Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Making the HelpDesk a Security Asset

The helpdesk is a vital part of the company who wants to get the most out of it's IT assets. This paper address potential security risks with helpdesks including social engineering, and various methods to reduce the risk of security incidents against the helpdesk.

Copyright SANS Institute
Author Retains Full Rights

AD

Making the HelpDesk a Security Asset.

The help desk is often quoted as a vulnerable point for social engineering attacks. A social engineer is a con man. He or she is someone who wants to take advantage of a person's helpfulness and use it to advance his strategy. The goal of the strategy is to get enough information to compromise a company's network. So most of the time the final goal of the social engineer is to get a user name and password for general network authentication of a specific network service. The attacks are used both against the help desk or on other employees who are told the helpdesk needs some information. At the same time, the helpdesk is a key area to preventing security incidents (for both Social Engineering and monitoring security policy). It is also crucial in collecting the evidence of a security incident. What steps can be taken to make the helpdesk a security asset ?

- Establish Call Logging
- Set Levels of Authentication
- Communicate Helpdesk's Role in Software Updates
- Evaluate Results

Establish Call Logging

How may I help you ?

I worked in telephone technical support for network backup software for 3 years. Everything I did with the customer was documented in a helpdesk database. This is a normal procedure for call centers and helpdesks for the following reasons:

1) It establishes a record of what happened.
2) It documents employee and customer comments.
3) If a call needs to be escalated to higher levels, the higher ups can read the record.
4) The record can serve as evidence when problems arise.

The call database can be just as important as server logs. In many cases it proved when customers were misinformed or misunderstood the information. As an example, we would have customers whose servers could not be restored. The customer would state that he was never told to apply certain patches. A review of the records would demonstrate otherwise. In the same way a helpdesk needs to collect evidence about the call and make it available to the security team.

So first if you are just establishing a helpdesk, a helpdesk / call center database is one of the most important tools for tracking internal IT issues. If you already

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

have an established helpdesk database, what can be done in addition to improve security ?

Warning, Danger Will Robinson !!

Add a field to the database record which flags the call as a security alert. Do this to set the call apart from other “Normal” calls. An example could be a check box menu (so all applicable situations can be checked)
with the following choices:

Normal
Unauthenticated
Policy Violation
Password Issue
Odd/Other

Each item should be supported with a short clear policy to give the helpdesk guidance on what would qualify as a security problem.

Normal - an issue where the caller is verified to be an employee, follows policy, did not ask for a password change, and generally the issue was executed standard procedure.
Over 90% of issues open are expected to be “Normal”.

Unauthenticated - an issue in which the helpdesk does not have a way to verify if the caller was an actual employee of this company.

Policy Violation - when a caller is unwilling to follow a security policy. For example, you notice that a mobile user is behind on a security patch and is unwilling to add the patch. Since the user is unwilling to follow the policy, check this box.

Password Issue - under normal conditions, each user is automatically warned about password expiration and a method to change passwords is provided to each user. Check this when a user calls for a change in a password.

Odd/Other - a broad category. It is used at the helpdesk’s discretion. It is to be marked
when something does not seem right.

Example: A caller is avoiding authentication and asks questions about the network.
Why would the caller avoid authentication ? Why would the caller ask about the network ?

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Example: A caller tries to pressure the helpdesk to let a policy violation slide or work on a password issue NOW!!! Both are known tricks of Social Engineers (usually unauthenticated), hence it would be unusual.

When a flag, other then Normal, is checked, an alert is sent to the security team the same way a server log monitor would send an alert. A security team member can review the information. If needed, the security team can audit the callers account and current activity. The security team can collect information to decide if the employee needs retraining or if an outside force is trying to social engineer. If this is a social engineering attempt, this record from the database can be used as evidence. With the addition of this field, the helpdesk caller database becomes a powerful tool to monitor and evaluate security policy. Without the extra field, this would just be another helpdesk call archived for eternity.

Use phones designed for call centers.
When I was in technical support, we used phones from Aspect. A great feature was the "emergency" button. Press the button, and it would record the phone call. When the call was completed, the system would forward the recorded call to a designated phone. The assigned phone was normally a manager. The manger could listen to the call. In many cases we used this for customers who lost their temper. The manager would hear the recording of the screaming customer and how the technician handled the caller. In some cases when the manger would call the customer back, he would ask the customer what had brought him to screaming. Sometimes the customers said they did not scream. The playback of the call would prove otherwise. After the playback, the customer usually would be sent to another tech to continue to troubleshoot the issue and the customer would keep control of his temper since he knows he will be recorded. The same feature should be used for the helpdesk. Social Engineers may use many odd tricks, may yell, may cry, anything to persuade the helpdesk to not follow policy. So if a helpdesk technician gets a call that tries to get him/her to change a password without authentication, or break some other policy, the call can be recorded. Then this provides a defense for the helpdesk in two different ways.

1) If this is a real employee (manager or otherwise) the recording will prove the helpdesk followed policy and was right to defend the company by following policy.
2) If this is a social engineer, the recording is evidence for identifying and prosecuting the social engineer.

To make the greatest use of this feature, train the helpdesk on how a social engineer may try to manipulate information. Various scenarios have been outlined in other papers and books as to what a social engineer may ask and what types of con games he/she may play. Use those resources as training

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

material. So now, the helpdesk staff will know of what situations to be aware and what to do when they may encounter a social engineer.

To make this strategy even more powerful, make sure the phone calls to the helpdesk begin with a standardized message that conversations may be monitored and recorded for quality assurance. This
places a warning to the caller that evidence may be collected and reviewed. Many social engineers feel an elevation in their risk of being caught when they hear this kind of message. The famous social engineer Kevin Mitnick stated, “Proactively recording calls could increase security as well … The 'monitoring this call for quality assurance' is really a deterrent because you don't know whether they are listening to you.”

So by adding the message you give the possible attacker a warning. By training the helpdesk technicians on the techniques of social engineering you create awareness of the methods of attackers on incoming calls. With the message recording and forwarding you have a way to collect the evidence of the attack and
notify management.

Set Levels of Authentication

Ronald Reagan had a good slogan for security during the 1980’s.
“Trust, but verify”.

When papers on Social Engineering are written, the papers usually make a case that the Social Engineer exploits trust. Since that concept has been established by so many papers then it would make sense that to secure a helpdesk from a Social Engineer, the element of exploitable trust needs to be removed.
To remove the amount of trust from the helpdesk, make a policy of authenticating the identity of the caller before help is given. This can be a tricky task. Ask for too little information and the helpdesk can still be exploited. Ask for too much information and the helpdesk becomes politically unpopular and employees treat it like an interrogation. Also evaluate the levels of authentication to be placed on internal calls versus calls from the remote users. When a policy is made, the practice of “defense in depth” needs to be applied. Just like a company should not rely solely on a firewall to protect a network, the helpdesk should not just rely on one basic method for verifying callers. Several levels of protection, each with an alert level, need to be in place to help in catching social engineering.

Internal Authentication

Many businesses do not have good physical security. Any determined individual can walk into a business usually with the help of other employees. Take as an example, if the restrooms are in the hallway of a multi-business building, someone can just be washing his hands at the sink and when someone is

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

leaving the restroom, the social engineer can follow him in out of the restroom and right into the office. Even with an access card, the real employee will open the door and walk in to the office and not even notice the social engineer behind him grabbing the door at the last minute, open it, and walk in as if he is just another employee. With this threat, internal authentication should be established.

One place to start with internal authentication to the helpdesk, is use make all telephones only accessible by a password. This was also a feature we had with Aspect phones. We could use any phone, but we had to login to use it. The phone system would then record from which location we were using the phone. With this feature, it would now require the social engineer to ask someone what the password is for a phone. If someone does not know the password, the person should be told to talk to his manager. Any manager should verify the person inquiring about the phone password. All but the boldest social engineers will walk away from this situation.

Another level of authentication is to check where this call is coming from. Most internal employees have an office or cubical in which they only need help for the machines within that work space. So it makes sense most employees will place a call for help regarding their computer from the phone assigned within their cubical or office. This approach may need some flexible planning applied to those who may be in charge of machines in different locations. But if this can be planned and applied to 80% of the internal users, then it increases the amount of research the social engineer has to do to be successful in manipulating the company. As an example, if the call source is from the copier room, then the helpdesk is alerted by this information. When the helpdesk receives the call they can proceed with the call to see if it is an innocent incident (the copier broke) or if the call proceeds to a trouble shooting issue. If the call is proceeding as if it were a troubleshooting issue, the helpdesk can call the building security or a manger to identify the person. Since it is unusual for a person to request help on the machine which is not in their workspace, an authority needs to check out the situation to see what has made this unusual. If a social engineer was able to sneak in, this intruder would need to know the policy of calling from the authorized phone and know the phone login number. If all employees have not put this information in public view (post-it note in cubical) it would be difficult for the Social Engineer to succeed.

In the book InsideInternetSecurity (What Hackers Don't Want You To Know) Author Jeff Crume offers a scenario in which someone may try to get around the above policy. A person calls a sales department, to which the callers wastes some time and then asks to be forwarded to the helpdesk. The helpdesk sees the call as coming from the sales department. Then proceeds as normal thinking this call was from sales.
To prevent this, make both a written policy and a phone policy. The written policy is that any phone call to the helpdesk needs to be a direct call. Explain that this is to assure that the helpdesk can get accurate information to allow them to do their

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

job. Then in the phone routing, make any forwarded call to the helpdesk route to the front desk. The front desk personnel will explain that any call to the helpdesk needs to be a direct call. If the person complains, let them know they will need to talk with their manager. This again will discourage a social engineer. Since forwarding calls is normally a feature to help customers reach other employees, and customers do not need to reach the company helpdesk, this policy should not cause problems with the image of the company's service to their customer base. Another way to authenticate a person before the helpdesk gets involved, is to have a helpdesk request internal web site. A domain name like helpdesk.ourcompanydomain.com. This web site is only available to users who authenticated to the network (such as an NT domain or an LDAP directory server). It can also check a certificate to verify that the request is coming from a specific machine. Then when the helpdesk web page appears, it asks for an employee id #. Now just like the phones, it checks that this is someone within the network, it checks the that the employee ID # is matched to the correct machine in which the request is made. (Just like the phone call should come from the employee whose employee ID # matches the phone number above). When all the items are correct, the helpdesk gets notified about the helpdesk issue and they can reply appropriately.

What both of the above methods do is qualify the caller before the helpdesk gets involved. Since a social engineer normally takes advantage of a person's ability to decide, the above methods remove most of the decision making. At worst case, the above methods make unauthenticated calling a difficult task.

External Authentication

External Authentication to the helpdesk is defined as anyone who is working outside of the physical company buildings. This will include sales people, field engineers, and executives on travel. External Authentication can be both complicated and problematic when all the pieces to assuring identity are not in place. Since most users who travel are at the mercy of the available technology and infrastructure, plans to authenticate remote users need to be planned to cover different scenarios. To make the plan easier, start with a overall policy for external users to reach the helpdesk and then write exceptions for specific situations.

To cover all the normal situations, have remote employees use an IPSEC VPN to authenticate to the company network. Then access the helpdesk via the helpdesk web site as stated in the internal authentication. To make the ability to access the company network even more difficult, use token access such as a Rainbow Ikey token and the network password. A token is a physical object that may hold
a piece of information to assure that the holder of the object and the right password must be the correct person to allow access. This is also known as 2 factor authentication. This way any intruder would need to get the token, the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

laptop, and crack the password to get access to the network and the employee ID number to verify that the other information is correct.

But what if…

What should happen if something is stolen ? How can we adapt, and still maintain security ?
If the laptop was stolen, but not the token, then the VPN access would not be accessible by the thief. But if the laptop and the token were stolen, then the helpdesk should have a number to call for this situation. When a call comes in, the caller can be authenticated by name, employee number, manager name and the hotel phone number to be reached. Then the helpdesk can check the manager's name in the company LDAP server of e-mail server address book. Then call the manager to verify that this employee is in the named location. This will verify that the person who called knows the company structure (at least the manger above him), the manager confirms that the person is in the location he claims to be, and a call back to the hotel will complete the process. If the caller needs new hardware to finish his task, then the new hardware (if available) will be shipped to the nearest FedEx or UPS in a "hold for pickup". This way the shipping service will ask for ID before turning over the inventory. These steps are to prevent some outside person from calling and claiming to be an employee who lost hardware, but in reality, is a con-man looking to get free hardware.

If the hardware is not stolen, but the employee forgot his password to the VPN, the following steps would be taken to resetting the password. Many e-mail programs use profiles. As an example the E-mail program Outlook can be set for more then one profile. By default the security team can make the users Outlook install with 2 profiles.

1) The normal profile which will access the network. This is the profile the employee will use for normal work.
2) This profile is for external uses to communicate to the helpdesk. It will access a basic smtp - imap server.

The user will login with profile 2). Write a message describing the problem with password and request to change the password. PGP is also installed on this machine. He/she will also leave a phone number to be called. The user will sign his e-mail with the PGP private key (which is kept on his token) and encrypt the e-mail with the company's public key. When the helpdesk gets the e-mail, they will decrypt the e-mail with the company's private key and verify the e-mail with the user's public key. Upon success, it would be reasonable that the user is who he/she claims to be. So the password change can be made and then the e-mail with the new password will be encrypted with the user's public key and e-mailed to the imap server. Then the helpdesk will call the user to let him/her know the change has been made. The user will open Outlook again in profile 2 and decrypt the e-mail and get the password.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

If the user has the laptop, but not the token, then he can call the helpdesk and use the same method to verify himself as if the laptop were stolen. Then upon verification from a manager, the helpdesk can instruct the caller to user profiles for the VPN. Many VPN clients also have profiles set just like Outlook does for e-mail. So the user is instructed to use profile 2 and asked what he/she will need to access. Then the helpdesk calls the security team to let them know that someone is going to use VPN profile 2. The helpdesk tells them the server(s) the user wants to get to and asks the security team what his logon and password will be (Profile 2 password access is changed every day). The user will use the new password, and the security team will monitor the traffic coming from the profile 2 VPN. If the traffic is what the user claimed, then as soon as the connection is terminated, the VPN password is changed. If the traffic shows and attack or some kind of mischief, then the connection is terminated, the password is changed and a call is placed with the helpdesk to deny any more help to this user until his manager calls back and the security team also calls back.

What if the user calls the helpdesk and claims to not have Internet access. Then basic authentication with name, employee # and manager would be fine. But the helpdesk needs to be aware that they should only talk about application and os related problems. Conversations about the company's network and Internet related or password related items should be treated with suspicion. Really, why is the caller interested in password related conversation when they currently do not have Internet access ?

All of the items are a rough policy to handling external authentication. External authentication is difficult since mobile users and the managers above them want flexibility and the reality of external conditions are out of the control of the company. A security policy can be flexible provided the overall goal is "can I reasonably trust that you are who you say you are". Each authentication method will have a consideration in cost, training, and the political climate in the organization. But if the above steps are taken, it should weed out all but the most crafty and well resourced of Social Engineers.

Communicate Helpdesk's Role in Software Updates.

The helpdesk has direct communication with the company's employees. They can be used to monitor and catch security issues. A large issue to address is what is the role for the helpdesk for software updates. In most organizations, it is reasonable for the helpdesk to state minimum patch levels and specific patches, but the installation of the patches are to be done without the user giving his/her password.

Are you sure you are on the right patch level ?

When I was in technical support, it was standard procedure to check OS version and Service Pack level, hardware, and in my case SCSI drivers (backup software uses SCSI tape drives) as standard operating procedure. It did not matter that

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the customer thought if it was relevant or not. It was always relevant to us. And guess what? Many times when the customer did not think the information was relevant, it actually was. A SCSI driver needed to be updated, Service Pack applied, or tape drive firmware upgraded. All the information leads to a clearer picture. The helpdesk and security team can help each other with this same mindset. The security team should outline the current patches and configuration the users should be on. As part of troubleshooting a machine, especially mobile users, the patches and configuration should be checked and documented. If something is not correct and the user does not comply with changing it, then the database field can be marked with "Policy Violation" and this now becomes a security issue. This will give the security team the ability to check the issue for either an update of the security configuration and patches outline, or to discuss the issue with management.

Companies should also be using Asset Management software. This is software which collects information about all client access machines. This information is normally installed software, patch levels, and hardware.
The helpdesk should have the asset management reports for each machine available to them. This way they can evaluate if the information given to them by the caller is the same as what is on the asset management report. This provides the following:

1) The helpdesk can use the report as a troubleshooting tool for problems.
2) The report can be used to verify if the caller is giving accurate information.
3) If the information is not accurate between the caller and the report, this can indicate that either the asset management software needs to be evaluated for problems or a social engineer may be on the phone. Either way, it has now become a good way to audit potential problems.

Are you sure you need to login to my machine ?

Many papers on Social Engineering will use an example of a helpdesk call to a random person in the company stating ,

" Hi I am Joe from the helpdesk. I need to login to your machine to install a patch.
What is your user name and password?"

This is where communication is important in a company. All users in the company should know that patches in the company are installed remotely without need of giving a password to the helpdesk. Some company's have software to install patches during network login (such features are included with asset management software). Others have software that logs into a directory service and installs software while everyone is at home. Other software updates itself in an automated fashion (Anti-virus programs are known for this). However the company distributes it's software, every employee needs to whole-heartedly grasp, "no one needs your password but you". When everyone understands this,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the company will benefit from having users who are wary of “calls from the helpdesk”.

To strengthen the resistance to a social engineer, the employee can ask the caller for his name and direct extension to call him/her back. If the caller is willing to do so, call back to the helpdesk and ask if this person and extension called. This will establish if the call is legitimate or not. If not, then the call can be marked as an “Odd\Other” type of call by the helpdesk.

Evaluate results

Review the call database and the phone log
All of the data collected in the database and full features of the call center style phone would go to waste if a review of the information did not take place. Have someone review if the helpdesk is typing complete information (this is a combined IT/Security task). Since the helpdesk has a field in the database to separate the “normal” calls and the “security related” calls, the security team should examine the number and types of security alerts. What are the most common types of security related calls? Are people having a lot of password or access related calls? How were the people authenticated before the details of the call happened? Questions like these mentioned can give insight as to the need for training or communicating how to keep good passwords. Review the phone logs to see if a large number of calls are coming from the same phone number or if a large amount are coming from outside the company. Just like with any server log, look to set a baseline pattern and then see if anything deviates from this pattern. It could also reveal Social Engineering attempts when someone calls different techs with a similar story and is looking for a password change or other information. The security team can use this information to determine if the FBI needs to get involved and can use the information as evidence if the need arises.

The helpdesk is a vital part of the company who wants to get the most out of it’s IT assets. It also is a rich resource for implementing and evaluating the security of a company. With well thought out policy, a good helpdesk database, well entered data and constant evaluation, the risk of social engineering security incidents against the helpdesk can be readily managed. When you can manage the attacks, the risk against the company should go down and the risk of the social engineer being caught should go up.

Crume, Jeff. Inside Internet Security - What Hackers Don’t Want You To Know. Addison-Wesley, 2000.

Berg, Al. Cracking a Social Engineer, Packet Storm.
URL: http://packetstormsecurity.org/docs/social-engineering/soc_eng2.html

Lemos, Robert. Mitnick teaches ‘social engineering’, ZDNet News. July 17 2000
URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2604480,00.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Donston, Debra. A healthy security attitude, eWeek. June 11, 2001
URL:
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2771373,00.html

Corcoran, David. Introduction To Authentication, LinuxSecurity.com. May 26, 2000
URL: http://www.linuxsecurity.com/feature_stories/feature_story-44.html

Andriole, Steve. 8 Keys To A Sane Security Strategy, Datamation.
URL: http://itmanagement.earthweb.com/secu/article/0,,11953_855161,00.html

© SANS Institute 2001, Author retains full rights

Last Updated: August 30th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Milan 2015	Milan, IT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
FOR578 Cyber Threat Intelligence	OnlineVAUS	Aug 31, 2015 - Sep 04, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced