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 (Security 401)"
at http://www.giac.org/registration/gsec

Access Management: Revalidation of User Access

© SANS Institute 2004, Author retains full rights.

Hendrik Vandendriessche

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b – Option 2

Submitted: April 6th, 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. INTRODUCTION 3

2. ACCESS MANAGEMENT 3

2.1. Account Administration 3
2.1.1. Request and approval of account 4
2.1.2. Creation of account 4

2.2. Account Maintenance 4

2.3. Account Monitoring 5

2.4. Account Revocation 5

3. IMPORTANCE OF ACCOUN T MAINTENANCE 5

4. REVALIDATION OF USER ACCESS 6

4.1. Prerequisites for an effective account maintenance process 6
4.1.1. Account ownersh ip information 7
4.1.2. Access to employee records 8
4.1.3. Ownership of special accounts 8

4.2. Employment Revalidation 9

4.3. Access Rights Revalidation 11

4.4. Employment Revalidation « Access Rights Revalidat ion 14

5. SUMMARY 14

6. REFERENCES 16

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Introduction

This paper gives a generalized overview of an access revalidation process to periodically revalidate user accounts and their access rights, which I have implemented during my current job.

In a first chapter I will explain how this access reval idation process fits in the bigger picture of access management and what the risks are of not having access revalidation processes.

I will discuss the access revalidation process in more detail in the next chapter. What are the prerequisites for this proc ess? What are the components of this process? I will split access revalidation in two processes; the employment revalidation and the access r ights revalidation.

Finally I am going to compare both access revalidation processes and discuss why the split was made and why it is good to have both processes in place.

2. Access Management

Access management is the process of defining access to systems and data, maintaining this access and removing it when no longer needed. According to the SANS Security Esse ntials Course, the access management process consists of four tasks [1]:

- account administration
- account maintenance
- account monitoring
- account revocation

2.1. Account Administration

To provide access to systems and data, an administration process must be put in plac e. The ad ministration process consist s of two tasks:

- request and approval of an account [2]
- creation of an account [3]

[1] SANS Institute, SANS Security Essentials, Volume One – version 2.1, page 392.
[2] Policy 6104, Access to Information Technology Resources and Systems, Longwood University.
[3] NYS Technology Policy # P03 -001, NYS Directory Services - Directory Account Management, James T. Dillon.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.1.1. Request and approval of account

When an account is required, a request must be sent by the user to the account administrator. This request must go through an approval cycle before it can be created (e.g. approved by the requester's manager and by the system or data owner). For modifications to an account, the same rules are applicable.

2.1.2. Creation of account

The account administrator must have a procedure that describes how user accounts will be created. A few topics that should be covered by this process are:

- account naming convention: e.g. an account for an employee consists of the first seven letters of the last name and the first letter of the first name (Thomas Johnson $\rightarrow$ johnsont)
- account information: when defining an account, the account administrator must provide certain owner information in the GECOS or description field. (e.g. last name, first name, HR employee number: Johnson;Thomas;3070 2)[4]
- initial password: to avoid easily guessable initial passwords (e.g. password=account name, password=welc0me,…), the account administrator must use a password generation tool. The initial password must be changed by the account owner at first logon. [5]
- password communication: the way a password will be communicated to the account owner must be defined (e.g.: by e-mail, phone, closed envelope)

2.2. Account Maintenance

A process to review the correctness of the account data and the correctness of the access authorizations must be in place. [6] This process verifies the syntax of the account information and whether the owner of the account is still employed by the company. Also the business need to access the system or data must be checked. [7] It is a control process for the account administration process and the account revocation process. [8]
Account maintenance is the subject of this paper and will be discussed more in detail in the next chapters.

[4] NYS Technology Policy # P03-001, NYS Directory Services - Directory Account Management, James T. Dillon.
[5] Department Of Defense, Password Management Guideline.
[6] Arizona State University, User Management Best Practices.
[7] Network Security Guide – Customer Reference, AT&T Global Network Services, p. 9.
[8] Network Security Guide – Customer Reference, AT&T Global Network Services, p. 9.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.3. Account Monitoring

A process to ensure that audit records are kept for each successful or unsuccessful access attempt must be in place. [9] This topic will not be discussed further in this paper.

2.4. Account Revocation

As important as the correct definition of an account is the revocation of an account when access is no longer required. (e.g. people leaving the company or being fired, people taking another job within the company) [10]

The responsibility for account revocation lays with the manager of the account owner.[11] The manager must notify the account administrator when an individual's account should be revoked. It also is the manager's decision what should be done with the remaining data.
In addition the account administrator could be informed by the human resources department when people leave the company.

3. Importance of Account Maintenance

Once an account has been created, two main problems remain with access management: employees leaving the company and employees taking other jobs inside the company.

In both cases the access to the systems and data must be revoked. If this access is not removed, there is a risk that it will be abused.

Removing the access is actually part of the revocation process. So what is the link with account maintenance? Well, the revocation process can fail at a number of stages:

- Human resources or management forgets to notify the account administrator that somebody has left the company or that an employee is moving to another division.
- The account administrator forgets to execute the revocation request.
- The account administrator for some systems or applications is not notified.
- The accounts are removed only on a part of the systems and applications the owner had access to.

[9] Network Working Group, Site Security Handbook – RFC 2196, p. 32.
[10] Arizona State University, User Management Best Practices.
[11] Network Security Guide – Customer Reference, AT&T Global Network Services, p. 9.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

If the revocation process fails, it is most likely that the account will be there forever. To make sure that there are no dorma nt accounts, all user accesses and access rights should be revalidated periodically. [12] In a large environment with hundreds of servers and applications, thousands of accounts and with a number of account administrators belonging to different divisions, this can be quite challenging. Automating thi s process as much as possible is a must.

4. Revalidati on of User Access

As stated before, the account maintenance process is a control process for the account administration process and the account revocation proc ess. This chapter will look at an automated account maintenance process that was put in place to verify that all existing accounts still require access.

When revalidating access, two verifications have to be performed:

- Is the account owner still employee of the co mpany? (Employment Revalidation)
- Does the account owner still need access to certain systems or data? (Access Right Revalidation)

Before going into more detail on how the employment revalidation and access right revalidation process should be set up, a number of prerequisites for an effective account maintenance process will be discussed.

4.1. Prerequisites for an effective account maintenance process

For the access revalidation process to be effective, the fo llowing prerequisites must be fulfilled:

- account ownership information
- access to employee records
- ownership of special accounts

[12] Arizona State University, User Management Best Practices.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.1.1. Account ownership information [13]

Account ownership information must be defined correctly and must follow a certain syntax. This is the most important prerequisite befo re an effective access revalidation process can be put in place.
Imagine a password file that looks like this:

```
...
johnsont:!:242:250:Thomas W Johnson:/home/johnsont:/usr/bin/ksh
saltw:!:243:250:Salt W:/home/saltw:/usr/bin/ksh
greenwor:!:244:250::/home/gr eenwor:/usr/bin/ksh
piersons:!:245:250:PIERSON:/home/piersons:/usr/bin/ksh
collinsj:!:246:250:temp account for Jenny:/home/collinsj:/usr/bin/ksh
...
```

When the list of accounts and the ownership information from this system is extracted it will be very hard – if not impossible – to compare the information with employment records from the human resources division.
Therefore some structure must be brought in the ownership information. The information needed is the first and last name of the owner and a unique identifier that can be matched with human resources database. This unique identifier can be the employee number.

Structured ownership information syntax:
Last_name;First_name;Employee_number

Additional information can be added here, e.g. when the account was cr eated, whether this is a personal account or an account for an automated job, whether the account belongs to the company or a third party, …

When the structure of the ownership information is applied to the previous example, the password file looks like this:

```
...
johnsont:!:242:250:Johnson;Thomas;30702:/home/johnsont:/usr/bin/ksh
saltw:!:243:250:Salt;William;33104:/home/saltw:/usr/bin/ksh
greenwor:!:244:250:Greenwood;Robert;30433:/home/greenwor:/usr/bin/ksh
piersons:!:245:250:Pierson;Stephen;30844:  /home/piersons:/usr/bin/ksh
collinsj:!:246:250:Collins;Jennifer;30457:/home/collinsj:/usr/bin/ksh
...
```

This information can be compared easily to human resources records.

[13] For this example the GECOS field in the Unix password file is used . The information can also be put in any other field that may be provided by an operating sy stem or application (e.g. Description field on Windows).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.1.2. Access to employee records

The second prerequisite is the need for access to the human resources database. It probably is the only source inside the company where the employee information will always be up to date. The level of access needed is very limited. Actually it will do if the human resources division provides a list of all employees currently working for the company stating the employee number and the responsible manager.

4.1.3. Ownership of special accounts

The third prerequisite concerns the handling of special accounts. All accounts within the organization must have an owner. This does not only apply to normal user accounts for employees, but also to special accounts like root accounts, administrator accounts, application administrator accounts, database administrator accounts, accounts for automated data transfer, emergency accounts, shared accounts for operations, …
Assigning an individual employee as owner of this type of accounts is not a good idea. When the owner leaves the company, the account cannot be removed anyway but it must be reassigned. This can be time consuming if this has to be done on a lot of systems or if the owner has many accounts.
One solution to avoid reassignment of these accounts is assigning the ownership of the account to the functional group that uses the account.

e.g.: root account used by UNIX Administration Team
administrator account used by Windows Administration Team
dbadmin account used by Database Administration Team
datatrans account used by Accounting Division for data transfer

For each of these functional groups a pseudo employee code should be defined. This pseudo code must be used instead of the individual employee number.

e.g.:	root account:	Unix;Admin;PEC01
	administrator account:	Windows;Admin;PEC02
	dbadmin account:	Database;Admin;PEC03
	datatrans account:	Accounting;Datatransfer ;PEC04

It is very important that the list of pseudo employee codes and their real owner (current manager of functional group) is kept up to date.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

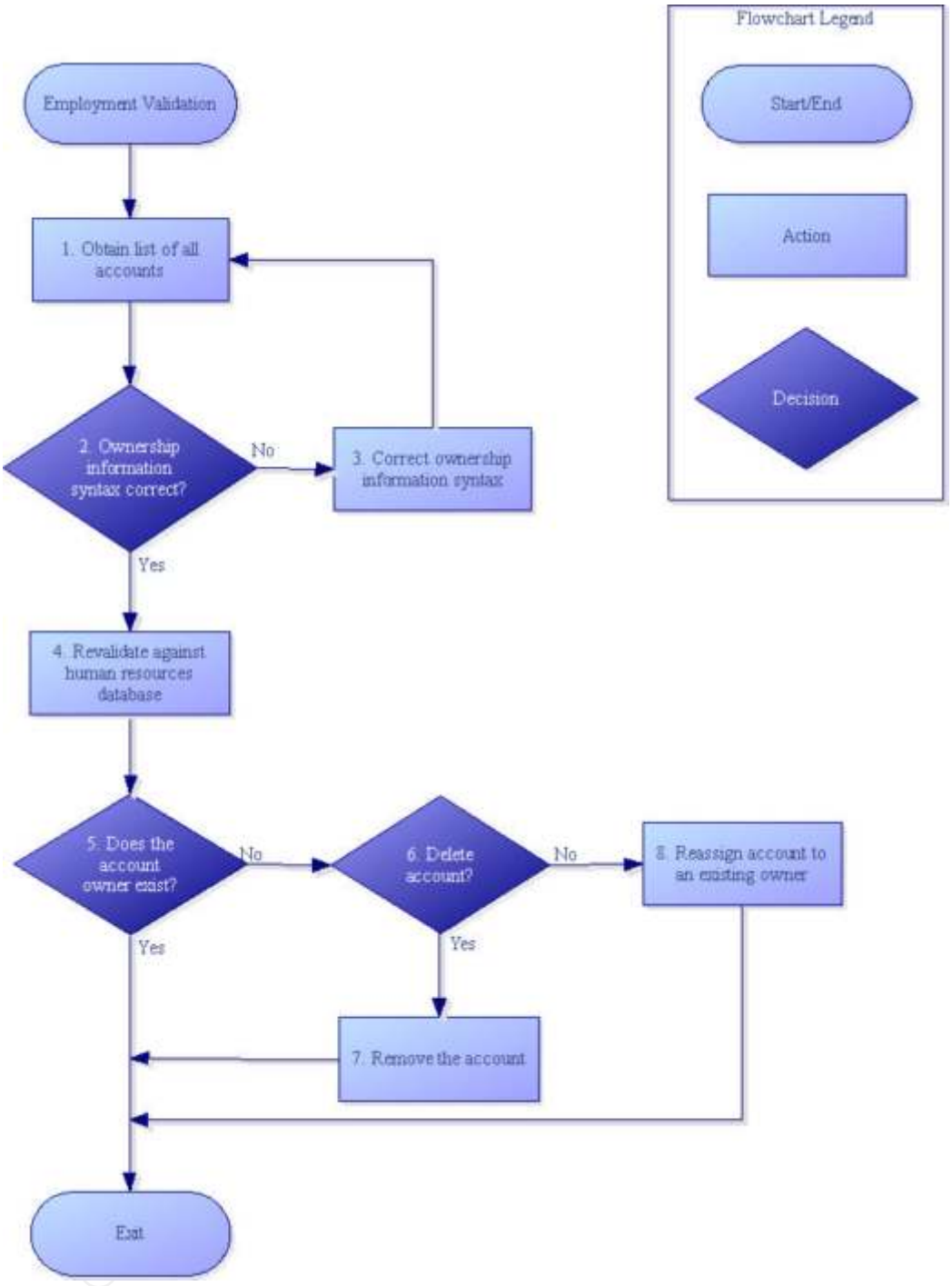
4.2. Employment Revalidation

Employment revalidation checks that the user accounts are owned by individuals that are still employed by the company. Discrepancies must be communicated to the account administrator for immediate action: reassignment, revocation or deletion.

Employment revalidation includes the following steps:

1. Obtain list of all accounts.
   From each system or application, a list of accounts and their ownership information must be collected by the user administrator. This data collection must be automated as much as possible.
2. Ownership information syntax correct?
   Verify if the ownership information is defined correctly. This is the first prerequisite for this process. If this information is not correct, the rest of the process will fail.
   If YES, continue to step 4.
   If NO, continue to step 3.
3. Correct ownership information syntax.
   The ownership information must be corrected by the user administrator and a new list of accounts must be collected.
4. Revalidate against human resources database.
   The ownership information is compared to the records in the human resources database. This step can be automated with a program that compares the employee numbers from both sources.
5. Does the account owner exist?
   Check whether the employee is still listed in the human resources database.
   If YES, no further action is required.
   If NO, continue to step 6.
6. Delete account?
   Verify if the account can be deleted or if there is still a need to keep it.
   If YES, continue to step 7.
   If NO, continue to step 8.
7. Remove the account.
   Depending on the security policy of the company, the account must be removed or disabled (possibly for a period of time and then removed).
8. Reassign account to an existing owner.
   When the employee number is not found in the human resources database, but there is still a need to keep the account (e.g. automated jobs are running under the account) then it should be reassigned to an existing owner.
9. Exit procedure.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.3. Access Rights Revalidation

The access rights revalidation process starts with an employment revalidation. Therefore, the first steps of this process are the same as for the employment revalidation.
In addition, for each account it must be validated that the owner still needs this type of access. For this, each manager must review a list of accounts owned by persons directly reporting to him. The manager has to verify the list and ask for modifications if necessary.

1. Obtain list of all accounts.
   From each system or application, a list of accounts and their ownership information must be collected by the user administrator. This data collection must be automated as much as possible.
2. Ownership information syntax correct?
   Verify if the ownership information is defined correctly. This is the first prerequisite for this process. If this information is not correct, the rest of the process will fail.
   If YES, continue to step 4.
   If NO, continue to step 3.
3. Correct ownership information syntax.
   The ownership information must be corrected by the user administrator and a new list of accounts must be collected.
4. Revalidate against human resources database.
   The ownership information is compared to the records in the human resources database. This step can be automated with a program that compares the employee numbers from both sources.
5. Does the account owner exist?
   Check whether the employee is still listed in the human resources database.
   If YES, continue to step 8.
   If NO, continue to step 6.
6. Delete account?
   Verify if the account can be deleted or if there is still a need to keep it.
   If YES, continue to step 11.
   If NO, continue to step 7.
7. Reassign account to an existing owner.
   When the employee number is not found in the human resources database, but there is still a need to keep the account (e.g. automated jobs are running under the account) then the user administrator should reassign it to an existing owner.
8. Identify account owner and manager.
   Obtain the manager for each account owner from the human resources database.
9. Send mail to manager.
   Send out a list of employees with their accounts and access rights on all systems and applications for revalidation.
10. Is the access still required?
    The manager verifies if the access is still needed. The employee is still

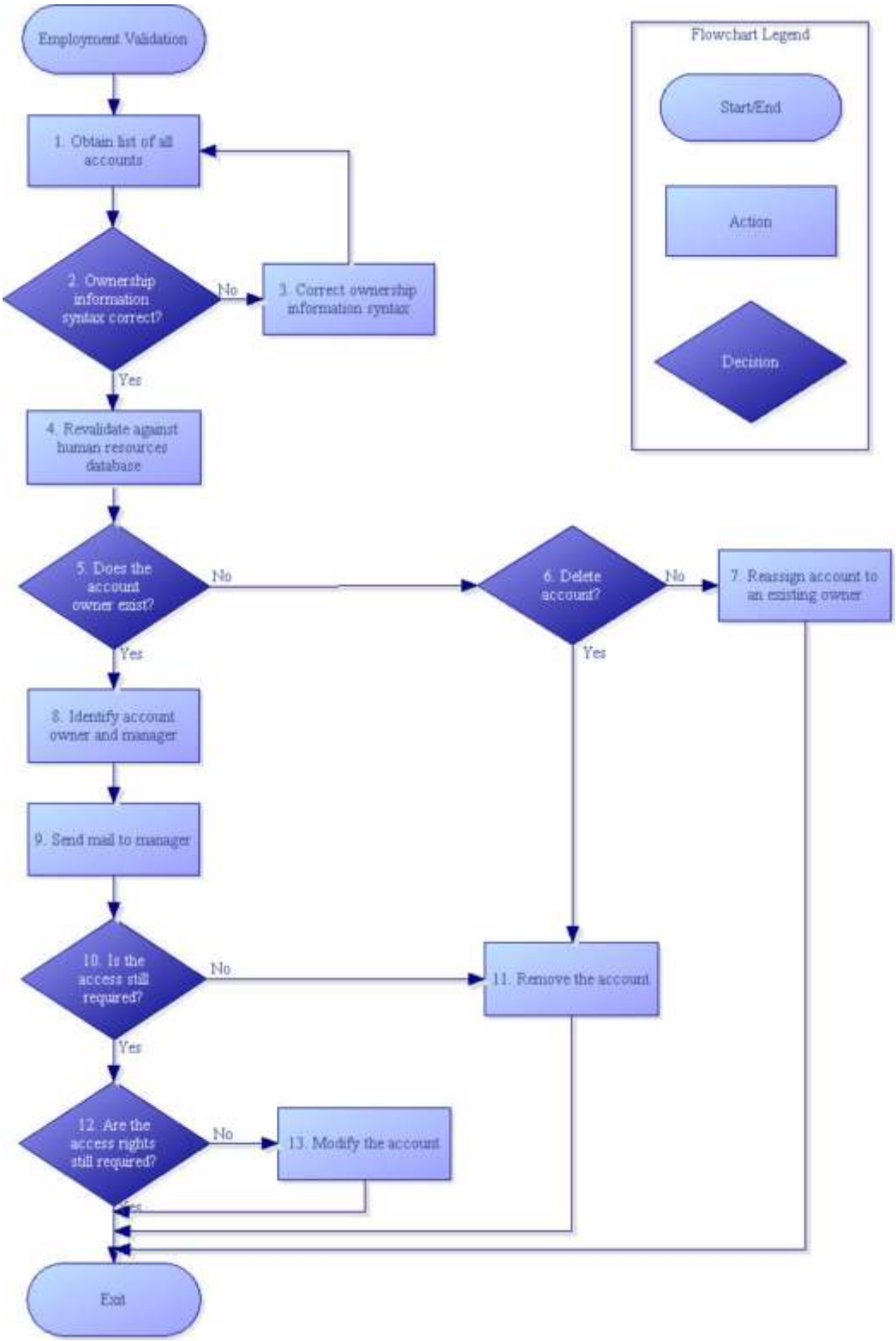
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

with the company but may have another job or role. It may be that access to certain systems or data is no longer required.
If YES, continue to step 12.
If NO, continue to step 11.

11. Remove account.
Depending on the securi ty policy of the company, the account must be removed or disabled (possibly for a period of time and then removed).
12. Are the access rights re quired?
The manager verifies whether the account owner needs certain privileges on a system or not and notifies the account administrator.
If YES, continue to step 14.
If NO, continue to step 13.
13. Modify user account.
The account administrator updates the access rights for the account.
14. Exit procedure.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.4. Employment Revalidation « Access Rights Revalidation

When revalidating access two verifications must be done:

- the account owner is still employed by the company
- the account owner still needs access to certain systems or data

The process for employment revalidation only addresses the first verification while the process for access rights revalidation covers both verifications. However the access rights revalidation process is a lot more complicated and time consuming than the employment revalidation process. Access rights revalidation consists of sending out all the lists of users to management, managers spending their time verifying access for their department staff, follow-up of manager responses, …
Looking at it from the risk side, there is also a difference between the two processes:

- Employee is fired and some/all of the employee's accounts are not revoked. This employee keeps his access to the systems and can misuse this access. The risk is high.
- Employee moves from one division to another. The access to the systems and data from his previous division is not revoked. Although there is no need for this employee to access the data of another division, the risk of the employee misusing his access is less than in the previous case. After all, the employee is still with the company.

So it is a good idea to have both processes in place but execute them at different intervals. For instance the employment revalidation could be performed on a monthly basis (fairly easy to do + high risk issues are addressed) and the access rights revalidation could be executed on a quarterly/bi-annual/annual basis.

5. Summary

Access management is an important part of security. Within access management, account maintenance is often overlooked. User accounts that have been defined on systems and applications remain there forever. A failing revocation process is one of the causes.

Having a control process for this revocation process is a must. In this paper, I have given a "user manual" to set up such a process: the access revalidation process.

The first step that should be implemented is the employment revalidation. This employment revalidation process can capture accounts of employees that have left the company but which were not revoked. It can trigger the removal of these accounts. With the deployment of the ownership information to all

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

accounts and with some programming for automated data collection and comparison with the human resources database, this process can be fully automated. When automated, this process can be executed regularly and it can limit the potential security risk associated with former employees still having access to the company's systems or applications.

The second step, the access rights revalidation process, is more time consuming than the employment revalidation. This process can capture accounts that give access to systems for which the account owner no longer has a business need. It can also capture incorrect access rights. The employment revalidation part can be automated, but the rest of the process is manual and needs the support of the managers. They must be convinced that the data on the systems must be protected.

In general, access revalidation is a heavy administrative job that needs cooperation of a number of different parties in the organization. But with the right approach and some level of automation it is feasible and it will increase the level of security control in the environment.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6. References

SANS Institute, SANS Security Essentials, Volume One – version 2.1, page 392.

Network Security Guide – Customer Reference, AT&T Global Network Services, URL:
http://businessdirect.emea.att.com/att/security_guide_v1_1_061801.pdf

Network Working Group, Site Security Handbook – RFC 2196, URL:
http://www.ietf.org/rfc/rfc2196.txt?number=2196

Arizona State University, User Management Best Practices, URL:
http://www.public.asu.edu /it/ag/unug/bestpractices/user_management.htm

NYS Technology Policy # P03 -001, NYS Directory Services - Directory Account Management, James T. Dillon, URL:
http://www.ir m.state.ny.us/policy/NYSTechPolicyP03 -001.htm

Indian Institute of Science, Supercomputer Education and Research Centre, User Account Revalidation Form, URL:
http://www.serc.iisc.ernet.in/notice/req.doc

Policy 6104, Access to Information Technology Resources and Systems, Longwood University, URL:
http://web.lwc.edu/hr/FINAL_POLICY_BASE/6000/6104.htm

Department Of Defense, Pass word Management Guideline, URL:
http://www.alw.nih.gov/Security/FIRST/papers/pass_word/dodpwman.txt

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.