy and its rationale, then it is unlikely that proper funding or commitment will be secured (Control Data Systems, p. 4). Upper management should sign-off on the policies so they have a clear understanding of the types of challenges that the Help Desk faces. Management should stand behind the Help Desk during tricky situations such as when the Vice President calls demanding that his password be reset, but the Help Desk cannot immediately authenticate him and needs time to do more research.

Procedures and Checklists

From the policies are derived procedures and checklists. While the Help Desk policy should address the who, what, and why, the procedures address how, where, and when. Help Desk procedures might include steps for handling password requests, guidelines for logging and closing incidents, checklists for authorizing users, and steps for backing up data. The procedures should be in sync with the higher-level policies of the organization. As with policies, procedures should be periodically reviewed and refreshed to ensure they keep up with changes in technology, personnel, evolving vulnerabilities, and other environmental factors.

Policies and procedures are fundamental building blocks in developing effective controls to counter potential security threats. As previously discussed, this includes preventing and detecting social engineering attacks to the Help Desk. Obviously, policies and procedures do not prevent all attacks, but act as part of the defense in depth posture to mitigate attacks and keep risks to an acceptable level.

Specific Help Desk Policies

The following, inspired by Kevin Mitnick's book The Art of Deception, provide some suggested Help Desk policies for consideration:

Caller ID: Caller ID should be available on all Help Desk personnel phone sets. Ideally, the phones should use a distinctive ring to differentiate calls that originate outside the company from calls that originate from inside the organization. While phone numbers can be spoofed, this acts as another data point for Help Desk personnel to authenticate a user. Additionally, if the employee can verify the identity of phone calls from outside the company, it might help them prevent an attack or to identify an attacker to the security team.

Phone System Configuration: The voice mail administrator should enforce security requirements by configuring the appropriate security parameters in the phone system. This will allow extra protection for sensitive data left on the Help Desk voice mail.

Security Awareness Training: All Help Desk personnel must attend security awareness training upon transfer to the Help Desk group. Additionally, Help Desk personnel should be required take a refresher course over specified periods. The purpose is to mitigate security breaches and understand how to identify and mitigate social engineering attacks.

Security Training for Help Desk Access: All Help Desk personnel must take a course on Help Desk procedures and systems usage. Social engineers often target newer employees for their attacks as newer employees are most likely to be eager to show their helpfulness and are least likely to be aware of the company's policies.

Remote Access Procedures: Help Desk personnel should not provide the details regarding remote access unless the requestor has been verified as authorized to receive internal information and verified as authorized to connect to the corporate network as an external user.

Resetting Passwords: Passwords may only be reset at the request of the account holder. Help Desk personnel must call back the requestor to the number provided by the corporate phone directory or the number listed in the system (versus the number provided by the requestor at the time of the request).

Changing Access Privileges: Requests for changes to access privilege must be in writing and approved in writing by the account holder's manager. This is because computer intruders that have comprised a user account can then try to elevate their privileges to gain additional control over the system.

User Trouble Tickets: The names of employees reporting computer incidents should not be revealed outside the company. A social engineer could pose as someone representing the Help Desk and contact an unsuspecting employee to say that they are troubleshooting a problem. During the call, the attacker could trick the user into

divulging proprietary information or into performing acts such as installing software that could be used by the attacker to illegally access the system.

Mandatory expiration: All computer accounts should be set to expire after a certain period such as one year. This is to reduce the existence of legacy computer accounts, which are frequently the target of dormant accounts.

Security Patches: Security patches for operating system and Help Desk application software should be installed as soon as possible after they become available and are tested. Once a vulnerability is identified and published, hackers can then take advantage of it to attack the system and companies risk suffering a security incident if patches are not up to date.

Contact Information on Websites: External websites should not reveal details of the corporate structure or identify of employees by name. Computer attackers can analyze such information to determine which targets have access to valuable, sensitive critical information.

Encryption of Offsite Backup Data: All Help Desk data stored in offsite backup facilities must be encrypted to prevent unauthorized access.

Initial Passwords: User passwords set to an initial value must be changed at the time of the initial logon attempt. This mitigates the risk of an unauthorized user gaining access to another user's account.

Invalid Login Attempts: Users should be locked out of the system for a period of time after x number of successive invalid login attempts. This is necessary to prevent brute force attacks such as dictionary attacks to gain unauthorized access to a system. In areas where high security is necessary, the system should lock-out user accounts until they are reset by a person with authorization to provide user account support. Prior to resetting the password, the Help Desk should follow procedures to identify the account holder.

Documenting Suspicious Calls: Help Desk personnel should be trained to document suspicious calls. They can try to learn details from the caller that might reveal what the attacker is trying to do. This can assist management in determining the objective of the attack or any patterns of attacks.

Passwords: Passwords should not be sent via email unless the email is encrypted. Leaving a message containing a password on a voicemail box should also be prohibited. Social engineers can gain access to another's voice mail box because voice mail owners often use an easy-to-guess access code. Additionally, passwords should not be faxed as most fax machines are accessible by many people.

Background Checks: A background check should be required for all personnel prior to reporting for Help Desk duty. Help Desk employees have access to sensitive information that can critically compromise corporate security if not properly managed.

Physical Security

Physical security is a very important, and often overlooked component to information security. The Help Desk manages sensitive corporate data and should be protected physically as well as logically from the threat of attacks. Ideally, access to the Help Desk area should be protected by access control methods such as a locked door. More sophisticated types of physical security include use of a Smart Card or use of a Smart Card with a passcode. The perimeter should be well defined and "restricted areas" should be marked as such. Filing cabinets and drawers within the Help Desk area should remain closed and locked when not in use.

Additionally, corporate dumpsters should be in a secure location, marked no-trespassing and Help Desk personnel should be instructed to shred sensitive documents versus disposing of them in the regular trash. This will prevent "dumpster divers" from searching the trash for useful information from which to launch a social engineering attack.

Summary

The Help Desk function is a customer facing function that often has access to highly sensitive corporate information. In addition to the traditional training on performance metrics and efficiency, Help Desk personnel need to be trained in security and security policies. Help Desk personnel should be aware of potential social engineering attacks and how to document and report such attacks. Additionally, Help Desk personnel should be informed about policies and procedures and why they are important. The more the Help Desk personnel understand the rational behind the policies/procedures, the more likely they are to follow the guidelines.

As people are arguably the weakest link in the security chain, attackers will often use unsuspecting employees to their advantage when trying to compromise a corporate system. Help Desk personnel should be armed with the tools, training, and management support to enable them to provide the customer service function they are hired to perform in a secure and reliable manner.

References

Cuff, Jeanne. “Stepping on Legos: A System is Only as Good as its People.” Compass Consulting. 2002. URL: http://www.compassmc.com/white_papers/1Legos.pdf (July 28, 2003).

Smith, Richard E. Authentication: From Passwords to Pubic Keys. New Jersey: Addison-Wesley, 2002. Page 3.

Security.Com. “Glossary: Hashing.” URL: http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci212230,00.html (July 28, 2003).

Gaudin, Sharon. ”Social Engineering: The Human Side of Hacking.” Datamation. May 10, 2002. URL: http://itmanagement.earthweb.com/secu/article.php/1040881 (July 28, 2003).

Anonymous. “Social Engineering: Examples and Countermeasures in the Real World.” Computer Security Institute. November 1999.

Gaudin, Sharon. “How to Thwart the ‘Social Engineers.” May 10, 2002. URL: http://itmanagement.earthweb.com/secu/article.php/1041161 (July 28, 2003).

Security.Com. “Glossary: Security Policy.” URL: http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci548251,00.html (July 28, 2003).

Cole, Eric. SANS Security Essentials with CISSP CBK version 2.1. The SANS Institute, SANS Press, February 2003. Page 341.

Andress, Mandy. “An Overview of Security Policies.” May 8, 2002. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci822681,00.html (July 28, 2003).

Control Data Systems, Inc. “Why Security Policies Fail.” 1999. URL: http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf (July 28, 2003).

Mitnick, Kevin. The Art of Deception. Indianapolis, Indiana: Wiley Publishing, Inc., 2002. Pages 266 – 329.